DE KETEN UITGEDAAGD

Besturen en verantwoorden in een wereld vol ICT

Onder redactie van:
Remco van Wijk
Nitesh Bharosa
Marijn Janssen
Niels de Winne

Colofon

Onder redactie van:
drs. R. van Wijk
dr.ir. N. Bharosa
ir. N. de Winne
prof.dr.ir. M.F.W.H.A. Janssen

Mede-auteurs:
mr.drs. S. Bal RA
drs. E. Rigter
dr. H. van der Voort
mr. W. Fokkema
ir. B. Hendriksen
ir. V. den Bak
ir. P. Leijnse

Delft, februari 2014
Dit onderzoek is uitgevoerd door TU Delft in opdracht van Logius.

Illustraties en cover design: Annemarie van der Linde

ISBN 978-90-5199-534-3 (gedrukt)
ISBN 978-90-5199-535-0 (ebook PDF)
DOI 10.3233/978-90-5199-535-0-i

Uitgegeven door IOS Press onder het imprint Delft University Press. Gepubliceerd onder 'Open Access' en gedistribueerd onder de voorwaarden van de 'Creative Commons Attribution Non-Commercial License'.

IOS Press BV
Nieuwe Hemweg 6b
1013 BG Amsterdam
The Netherlands
tel: +31-20-688 3355
fax: +31-20-687 0019
email: info@iospress.nl
www.iospress.nl

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TU Delft

Inhoudsopgave

Voorwoord directeur Logius

Logius biedt standaard ICT oplossingen voor elektronisch zakendoen van burgers en bedrijven met publieke dienstverleners. Elektronisch zakendoen neemt een steeds grotere vlucht en deze trend is niet te stoppen. Standaardisatie is hierbij cruciaal. Als ieder zijn eigen weg gaat in de digitalisering, dan benutten we niet de kansen die ICT biedt om samen – op forse schaal – meer met minder te doen. Dat is dom en zelfs gevaarlijk. Geld is immers schaars geworden. Bovendien moeten we ons realiseren dat de arbeidsmarkt door de demografische ontwikkelingen snel krimpt, hoe vreemd dat met de huidige werkloosheidscijfers sommigen ook lijkt.

Voor Logius is het evident dat standaardisatie niet leidt tot inperking, maar juist vergroting van vrijheid om organisatiedoelen te bereiken. Slim gekozen standaard bouwblokken en -diensten bieden flexibiliteit, omdat zij zich in talloze variaties gemakkelijk laten configureren al naar gelang nieuwe behoeften en toepassingen zich ontwikkelen. Bij grootschalig gebruik – "massa is kassa" – kun je aldus de maatschappelijke transactiekosten voor de BV Nederland fors lager maken en houden. En dat is essentieel, want alles wat tussen voortbrenging en gebruik van goederen en diensten aan de strijkstok blijft hangen, is zonde van het geld.

In 2009 had ik het genoegen om de uitvoering van het programma Standard Business Reporting (SBR) onder mijn hoede te krijgen. Dit programma zette zich in voor verregaande uniformering van de uitwisseling en verwerking van verantwoordingsinformatie tussen bedrijfsleven en overheid. Die uniformering vergt stringente sturing op standaardisatie van én gegevens én processen én techniek. Logius kreeg de rol van (keten)regisseur in deze complexe, publiek-private samenwerking.

Op de tekentafel klopt het concept, maar in 2009 was er slechts een beperkt aantal mensen in Nederland dat dit werkend kon krijgen. Om op nationale schaal dit standaardisatiespel op het juiste niveau te kunnen spelen, was meer kritische massa nodig. Ik heb in het kader van het programma daarom een ambitieuze kennisagenda ontwikkeld. Eén van de resultaten daarvan is een door de Technische Universiteit Delft ontwikkelde universitaire masteropleiding, waarvan inmiddels de eerste afgestudeerden bij onder meer Logius werkzaam zijn. Het thans voor u liggende boek stoelt op het lesmateriaal dat bij deze opleiding hoort. Een bruikbaar handboek voor Logius en alle andere partijen die met Standard Business Reporting aan de slag zijn of aan de slag willen. Daarnaast is het boek een mooie inspiratiebron voor iedereen die meer inzicht wil krijgen in de grote en complexe transities die in onze maatschappij onder de noemer van digitalisering gaande zijn. Want dit boek gaat niet alleen over verantwoordingvraagstukken tussen organisaties. Ook voor de ontwikkeling van andere informatie-intensieve samenwerkingsketens is dit boek naar mijn vaste overtuiging zeer toepasselijk en bijzonder relevant.

Graag benut ik deze gelegenheid om mijn dank uit te spreken. Om te beginnen aan de auteurs en reviewers voor de inspanning die zij hebben geleverd met het schrijven van dit werk. Ik ondersteun de uitnodiging die zij met dit boek doen aan een ieder die actief in het keteninformatiseringsdomein om te participeren bij de totstandkoming van de volgende drukken van dit boek. En uiteraard dank ik ook de Belastingdienst voor haar beslissende rol van 'launching customer' voor Standard Business Reporting in Nederland. Ons land loopt in deze ontwikkeling voorop in de wereld. Dat is goed voor onze concurrentiepositie en iets om trots op te zijn.

Steven Luitjens,
Directeur Logius

Voorwoord DG Belastingdienst

De Belastingdienst is in de loop der jaren onderdeel geworden van steeds langere ketens waarin met tal van partijen wordt samengewerkt. In het Middellangetermijnplan 2014 – 2017 van de Belastingdienst is “samenwerken” uitgeroepen tot één van de vier speerpunten. Om een aantal voorbeelden te noemen: inhoudingsplichtigen zijn al lang niet meer alleen verantwoordelijk voor de berekening en afdracht van loonheffingen. Zij zijn ook leverancier geworden van maandelijkse loongegevens die door het UWV worden beheerd en breed in de publieke sector worden gebruikt. En de Belastingdienst is voor cruciale onderdelen van de elektronische infrastructuur afnemer geworden van Logius, dat onder meer DigiD en de Digipoort exploiteert.

Met de Digipoort is één van de samenstellende delen (naast de Nederlandse Taxonomie en XBRL) van SBR genoemd. En SBR is het voorbeeld bij uitstek van samenwerking die zich niet beperkt tot de overheid, maar die zich uitstrekt tot partners als fiscale dienstverleners, accountants, softwareontwikkelaars en private gegevensgebruikers zoals banken.

Na een lange aanloopperiode is SBR nu vol op stoom (alhoewel dat een wat rare beeldspraak is als we het hebben over een innovatief project): inmiddels heeft de Belastingdienst in de periode 2008 tot medio januari 2014 meer dan 4 miljoen berichten ontvangen, waarvan 3,5 miljoen in 2013, zijn er 400.000 machtigingen geregistreerd en 50.000 digitale kopie-aanslagen verzonden. En de Kamer van Koophandel heeft in dezelfde periode 40.000 berichten ontvangen, waarvan 28.000 in 2013. De groei zit er dus in.

Vanaf het begin heeft de Belastingdienst meegedaan aan de ontwikkeling van SBR, overtuigd als hij is van de meerwaarde van standaardisering. Een gestandaardiseerde gegevensuitvraag is goed voor bedrijven die gegevens moeten aanleveren aan de overheid en goed voor de overheidsorganisaties die die gegevens vragen. Nu het uitwisselingsproces is ingeregeld en grote aantallen berichten gebruikmaken van de infrastructuur, is het moment gekomen om verder te kijken; dan gaat het over verbreding van het gedachtegoed naar andere sectoren uit de samenleving. Daarom ben ik blij met dit boek. Het geeft een realistisch beeld van de opgave die wacht wanneer een maatschappelijke sector besluit SBR te gaan hanteren. En het geeft tegelijkertijd een beeld van de te managen risico’s en van de geboden kansen. Daardoor kan het een positieve impuls aan verbreding geven. Vanuit mijn rol als voorzitter van het SBR-Beraad vind ik dat waardevol: ik gun iedereen SBR.

Daarom vind ik het ook zo’n goed idee van Logius om dit boek als relatiegeschenk aan zijn afnemers aan te bieden. Het is echt een cadeau waar je wat aan hebt.

Ik feliciteer de redactie en auteurs met het boek, Logius met het cadeau-idee en de ontvangers met het feit dat zij kennis kunnen nemen van de mogelijkheden die SBR biedt. En het is bovenal een aansporing tot samenwerken!

Peter Veld,
Directeur-Generaal Belastingdienst

Over de redactie

Remco van Wijk
De heer Remco van Wijk MSc. was als redactielid verantwoordelijk voor het ontwerp van de samenhangende boekstructuur. Een structuur die enerzijds recht moet doen aan de complexiteit van het SBR programma en haar historie, maar anderzijds een verduidelijking moet bieden voor degene die met SBR aan de slag willen.

Remco is hoofdauteur van de hoofdstukken 1 (Inleiding), 4 (Het besturingsvraagstuk van keteninformatiesystemen), 5 (I-Processen), 9 (Governance en beheer) en 11 (Slotbeschouwing) en medeauteur van alle overige hoofdstukken. Hij is sinds 2007 vanuit diverse rollen (praktijk en wetenschap) betrokken geweest bij SBR, waar hij regelmatig werd aangemerkt als het 'inhoudelijk geweten'. Remco was het aanspreekpunt binnen Logius in de opmaat naar verplichtstelling en maakte de organisatorische blauwdruk voor de afdeling ketendienstverlening. Remco heeft zich in het programma altijd sterk gemaakt voor kennisoverdracht, deugdelijk project- en programmamanagement en open innovatie.

Remco is thans directielid bij Thauris | Management Centrum. Hij geeft regelmatig colleges en voordrachten over SBR en andere keteninnovaties. Remco is te bereiken via r.vanwijk@thauris.nl

Nitesh Bharosa
De heer dr.ir. Nitesh Bharosa was vanuit de Technische Universiteit Delft verantwoordelijk voor de penvoering en de coördinatie rond de totstandkoming van dit boek. Gedurende het kennisborgingsproject heeft Nitesh zich geconcentreerd op het leggen en behouden van de relaties tussen de benoemde praktijkvraagstukken en theoretische concepten, inzichten en methodieken. Nitesh is hoofdauteur van de hoofdstukken 7 (Technische inrichting SBR) en 8 (Beveiliging van informatieketens). Daarnaast is hij als medeauteur betrokken geweest bij de hoofdstukken 1 (Inleiding), 4 (Het besturingsvraagstuk van keteninformatiesystemen) en 6 (Gegevens).

Als onderdeel van het kennisborgingsproject was Nitesh verantwoordelijk voor het (tussentijds) overdragen, toetsen en verrijken van de ontwikkelde kennis in de vorm van wetenschappelijke publicaties. Hij promoveerde eerder op het verbeteren van informatie-uitwisseling in netwerken.

Nitesh is thans adviseur bij Thauris | Management Centrum en modulemanager/docent aan de Technische Universiteit Delft. Hij is te bereiken via n.bharosa@tudelft.nl

Niels de Winne
De heer ir. Niels de Winne heeft vanuit zijn ruime praktijkervaring de inhoudelijke kwaliteit van dit boek geborgd. Niels is betrokken geweest bij de totstandkoming van alle hoofdstukken en heeft zich daarbij met name gericht op de perspectieven (technische) juistheid, structuur (bruikbaarheid) en samenhang. Hij trad op als klankbord bij het opzetten van de structuur van het boek. Niels is vanaf 2004 in diverse rollen betrokken geweest bij de SBR initiatieven. Hij is de grondlegger van de overall architectuur van SBR. Niels was programmamanager van het Programma van Eisen Generieke Infrastructuur (GEIN). Resultaat van dit programma was de (service georiënteerde) architectuur voor elektronische communicatie tussen het bedrijfsleven en overheden. Niels was projectleider voor de realisatie en ingebruikname van de procesinfrastructuur en legde zo de basis voor de Digipoort, die onder andere wordt gebruikt voor SBR. Van eind 2009 tot begin 2013 is hij als operationeel programmamanager namens Logius verantwoordelijk geweest voor de implementatie-impuls van SBR. Niels heeft zich binnen het programma altijd sterk gemaakt voor een heldere architectuurbenadering.

Niels is thans directielid bij Thauris | Management Centrum en is te bereiken via n.dewinne@thauris.nl

Marijn Janssen
De heer prof.dr.ir. Marijn Janssen was opdrachtnemer van het kennisborgingsproject. Hij is medeauteur van hoofdstuk 5 (I-Processen). Als tegenlezer voor hoofdstukken concentreerde hij zich op de relaties tussen praktijkvraagstukken en theorie (concepten, inzichten en methodieken).

Marijn Janssen is Antoni van Leeuwenhoek hoogleraar in 'ICT & Governance' aan de Faculteit Techniek, Bestuur & Management van de Technische Universiteit Delft. Hij doceert verschillen vakken, waaronder 'Design of Innovative ICT-infrastructure and Services' en 'Business & IT architecture'. Hiernaast geeft hij het vak 'Business Process & Technology' aan de MBA Business Information Technology van de Business University Nyenrode. Marijn is daarnaast betrokken bij opleidingen aan de Erasmus Universiteit Rotterdam. Hij is tevens opleidingsdirecteur van de Master 'Compliance Design & Management', waar dit boek integraal als lesstof wordt behandeld.

Marijn is te bereiken via M.F.W.H.A.Janssen@tudelft.nl

Dankwoord

Standard Business Reporting (SBR) is een oplossing voor system-to-system uitwisseling en verwerking van informatie in ketens. In de setting van een praktische leerschool hebben diverse specialisten uit verschillende kennisdisciplines gewerkt aan de totstandkoming van SBR. Er zijn diverse redenen voor het beschikbaar maken van de opgedane kennis in de vorm van een publiek toegankelijk boek.

Allereerst is het voor de betrokken partijen (de insiders) van belang dat de ervaringen, leerpunten en andere impliciete kennis (tacit knowledge) van de betrokken specialisten integraal bij elkaar worden gebracht. Hiermee ontstaat er een overzicht van het geheel en gedetailleerde beschrijvingen van de bouwblokken van de SBR-oplossing. De relevante begrippen en verbanden zijn in dit boek in relatie met elkaar beschreven, waardoor communicatie en samenwerking tussen specialisten kan worden gefaciliteerd.

Ten tweede is het voor de 'outsiders' – partijen die eventueel geïnteresseerd zijn om SBR toe te passen in nieuwe domeinen – van belang dat ze een overzicht en een goed beeld krijgen van de SBR-bouwblokken en condities voor een positieve business case bij toepassing van SBR in een informatieketen.

Ten derde vormt de opgedane kennis benodigd onderwijsmateriaal. Hoewel er veel leerboeken zijn te vinden op afzonderlijke disciplines, zoals ICT, recht, bestuur en management, zijn er minder integrale boeken te vinden die over de verschillende disciplines heen de opgave en de oplossing beschrijven. Nieuwe opleidingen kunnen hier gebruik van maken om mensen in dit gebied op te leiden.

Tenslotte is het voor de academische gemeenschap van belang dat de prangende onderzoeksvragen en braakliggende onderzoeksterreinen worden beschreven. We hebben bij het schrijven van dit boek dankbaar gebruikgemaakt van de bestaande literatuur. Hierbij hebben we geconstateerd dat sommige concepten en verbanden in de literatuur niet integraal geadresseerd worden. In verschillende hoofdstukken belichten we in de afsluiting enkele aanwijzingen voor verder onderzoek.

Dit boek is het resultaat van een team effort met mensen uit de praktijk en wetenschap. De redactie – Remco, Nitesh, Niels en Marijn – heeft delen van dit boek geschreven en bijdragen van anderen gecoördineerd. Bijdragen van anderen kunnen worden gevat in auteurschap, review en algemeen (waaronder deelname aan denksessies en interviews, leveren van input etc.). De sectie 'Over de betrokken personen' biedt een overzicht. In dit dankwoord staan we stil bij de aard van de bijdragen van de betrokken personen.

We beginnen bij de auteurs. Zij zijn allen deskundigen op hun vakgebied. Gedurende het schrijfproces werd duidelijk dat het schrijven van een boekhoofdstuk, zeker gezien de hoge lat die door de opdrachtgever is gelegd, geen 'walk in the park' was. De hoofdstukken moesten de in SBR ontwikkelde kennis in de breedte en diepte beschrijven, alsook actueel en feitelijk correct zijn. Tevens moesten de hoofdstukken concreet zijn, terwijl een deel van het SBR-verhaal nog diffuus en in ontwikkeling was. Tenslotte moesten de aangeleverde teksten ook prettig te lezen zijn. Om aan deze eisen te voldoen, vergde het schrijfproces van de auteurs naast deskundigheid ook veel tijd en flexibiliteit. Het resultaat mag er dan ook zijn.

In nauw overleg met de auteurs hebben wij diverse personen verzocht een hoofdstuk te reviewen, oftewel te controleren op inconsistenties en feitelijke onjuistheden. In alle gevallen hebben de reviewers direct enthousiast gereageerd en 'ja' gezegd op het verzoek om een hoofdstuk te reviewen. Kort hierna gingen de hoofdstukken en de reviewformulieren de deur uit. Tussentijdse gesprekken met de reviewers lieten doorschemeren dat het reviewproces een taaie klus bleek te zijn. Één van de reviewers vatte dit proces mooi samen als "*het doorlichten van interessante, maar complexe materie met een veelheid aan perspectieven, concepten en verbanden… ik doe mijn best om dit binnen vier weken af te ronden…*". Wie de hoofdstukken heeft gelezen herkent waarschijnlijk wat deze reviewer zegt. De reviews zijn van grote betekenis geweest. Niet alle hoofdstukken waren even positief beoordeeld, waarna de auteurs weer hard aan het werk gingen. Gelukkig boden de reviewers ook concrete verbeterpunten, waardoor we in overleg met de auteurs een verbetertraject konden starten. Merendeels betrof het versimpeling en verduidelijking (door middel van herkenbare voorbeelden). Hierbij moeten we eerlijk toegeven dat uiteindelijk niet alle verbetersuggesties zijn doorgevoerd. Dit vanwege de rode draad die we als redactie moesten bewaken. Sommige verbetersuggesties – zoals het nader beschrijven van Digipoort in hoofdstuk 1 – waren, gezien vanuit één gereviewd hoofdstuk, terecht. Het vasthouden van de rode draad (waarbij Digipoort als onderdeel van de SBR oplossing in hoofdstuk 7 wordt uitgewerkt) vereist dat we suggesties van deze orde niet hebben doorgevoerd. Desalniettemin zullen de reviewers het leeuwendeel van hun commentaar herkennen in het eindresultaat.

Tot slot ontkomen we er niet aan om vier individuen extra in het zonnetje te zetten. Als eerste willen we Frans Hietbrink bedanken voor zijn zeer actieve feedback op de hoofdstukken. Frans speelt een belangrijke rol in SBR en we hebben in meerdere hoofdstukken de verleiding moeten weerstaan om hem in het lijstje van succesfactoren op te nemen. We willen ook Rob Kuipers bedanken. Rob levert in zijn rol als Rijksregisseur SBR een belangrijke bijdrage aan de grootschalige implementatie van SBR. Ella Broos en Jan Pasmooij verdienen ook veel dank voor hun geduld als procesbewakers vanuit Logius. De hoge kwaliteitslat waar de afzonderlijke hoofdstukken aan moesten voldoen vergde veel afstemming en geduld. Ideeën moesten tot bloei komen en soms moesten ogenschijnlijk afgeronde stukken worden afgebroken en opnieuw worden opgebouwd. Ella en Jan wisten dit uitstekend te faciliteren. Allen, bedankt!

De redactie,
Delft, februari 2014.

Ten geleide

Als iemand je op een feestje vertelt dat zij zich bezighoudt met financiële verslaglegging, softwareontwikkeling, accountancy, assurance, bestuurs- en fiscaal recht, auditing, public key infrastructures, kredietrapportages, informatieprocessen, XBRL, taxonomieën én publiek-private samenwerking, sta je mogelijk even met je oren te klapperen. Of je concludeert dat de dame in kwestie lijdt aan een narcistische persoonlijkheidsstoornis. We kunnen je geruststellen, misschien is zij minder gek dan je vreest. Mensen die zich bezighouden met de implementatie van Standard Business Reporting (SBR) ontkomen er niet aan van alle eerder genoemde kennis- en vakgebieden iets te weten. Sterker nog, de opsomming was niet eens uitputtend. Dit wil niet zeggen dat zij overal specialist in zijn. De basisprincipes en het onderlinge verband dienen echter wel eigen te zijn gemaakt.

SBR staat voor het gestandaardiseerd verantwoorden door bedrijven aan overheden. Het kan hierbij gaan over de belastingaangifte en het deponeren van de jaarrekening. Om het gestandaardiseerd verantwoorden te kunnen realiseren, gebruiken partijen

een gezamenlijk afsprakenstelstel dat voorschrijft hoe verantwoordingsketens ingericht worden. Een verantwoordingsketen begint bij het bedrijf dat zich verantwoordt en eindigt bij de uitvragende partij. Om de verantwoordingsinformatie uit te wisselen, maken de ketens gebruik van diverse gemeenschappelijke voorzieningen. Hierdoor ontstaan afhankelijkheden tussen de partijen in deze ketens, wat gezamenlijke begripsvorming noodzakelijk maakt. Dit betekent zeker niet dat SBR een concept is dat alleen weggelegd is voor de Uomo universale. Juist niet. Uiteindelijk gaat het er bij SBR om een zekere dwarsdoorsnede van de wereld integraal te begrijpen. Doordat deze doorsnede afwijkt van wat wij gewend zijn, lijkt deze misschien allesomvattend, maar dit valt in de praktijk mee. Het probleem is met name dat geïnteresseerden vooralsnog tevergeefs zochten naar een overzichtswerk dat de dwarsdoorsnede op hoofdlijnen in beeld brengt. Dit boek biedt hiervoor een eerste aanzet.

Het idee voor een eerste consolidatieslag van de kennis rond SBR ontstaat eind 2010. Op dat moment past de overheid SBR in het financiële domein al bij verschillende verantwoordingsketens succesvol toe. Het gaat hier echter nog om relatief kleine volumes, terwijl, zoals bij standaardisatie in het algemeen geldt, de business case van SBR gebaat is bij grootschaliger en breder gebruik van de standaard. Een stabiele en brede kennisbasis kan helpen deze opschaling handen en voeten te geven. De mogelijke opschaling komt evenwel ineens een stuk dichterbij wanneer de Belastingdienst in december 2010 een plan presenteert om vanaf 2013 te beginnen met het uitfaseren van de met SBR concurrerende uitwisselingsstandaard: BAPI. De Vereniging Kamers van Koophandel (KvK) en Centraal Bureau voor de Statistiek (CBS) geven eveneens aan dat zij op termijn maatregelen gaan nemen om het papieren verkeer te verminderen en dat SBR ook voor hen de standaard is bij het inrichten van het elektronische kanaal. Plotseling is de gewenste kennisbasis geen ‘nice to have’ meer, maar een ‘must have’. Logius en de Technische Universiteit Delft hebben daarom de kennis en ervaring van deskundigen uit het SBR-domein gebundeld in één overzichtswerk.

De ervaringen van bij SBR betrokken professionals vormt het fundament voor het boek. Wetenschappers met verschillende achtergronden hebben de praktijkvoorbeelden in een breder theoretisch kader geplaatst, waarna de samenstellers de diverse schakels aaneen hebben geregen tot een samenhangend geheel.

Uit het resultaat blijkt dat het SBR Programma te karakteriseren is als een bewogen en inhoudelijk rijk veranderingsinitiatief met een behoorlijke informatie- en communicatietechnologie (ICT) component. Auteurs besteden in hun uitwerking veel aandacht aan de wordingsgeschiedenis: ‘hoe is het allemaal zo gekomen?’ en de achtergrondinformatie die nodig is om de huidige SBR-toepassing te begrijpen. De ontwikkeling van SBR is sterk gedreven door de beleidsambitie ICT in te zetten tegen administratieve lastendruk. SBR maakt zodoende deel uit van een serie – vaak nog lopende – initiatieven, die middels een systematische herinrichting van ketens een kleinere en effectieve overheid beogen. De retrospectieve beschouwingen van de SBR-casus in dit boek bieden inzichten en best practices die ook voor ‘niet-SBR-ers’ relevant zijn bij hun zoektocht naar kosteneffectieve informatieketens.

Op de keper beschouwd behandelt het boek twee perspectieven op SBR. Enerzijds geeft het inzicht in de totstandkoming van een initiatief als SBR en beschrijft het de uitdagingen die hierbij een rol spelen. Wij spreken hier over SBR als opgave. Anderzijds geeft het boek zeer concrete informatie over de gerealiseerde SBR-voorzieningen, die bij wijze van spreken morgen in een nieuwe verantwoordingsketen ingezet kunnen worden om deze kosteneffectiever te laten opereren: SBR als oplossing. De black box wordt in empirische zin 'opengebroken' – om de technologie, interacties, verwevenheden en afhankelijkheden die de ontwikkelingen en keuzes sturen – in kaart te kunnen brengen. In onze optiek past het verbinden van deze benaderingsperspectieven – opgave en oplossing – bij de algemene beleidswaardering van ICT initiatieven.

Van de overheid worden flinke bezuinigingen gevraagd. De serviceverwachting van de burger lijkt echter alleen maar te stijgen. Al lange tijd is er een beleidsdruk om meer met minder te doen. Veel werkprocessen die de overheid uitvoert, zijn kennisintensief (zoals beleidsvorming en wetgeving) of administratief (zoals het verwerken van aanvragen en verantwoordingsinformatie) van aard. Hierdoor ligt de gedachte voor de hand dat de overheid enorme voordelen moet kunnen behalen door de efficiënte inzet van ICT. Op ICT gebaseerde innovaties worden veelal als de 'Haarlemmer wonderolie' bestempeld, die ons naar een compacte overheid gaan leiden. Zo constateert de Wetenschappelijke Raad voor Regeringsbeleid (WRR) dat de inzet van technologie op zowel nationaal, lokaal als Europees niveau als welhaast vanzelfsprekend wordt gezien (WRR, 2011). Technologie wordt 'uitgerold', praktijken worden 'gestroomlijnd' en diensten 'geüpdatet'. Het 'technovertrouwen' van politiek en beleid vertaalt zich in grote ambities met ICT, niet alleen in technische, maar zeker ook in beleidsinhoudelijke zin.

Wie het nieuws volgt, wordt echter steeds weer geconfronteerd met falende ICT-projecten bij de overheid. Grote ICT-projecten hebben de neiging uit de hand te lopen, ze zijn duurder en werken minder goed dan verwacht. In 2007 publiceerde de Algemene Rekenkamer een tweedelig en diepgaand rapport over dit thema: Lessen uit ICT-projecten bij de overheid (Algemene Rekenkamer, 2007, 2008). Conclusie: miljarden gaan er verloren met grote ICT-projecten. De oorzaak ligt volgens de Rekenkamer in onrealistische ambitieniveaus, de neiging van overheden om de projecten complexer te maken dan noodzakelijk en later met aanvullende wensen te komen (scope creep). Volgens dit rapport wordt het spanningsveld tussen politieke, organisatorische en technische factoren onderschat. Voortdurende veranderingen, onzekerheid rond de impact en gebrek aan gedragen business cases zijn andere factoren die een rol spelen (Janssen et al., 2010). Bij (dreigend) projectfalen is het stilzetten van een investeringsproject een uiterste maatregel (Wortmann & Kremer, 2011). Veelal gaat hier een moeizaam traject aan vooraf. Helaas zijn er in een dergelijk geval alleen maar verliezers. Niemand zit hierop te wachten: de opdrachtgevende partij niet, maar ook de opdrachtnemer niet. Enkele populaire voorbeelden van problematische ICT-implementaties in de (semi)publieke sector zijn het gezamenlijke belastinginningssysteem van de waterschappen (Tax-i) waarvan de invoering wordt gestaakt, het Elektronisch Patiëntendossier dat weerstand ontmoet van artsen en patienten of de basisvoorziening Handhaving bij de Nederlandse Politie die leidt tot grote problemen.

Het falen van projecten – zowel in de publieke als de private sector – is niet onopgemerkt gebleven en heeft geleid tot een toenemende hoeveelheid onderzoek, zowel binnen als buiten Nederland. Hoewel het merendeel van het onderzoek gericht is op het achteraf blootleggen van de oorzaken voor het mislukken van projecten, zien we ook steeds meer 'best practices' – methodieken die begeleiding zouden moeten bieden in het succesvol realiseren van programma's en projecten. De best practices richten zich op projectmanagement in het algemeen (bijvoorbeeld PRINCE2 en MSP), maar ook op ICT projecten in het bijzonder (bijvoorbeeld Agile en Scrum).

Echter, juist gegeven de hoeveelheid beschikbare best practices is het aantal onsuccesvol afgeronde ICT-projecten nog steeds onverklaarbaar hoog. Deze tegenstelling wordt elegant verwoord in de 'Cobb paradox', welke luidt: *"We know why projects fail, we know how to prevent their failure – so why do they still fail?"* – (Martin Cobb, Treasury Board of Canada Secretariat geciteerd in een rapport van The Royal Academy of Engineering (2004)).

Kenmerkend voor voorbeelden van problematische ICT-implementaties is dat het om complexe veranderopgaven gaat. De complexiteit komt in verschillende dimensies tot uiting. Denk bijvoorbeeld aan de doorlooptijd, het financieringsmodel, de besturing van de verandering, het grote aantal betrokkenen en de hoge onzekerheid betreffende de technologie en de impact hiervan op cultuur, organisatiestructuur en processen. Uitvoering vergt kennis en ervaring uit verschillende (specialistische) disciplines. Veelal gaat het om meerdere partijen met zelfstandige bevoegdheden, die willen komen tot een systeem dat ingrijpt op kernprocessen van –in ieder geval enkele van de – betrokkenen. De initiatieven raken aan het publieke belang en kennen dientengevolge een forse politieke bemoeienis. Het leveren van diensten moet doorgang blijven vinden (de winkel blijft open tijdens de verbouwing). De publieke context vraagt om een sterke koppeling tussen de uitvoering, de wetgeving en de algemene beginselen van behoorlijk bestuur. Het gaat dan om dwingende kaders die niet gemakkelijk te veranderen zijn. De samenwerking van partijen met een publieke taak komt op een andere wijze tot stand dan in het bedrijfsleven. In het publieke domein zijn partijen 'formeel' op elkaar aangewezen. Er is in beperkte mate sprake van een hiërarchische relatie tussen de samenwerkende partijen, een gezamenlijk vastgestelde business opportunity of een door de markttucht opgelegde noodzaak tot coöperatie.

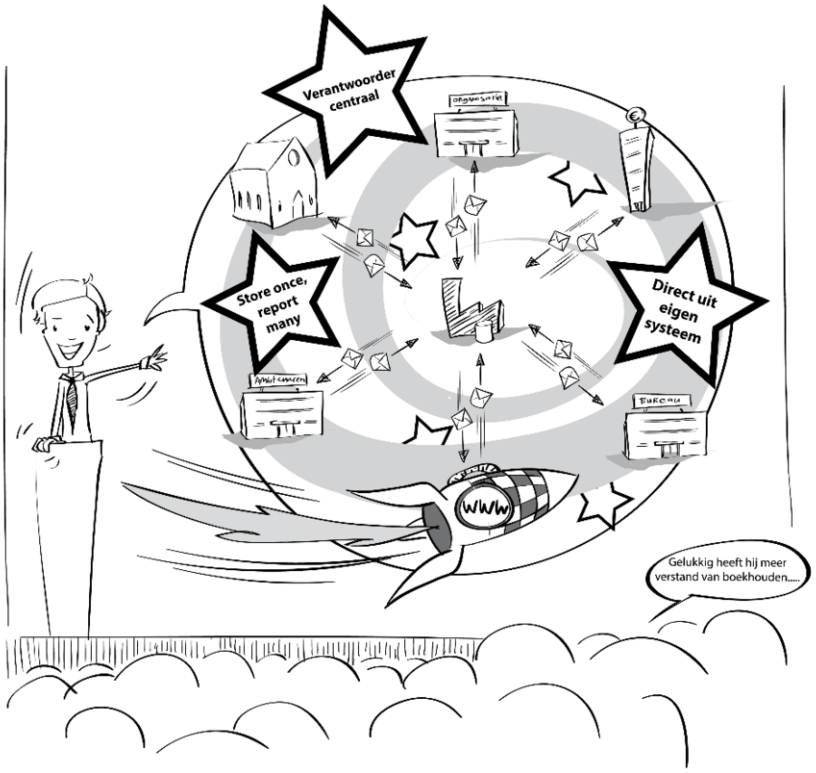
Hoewel bovenstaande omschrijving van de opgave slechts enkele punten raakt, moeten we ons de vraag stellen of de genoemde ICT-initiatieven überhaupt nog te karakteriseren zijn als ICT-projecten. Of plakken wij onterecht dit label op veel fundamentelere veranderingen binnen de maatschappij? Moeten wij onze verwachtingen bijstellen over de kracht van ICT in het publieke domein, of zijn er in de ketens wel degelijk fundamentele voordelen te halen? Zijn er al geleerde lessen die een toepassing tot een zekere oplossing maken?

Dit boek geeft een uniek inzicht in de historie, context én realisatie van zo'n groot ICT-programma. Het verschaft de lezer via de concrete casus nieuwe inzichten om antwoord te geven op bovenstaande vragen. Deze inzichten hebben geenszins het karakter van 'hoe dan wel' als het gaat om het beheersen van grote ICT-programma's.

We pretenderen niet een oplossing voor alle problemen die zich in ICT-programma's manifesteren te hebben. Desalniettemin hebben we ervoor gekozen om de problemen, dilemma's en oplossingen zo generiek mogelijk te formuleren, zodat deze ook in andere contexten en programma's te herkennen en te gebruiken zijn. Hiervan kunnen anderen leren, zodat het leerproces niet nog een keer doorlopen hoeft te worden. Het boek maakt hierbij dankbaar gebruik van de kennis en ervaring van deskundigen die bij SBR betrokken zijn.

Hoewel alle hoofdstukken elementen bevatten van de opgave én de oplossing is in het boek op hoofdlijnen wel een duidelijke tweedeling te maken. In het eerste deel (A) ligt de nadruk op de uitdaging rond het herinrichten van informatieketens; de opgave. SBR wordt in deze hoofdstukken met name gebruikt om aan te geven hoe geschetste dilemma's spelen of hebben gespeeld in de praktijk en op welke manier ermee omgegaan is. De keuzes die bij SBR zijn gemaakt om bepaalde problemen te tackelen worden als voorbeeld opgevoerd. Het tweede deel (B) gaat in op de concrete inrichting van SBR en hoe deze inrichting bijdraagt of op termijn bij kan dragen aan een kosteneffectieve informatie-uitwisseling in verschillende ketens.

1 Inleiding



1.1 Achtergrond

Het SBR Programma en de projecten waar zij uit voortkwam[1] hadden als doel de verantwoording voor ondernemingen en overheidsinstellingen goedkoper en beter te maken. Dit door de juiste inzet van ICT in de talrijke verantwoordingsketens die de overheid kent. Onder de kreten '*store once, report many*' en 'ketenomkering', werd in 2006 een schets neergelegd van de beoogde oplossing. Dienstverleners betrokken bij verantwoording en overheden sloten een convenant waarin zij plechtig beloofden zich in te spannen om de verantwoordingsketens conform schets in te

[1] Bijlage A biedt een overzicht van gerelateerde projecten.

richten. Onder het document prijkten de handtekeningen van vele softwareleveranciers, de belangrijkste accountantskantoren (en iets later de handtekeningen van VNO-NCW en MKB-Nederland), de handtekeningen van drie ministers en één staatsecretaris.

De opgave bleek toch te groot. Pas 7 jaar na ondertekening en 2 jaar na het aflopen van het convenant was er sprake van grootschalige toepassing van SBR in één fiscale keten. Waarom duurde implementatie langer dan gedacht? Het eerste deel van dit boek (deel A) dient om begrip te krijgen van de opgave. Was het de technologie? Het is waar dat de geschetste oplossing – die wij in deze inleiding nader uiteenzetten – moet voorzien in een complexe behoefte. Bovendien kende de randvoorwaardelijke technologie bij de start van de SBR gerelateerde initiatieven nog geen brede toepassing. Er lagen dus nog verschillende ontwerp- en ontwikkelvraagstukken op technisch vlak. Toch willen we achteraf stellen dat de opgave in veel grotere mate een organisatorisch karakter dan een technologisch karakter had. De uitdaging, zo denken wij, bestond met name uit de noodzaak voor de tot wasdom komende oplossing steeds een passende organisatie te realiseren die:

- enerzijds voldoende slagkracht had om de volgende stap in de ontwikkeling en implementatie van de oplossing te realiseren en
- anderzijds voldoende aansloot bij de toekomstige structuren. Structuren waarin de oplossing en ook de organisatie zelf uiteindelijk moesten landen (de definitieve organisatorische verankering).

Onze stelling wordt ondersteund door de wetenschap van vandaag dat de geschetste technologie en onderliggende architectuur – die bij aanvang van het SBR Programma werden gehanteerd – in essentie weinig zijn veranderd. De organisatie en de verankering daarvan binnen de bestaande organisatie heeft daarentegen verscheidene ingrijpende metamorfoses ondergaan en door de toename van de (volwassen) toepassing van SBR bij verantwoording ligt er in ieder geval nog één ingrijpende transitie in het verschiet. De hoofdstukken van het deel – 'SBR als opgave' – hebben dan ook met name betrekking op de organisatorische aspecten van de opgave. Achtereenvolgens behandelen deze hoofdstukken de organisatorische context (ketens, schakels en afhankelijkheden), de uitdagingen van verandermanagement binnen ketens en het besturen van wijzigingen in keteninformatiesystemen.

Inmiddels wordt SBR succesvol substantieel toegepast in fiscale en financiële verantwoordingsketen (denk aan de jaarrekening). Hiervoor zijn binnen de overheid generieke voorzieningen gerealiseerd die gebruik maken van de SBR standaarden. In deel B wordt SBR als oplossing voor verantwoording aan publieke uitvragers beschreven. In de hoofdstukken wordt, waar relevant, ingegaan op de theorie achter bepaalde 'bouwblokken', maar alle hoofdstukken beschrijven ook de actuele stand van zaken binnen SBR. Aan de orde komt hoe binnen SBR omgegaan wordt met gegevensmanagement, procesmanagement, techniek, informatiebeveiliging, governance en beheer en tot slot de wijze waarop belanghebbenden voor een bepaalde verantwoordingsketen gestructureerd over kunnen gaan naar SBR. Het boek wordt afgesloten met een beschouwing op de mogelijkheden en bedreigingen van SBR als oplossing.

Om de lezer de nodige bagage mee te geven voor deel A en B, evenals de samenhang tussen beide delen te schetsen, geeft deze inleiding inzicht in de visie waar het SBR Programma en haar voorlopers op gebaseerd waren. Daarbij hoort de schets van SBR als generieke overheidsoplossing voor system-to-system (S2S) uitwisseling en gedeelde verwerking van verantwoordingsinformatie.

Tegen deze achtergrond is de rest van dit hoofdstuk als volgt ingedeeld. § 1.2 begint met de technologische ontwikkelingen die leiden tot S2S-geïntegreerde informatieketens. Hierbij staan we stil bij de potentie en consequenties van S2S-informatieverwerking. § 1.3 behandelt de toepassing van S2S-integratie in verantwoordingsketens. We beschrijven de ontwerpeisen die – gezien de karakteristieken van de verantwoordingsketens – voor de beoogde oplossing golden. In § 1.4 behandelen we de technologische componenten van de geschetste oplossing waarmee aan de complexe ontwerpeisen zou kunnen worden voldaan. Hierna gaat § 1.5 verder met een analyse van de organisatorische context waarbinnen de technologie geïmplementeerd moest worden. We staan hier stil bij ketengovernance als onderbelicht onderdeel van de oplossing. We sluiten deze inleiding af met een leeswijzer (§ 1.6), waarin de volgende hoofdstukken wordt geïntroduceerd.

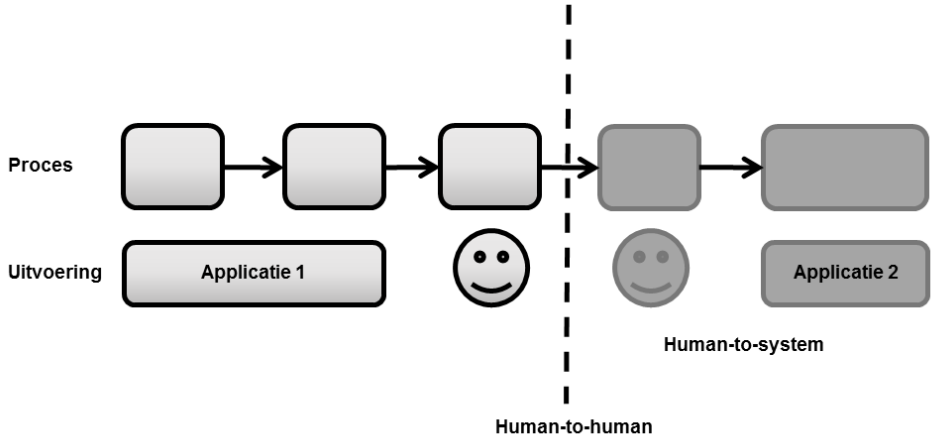
1.2 De opkomst van system-to-system en human-to-system ketenintegratie

1.2.1 *Automatisering en keteninformatiesystemen*

Eind jaren 80 en begin jaren 90 neemt de automatisering van informatieverwerking binnen organisaties een enorme vlucht (Chaffy, 2004; van Oost, Alberts, van den Ende, & Lintsen, 1998). Informatieprocessen worden geheel of gedeeltelijk geautomatiseerd afgehandeld door zogenaamde ICT-systemen[2]. Binnen de organisatie komt de informatieverwerking in het kader van de administratieve processen – zoals de boekhouding, voorraden en dergelijke – als eerste in aanmerking voor automatisering (Jans, 1991). Waar organisaties samenwerken maken zij feitelijk deel uit van een organisatie-overstijgend informatiesysteem. Dit noemen wij het keteninformatiesysteem. Ook binnen dit systeem ontstaat de behoefte tot verdere automatisering.

Neem het voorbeeld van een auto-onderdelenverkoper en zijn leverancier die geen gekoppelde informatiesystemen hebben. In het voorraadbeheersysteem ziet de verkoper de melding dat er nog maar twee exemplaren van een onderdeel op voorraad zijn. De verkoper besluit telefonisch extra exemplaren te bestellen bij een leverancier. De leverancier noteert de bestelling op papier en plaatst de bestelling in het verkoopsysteem. Voor het verwerken van de informatie tussen de verkoper en leverancier is menselijke tussenkomst noodzakelijk: er is sprake van human-to-human (H2H) koppeling binnen het informatiesysteem. Figuur 1.1 schetst deze situatie.

[2] Met de komst van informatie-en communicatietechnologie (ICT) begint het tijdperk van (semi)geautomatiseerde informatiesystemen, vaak gemakshalve als 'systemen' aangeduid. Van meet af aan bestaan dergelijke informatiesystemen uit een samenstelling van één of meer computers (hardware), programmatuur (software), gegevensverzamelingen, procedures en mensen (Looijen, 2004).



Figuur 1.1 –H2H interactie tussen organisaties binnen een keteninformatiesysteem

Wanneer organisaties voor de gedeelde informatieverwerking aangewezen zijn op human-to-human communicatie blijkt dit vaak de zwakke schakel in het keteninformatiesysteem: gebruikers typen informatie over (met kans op fouten), de tussenhandelingen (goedkeuring) kosten veel tijd en doordat de rekenkracht en opslag goedkoper worden, worden de menselijke handelingen relatief duurder. Deze nadelen wegen met name zwaar vanaf het moment dat het volume en de frequentie van informatieverwerking tussen organisaties toeneemt. Een goed gedocumenteerd voorbeeld hiervan is de 'automotive supply chain', waarin bedrijven voor interne bedrijfsprocessen steeds afhankelijker zijn geworden van informatie uit de systemen van andere bedrijven (Tuunainen, 1999).

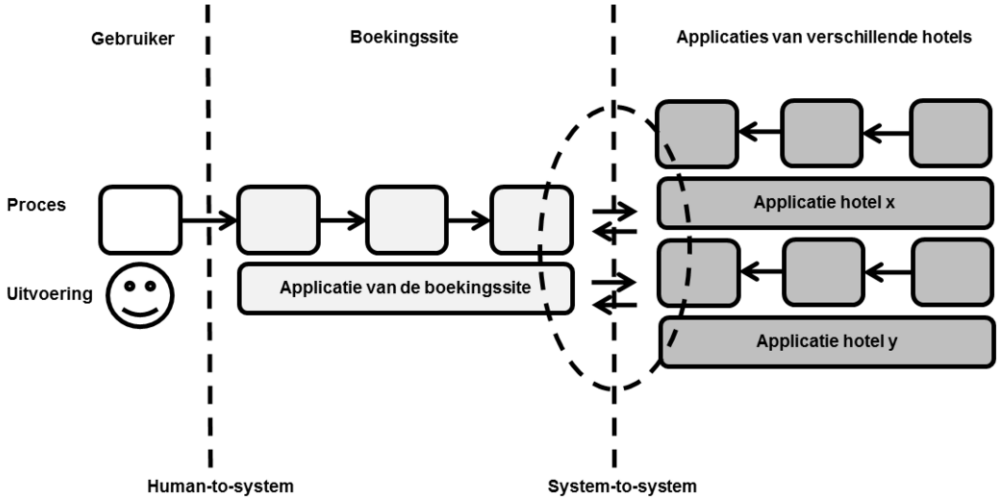
Met de opkomst van informatie-uitwisselingsstandaarden als Electronic Data Interchange (EDI) in de jaren 80 tracht men steeds meer eerder genoemde nadelen te mitigeren en de rol van de mens in organisatieoverstijgende informatieverwerking te reduceren. Hansen & Hill (1989) bieden de volgende definitie van EDI: "*the movement of business documents electronically between or within firms (including their agents or intermediaries) in a structured, machine-retrievable data format that permits data to be transferred, without re-keying, from a business application in one location to a business application in another location*".
Bovenstaande definitie van EDI benadrukt de volgende punten:

1. De verplaatsing van gegevens tussen applicaties vindt elektronisch plaats binnen of tussen organisaties.
2. Machines (computers) kunnen informatie ophalen en overzetten, zonder dat overtypen (menselijke tussenkomst) nodig is.

De koppeling van de IT-systemen van organisaties zonder menselijke tussenkomst wordt in de literatuur aangeduid als S2S-ketenintegratie[3] (zie bijv. Kauremaa, Kärkkäinen, & Ala-Risku, 2009).

[3] Integratie kan door middel van harde of losse koppelingen (tight or loose coupling) tussen verschillende systemen (Hofman, 2003). Een koppeling kan worden gelegd door middel van een zogenaamd koppelvlak

Halverwege de jaren 90 en aan het begin van deze eeuw voltrekt er zich een tweede revolutie op automatiseringsgebied. Door de brede adoptie van het TCP/IP protocol, de opkomst van het internet en de enorme toename van bandbreedte, raken partijen met elkaar verbonden en ontstaat er voldoende 'ruimte' voor het goedkoop overzenden van grote hoeveelheden data. De S2S-ketenintegratie wordt hiermee gemakkelijker en lucratiever (Hofman, 2003; Vidgen, Avison, Wood, & Wood-Harper, 2002). Maar ook zien we met de opkomst van het internet een enorme toename van zogenaamde human-to-system (H2S) ketenintegratie. Mensen loggen direct in op systemen van andere partijen in een keten.



Figuur 1.2 – Een boekingssite als voorbeeld van ketenintegratie over het internet. H2S-ketenintegratie (gebruiker logt in op boekingssite) en S2S-ketenintegratie (tussen de boekingssite en de systemen van de hotels)

Bovenstaande afbeelding geeft een voorbeeld van ketenintegratie over het internet. De gebruiker logt direct in op de systemen van een boekingssite. De boekingssite is S2S-geïntegreerd met achterliggende systemen van talloze hotels.

1.2.2 *Horizontale en verticale S2S-integratie*

Bij SBR speelt met name de S2S-ketenintegratie een belangrijke rol en het is hierbij relevant twee verschillende integratietypen te onderscheiden. Integratietype één is al benoemd en betreft het efficiënter en effectiever koppelen van IT-systemen van organisaties. Wij noemen dit horizontale S2S-integratie van het keteninformatiesysteem. Onderstaand een nadere uitwerking van de voordelen van horizontale integratie:

(interface). Een koppelvlak (specificatie) geeft een beschrijving van afspraken en standaarden voor het opzetten van een S2S verbinding tussen informatiesystemen; de wijze waarop informatie wordt uitgewisseld.

- **Efficiëntere verwerking:** Systemen (front-/back-office en tussen organisaties) kunnen in slechts een fractie van de tijd die mensen eerder nodig hadden, informatie verwerken. Daarnaast besparen organisaties tijd doordat ze niet steeds opnieuw hoeven te zoeken naar het adres en de bron van de informatie, evenals de condities voor uitwisseling, bijvoorbeeld de maximale berichtgrootte. Doordat de verbindingsparameters vaststaan en de verwerking automatisch verloopt, kan er snel worden teruggekoppeld in de vorm van bijvoorbeeld een ontvangstbevestiging of een foutmelding. Meer efficiëntie wordt bereikt door het elimineren van dubbele/meervoudige handelingen, bijvoorbeeld door het overtypen van informatie overbodig te maken.
- **Minder fouten/hoge gegevenskwaliteit:** Onderzoek laat zien dat het overtypen van informatie vaak tot fouten leidt (Redman, 1995). Ook zal de kans op onrechtmatige inzage of wijziging afnemen wanneer met S2S-integratie wordt gewerkt. Dat komt doordat bij S2S-integratie de toegang beter gereguleerd kan worden dan wanneer menselijke tussenkomst nodig is. Andere informatiebeveiligingsaspecten komen naar voren in het tweede deel van dit boek.

Een belangrijkste randvoorwaarde voor de horizontale S2S-integratie is een hoge mate van interoperabiliteit. Over het algemeen verwijst dit begrip naar de mate waarin verschillende in een informatieketen gebruikte technologieën met elkaar kunnen communiceren of gezamenlijk kunnen worden ingezet voor een bepaald doel. Informatiesystemen zijn gelaagde entiteiten (Reynolds & Stair, 2013). Ten behoeve van de interoperabiliteit dienen organisaties vaak op meerdere lagen afspraken te maken. In de literatuur zien we dat wetenschappers, afhankelijk van het accent (een of meerdere lagen), verschillende definities aan dit begrip koppelen. Hieronder vatten we enkele definities uit de literatuur (Scholl & Klischewski, 2007) samen:

- Technische interoperabiliteit: Het vermogen van systemen om met elkaar te communiceren op het niveau van infrastructuur (communicatienetwerk) en software. Simpel gesteld gaat het hier om de onderlinge communicatie tussen twee of meer applicaties, via een fysiek netwerk.
- Syntactische interoperabiliteit: Het vermogen van systemen om ontvangen gegevens direct (zonder handmatige conversies) in een informatieverwerkingsproces (i-proces) te gebruiken. Dit is een indicatie dat samenwerkende partijen een gemeenschappelijke metataal hebben waarmee zij de gegevens vastleggen. Zie het als het toepassen van dezelfde grammatica en hetzelfde alfabet op de gezamenlijke woordenschat. XML en XBRL zijn voorbeelden van veelgebruikte metatalen die we ook in hoofdstuk 6 beschrijven.
- Semantische interoperabiliteit: Het vermogen van systemen om de gegevens aan de kant van zender en ontvanger op dezelfde manier te interpreteren. Het verdient de voorkeur om deze betekenis van gegevens expliciet vast te leggen.
- Organisatorische interoperabiliteit: Het vermogen van organisaties om systemen (inclusief rollen, taken, structuren en processen) zodanig in te richten dat gegevens geautomatiseerd kunnen worden uitgewisseld. Dit vraagt vaak

om afstemming van veronderstellingen over verantwoordelijkheden, veiligheid, financiering, etc.
- Juridische interoperabiliteit: Het vermogen van organisaties om enerzijds afspraken te maken over de communicatie en/of uitwisseling van gegevens en om anderzijds - conform deze afspraken en algemene juridische kaders - de daadwerkelijke communicatie/uitwisseling van gegevens te laten plaatsvinden.

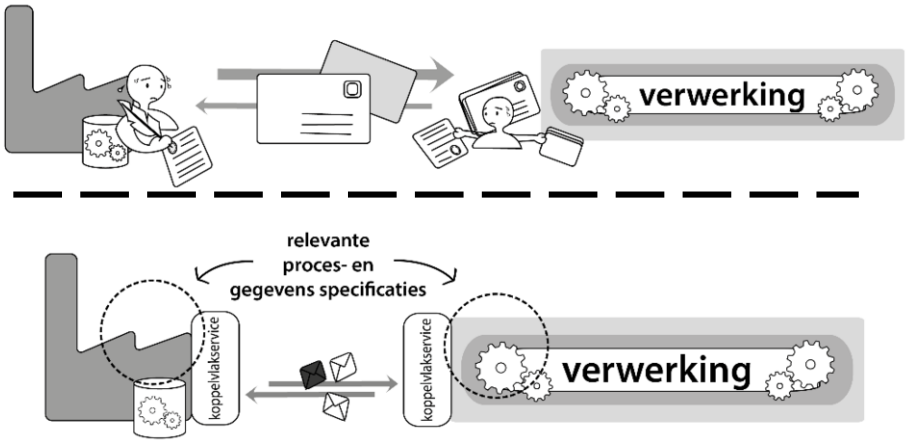
Bovenstaande is vrij abstract. Als illustratie van interoperabiliteit gebruiken we het voorbeeld van de boekingssite:

- De systemen van de boekingssite moeten de systemen van het hotel kunnen vinden en kunnen aanspreken (technische interoperabiliteit).
- De systemen van het hotel moeten het formaat waarin de boekingsvraag is opgestuurd (bijvoorbeeld XML) kunnen verwerken (syntactische interoperabiliteit).
- Er moet een gedeelde definitie zijn van kindvriendelijke kamers (semantische interoperabiliteit).
- De acties van de gebruiker via de boekingssite moeten worden verwerkt in de juiste database van het te boeken hotel (organisatorische interoperabiliteit).
- De boekingssite en de hotels moeten afspraken maken over de wijze waarop zij met de gegevens omgaan (bijvoorbeeld maatregelen in het kader van privacybescherming) en over de verantwoordelijke partij bij verlies, beschadiging of fouten in de verwerking van de gegevens (juridische interoperabiliteit).

Kijken we naar de technische systemen (de geautomatiseerde verwerking), dan zien we bij de horizontale system-to-system integratie dientengevolge de volgende 'onderdelen' die organisatie-overstijgend van belang zijn:

- Gegevensspecificaties:
    - Specificaties van de berichten die tussen systemen worden uitgewisseld:
        - Welke gegevens worden onderscheiden
        - Welke berichten worden onderscheiden
- Processpecificaties:
    - Beschrijving van de wijze waarop de informatie verwerkt wordt met als belangrijke component de relevante uitkomsten van het proces voor voorliggende ketenpartijen.
- Koppelvlakservices:
    - Technische services die op basis van een uitwisselingsprotocol de dialoog tussen systemen van organisaties afhandelen.

In onderstaande figuur is zowel H2H informatieketen als ook de S2S-geïntegreerde keten weergegeven, met hierin opgenomen de benoemde onderdelen.



Figuur 1.3 – Een H2H-informatieketen (boven) en een horizontaal S2S-geïntegreerde informatieketen met de onderdelen gegevenspecificaties, processpecificaties en koppelvlakservices (onder).

Het tweede integratietype is eigenlijk een afgeleide van het eerste type. Het betreft het outsourcen van informatiediensten aan een gespecialiseerde dienstverlener. Door de behoefte aan het koppelen van IT-systemen, werd een modulaire opbouw van IT-systemen steeds gangbaarder (Baldwin & Clark, 2000). Iedere module is te beschouwen als een apart, autonoom blok functionaliteit dat een bepaalde input verwerkt tot output (Parnas, 1972). Tegenwoordig worden de meeste informatiesystemen modulair ontwikkeld en beheerd (Reynolds & Stair, 2013).

Dankzij de mogelijkheden tot horizontale S2S-ketenintegratie kunnen bepaalde modules door organisaties (dienstverleners) gemakkelijk worden aangeboden aan meerdere organisaties. Dit leidt tot verticale integratie. Een bijzondere vorm van outsourcing is het gebruik van de services van een shared service center (SSC). Een SSC – vaak aangeduid als een gedeelde dienstverlener – is een partij die aan meerdere (soms vergelijkbare) partijen dezelfde services levert (Bergeron, 2003). In dit boek gaat het bij de term outsourcing over deze vorm: het gebruik van een SSC. Ook hier zijn er effectiviteit- en efficiëntievoordelen:

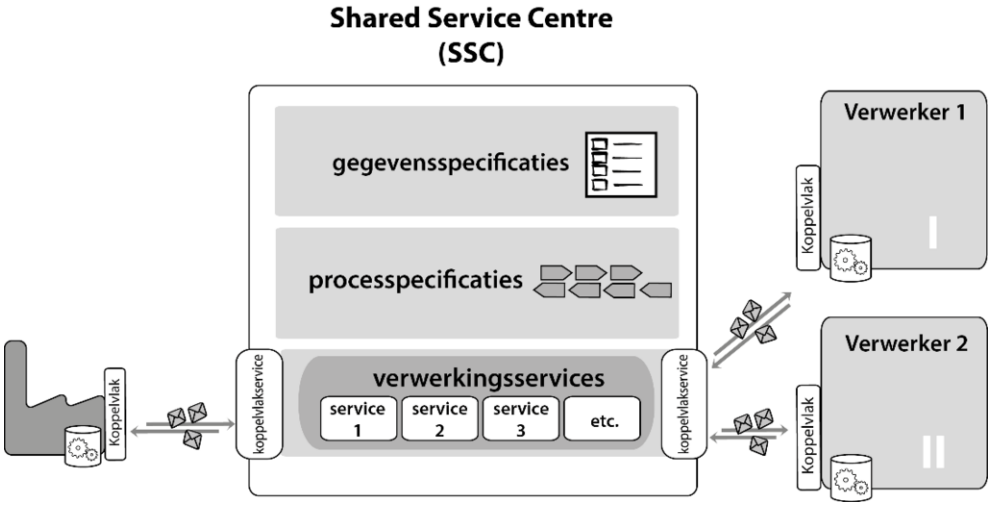
- **Efficiëntere verwerking:** Volgens de wet van de economische specialisatie bereiken partijen schaalvoordelen door zich te specialiseren in bepaalde diensten. Volgens de literatuur worden deze schaalvoordelen behaald door specialisatie, de concentratie van specialistische kennis, het hergebruik van standaardoplossingen en het grootschalig uitvoeren van gedeelde processen (Janssen & Wagenaar, 2004). Dit werkt als volgt:
  - De marginale kosten, de kosten voor het aanbieden van één extra informatieproces op een bestaande infrastructuur, zijn laag.
  - De kosten voor de infrastructuur en de kosten voor ontwikkeling kunnen worden verdeeld over een grote of zelfs groeiende groep geleverde diensten, ofwel gebruikers van diensten.
  - Hierdoor kunnen de kosten die worden doorberekend per gebruiker afnemen.

Ook op de kosten van IT kan worden bespaard door systemen te centraliseren; er wordt bespaard door minder lokale hardware, lagere doorontwikkelkosten en lagere beheerkosten (Looijen, 2004). Verder kan op de personele en huisvestingskosten worden bespaard. Voor veel organisaties was kostenbesparing destijds - en is nog steeds - één van de belangrijkste redenen om een SSC in te schakelen. Het is echter zeker niet meer de enige reden (Buijs, Doorn, & Noordam, 2004).

Tot slot kan een SSC aanzienlijke efficiëntievoordelen met zich mee brengen voor partijen die zich in de keten vóór het SSC bevinden. Het SSC werkt dan als standaardisatieplatform. Denk hierbij bijvoorbeeld aan IDEAL. Met dezelfde koppeling kunnen mensen – ongeacht hun bank – zaken doen met meerdere webshops. Dit is een stuk gemakkelijker dan wanneer iedere webshop voor iedere bank een aparte applicatie voor betaling aan zou bieden. Het doorvoeren van systeemwijzigingen in de verwerkingsketen is eenvoudiger via een SSC. Dit komt doordat de impact van de verandering gereduceerd wordt tot één schakel in de keten (het SSC) in plaats van de gehele keten.

- **Effectievere verwerking:** De uitbestedende organisaties kunnen hun resources laten focussen op het toevoegen van waarde in hun kerntaken (Lee, Huyn, Kwok, & Pi, 2003). De schaalomvang maakt het mogelijk om meer specialisaties op te bouwen. Immers, een deel van de optredende efficiëntievoordeel voor het SSC kan worden aangewend om te investeren in kwalitatieve versterking. Dit kan bijvoorbeeld door zwaardere, gespecialiseerde deskundigen aan te trekken, zoals juridische, informatiebeveiligings- en organisatieadviesdeskundigen.

Bij de verticaal geïntegreerde keten krijgen de verwerkingsservices van de gedeelde dienstverlener een organisatie-overstijgend belang. Een verwerkingsservice moet voor meerdere organisaties in meerdere informatieketens kunnen worden ingezet. Hoe vaker een verwerkingsproces wordt hergebruikt, hoe efficiënter de dienstverlener. In onderstaande figuur is een verticaal geïntegreerde dienstverlener weergegeven, met daarin opgenomen gedeelde verwerkingsservices. In dit voorbeeld is één partij via een gedeelde dienstverlener verbonden met twee vergelijkbare verwerkers. De gedeelde dienstverlener heeft koppelvlakservices aan de kant van de aanleverende partij en de twee verwerkers.



Figuur 1.4 – Verticale S2S-ketenintegratie met (outsourcing naar) een gedeelde dienstverlener ofwel Shared service center (SSC)

1.2.3 *Afhankelijkheid als 'prijs' van S2S-ketenintegratie*

Zowel de horizontale S2S-ketenintegratie als de verticale ketenintegratie hebben een prijs. Partijen die koppelingen willen onderhouden, moeten gezamenlijk de interoperabiliteit waarborgen. Zo ontstaan afhankelijkheden. Partijen kunnen onder andere niet meer eenzijdig wijzigingen in hun gegevensmodel doorvoeren. Hiermee zou de semantische interoperabiliteit worden aangetast. Elke verandering in de gedeelde aspecten kan de andere delen van de keten raken.

We komen ter illustratie terug op het voorbeeld van de boekingssite en nemen als casus de optionele functionaliteit waarmee een gebruiker de aanwezigheid van vloerbedekking op de hotelkamer kan selecteren. Het doorvoeren van deze functionaliteit betekent dat alle aangesloten hotels deze classificatie moeten (er)kennen en dat zij informatie moeten kunnen aanbieden over de aanwezigheid van vloerkleed in hun kamers. Dit vereist afstemming, en daarmee tijd en inspanning. Partijen in de keten hebben echter vaak verschillende business cases, wijzen van financiering en doelstellingen. Indien de partijen niet tot één gedeelde oplossing kunnen komen, dan zullen ze moeten differentiëren en dat leidt tot aanvullende kosten. Ook bij de verticale integratie ontstaan er nieuwe afhankelijkheden. Zo ontstaat er een wederzijdse afhankelijkheid tussen de opdrachtgever en de opdrachtnemer (het SSC). De opdrachtgever is voor haar doelstelling afhankelijk van de (kwaliteit) van de dienstverlening bij de opdrachtnemer. De opdrachtnemer krijgt hiervoor de noodzakelijke middelen (geld, autorisaties, informatie). Vanuit de opdrachtgever bezien is het denkbaar dat deze mee wil beslissen over zaken rond de uitvoering van uitbestede processen. Deze betrokkenheid brengt zogenaamde agency costs met zich mee. Om de agency costs zo laag mogelijk te houden dienen partijen afspraken te maken over wie er op welke manier betrokken zijn bij welke beslissingen (governance). De opdrachtnemer zal vanuit efficiëntiedoelstellingen proberen om de diversificatie in de dienstverlening te verkleinen en hergebruik te optimaliseren. Dit geldt zeker bij geautomatiseerde

services, omdat een opdrachtnemer op nieuwe varianten niet (meteen) de eerder genoemde economies of scale kan behalen, of de economies of scale op de bestaande diensten niet wil laten afnemen doordat er opnieuw ontwikkelkosten moeten worden gemaakt.

1.2.4 *De business case voor S2S-ketenintegratie*

De benoemde voordelen van de koppeling van IT-systemen tussen organisaties en de toepassing van shared service centers moeten opwegen tegen de 'prijs' van de toegenomen afhankelijkheden. Er zijn verschillende karakteristieken van informatieketens te noemen die bepalend zijn voor de business case van ketenintegratie.

De voordelen van horizontale S2S-ketenintegratie komen het beste tot uiting in informatieketens die voldoen aan de volgende karakteristieken:

- De keten bevat processen waarin organisaties gezamenlijk periodiek hetzelfde informatieproces uitvoeren.
- De informatieketen kent een groot verwerkingsvolume (veel berichtenverkeer).
- Organisaties kunnen de aansluitende backoffice taken geautomatiseerd afhandelen, met behulp van software.

Het overgaan op een SSC voor verwerking van informatieprocessen is lucratief wanneer het volgende geldt:

- Verschillende organisaties staan voor een vergelijkbare informatieverwerking:
    - Vergelijkbaar in functionaliteit.
    - Vergelijkbaar in inhoudelijke kennisgebieden.
    - Vergelijkbaar in geldende formele kaders (bijvoorbeeld juridisch).
- Verschillende organisaties hebben een rol in meerdere verantwoordingsketens (SSC als standaardisatieplatform).
- Het is mogelijk om de uit te besteden processen en de zelf uit te voeren kernprocessen van de uitbestedende dienst te ontvlechten. De uitbestedende dienst kan een heldere beschrijving geven van het door het SSC af te handelen (bestaande of gewenste) proces (gebaseerd op Buijs; 2004).

1.3 Potentie S2S-integratie in het verantwoordingsdomein

Verantwoordingsketens zijn ketens die zijn ingericht ten behoeve van het genereren en verwerken van verantwoordingsinformatie. Verantwoordingsinformatie betreft informatie aangaande de prestatie van of situatie in een organisatie ten behoeve van een derde. Dit boek richt zich met name op verantwoordingsketens die hun grondslag vinden in wet- en regelgeving. Voor deze ketens geldt dat private en publieke partijen verplicht verantwoordingsinformatie bij de overheid aanleveren, om de overheid - ten behoeve van het algemeen belang - in staat te stellen haar taken op het gebied van beleidsvorming en wetgeving, beleidsuitvoering en toezicht en handhaving uit te voeren en tevens het maatschappelijk verkeer in staat te stellen haar eigen doelen te realiseren en belangen te dienen.

De behoefte aan verantwoordingsinformatie komt voort uit het feit dat de overheid, voor sturend optreden op terreinen als financiën/belastingen, veiligheid, sociale zekerheid, milieu, gezondheidszorg, onderwijs en arbeidsomstandigheden, niet zonder het verzamelen van informatie van private en publieke organisaties kan (Nijsen, 2003). Voor controle op en handhaving van de naleving van het beleid, dienen het bedrijfsleven en andere organisaties de overheid te informeren over hun prestaties en interne/externe situatie. De overheid stelt ten behoeve van het algemeen belang (Rutgers, 2011) het aanleveren van benodigde informatie door private en publieke organisaties verplicht.

We geven enkele voorbeelden van verantwoordingsinformatie en waarvoor zij gebruikt kan worden (gebaseerd op: Nijsen, 2003 en Rutgers, 2011):

- Informatie over het functioneren van (semi-)publieke organisaties die belast zijn met de uitvoering van bijvoorbeeld zorg, onderwijs en woningbouw.
- Financiële toezichtinformatie van private organisaties.
- Informatie over persoonlijke inkomstenwervingen en de omzet, winsten en intracommunautaire leveringen van bedrijven: dit betreft informatie die het mogelijk maakt om partijen een bijdrage te laten leveren aan de staatskas en het primaire inkomen te (her)distribueren.
- Statistische informatie op macroniveau als input voor beleid en wetgeving. Denk daarbij aan jaar- en productiestatistieken, investeringsgegevens en omzetstatistieken.
- Openbare financiële bedrijfsgegevens. Dit betreft informatie die openbaar wordt gemaakt ten behoeve van het bedrijfsleven zelf, om burgers te beschermen tegen 'de markt' en de rechtszekerheid in het economisch verkeer te bewerkstelligen.

Er zijn binnen de overheid meerdere partijen die verantwoordelijk zijn voor de uitvoering van de verantwoordingsketens. Wij gebruiken voor deze partijen in dit boek soms de term 'uitvragende partij'. De uitvragende partijen dienen zich bij de inrichting van de verantwoordingsketen stuk voor stuk te houden aan de Wet elektronisch bestuurlijk verkeer en voeren vergelijkbare verrichtingen uit. Denk hierbij aan authenticatie, het controleren van de machtiging van de aanleveraar of volledigheidcontroles. De informatieverwerking geschiedt veelal geautomatiseerd.

Waar verantwoord wordt, gaat dit vaak op voor een groot aantal betrokken verantwoordende partijen. De verantwoording is periodiek. Voor de verantwoordingsplichtige organisaties geldt dat zij in de regel bij meerdere uitvragende partijen verantwoording afleggen. Deze informatie is vaak direct afkomstig uit de (geautomatiseerde) bedrijfsadministratie of wordt daaruit afgeleid. De verantwoordingsplichtigen maken bij de verantwoording niet zelden voor verschillende ketens gebruik van dezelfde of vergelijkbare financieel dienstverleners (administratiekantoren, fiscalisten, accountants).

Het verantwoordingsdomein scoort hoog op de condities die bepalend zijn voor de business case voor S2S-ketenintegratie. Samengevat geldt:

1. Uitvragende partijen vragen steeds over een andere periode dezelfde soort informatie uit.
2. Door het groot aantal verantwoordingsplichtigen is het verwerkingsvolume van veel verantwoordingsketens groot.
3. Zowel de verantwoordingsplichtige als de uitvragende partij maken voor de verwerking van verantwoordingsinformatie veelvuldig gebruik van IT.
4. De uitvragende partijen kennen dezelfde wettelijke kaders voor het bestuurlijk verkeer, voeren vergelijkbare verwerkingen uit en hebben behoefte aan kennis van de administratieve organisatie en interne beheersing.
5. Dezelfde verantwoordingsplichtige partijen (of hun dienstverleners) leveren aan bij meerdere uitvragers en hebben dus baat bij een standaardisatieplaform.
6. Eisen aan het elektronisch verzenden en ontvangen van verantwoordingsinformatie (en de verwerking die hierbij een rol speelt) die bepalend zijn voor de inrichting van het verantwoordingsproces, zijn opgenomen in een generieke wet op het elektronisch bestuurlijk verkeer.

1.4 De voorziene SBR oplossing

1.4.1 *Op zoek naar de architectuur voor standaard S2S-verantwoording*

Gezien de bovenstaande analyse wekt het geen verbazing dat vanaf het begin van het millennium de mogelijkheden van een system-to-system ketenintegratie (horizontaal en verticaal) tussen verantwoordingsplichtigen en uitvragende partijen verkend wordt. Op dat moment is er volop politieke aandacht voor de last die de verwerking van de verantwoording van bedrijven aan de overheid met zich meebrengt. Horizontale koppeling van geautomatiseerde verantwoordingssystemen is een interessante optie, die in de fiscale keten (met behulp van de zogenaamde BAPI-specificaties en -voorzieningen) ook reeds toegepast wordt. Daarnaast streeft de overheid ook dan al naar een kleinere en efficiëntere overheid middels de inzet van generieke ICT-toepassingen. Het beleggen (outsourcen) van generieke onderdelen van verantwoordingsprocessen bij een gedeelde dienstverlener zou een efficiëntere overheid met zich mee kunnen brengen. De oplossing moet wel aansluiten bij de karakteristieken van de informatieketens uit het verantwoordingsdomein. Projecten als het Nederlandse Taxonomie Project (NTP) en het programma GEIN bepalen in 2004-2005 de architectuur voor S2S-geïntegreerde verantwoordingsketens.

1.4.2 *Karakteristieken van het verantwoordingsdomein en eisen aan de oplossing*

De koppeling met verantwoordingspecifieke wet- en regelgeving
De belangrijke aspecten van een verantwoordingsketens zijn in wet- en regelgeving vastgelegd. Zo is vaak beschreven welke verantwoordingsinformatie in welke vorm en op welk tijdstip moet worden aangeleverd. Deze eisen uit wet- en regelgeving kunnen door uitvoeringsinstanties niet genegeerd worden. Dit betekent dat op bepaalde punten weinig ruimte kan zijn voor het herontwerpen van het verantwoordingproces, ook wanneer het een relatief kleine ingreep met een grote winst betreft. Niet alle, toch veelvoorkomende verrichtingen bij de informatieverwerking zijn relevant voor

alle verantwoordingsketens. Ook geldt dat wanneer een wet wijzigt de verantwoordingsketen hoe dan ook aangepast moet worden. Bepaalde wijzigingen – bijvoorbeeld van de inhoudelijke fiscale uitvraag – komen regelmatig voor.

Het aanleveren van bepaalde verantwoordingsinformatie moet binnen een bepaalde termijn gebeuren, maar in sommige verantwoordingsketens kan er op verschillende momenten over verschillende periodes of momenten tegelijkertijd verantwoord worden. Ook is het mogelijk dat voorafgaand aan de verantwoording of op basis van de verantwoording door de uitvragende partij een mededeling wordt verstrekt. De eenheid van de verantwoordende partij kan verschillend zijn. Zo kan een fiscale eenheid of controleplichtige eenheid opgebouwd zijn uit meerdere rechtspersonen. Tot slot zijn er verantwoordingsketens (bijvoorbeeld het jaarrekeningenrecht) waar niet één model voor de uitvraag wordt gehanteerd, maar de wet vraagt om voldoende inzicht. Dit inzicht kan via verschillende modellen verkregen worden en per sector specifieke elementen vragen. Al deze karakteristieken nemen de volgende eisen voor de opzet van de system-to-system integratie met zich mee:

- Verschillende berichten uit verschillende ketens moeten toch op een standaard manier gegenereerd, uitgewisseld en gecontroleerd (gevalideerd) kunnen worden. Dit vraagt om een standaard formaat voor het definiëren en generen van berichtspecificaties.
- Binnen het gekozen formaat moeten berichtspecificaties van de verantwoordingsketens gemakkelijk uit te breiden zijn met specifieke elementen.
- Wanneer uitvragende partijen hetzelfde vragen, moeten zij gebruik kunnen maken van hetzelfde element. Het formaat dat gekozen wordt voor het inrichten van de berichtspecificaties moet op basis van dezelfde elementen meerdere rapportages kunnen ondersteunen.
- De berichtspecificaties moeten onafhankelijk van de processpecificaties gewijzigd kunnen worden.
- De verwerkingsprocessen bij het SSC moeten opgebouwd zijn uit generieke verwerkingsservices die ieder een veelvoorkomende verrichting uitvoeren. Deze services moeten los van elkaar in te zetten zijn en tevens los van elkaar aan te passen zijn.
- De processpecificaties van (voor de keten relevante onderdelen van) de verantwoordingsprocessen moeten in een standaard formaat worden vastgelegd.
- Een nieuw aanleverproces moet gemakkelijk aangemaakt kunnen worden.
- Hetzelfde aanleverproces moet verantwoording over verschillende periodes tegelijkertijd kunnen ondersteunen.

De bestuursrechtelijke consequenties van verantwoording
Zoals eerder genoemd valt de elektronische verantwoording aan overheidspartijen onder het bestuursrecht (de Wet elektronisch bestuurlijk verkeer). Deze wet stelt eisen aan onder andere de betrouwbaarheid en vertrouwelijkheid van de informatieverwerking en de gronden waarop de overheid een bericht mag weigeren. De wet schrijft in dit geval ook voor hoe de overheid in zo'n geval moet handelen. Kenmerkend voor het bestuursrecht is dat het doel en de aard van de verantwoording bepaalt hoe er met tegengestelde eisen (gebruikersgemak tegenover vertrouwelijkheid) wordt omgegaan. Doelbinding is een belangrijk principe van het bestuursrecht. Op

basis van deze en vergelijkbare bepalingen (Wet bescherming persoonsgegevens, Archiefwet) kunnen de volgende eisen aan de oplossing voor S2S-integratie bij verantwoording gesteld worden:

- Verantwoordingsplichtigen, de dienstverlener en uitvragende partijen moeten elektronisch herkend kunnen worden.
- Partijen moeten veilig namens anderen kunnen deelnemen in de verantwoording. Dit vraagt om mogelijkheden voor het vaststellen van een machtiging.
- De informatieverwerking moet gepaard gaan met terugkoppeling over de uitkomsten van de verantwoording.
- Uitvragende partijen moeten kunnen differentiëren in betrouwbaarheidsniveaus wanneer het doel of de aard van de verantwoording hier om vraagt.
- Verantwoordingsplichtigen moeten – ondanks de plichten – zelf kunnen kiezen wanneer zij voor welk doel informatie uit hun administratie als verantwoordingsinformatie aanleveren.

Verantwoording als maatschappelijk proces

'Ketenomkering' is een centraal thema geweest vanaf het moment dat de overheid onderzoek deed naar de grootschalige S2S-integratie in verantwoordingsketens. Ketenomkering geeft aan dat de bedrijfsadministratie als primaire bron voor de verantwoording wordt gezien. Het verschil met het oude paradigma is dat niet de informatieverwerking van de uitvragende partij, maar deze bron als dominant uitgangspunt wordt gezien bij het inrichten van de verantwoording. Dit betekent dat waar vanuit de bron aangesloten moet worden bij verschillende verantwoordingsprocessen, dit zoveel mogelijk op een standaard manier moet kunnen geschieden. Het is vanuit dit punt logisch dat de overheid voor de generieke onderdelen van de verantwoording standaardmethoden en -technieken toepast. Nu heeft verantwoording een belangrijke maatschappelijke functie, ook waar het verantwoording in het kader van privaatrechtelijke overeenkomsten betreft. Denk aan partijen die zich in het kader van de kredietverstrekking verantwoorden aan banken of een bedrijf dat zich over zijn maatschappelijk verantwoord handelen verantwoordt aan een keurmerkorganisatie.

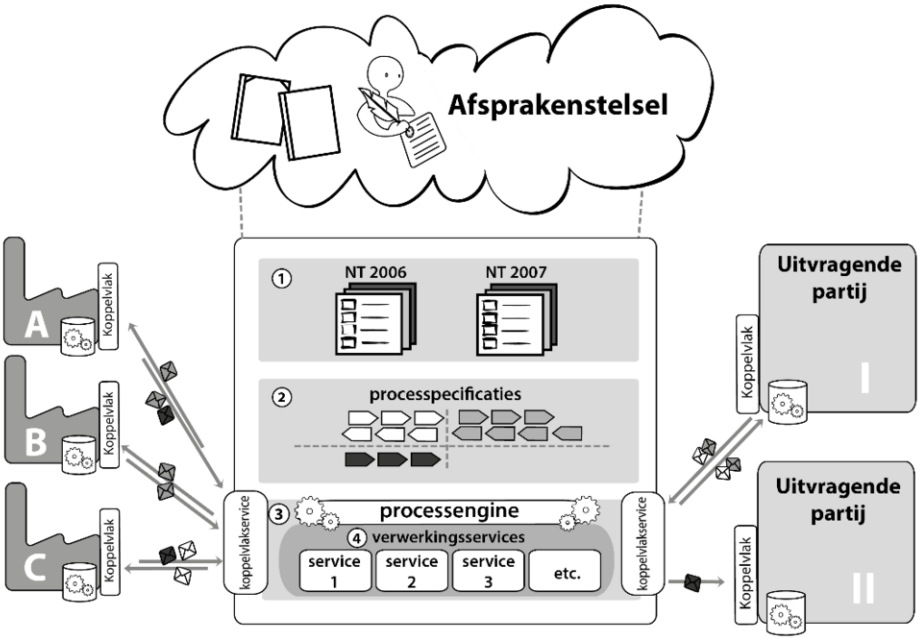
Voor verantwoordende organisaties is het zeer interessant wanneer niet alleen de publieke uitvragende partijen, maar alle stakeholders zouden werken via het principe van ketenomkering. Wanneer private partijen dezelfde technische standaarden als de overheid toepassen, kan de verantwoording in de breedte efficiënter vormgegeven worden.

Met deze visie in het achterhoofd is het noodzakelijk de standaarden en de wijze van toepassing van deze standaarden in de verantwoordingsketen integraal openbaar te maken. Doordat de standaardisatie zich niet meer beperkt tot de verticale ketenintegratie (het gebruik van een SSC als standaardisatieplatform) moeten de kaders voor de S2S-integratie binnen verantwoordingsketens op een hoger abstractieniveau uitgewerkt worden. De adoptie van een dergelijk afsprakenstelsel wordt bevorderd wanneer er gebruik gemaakt wordt van algemeen geaccepteerde en reeds bekende standaarden.

De ambitie om de S2S-integratie binnen zowel publieke als private verantwoordingsketens op een standaard wijze vorm te geven levert de volgende eisen op aan de architectuur van de oplossing:

- De onderdelen uit de oplossing zijn bij voorkeur gebaseerd op algemeen geaccepteerde standaarden.
- Er worden waar nodig architecturen – het SBR afsprakenstelsel - opgesteld om de eenduidige toepassing van standaarden in verschillende verantwoordingsketens te waarborgen.

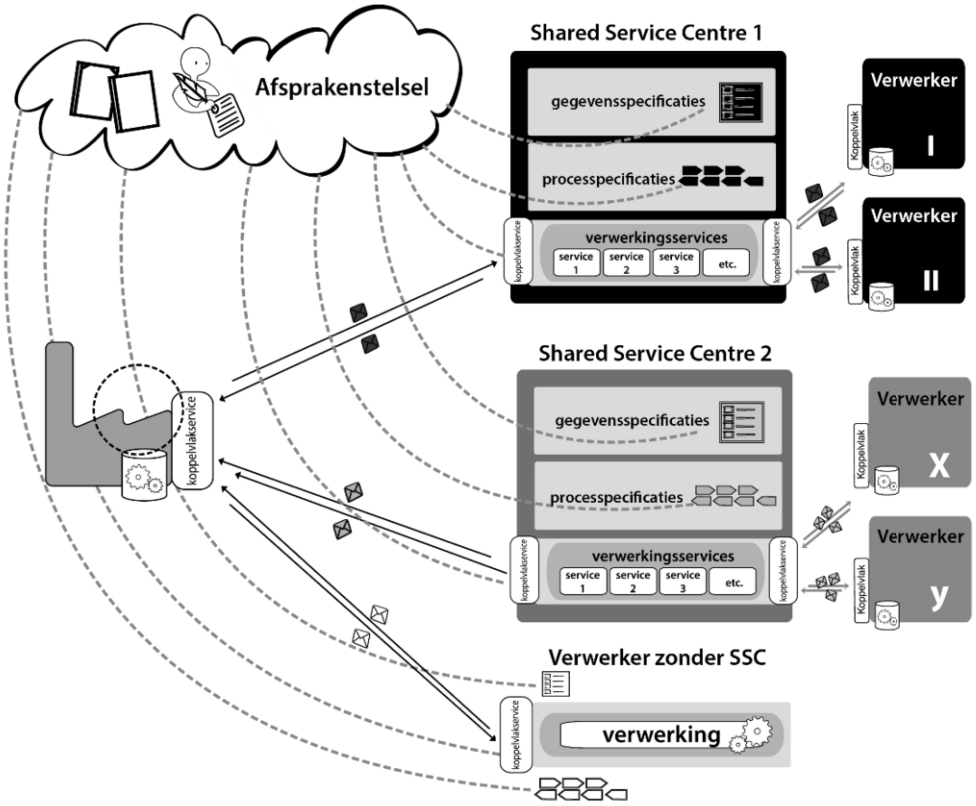
De schets van de oplossing



Figuur 1.5 – Schets van de SBR-oplossing als basis voor verantwoordingsketens van publieke uitvragende partijen in 2006

Op basis van de gedefinieerde eisen in de verantwoording lag er in 2006 de bovenstaande architectuurschets voor SBR als basis voor standaard verantwoordingsketens voor publieke uitvragers.

De architectuur van het afsprakenstelsel werkt als basis voor alle partijen die S2S geïntegreerd informatie willen uitwisselen. De positie van de verschillende partijen (publieke en private) zijn in de volgende figuur weergegeven.



Figuur 1.6 – De bredere reikwijdte van het SBR afsprakenstelsel. Basis voor S2S-integratie in verantwoordingsketens door verschillende publieke en private partijen.

De belangrijkste aspecten uit de schets van de SBR-oplossing uit 2006 worden hierna toegelicht. Bepaalde onderdelen zijn later verfijnd en er hebben binnen dezelfde architectuur verschillende uitbreidingen plaatsgevonden (er is functionaliteit bijgekomen), maar het wezen van de oplossing is in hoge mate hetzelfde gebleven. In deel B van dit boek wordt de oplossing een stuk gedetailleerder beschreven en geldt de actuele stand van zaken als uitgangspunt.

1. De Nederlandse XBRL Taxonomie

Iedere verantwoording begint met de vraag wat een uitvragende partij aan informatie wil hebben of in het kader van de verantwoording wil mededelen. De Nederlandse XBRL Taxonomie of Nederlandse Taxonomie (NT) betreft een voor computers leesbare beschrijving van de informatie die de uitvragende partij voor verwerking wil ontvangen van of aanbieden aan een verantwoordende organisatie. Voor het structureren maakt de SBR oplossing gebruik van eXtensible Business Reporting Language (XBRL). XBRL is een internationaal geaccepteerde standaard voor bouw en gebruik van taxonomieën voor verantwoording. Met de vastlegging van de specificaties wordt de interpretatie van gegevens systeem-onafhankelijk en eenduidig bepaald. In het NTP is de eerste versie van de gedeelde taxonomie opgeleverd. De taxonomie is

op een losse manier gekoppeld aan de technische infrastructuur (een vorm van loose coupling).

2. Processpecificaties van verantwoordingsprocessen in BPMN

Behalve dat bekend moet zijn welke gegevens door een uitvragende partij moeten worden aangeleverd, is het voor een S2S-geïntegreerde keten van groot belang dat de verwerking bekend is. De processpecificaties geven een beschrijving van de wijze waarop de uitvragende partij de aangeboden of aan te bieden gegevens wil verwerken. Voor de partijen in de keten zijn bepaalde aspecten van de processen relevanter dan andere. Verrichtingen in de verantwoording die door het SSC worden uitgevoerd – zijn in ieder geval relevant omdat zowel de verantwoordingsplichtige partij als de uitvragende partij hier een directe koppeling mee heeft. Bovendien geldt dat het uitvoeren van deze verrichtingen door het SSC door de uitvragende partij als dienst wordt afgenomen. Dit deel van de verantwoordingsprocessen wordt altijd in de open standaard Business Process Modeling Notation (BPMN) beschreven. Dit heeft twee redenen. Ten eerste is het voor partijen gemakkelijker de processen te doorgronden en te vergelijken wanneer er gebruik wordt gemaakt van één uniforme taal. Ten tweede dwingt de taal een zekere mate van eenduidigheid af en is deze door technici gemakkelijk om te zetten naar code (waaronder de open standaard BPEL). Deze technische code is door het SSC direct te implementeren in de zogenaamde procesinfrastructuur. Het SSC handelt de procesonderdelen volledig geautomatiseerd af. Wanneer wij het in dit boek hebben over het de verrichtingen uit het verantwoordingsproces die worden uitgevoerd door het SSC spreken wij veelal van het i-proces.

3. Koppelvlakservices

De koppelvlakservices zijn de technische applicaties die berichten van buiten het SSC kunnen aannemen of bij een andere koppelvlakservice kunnen afleveren. Het kan gaan over inhoudelijke berichten of berichten waarin de status van de verwerking van een bericht is opgenomen. De beschrijving van de wijze waarop een koppelvlak 'functioneert' maakt onderdeel uit van de specificatie van het informatieverwerkingsproces. Het technische uitwisselingsprotocol dat gekozen is (de technische envelop waar een bericht in verpakt wordt), is het simple object access protocol (SOAP). Omdat de koppelvlakservices voor de buitenwereld aanspreekbaar zijn bevatten zij de belangrijke controles voor toegangsbeveiliging. Hier is binnen de oplossing voor een standaard beveiligingsprotocol voor system-to-system verkeer gekozen. Er wordt op basis van een x.509 certificaat een dubbelzijdige beveiligde verbinding opgezet tussen een partij en het SSC. Tevens moet met eenzelfde soort certificaat het bericht verzegeld worden. Binnen de oplossing is ook ruimte om een bericht te voorzien van een persoonsgebonden gekwalificeerde handtekening. Er zijn vanuit het perspectief van het SSC drie soorten koppelvlakken te onderscheiden: (1) berichtafleverkoppelvlakken, (2) bericht-ophaalkoppelvlakken en (3) statusinformatiekoppelvlakken. Middels de statusinformatiekoppelvlakken kan een partij vaststellen wat er met een aangeleverd bericht of bij een aanvraag gebeurd is.

4. Verwerkingsservices

De verwerkingsservices zijn de te onderscheiden applicaties die onderdelen van het i-proces geautomatiseerd afhandelen. Een koppelvlakservice 'pakt' een bericht op van een partij en op basis van de processpecificaties voor dat type bericht bepaalt de

engine welke verwerkingsservices met het bericht aan de slag moeten en in welke volgorde dit moet gebeuren. De belangrijkste verwerkingsservices uit de generieke oplossing zijn:

- Authenticatieservice: Controleert de integriteit van het bericht en stelt op basis van het certificaat bij een black list of het certificaat niet ingetrokken is.
- Autorisatieservice: Controleert bij een vertrouwd register of een partij gemachtigd is een bepaald bericht in te zenden of op te vragen.
- Validatieservice: Kan op basis van de specificaties uit de Nederlandse Taxonomie voor iedere aangeleverde verantwoording vaststellen of het voldoet aan de eisen die er door de NT aan gesteld zijn.

Door loose coupling toe te passen kan worden geborgd dat bouwblokken zoals de berichtspecificaties, i-processen en services los van elkaar functioneren en los van elkaar te wijzigen zijn.

5. Afsprakenstelsel

Het afsprakenstelsel beschrijft welke standaarden je toepast bij het inrichten van een SBR-verantwoordingsketen. Hiermee wordt SBR ook in andere domeinen toepasbaar. Kijken we naar de onderdelen uit het geschetste afsprakenstelsel, dan dient er onderscheid gemaakt te worden tussen specifieke specificaties voor SBR-verantwoording en niet-specifieke specificaties. Deze laatste 'specificaties' zijn op zichzelf al standaarden die buiten de oplossing breder worden toegepast, zoals BPMN en XBRL. Vanaf de start van de schets hebben de Nederlandse Taxonomie Architectuur, een architectuur voor i-processen (gebaseerd op GEIN) en een Technische Architectuur deel uitgemaakt van het afsprakenstelsel.

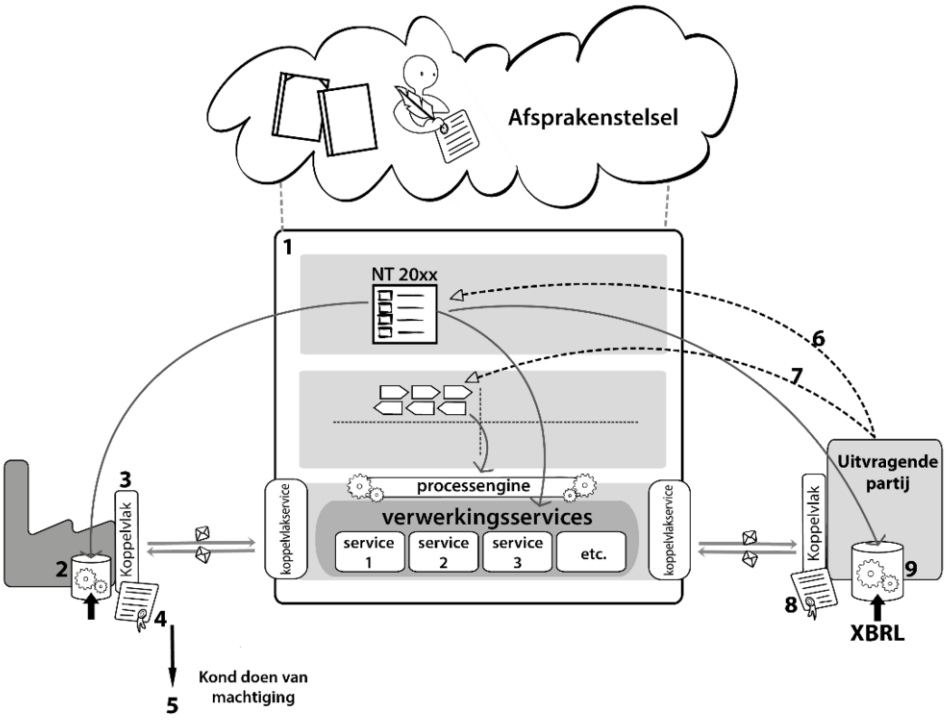
1.5 Implementatie in een pluriform domein

1.5.1 *Het enorme transitiedomein*

Met de geschetste oplossing onder de arm werden bestuurders en directeuren van grote stakeholders geënthousiasmeerd om in 2006 een convenant te tekenen. Iedereen zag de potentie van de ontwikkeling. Zoals gezegd spraken de convenantpartijen af dat iedereen zich zou inspannen om hun deel van de oplossing te implementeren. Voor de gekozen scope (verantwoording voor de domeinen van de Belastingdienst, CBS en KvK) bestond het transitiedomein ruwweg uit:

- 12.000 fiscalisten
- 2.000 accountants
- 500 softwareleveranciers
- 1.300.000 bedrijven
- 3 uitvragende partijen (Belastingdienst, CBS, KvK)
- 6 verantwoordingsketens
- het NTP project en Logius (toen nog GBO.Overheid)

Het convenant besloeg een enorm wijzigingsgebied waarin de verschillende partijen aan de lat stonden voor een technische implementatie. Deze technische implementatie is in de figuur op hoofdlijnen weergegeven, en daarna aan de hand van de cijfers uit de figuur in tekst toegelicht.



Figuur 1.7 – Omvangrijk wijzigingsgebied; de 9 aspecten van de door de verschillende betrokken partijen te realiseren technische implementatie.

1. Om de transities van de verschillende verantwoordingsketens mogelijk te maken moest voor het SSC vanzelfsprekend het SBR standaardisatieplatform worden gerealiseerd. Hiervoor moesten eerste versies van de generieke koppelvlakservices opgeleverd worden. De verwerkingsservices moesten gemaakt worden en er moest een procesinfrastructuur gerealiseerd worden, waarin al deze componenten aan elkaar geknoopt konden worden. Dit platform is nu bekend onder de naam Digipoort.

Voor een SBR-verantwoordingsketen in productie moeten alle onderstaande zaken geregeld zijn:

2. De software van verantwoordingsplichtigen moet een XBRL taxonomie kunnen 'lezen'. Gebruikers moeten een mapping kunnen maken tussen hun eigen database en de elementen uit de taxonomie. De software moet op basis van de NT een bericht kunnen genereren.

3. De software van verantwoordingsplichtigen moet een koppelvlakservice implementeren, zodat de software berichten op de juiste wijze (de juiste digitale envelop) af kan leveren bij het SSC.
4. De verantwoordingsplichtigen moeten beschikken over een certificaat, zodat de authenticiteit van het berichtenverkeer door het SSC kan worden vastgesteld.
5. Waar een verantwoordingsketen een machtigingscontrole vereist, moet de partij een machtiging aanleveren bij een hiervoor aangewezen partij.[4]
6. De uitvragende partij moet de berichtspecificaties beschikbaar maken in XBRL.
7. De uitvragende partij moet de processpecificaties van de i-processen opstellen in BPMN.
8. De uitvragende partij moet beschikken over een certificaat, zodat de authenticiteit van het berichtenverkeer door het SSC kan worden vastgesteld.
9. De software van de uitvragende partij moet een XBRL-taxonomie kunnen 'lezen'. De uitvragende partij moet een mapping kunnen maken tussen de eigen database en de elementen uit de taxonomie. De software moet een XBRL-bericht dat op basis van de NT is opgesteld, kunnen verwerken.

Lichtpuntje bij de implementatie was dat wanneer een partij aansluit op SBR hij vervolgens heel gemakkelijk een nieuwe SBR verantwoordingketen kan implementeren. Wanneer een softwareleverancier bijvoorbeeld een koppelvlak heeft geïmplementeerd, kan deze alle soorten verantwoordingsberichten uitwisselen met de Digipoort. Een partij die informatie wil aanleveren bij Digipoort hoeft maar één keer een certificaat aan te schaffen. Er valt dus bij de realisatie van SBR een onderscheid te maken tussen het realiseren van de SBR-fabriek (het SSC-platform), het aansluiten op SBR van verantwoordingsplichtigen en uitvragende partijen en het implementeren van een nieuwe SBR-verantwoordingsketen. Thans geldt dat de dienstverlening van Logius staat. Sommige ketens moeten nog over op SBR, maar doordat fiscale stromen grootschalig in productie zijn, geldt dit voor steeds minder ketenpartijen. Het operationaliseren van nieuwe SBR-verantwoordingsketens heeft dus steeds minder voeten in de aarde. In 2006 gold echter dat alle drie in samenhang en voor de eerste keer gerealiseerd moesten worden. Dit traject vroeg om een sterkere coördinatie en regie dan aanvankelijk werd gedacht.

1.5.2 *Impasse in de implementatie*

Door het ontbreken van een eenduidige besturing op SBR zaten partijen met een aantal vragen waar zij maar lastig antwoord op konden krijgen:

- Hoe serieus is SBR? Hoe relevant is het om nu al te investeren?
- Waar kan ik terecht met vragen over de aansluiting en wie bepaalt hoe die ondersteuning eruit ziet?
- Hoe kan ik invloed uitoefenen op de wijze waarop SBR geïmplementeerd moet worden?

[4] Dit onderdeel is binnen de huidige oplossing aangepast en meer in lijn gebracht met de generieke architectuur. Zie hiervoor ook de tekstboxen in dit hoofdstuk.

Waar het convenant uitging van een brede en vrijwillige uitrol van de oplossing in dit enorm pluriforme domein, bleek een realisatie van werkende SBR-ketens op basis van een papieren convenant een te grote opgave. Eind 2009 waren er door diverse koplopers stappen gezet en stukjes van de keten geïmplementeerd, maar er was nog geen SBR-keten grootschalig in productie. Sceptici werden bevestigd in hun oordeel dat SBR voorlopig niets zou worden en raadden partijen of hun bazen af actief te investeren in SBR. SBR zat in een impasse.

Praktijkvoorbeeld van de noodzaak van een gedragen governance
De noodzaak van een gedragen governance voor implementatie, laat zich het beste toelichten met een voorbeeld uit de SBR casus. In de initieel geschetste SBR oplossing gold dat partijen (bijvoorbeeld fiscale dienstverleners) voor het aanleveren van berichten namens hun klanten een machtigingsbewijs moesten aanleveren bij een private Autorisatie service provider. Hoewel het vanuit het bestuursrecht aantrekkelijk is de machtiging geautomatiseerd te controleren, bleek de wijze waarop het binnen de oplossing was vormgegeven een grote blokkade voor implementatie. Ten eerste was de autorisatiemarkt niet volwassen, waardoor de processen nogal houtje-touwtje waren ingericht. Dit maakte dat het kond doen van machtiging vaak een lastige exercitie was. Ten tweede werd er over de noodzaak van het formeel kond doen van de machtiging voor het aanleveren van berichten gediscussieerd: waarom zou iemand ongevraagd voor zijn buurman aangifte doen? Ten derde moesten de partijen betalen voor de dienstverlening van de service provider. Dit waren zij niet gewend en gold als een lastenverzwaring. Tot slot vonden dienstverleners het een onaantrekkelijk idee om hun klantrelaties aan een derde kenbaar te maken. Het was duidelijk dat om deze implementatiedrempel weg te nemen dit deel van de oplossing gewijzigd moest worden. Maar wie moest vaststellen of dit kon? Wie was verantwoordelijk voor het aandragen van een alternatieve oplossing? Wie moest beslissen of deze oplossing toereikend was en wat de reikwijdte van deze oplossing moest zijn? Tot en met eind 2009 werd er ongestructureerd met voorlopers over het probleem gesproken, maar de structuren voor het oplossen van dit probleem ontbraken. Dit veranderde met de interventie op het SBR Programma.

1.5.3 *Governance voor het besturen van de implementatie*

In het kader van de impuls aan de implementatie van SBR werden er op hoofdlijnen drie interventies gepleegd die zorgden dat SBR uit de impasse kon komen:

1. Er werd een Rijksregisseur aangesteld. Het Ministerie van Economische Zaken (EZ) en de uitvragende partijen sloten op hoog bestuurlijk niveau aan bij de besturing op de implementatie. Met deze interventie liet de overheid zien dat SBR menens was en werd het ook voor criticasters duidelijk dat SBR wel eens een blijvertje zou kunnen zijn. Hiermee werd hun bereidheid om deel te nemen aan afstemmingsgremia groter.
2. Er werden diverse gremia opgericht waar gestructureerde besluitvorming over verschillende onderdelen van de implementatie en (door)ontwikkeling van SBR kon plaatsvinden.
3. Bij Logius werd een programmateam van deskundigen ingericht, dat de opdracht kreeg de governance actief en inhoudelijk te faciliteren en een bijdrage te leveren aan de implementatie van SBR in de verschillende verantwoordingsketens.

Hoewel bovenstaande interventie gericht was op het programmatisch besturen en coördineren van de SBR-implementatie, raakten steeds meer betrokkenen overtuigd

van het volgende: de SBR-oplossing die geïmplementeerd moest worden bestond naast de nieuwe technologie ook uit een zeer grote organisatorische component. Wijzigingen zouden namelijk ook na de eerste implementatie van SBR aan de orde blijven. Nieuwe verantwoordingsketens moesten gemakkelijk kunnen toetreden. Dus ook na implementatie zou een werkende governance nodig zijn om de afhankelijkheden van de S2S-integratie te blijven coördineren. Hier was in 2006 nog geen duidelijke schets van voorhanden geweest. Een inhaalslag was vereist. Ook werd het beleidsopdrachtgevers en afnemers van de diensten van Logius duidelijk dat de rol van Logius veel meer zou inhouden dan het laten draaien van een machine voor standaard verantwoording. Het inhoudelijk en procesmatig faciliteren van de governance zou een van haar kerntaken worden. Duidelijk moest worden hoe Logius invulling zou kunnen geven aan deze kerntaak en welke competenties hiervoor nodig waren. Dit behoefde een nadere uitwerking van de oplossing.

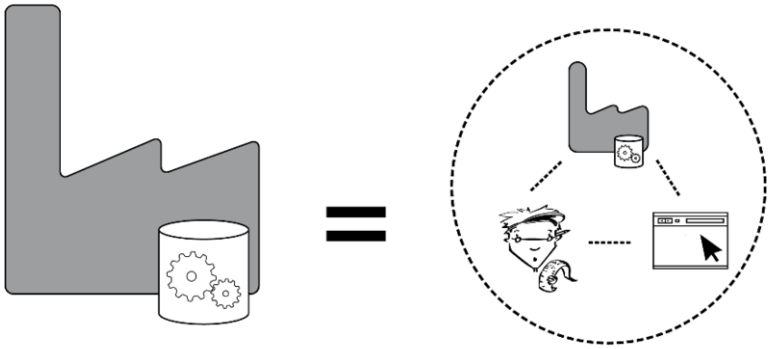
Praktijkvoorbeeld van het wegnemen van een drempel door middel van een gedragen governance
Door het gebruik van de afstemming in de nieuwe en gedragen gremia kon het SBR Programma met een voorstel komen om het AuSP-probleem op te lossen. De roadblock voor implementatie werd als volgt uit de weg genomen. De zekerheid over authenticatie werd versterkt. Voortaan zou gebruik gemaakt worden van PKIoverheid certificaten. PKIoverheid werd hiermee een item in het afsprakenstelsel. Aanleverketens konden de autorisatieservice vervolgens standaard aanzetten, uitzetten of optioneel maken. De uitvragende partijen besloten gezamenlijk te kiezen voor de optionele variant. Vanzelfsprekend waren de partijen die voorgesorteerd waren voor de autorisatie-dienstverlening niet blij met deze keuze, maar zij snapten dat wanneer de SBR-dienstverlening niet op gang zou komen zij ook niets aan hun dienst zouden verdienen. Koplopers (fiscale dienstverleners) die al hun processen op het gebruik van een AuSP hadden ingericht, hoefden, door het optionele karakter, geen wijzigingen door te voeren in hun proces. Inmiddels is er een voorziening gegenereerd voor het ontvangen van mededelingen, waarbij het kond doen van een machtiging digitaal mogelijk is vanuit de systemen van de dienstverleners. Hierbij wordt gebruik gemaakt van de Digipoort.

1.5.4 *Governance en beheer als onderbelicht onderdeel van de oplossing*

In 2006 is bepaald dat Logius (toen nog GBO.Overheid) als SSC het beheer zou voeren over de Nederlandse Taxonomie en de procesinfrastructuur (i-processen, koppelvlakservices en verwerkingservices). Hoe partijen zich zouden verhouden bij wijzigingen was echter niet opgenomen. Tevens bestond er geen exact beeld hoe de verschillende actoren door de toepassing van SBR met elkaar verbonden zouden raken en hoe de nieuwe afhankelijkheden zich verhielden met de bestaande situatie.

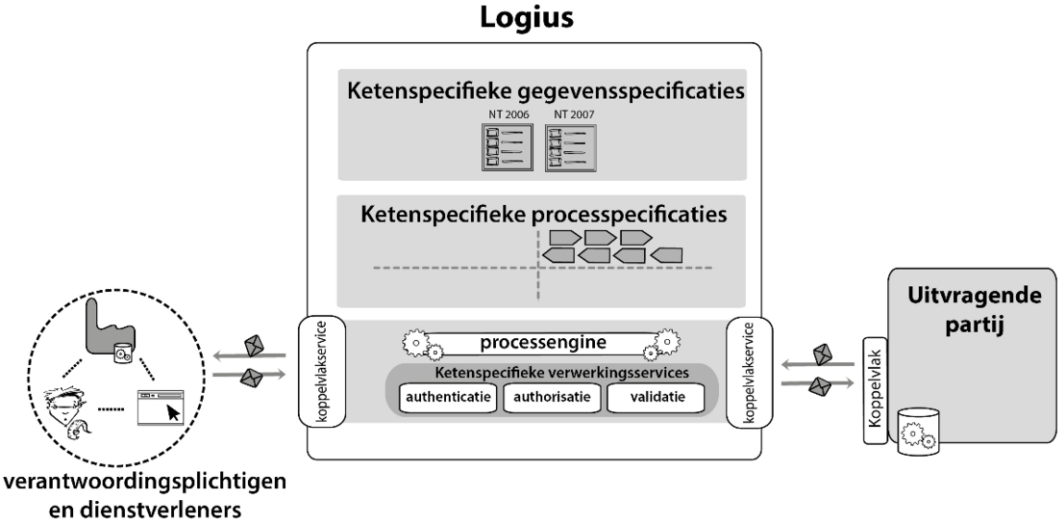
1. Horizontale afstemming per verantwoordingsketen
Allereerst vraagt de toepassing van SBR in een verantwoordingsketen (bijvoorbeeld IB/VPB) voor zowel de implementatie als het onderhoud en de doorontwikkeling, om afstemming vanuit het perspectief van een specifieke verantwoordingsketen. De bestaande situatie wijkt af per verantwoordingsketen. In 2006 waren de fiscale ketens al S2S-geïntegreerd (hiervoor werd het BAPI-protocol gebruikt). De KvK keten was nog in grote mate papier-gebaseerd. Digitale aanlevering gebeurde op basis van e-mail. Statistiekopgaven kenden een human-to-system interface als dominante aanlevermodaliteit. Binnen ketens golden weer verschillende uitgangspunten. Bij de

verwerking van de verantwoordingsinformatie zijn naast de onderneming vaak ook nog dienstverleners betrokken.



Figuur 1.8 – Naast de verantwoordingsplichtige onderneming zijn vaak nog dienstverleners betrokken in de verantwoordingsketen, zoals fiscaal dienstverleners en softwareleveranciers.

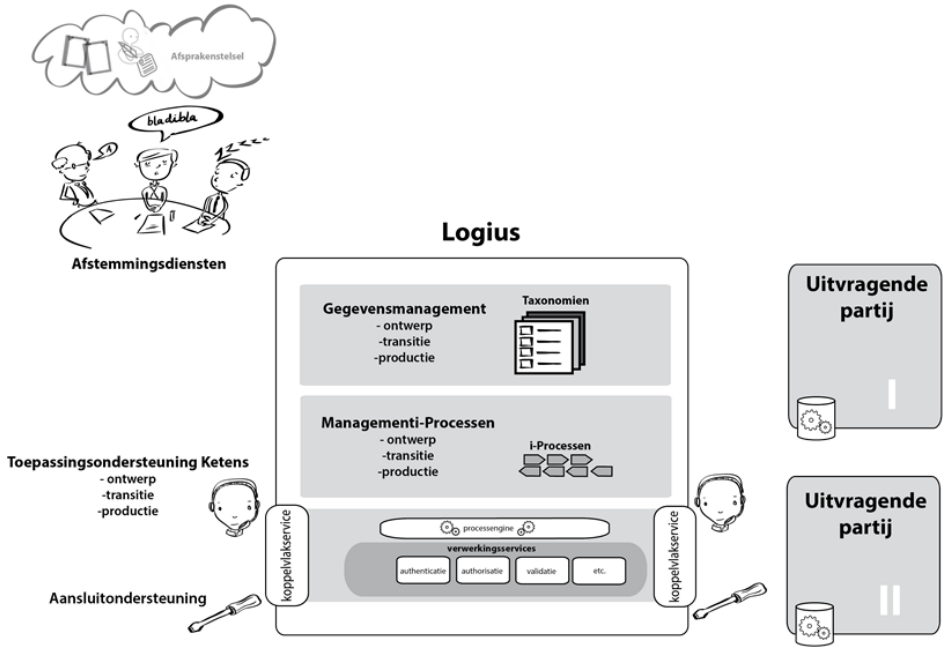
Een verantwoordingsplichtige kan een zelfstandige pottenbakker zijn of een bedrijf als Shell. Een fiscaal dienstverlener kan de plaatselijke intermediair uit Oss zijn of een van de grote vijf kantoren. Hierdoor zijn er tevens verschillen te verwachten in investeringscapaciteit en volwassenheidsniveau in ICT. Bij de horizontale afstemming is de uitvragende partij in de lead. Hij bepaalt op welke wijze de afstemming moet geschieden. Als gedeelde dienstverlener kan Logius generieke aansluitondersteuning voor SBR ontwikkelen, maar de uitvragende partij bepaalt hoe en wanneer hij dit voor zijn keten wil afnemen. In onderstaande figuur is dit besturingsperspectief weergegeven. De figuur maakt de onderdelen die voor de specifieke keten relevant zijn transparant.



Figuur 1.9 – Horizontale afstemming: uitvragende partij in de lead t.a.v. de inrichting van de keten en de afstemming zelf.

2. Verticale afstemming met SSC

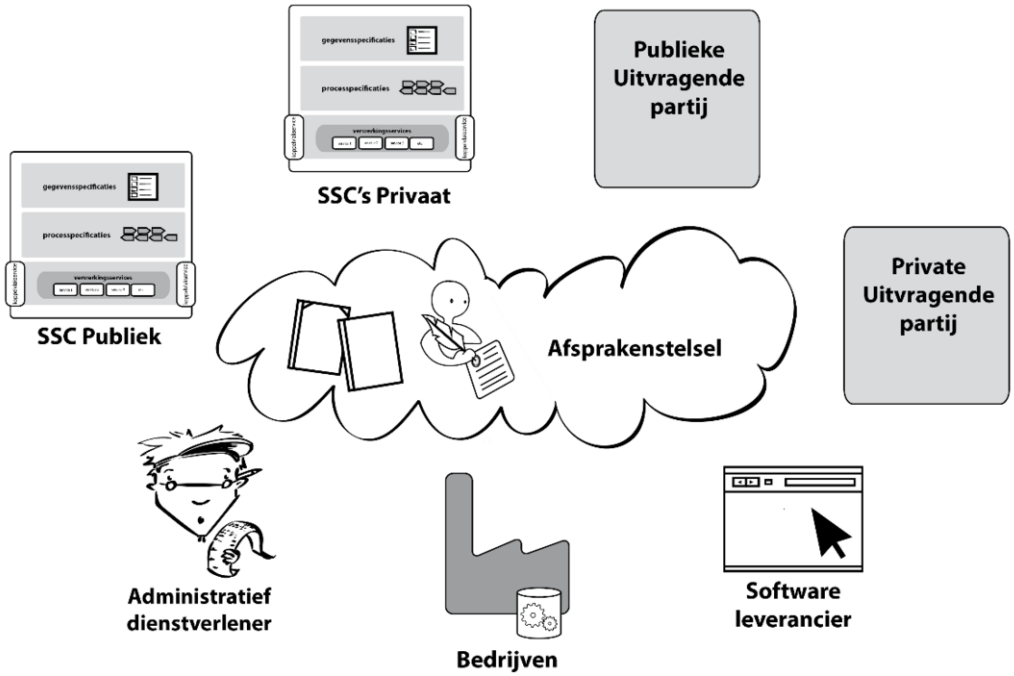
Ook de verticale ketenintegratie vraagt een specifieke afstemmingsvorm. Als gemeenschappelijke afnemers bij Logius hebben de uitvragende partijen (zoals KvK, Belastingdienst en CBS) te maken met een gedeelde dienstverlener. De wijze waarop deze dienstverlener functioneert, hoe deze vorm geeft aan de dienstverlening en hoe de dienst zich verder ontwikkelt, moet worden afgestemd. Onderstaande figuur geeft dit afstemmingsdomein schematisch weer. Bij een SBR-domein in ontwikkeling is het logisch dat bij deze afstemming ook beleidsopdrachtgevers aanschuiven.



Figuur 1.10 – Verticale afstemming: afstemming over de dienstverlening van de gedeelde dienstverlener met de gemeenschappelijke afnemers (uitvragende partijen).

3. Afstemming over het afsprakenstelsel (netwerkniveau)

Tot slot geldt dat het SBR afsprakenstelsel ook voor andere business-to-business verantwoordingsketens toepasbaar moet zijn. Om gebruik te stimuleren is het van belang dat het stelsel aansluit bij de behoefte van de private verantwoordingsketens. Hier is op 'netwerkniveau' afstemming noodzakelijk. Dit afstemmingsgebied is weergegeven in de volgende figuur.



Figuur 1.11 – Afstemming op netwerkniveau: afstemming tussen private en publieke betrokken partijen ten behoeve van de bredere reikwijdte van het afsprakenstelsel.

4. De organisatorische opgave

Door de ketenintegratie die SBR met zich mee brengt blijft het noodzakelijk al deze afstemmingsvormen vorm te geven en in stand te houden. Deze organisatorische component maakt dus deel uit van de SBR oplossing. Dat de onderlinge integratievormen een grote samenhang kennen blijkt al uit het voorbeeld in onderstaande tekstbox. Door de centrale positie van het SSC, in dit geval Logius, is dit feitelijk de enige partij die de afstemming in samenhang inhoudelijk kan faciliteren en coördineren. Zij doet dit vanzelfsprekend in opdracht van de afnemers en beleidsopdrachtgevers.

Samenhang van integratievormen
Het volgende voorbeeld illustreert stapsgewijs de samenhang tussen de verschillende integratievormen:

i. Onvrede met het verwerkingsresultaat (performance) voor complexe berichten vraagt bij één uitvragende partij binnen een verantwoordingsketen om een andere opzet van de verwerking. Dit is een probleem vanuit het horizontale integratieperspectief.
ii. Hiervoor is het nodig de berichtspecificaties (syntax) aan te passen: dimensionele opzet van de berichten. Dit moet dus ook door de architectuur van de Nederlandse taxonomie ondersteund worden.
iii. De benodigde berichtopzet past nog niet binnen de afspraken, dus de afspraken moeten aangepast worden. Partijen besluiten vast te houden aan de standaardisatiewens. Dit mede omdat zij voorzien dat zij bij toename van berichtenverkeer in de toekomst toch over zullen moeten op een dimensionele taxonomie. Zij willen daarom gaan werken aan een architectuur voor de taxonomie die de dimensionele vorm verplicht voorschrijft. Het afsprakenstelsel wordt hierop aangepast.
iv. Dit heeft als consequentie dat de berichtspecificaties van de andere partijen voortaan ook volgens de dimensionele architectuur opgezet moeten worden. Het raakt nu dus aan alle horizontaal geïntegreerde verantwoordingsketens.
v. Hiervoor is het tevens nodig de technische generatie van berichten en de validatie van berichten door alle uitvragende partijen aan te passen.
vi. De uitvragende partijen die geen probleem hadden in de verwerking, dienen mogelijk toch hun verwerkingssysteem aan te passen.
vii. Logius moet als dienstverlener haar dienst van taxonomie-ontwikkeling aanpassen op de nieuwe architectuur. Hier zijn kosten aan verbonden. De afnemers bij Logius moeten het er – gezien hun verticale integratie – over eens worden wie hier voor op moet draaien. De uitvragende partij die als eerste over wilde op de dimensionele taxonomie, of alle uitvragende partijen?

Gaandeweg de SBR-implementatie is dus gebleken dat Logius inhoudelijk een veel belangrijkere en complexere rol moest gaan vervullen dan vooraf gedacht. Het beheer van de gemeenschappelijke onderdelen van SBR betekent, naast het in stand houden van de uitwisseling van berichtenverkeer, in de praktijk ook het orkestreren van ontwikkelingen op verschillende integratieniveaus. Het ontwerpen van de governance en de beheercomponent en het sturen op de implementatie hiervan, kan gezien worden als de onderbelichte component van SBR, die haar evenwel tot een aanzienlijke opgave maakte.

1.6 Leeswijzer

Dit boek is in twee delen opgedeeld: een deel A en een deel B. In deze leeswijzer belichten we kort de essentie van de hoofstukken in beide delen.

1.6.1 *Deel A - SBR als opgave*

Hoofdstuk 2 –Ketens en ketencoördinatie
Dit hoofdstuk gaat in op de ketenbenadering: de dwarsdoorsnede van de werkelijkheid die de basis vormt voor het boek. Via een aantal vragen worden theoretische concepten en praktische inzichten rond de ketenbenadering aangeboden. Allereerst de vraag: wat is een keten? De auteurs beantwoorden deze vraag en beschrijven de voordelen en beperkingen van een ketenbenadering. Deze worden pas goed duidelijk wanneer we bedenken dat het hier in feite om een metafoor van een reeks gekoppelde schakels gaat. De auteurs behandelen hierna vragen als ‘hoe zijn ketens te categori-

seren en wat is er bijzonder aan een informatieketen?' Beantwoording van deze vragen vergt een reflectie op de eigenschappen van ketens en datgene wat er door de schakels stroomt: informatie. Een andere relevante vraag voor partijen die een keten willen of moeten veranderen is, vanuit politiek perspectief: 'hoe is de macht verdeeld in een keten?' Het hoofdstuk beschrijft hoe de ketenstructuur invloed heeft op deze machtsverhoudingen en de rol van vertrouwen. Hierbij komen verschillende vormen van vertrouwen aan bod en wordt nader ingegaan in op de inwisseling van autonomie voor inspraak. De beantwoording van eerder genoemde vragen legt de basis voor een beschrijving van het ketencoördinatievraagstuk: wat is ketencoördinatie en waarom is het nodig? Het hoofdstuk beschrijft verschillende factoren waarmee rekening gehouden moet worden bij het inrichten van de governance – een thema waar hoofdstuk 4 uitgebreider op ingaat. Het hoofdstuk vervolgt met een toepassing van de ketenbenadering in verschillende SBR verantwoordingsketens en slaat afsluitend een brug naar de opgave van verandermanagement in S2S-geïntegreerde verantwoordingsketens – een thema waar hoofdstuk 3 uitgebreider op ingaat.

Hoofdstuk 3 – Verandermanagement in informatieketens
Dit hoofdstuk is geschreven vanuit het perspectief van 'het verandermanagement'. Hierbij kan gedacht worden aan een persoon – de verandermanager – of aan een (permanent) ingerichte veranderorganisatie (programma of afdeling) waar meerdere personen onderdeel van uit maken. Met welke uitdagingen krijgt het verandermanagement bij de herinrichting van informatieketens te maken? Het hoofdstuk beschrijft de intrinsieke weerbarstigheid van informatieketens en gaat uitgebreid in op het strategische gedrag dat in ketens kan voorkomen. De SBR-casus wordt gebruikt om aan te geven hoe dit gedrag zich in de praktijk heeft voorgedaan, welke gevolgen dit heeft gehad en welke maatregelen zijn genomen om met dit gedrag om te gaan. Een van de kernvragen waar dit hoofdstuk op ingaat, is: 'wat zijn de bestaande verandermethoden die het verandermanagement kan toepassen bij de verandering van informatieketens?' Het hoofdstuk behandelt deze vraag langs vier perspectieven, te weten: (1) direct verandermanagement, (2) procesmanagement, (3) veranderen van ketencondities en (4) dilemmamanagement. Afhankelijk van de situatie kan het verandermanagement het voor hen meest aansprekende perspectief verder invullen, waarbij hybride vormen (sequentieel of voor onderdelen) mogelijk zijn. Met de SBR casus wordt de theorie wederom toegelicht aan de hand van de praktijk.

Hoofdstuk 4 – Het besturingsvraagstuk van keteninformatiesystemen
Dit hoofdstuk bevat een beschouwing over een problematisch onderdeel van de opgave: het bepalen van de meest geschikte vorm voor de besturing van wijzigingen in informatieketens. We noemen dit het besturingsvraagstuk van keteninformatiesystemen. Het is gebaseerd op de gedachte dat twee verandergrootheden – governance en technologie – van elkaar zijn te onderscheiden, maar elkaar sterk beïnvloeden. Sterker nog, gezien de continue behoefte aan acceptatie van onvermijdelijke wijzigingen in beide grootheden, is een daarop berekende sturingsvorm vereist. Populaire sturingsvormen zijn programma's, projecten en procedures. Een verkeerde berekening kan leiden tot weerstand, stagnatie, hogere kosten en zelfs falen. Het enthousiasme van de markt om een technologie aan de man te brengen draagt bij aan de verkeerde berekening. Hoe vaak zien we niet dat een technologie als 'plug & play' of 'met één druk op de knop' wordt geadverteerd, terwijl bij de implementatie blijkt dat de

technologie nog niet volwassen is? Maar ook de drang van bestuurders en beleidsmakers om met technologische innovaties op korte termijn beleidsdoelen te realiseren speelt uiteraard een rol. Er is veel literatuur die zich exclusief concentreert op sturingsvormen, technologie en governance. Hiertegenover staat dat er geen literatuur te vinden is die integraal iets zegt over op basis waarvan de staande ketengovernance (de overkoepelende autoriteit met bevoegdheden, voorzover die er al is) de meest geschikte sturingsvorm kan bepalen voor het succesvol doorvoeren van een ketenwijziging. Met andere woorden: wanneer moet wie een wijziging sturen en met welke sturingsvorm? Bewapend met de inzichten uit hoofdstukken 2 en 3 onderzoekt hoofdstuk 4 het besturingsvraagstuk. Hiervoor belichten we zogenaamde black box concepten als technologie en governance en de literatuur die iets zegt over de acceptatie van beide. De conclusie van de beschouwing in dit hoofdstuk zal zijn dat de effectieve wijziging van technologie en/of governance in ketens vereist dat de staande ketengovernance de type ketenwijziging goed bepaalt en de daarbij passende sturingsvorm weet te lanceren. Voor het adequaat bepalen worden enkele handvatten geboden.

1.6.2 *Deel B - SBR als oplossing*

Hoofdstuk 5 – I-Processen
Processen vormen de basis voor de realisatie van doelstellingen van de schakels in de keten. Procesgericht denken wordt alom gestimuleerd, maar wat is een goed proces? Hoe wordt het gemodelleerd? Wat zijn specifieke eisen aan SBR-processen? In dit hoofdstuk bieden de auteurs handvatten voor de gerichte toepassing van processen bij de herinrichting van informatieketens. Het hoofdstuk begint met de algemene karakteristieken van processen, waarna SBR als casus wordt gebruikt om duidelijk te maken hoe deze algemeenheden op een systematische wijze om te zetten zijn naar een specifieke en gestructureerde procesimplementatie en procesbeheer. Bijzondere aandacht gaat uit naar de gestandaardiseerde procesonderdelen van SBR. Het subject van deze processen is de XBRL-instance, waarvoor geldt dat deze generieke processen met name geautomatiseerd afgehandeld worden. Procesimplementatie heeft dus een duidelijke koppeling met de volgende onderdelen uit de verdieping: gegevens en techniek. Tot slot geldt dat er op het gebied van procesautomatisering nog een aantal vraagstukken open staat en er enkele ontwikkelingen lopen die het noemen waard zijn.

Hoofdstuk 6 – Gegevens
In het kader van SBR wordt XBRL als gegevensstandaard gehanteerd. XBRL is een standaard om bedrijfsgegevens op een uniforme wijze vast te leggen en te presenteren aan verschillende partijen. De standaard zorgt ervoor dat verschillende partijen zowel financiële als niet-financiële gegevens uit hun boekhoudsoftware direct kunnen gebruiken voor interne- en externe rapportages. Omdat de syntax (de manier waarop je iets opschrijft) gestandaardiseerd is, kan iedere ontvanger van gegevens via een eigen invulling van de semantiek (betekenis) aangeven welke ordening (definitie) van de gegevens voor hem of haar relevant is. Een belangrijke voorwaarde hiervoor is het gebruik van een gedeelde set van definities, oftewel een taxonomie. In het kader van SBR gebruiken de uitvragende partijen een gedeelde taxonomie: de Nederlandse Taxonomie (NT). Hiermee kan een bedrijf snel en gemakkelijk een rap-

portage uit haar eigen administratie genereren conform de definities en informatiebehoeften van de Belastingdienst of een andere uitvragende partij. De standaardisatie van syntax en semantiek vergemakkelijkt op deze manier het verzamelen, verwerken en uitwisselen van gegevens en levert zo een grote kostenbesparing op. Voor zowel degene die de informatie levert – geen verschillende onafhankelijk van elkaar in te vullen en verzenden rapportages meer – als voor degene die de informatie wenst en ontvangt. Het hoofdstuk beschrijft ook de andere concepten die in het kader van gegevensuitwisseling van belang zijn, zoals normalisatie, harmonisatie, gegevenskwaliteit, taxonomieontwerp en gegevensbeheer. Aan de hand van de SBR-casus worden deze concepten uitgewerkt, zodat de verbanden voor de lezer duidelijk worden. Tenslotte reflecteren de auteurs op relevante ontwikkelingen op dit gebied.

Hoofdstuk 7 – Technische inrichting SBR
Dit hoofdstuk zoomt in op de techniek achter de generieke procesinfrastructuur die bij SBR wordt gebruikt. De procesinfrastructuur is een generieke voorziening en dient zorg te dragen voor de geautomatiseerde afhandeling van elektronische berichtenverkeer op basis van standaarden voor gegevensmodellen, processtandaarden en technische standaarden. Conceptueel gezien staat de procesinfrastructuur tussen de aanleverende en de uitvragende partij. Vandaar ook de benaming Digipoort. Het hoofdstuk bestaat uit drie delen. Het eerste deel concentreert zich op de vraag 'welke technische inrichting past bij SBR?' Hiervoor zijn vier scenario's voor gestructureerde elektronische berichtenuitwisseling denkbaar, namelijk: (1) traditionele/heterogene procesinfrastructuur, (2) eigen procesinfrastructuur, (3) concern-procesinfrastructuur en (4) gedeelde dienstverlener. Het tweede deel concentreert zich met name op de relevante technische standaarden voor de uitwisseling van informatie. De auteurs beschrijven hier met name de ontwikkelingen rond koppelvlakken, webservices en SOA voor de ondersteuning van flexibele i-processen, aangezien deze het fundament vormen voor de gerealiseerde procesinfrastructuur. Het derde deel van dit hoofdstuk legt de architectuur van Digipoort – de gerealiseerde procesinfrastructuur – bloot en beschrijft hoe deze in de praktijk werkt. Bijzondere aandacht gaat uit naar de koppelvlakken, de processen en de webservices die hiervoor worden gebruikt. Vragen die behandeld worden in dit deel zijn: welke afspraken zijn er rond koppelvlakken gemaakt? Wat doet Digipoort? Hoe is de gewenste flexibiliteit in i-processen gerealiseerd? Welke i-processen worden georkestreerd? Welke services worden uiteindelijk aan de uitvragende partijen geboden? Wat zijn de implicaties voor de gebruikers? De auteurs sluiten dit hoofdstuk af met een reflectie op de uitdagingen die zijn overbrugd.

Hoofdstuk 8 – Beveiliging van informatieketens
Met de erkenning dat de overheid een bijzondere verantwoordelijkheid heeft bij het beveiligen van gegevens die zij vraagt van burgers en bedrijven heeft men in het kader van SBR veel aandacht besteed aan 'end-to-end' ketenbeveiliging. Het gaat hier immers om de geautomatiseerde afhandeling van grote hoeveelheden vertrouwelijke informatie. Aan de afhandeling gelden wettelijke eisen die ook bepalend zijn voor de maatregelen die er genomen kunnen worden. Dit hoofdstuk geeft antwoord op de vraag 'hoe is informatiebeveiliging in het kader van SBR geregeld?' Beantwoording van deze vraag geschiedt langs een driedeling. Het eerste deel beschrijft de relevante

wetgeving op dit gebied, gevolgd door meer generieke richtlijnen voor informatiebeveiliging. Deze kaders zijn relevant aangezien ze de fundamentele eisen aan en randvoorwaarden voor de informatiebeveiliging bevatten. Ondanks het generieke en voorschrijvende karakter van de kaders, zien we dat de end-to-end beveiliging van informatieketens om verregaande ketenwaarborgen vragen die niet door één partij geregeld kunnen worden. Deze verregaande ketenwaarborgen worden in het tweede deel van dit hoofdstuk beschreven. Het gaat hier vooral om behoeften rondom identificatie (dit ben ik), authenticatie (ben je inderdaad wie je claimt te zijn?) en autorisatie (mag je optreden namens een ander?) van partijen die deelnemen aan het elektronisch berichtenverkeer. Identificatie, authenticatie en autorisatie worden vaak als doel gezien, maar fungeren in dit kader als een ketenspecifieke set van middelen (technieken en procedures) die in de fundamentele beveiligingseisen (vertrouwelijkheid, integriteit en beschikbaarheid) dienen te voorzien. In het derde deel van het hoofdstuk vindt concretisering van de ketenwaarborgen plaats. Hoe vindt authenticatie in SBR plaats? En hoe vindt autorisatie bij SBR plaats? Middels beantwoording van deze vragen willen de auteurs de partijen die met SBR aan de slag willen inzicht bieden in het huidige stelsel van ketenwaarborgen. Hierbij wordt nadruk gelegd op het gebruik van 'public key infrastructure' certificaten en het gebruik van een centraal machtigingsregister.

Hoofdstuk 9 – Governance en beheer
We zien bij SBR drie vormen van integratie van keteninformatiesystemen: netwerkintegratie, horizontale integratie en verticale integratie. De verschillende vormen van integratie leiden tot verschillende afhankelijkheden, waardoor er een behoefte ontstaat aan een overkoepelend bestuur en een gedeelde uitvoering. Voor iedere vorm van integratie zijn andere uitgangspunten van de governance aan de orde. Dit hoofdstuk beschrijft de aspecten die voor de verschillende integratievormen relevant zijn. Tevens geeft het de uitgangspunten voor de ketengovernance binnen SBR weer. Het hoofdstuk beschrijft hoe de governance binnen SBR thans is ingericht en hoe zich dit verhoudt met de verschillende integratievormen. Doordat Logius als gedeelde dienstverlener zich kan specialiseren in de materie en doordat zij belangrijke onderdelen van de keten onder haar hoede heeft, is zij bij uitstek de partij die het complexe speelveld kan overzien. Het hoofdstuk gaat in op de beheerorganisatie van Logius om invulling te geven aan haar orkestratierol. Het beschrijft het driehoeksbeheermodel, met een centrale rol voor architectuur als spil tussen de verschillende integratievormen.

Hoofdstuk 10 – De SBR-verbredingsmethodiek
Met SBR kunnen publieke en private partijen onderdelen van hun verantwoordingsketen op efficiënte en effectieve wijze afhandelen. Om gebruik te kunnen maken van SBR dienen de ketenpartijen de SBR-technologie te implementeren en aan te sluiten bij de ketengovernance op de verschillende integratievormen van SBR. Het wijzigingstraject, van interesse in SBR tot een werkende SBR-keten in productie, vraagt om een methodische aanpak. Vanuit het SBR Programma is voor het traject een methodiek ontwikkeld, die in dit hoofdstuk besproken wordt. Het startpunt van een verantwoordingsketen die (mogelijk) gaat aansluiten bij SBR is altijd anders. Denk hierbij onder andere aan de technische, politiek-bestuurlijke, historische, wettelijke

en organisatorische kenmerken van de bestaande keten. Voor iedere verantwoordingsketen dient er een uniek traject doorlopen te worden. De methodiek laat dan ook ruimte voor deze ketenspecifieke aanpak doordat partijen zelfstandig de route kunnen bepalen die voor hun keten doorlopen wordt. De methodiek dicteert wel een viertal fasen, waarmee voor iedere fase go/no go beslissingsmomenten zijn geïdentificeerd en ketenpartijen de kwaliteit van de voortgang kunnen waarborgen langs checkpoints. Tevens reikt de SBR-verbredingsmethodiek een inhoudelijke leidraad aan waarlangs partijen de fasen doorlopen. Bovendien worden voor iedere fase do's en don'ts aangegeven. De SBR-verbredingsmethodiek biedt partijen die aan de slag gaan met verbreding daarmee waardevolle inzichten over onder andere de relatie tussen de veranderwens, de veranderopgave en de veranderstrategie, aandachtspunten bij de besluitvorming, de rol van acceptatie en de diensten die zij kunnen afnemen bij Logius om een verbredingstraject tot een succes te maken.

Hoofdstuk 11 – Slotbeschouwing
Dit hoofdstuk geeft een slotbeschouwing op de oplossing van SBR. Het gaat in op de kracht van het concept, maar bespreekt ook waar het initiatief kwetsbaar is. De auteurs beschouwen de mogelijkheden die nog voor de SBR-oplossing in het verschiet liggen en welke hindernissen zij nog op haar weg kan vinden.

1.6.3 *Bijlagen*

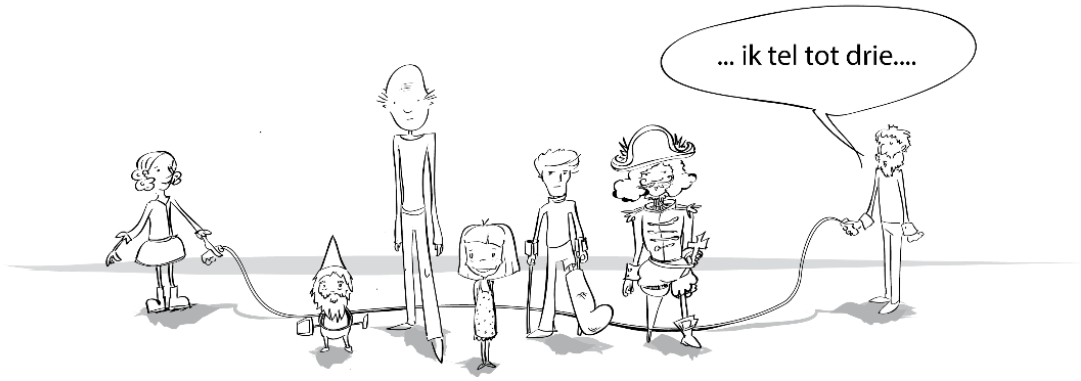
Bijlage A – Achtergrond SBR
Bijlage A bevat een uitgebreide analyse van SBR vanuit historisch perspectief. Deze beschrijving geeft de lezer het nodige begrip van de achtergrond van SBR om de rode draad in het boek te begrijpen. De beschrijving geeft hiervoor inzicht in de historie en de onderliggende beleidsdoelstellingen. Vooral voor de lezer die niet bekend is met SBR biedt deze bijlage relevant materiaal.

Bijlage B – Verantwoording
Bijlage B geeft een overzicht van de onderzoeksactiviteiten die zijn verricht voor de totstandkoming van dit boek.

Bijlage C – Begrippen en afkortingen
Bijlage C geeft een overzicht van de kernbegrippen en afkortingen die in de verschillende hoofdstukken zijn gebruikt.

Deel A – SBR als opgave

2 Ketens en ketencoördinatie



2.1 Kenmerken van ketens

Dit hoofdstuk gaat over ketens. Achtereenvolgens zullen we het concept 'ketens' introduceren en nagaan wat er bij ketensamenwerking komt kijken. Hierbij wordt met name de politieke kant van ketens belicht. Er wordt stilgestaan bij zachte factoren die wel heel richtinggevend zijn voor de organisatie en resultaten van ketens. Voorbeelden van dergelijke factoren zijn vertrouwen en macht. In de slotparagraaf geven we de betekenis van dit politieke perspectief op ketens voor ketencoördinatie.

Een keten is een aaneengeschakelde opeenvolging van handelingen of gebeurtenissen (Van Dale woordenboek). In veel gevallen worden ook opeenvolgende organisaties als ketens gezien. Ketens bestaan uit zogenaamde schakels en stroomelementen. Schakels zijn de opeenvolgende handelingen, gebeurtenissen of organisaties. Stroomelementen lopen door de keten heen. Iedere schakel moet toegevoegde waarde leveren aan of voor het stroomelement. Er zijn verschillende soorten ketens, allen met verschillende schakels en/of stroomelementen. Bekende vormen zijn:

- Productieketens, waarbij iedere schakel een opeenvolgend productieproces vormt. Stroomelementen zijn de producten-in-wording. Iedere schakel levert toegevoegde waarde door het product-in-wording verder te ontwikkelen.
- (Personen)vervoersketens, waarbij de stroomelementen personen zijn die als het ware hun eigen keten construeren. Schakels zijn in dit geval vervoersmiddelen. Iedere schakel levert toegevoegde waarde door de persoon verder naar zijn/haar bestemming te brengen.
- Informatieketens, waarbij informatie het stroomelement is. Schakels zijn organisaties die de informatie delen. Toegevoegde waarde wordt gecreëerd

door enerzijds de informatie dichterbij de plaats van bestemming te brengen. Anderzijds kan de informatie ook waarde hebben voor iedere schakel.
- Beleidsketens. Beleid-in-wording is daarbij het stroomelement en organisaties de schakels. Toegevoegde waarde is gelegen in het verder brengen van een beleidsidee tot en met de uitvoering. Als er een onderscheid wordt gemaakt tussen beleid en uitvoering, dan kan er ook worden gesproken van 'uitvoeringsketens' naast beleidsketens.

Ketens worden vaak in één adem genoemd met 'netwerken'. Ook een 'netwerk' is een metafoor voor een verzameling actoren en hun relaties, maar deze metafoor benadrukt meer dan 'ketens' de veelheid en wederzijdse afhankelijkheden van actoren (Bruijn & Heuvelhof, 2007), ofwel de gedachte dat 'alles met alles samenhangt'. De ketenmetafoor drukt eerder de volgtijdelijkheid van processen uit en de afhankelijkheden die daar uit voortvloeien. Een keten kan onderdeel uitmaken van een netwerk, maar vormt dan een specifieke, vooraf gedefinieerde set van verbindingen binnen dat netwerk.

Voor ieder type keten geldt dat verschillende actoren, vanuit verschillende rollen, betrokken zijn. Zij kunnen onderdeel uitmaken van de keten, maar zij kunnen ook de omgeving van een keten vertegenwoordigen. Een veelheid aan actoren maakt dat ketens onderling sterk kunnen verschillen. De volgende variabelen zijn van belang.

- Ketens kunnen sterk vraaggedreven of aanbodgedreven zijn. Een voorbeeld van een vraaggedreven keten is de voedselketen. De detailhandel (vraagzijde) ziet de consumenten namelijk in de ogen, terwijl ze voedsel aangeleverd krijgt van de ketenpartners. Zij wordt verantwoordelijk gehouden voor de geleverde producten. Op instigatie van de detailhandel worden daarom kwaliteitssystemen ontwikkeld, om de kwaliteit van aanleverende partijen te kunnen beheersen. Aanbodgedreven ketens zijn eerder te vinden in high-tech markten, waarbij consumenten zich minder bewust zijn van de normen die ze aan het product of de dienst kunnen stellen.
- De machtsbalans tussen aanbod en vraag in een keten is belangrijk. Sommige schakels worden bezet door een beperkt aantal actoren, die gemakkelijk onderling afspraken kunnen maken, zodat zij een vuist kunnen maken naar andere schakels.[5] In de e-commerce is de aanwezigheid van een machtige partij gezien als een factor welke bijdraagt aan het succes van een keten (Monczka, Petersen, Handfield, & Ragatz, 1998). Bijna iedere keten heeft wel een dergelijke schakel. Een variabele is dan aan welke kant van de keten deze zich bevindt. Aan de vraagzijde of aan de aanbodzijde? Dit bepaalt voor een goed deel de machtsbalans in de keten. In de voedselketen is Albert Heijn bijvoorbeeld een zeer machtige schakel. Deze bevindt zich aan de vraagzijde.
- Het absorptievermogen van organisaties kan per keten en per schakel in de keten verschillend zijn. Dit is het vermogen om nieuwe kennis van buiten de

[5] *Power* can be defined as the potential of an actor to influence the behavior of another actor on a particular issue (Tushman, 1977).

organisatie op te nemen, wat dus sterk bepalend is voor de toegevoegde waarde die een schakel kan leveren aan de volgende schakel. Absorptievermogen van organisaties is afhankelijk van de werknemers en afhankelijk van het verleden (Cohen & Levinthal, 1990). Kennis, expertise en beschikbare capaciteit verschillen.

- Ketens kunnen al of niet (horizontaal of verticaal) integreren of juist desintegreren. Integratie houdt in dat sommige partijen meerdere schakels beheersen. Bij desintegratie worden schakels door partijen afgestoten. Een bekend voorbeeld is de vroegere energieketen, waarbij productie, netwerkbeheer en levering door dezelfde partijen geschiedden, maar waar later de schakels over verschillende leveranciers zijn verdeeld. De legpluimveeketen is nauwelijks geïntegreerd: er zijn broederijen, fokkerijen, legpluimveehouders, verzamelaars, verhandelaars en retailbedrijven. Iedere schakel wordt bezet door verschillende partijen. De melkveeketen is meer geïntegreerd: er zijn fokkerijen, veeboeren, coöperaties en retailbedrijven. Voor een vergelijkbaar proces zijn er minder schakels. Een enkele schakel, in dit geval de coöperatie, neemt meerdere processen voor haar rekening.
- Binnen ketens kan sprake zijn van horizontale en verticale collaboratie. In dat geval werken schakels intensief samen om daarmee een gezamenlijk doel te halen. Er is bijvoorbeeld sprake van verticale collaboratie wanneer de transporteur en supermarkt verantwoordelijkheden en informatie delen in het kader van voorraadbeheer. Bij horizontale collaboratie delen vergelijkbare of zelfs concurrerende partijen hun middelen. Twee supermarktketens gebruiken bijvoorbeeld een gedeeld distributiecentrum (Simatupang & Sridharan, 2002).
- Ketens kunnen met elkaar verstrengeld raken. Een voorbeeld is diervoeding. Er is een diervoedingsketen die interfereert met de vleesketen. De dieren die het vlees leveren eten immers het voedsel van de andere keten. Zo ontstaan selecterende en allocerende schakels (zie § 2.3).
- De incentivestructuur van de keten is van belang. Dit gaat over de vraag wie profiteert van de investeringen die in de keten plaatshebben. Is de investeerder dezelfde als de begunstigde? Indien niet, dan kan dit gevolgen hebben voor het delen van informatie. (Meijer, 2009; Teece, 1998). Vaak moeten opbrengsten niet alleen over partijen verdeeld worden, maar ook over de tijd. Investeringen worden gedaan in het begin, door een andere partij dan de partij die er later van profiteert.
- En er zijn de zogenaamde 'zachte variabelen'. Hoe komt het dat de ene keten gebroederlijk samenwerkt en de andere een politieke arena is? Dit hangt mede samen met de sociale structuur van de keten (Meijer, 2009; Uzzi, 1997). Factoren hierbij zijn bijvoorbeeld de cultuur van de sector waarin de keten zicht bevindt, de fysieke nabijheid van ketenpartners en de rijkdom/armoede van de keten (Duivenboden, Veldhuizen, & Twist, 2000).

Dergelijke ketenvariabelen zijn nuttig om te gebruiken in een ketenanalyse. Naast deze keten-gerelateerde variabelen, zijn er ook basiskenmerken welke helpen om een case te begrijpen. Denk aan kenmerken als de eigenschappen van de sector, het soort

informatiesystemen dat gebruikt wordt, de huidige status, en – voor verantwoordingsketens - het soort overheidstaak dat wordt ondersteund (belastingaangifte; inspectie; aangifte goederen).

Deze criteria maken ketens ook meer of minder geschikt om te automatiseren of anderszins te veranderen. Een keten die bestaat uit actoren met een laag absorptievermogen zal bijvoorbeeld minder snel geneigd zijn om veranderingen te accepteren.

2.2 SBR en informatieketens

Ieder type keten kent haar eigen problematiek. SBR heeft betrekking op verantwoordingsketens. Verantwoordingsketens zijn informatieketens. Informatie over de bedrijfsvoering van publieke en private organisaties (verantwoordingsinformatie) is het stroomelement.

Informatieketens zijn bijzonder, omdat:

- Informatie een bijzonder vluchtig en snel stroomelement is
- Informatie in vele vormen en gedaanten voorkomt
- Informatie sterk aan interpretatie onderhevig is en daarmee subjectiever is dan bijvoorbeeld goederen
- Informatie vaak 'ongrijpbaar' is
- Informatie niet opraakt en het derhalve altijd mogelijk is om het te kopiëren.

In de verantwoordingsketen zijn minimaal twee partijen betrokken, te weten de belanghebbende en de uitvragende partij:

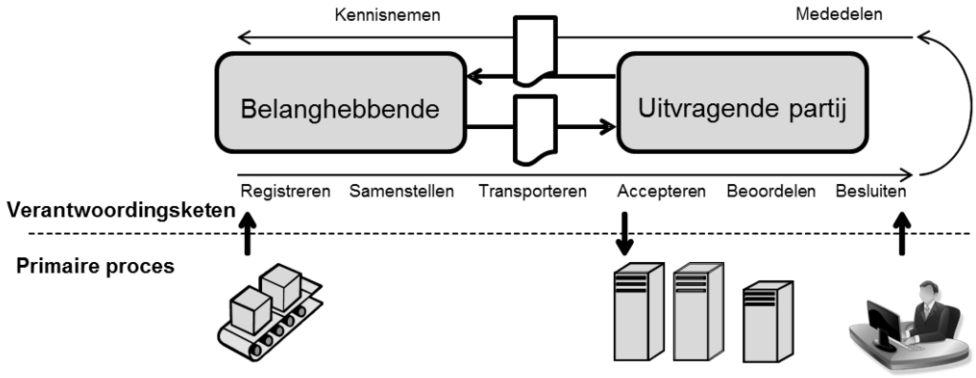
- Belanghebbenden of de informatieleverende partijen. Deze partij dient de gevraagde informatie over de bedrijfsvoering beschikbaar te stellen.
- Uitvragende partijen. Dit is de stakeholder aan wie een belanghebbende informatie levert en dus de partij die de eisen stelt aan de informatie en de leverantie (welke informatie wordt wanneer, hoe vaak, met welke betrouwbaarheid verwacht?). Wanneer de uitvrager een publieke partij is, hebben deze eisen hun basis in wet- en regelgeving. Andersom geldt dat de bevoegdheden van een publieke uitvrager wettelijk begrensd zijn. De Belastingdienst dient bijvoorbeeld te specificeren welke gegevens ze van bedrijven opvraagt.

In de verantwoordingsketen zien we op hoofdlijnen de volgende handelingen terugkomen:

- Registreren: de belanghebbende registreert gegevens over de bedrijfsvoering.
- Samenstellen: op basis van de geregistreerde gegevens stelt de belanghebbende een verantwoordingsrapportage op.
- Transporteren: de belanghebbende verzendt de informatie naar de uitvragende partij.
- Accepteren: de uitvragende partij stelt vast of de verantwoordingsinformatie aan de verwerkingseisen voldoet.
- Beoordelen: de uitvragende partij velt op basis van de informatie een inhoudelijk oordeel.

- Besluiten: het oordeel leidt tot een formeel besluit van de uitvragende partij. Dit is niet bij alle uitvragende partijen het geval. De Belastingdienst maakt een beschikking op (een besluit). De Kamer van Koophandel (KvK) en het Centraal Bureau voor de Statistiek (CBS) kunnen zich beperken tot het mededelen van de ontvangst van een rapportage.
- Mededelen: de uitvragende partij deelt het besluit mede aan de belanghebbende. In de omzetbelastingketen deelt de Belastingdienst overigens niets mee als aangifte en betaling met elkaar in overeenstemming zijn (en beiden tijdig waren).
- Kennisnemen: de belanghebbende neemt kennis van het besluit.

De handelingen zijn in onderstaande figuur schematisch weergegeven.



Figuur 2.1 – Handelingen in de verantwoordingsketen

In de getoonde opzet valt op dat voor de uitvragende partij geldt dat het beoordelings- en het besluitvormingsproces onderdeel uitmaken van het primaire proces. Een bedrijf verantwoordt zich bijvoorbeeld over zijn reële handel in televisies, maar zijn verantwoordingsrapportage vormt een 'grondstof' voor de Belastingdienst, die op de verantwoording een aanslag baseert. Deze situatie doet zich vaker voor bij uitvoeringsorganisaties met een publieke taak, zoals bijvoorbeeld het UWV of Agentschap.nl. Verder moet opgemerkt worden dat het kan voorkomen dat op basis van het meegedeelde besluit van de uitvragende partij de belanghebbende weer actie moet ondernemen: op een belastingaanslag volgt (over het algemeen) een betaling. De verantwoordingsketen maakt dan ook doorgaans onderdeel uit van een langere informatieketen. Tot slot toont het figuur alleen de zogenaamde 'happy flow'. De schakels in de verantwoordingsketen kennen in praktijk meerdere uitkomsten. Zo kan een belastingaangifte onvolledig en dus niet verwerkbaar blijken. Betrokken partijen grijpen in zo'n geval (al dan niet op vooraf vastgestelde wijze) in en proberen alsnog de gewenste uitkomst te bereiken. In de praktijk zie je dat veel van de werkzaamheden in een keten gericht zijn op deze zogenaamde 'error handling'.

De betrokken partijen streven een kosteneffectief verantwoordingsproces na. Zij zullen taken, daar waar dit efficiënt en effectief is, willen automatiseren. In de Inleiding hebben we gezien welke voordelen automatisering, meer specifiek S2S-integratie,

biedt. Ook het uitbesteden (outsourcen) van taken aan derden is een optie om de kosteneffectiviteit in de keten te verhogen. Hierdoor, en door de eigenschap van het verantwoordingsdomein dat er doorgaans meerdere dienstverleners bij betrokken zijn (accountants, softwareleveranciers, beide, zoals we hebben aangestipt in de Inleiding, in verschillende verschijningsvormen), zijn er niet zelden meer dan twee partijen bij de verantwoording betrokken. Hoe verantwoordingsketens er in de praktijk uit komen te zien wordt bepaald door een veelheid van variabelen en is – mede onder invloed van SBR – sterk in ontwikkeling. Na een verdere uiteenzetting van de ketentheorie zal hier in § 2.4 nader op ingegaan worden.

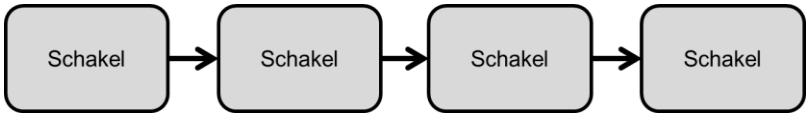
2.3 De politieke dimensie van ketens

Voorgaande laat de variëteit tussen ketens zien en geeft een illustratie van deze variëteit voor SBR. Het nu volgende zoomt in op gedrag in ketens. Hier komt de politieke dimensie van ketens om de hoek kijken. Wat bepaalt gedrag in ketens? Dit is van groot belang als we later gaan kijken naar ketencoördinatie (§ 2.5) en verandermanagement (hoofdstuk 3).

2.3.1 *Afhankelijkheden*

Hoe is de macht verdeeld in een keten? Dat is de centrale vraag vanuit een politiek perspectief. Macht is het vermogen om beslissingen van anderen af te dwingen. Ketens bestaan uit verschillende organisaties. Het idee van een keten, namelijk een sequentiële afhankelijkheid tussen organisaties, is bepalend voor de ruil- en onderhandelingsrelaties tussen organisaties. Relaties staan in het teken van de ongelijke toegang, de verdeling en het gebruik van schaarse hulpbronnen zoals informatie (Bekkers, 2000). Samenwerking tussen partijen is daarom niet vanzelfsprekend, maar wel noodzakelijk.

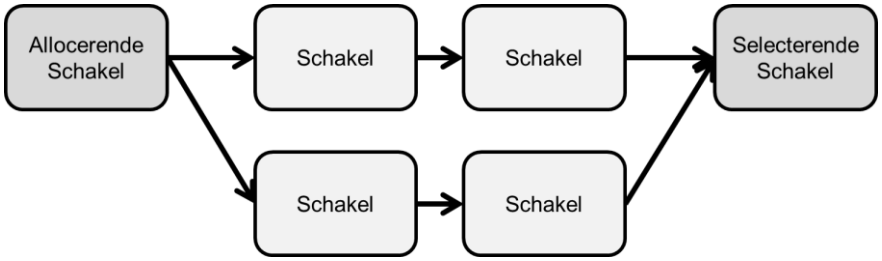
Ketens geven de functionele sequentie van activiteiten weer. Daarmee zeggen ze ook iets over de afhankelijkheden tussen organisaties.



Figuur 2.2 – Schakels in een keten

In een dergelijk eenvoudige weergave is te zien dat voor het functioneren in een keten iedere schakel afhankelijk kan zijn van de voorgaande en van de volgende schakel. In deze weergave levert elke schakel een goed of dienst dat/die benodigd is om toegevoegde waarde te creëren in de keten.

Er zijn natuurlijk ook ingewikkelder ketens. Ingewikkelder ketenstructuren geven vaak indicaties van meer afhankelijkheden. Eerder is al gesproken over selecterende of allocerende schakels. Het bestaan van dergelijke schakels verandert de afhankelijkheden in een keten.



Figuur 2.3 – Positie van de allocerende en selecterende schakel

De structuur van de keten kan voor een belangrijk deel de machtspositie van actoren bepalen. De Bruijn en Ten Heuvelhof (1995) noemen twee voorbeelden:

- Selecterende schakels kunnen kiezen uit verschillende producten of diensten die het resultaat zijn van de activiteiten in de voorafgaande schakels. Hiermee worden de processen in de daarop volgende schakels in belangrijke mate geconditioneerd. Bovendien worden selecterende schakels een aantrekkelijke partner voor voorafgaande schakels, omdat hun producten of diensten al of niet worden geselecteerd. Daarmee hebben selecterende schakels een sterke positie.
- Allocerende schakels kunnen invloed uitoefenen op hoe een keten divergeert. Ook dit conditioneert het verloop van de processen in de opvolgende schakels. Allocerende schakels zijn bovendien minder afhankelijk van een enkele volgende schakel, omdat ze alternatieven hebben.

De ketenstructuur geeft aldus een goede indicatie van de machtsbalans en afhankelijkheden binnen een keten. Er is echter meer. Ook andere factoren bepalen de afhankelijkheden in ketens. Van Dalen (2000) geeft een korte opsomming:

- Omvang van een schakel (personeel, spreiding over het land, omzet of vermogen)
- Speciale competenties (technologie, speciale niche producten of netwerkkennis, netwerkrelaties)
- Wet- en regelgeving (overheidspartijen, handhavers, speciale bevoegdheden)

Daarnaast bestaan schakels in sommige ketens uit meerdere actoren. Denk hierbij aan een productieketen, waarbij verschillende marktpartijen halffabricaten maken en weer andere marktpartijen eindfabricaten. In een dergelijk geval zijn er weer andere factoren van belang voor de machtsbalans:

- Het aantal actoren dat een schakel bezet: hoe kleiner het aantal, des te machtiger de betreffende actoren (‘voor u weinig anderen’).
- Het aantal schakels dat wordt bediend door een enkele actor.

Machtige actoren kunnen voor het functioneren van een keten sterk bepalend zijn. Ze kunnen bijvoorbeeld in hoge mate de sociale structuur bepalen. Ook kunnen ze standaarden opleggen aan anderen in ketens. Bovendien kunnen zij de incentivestructuur bepalen. Dit betekent dat zij invloed kunnen hebben op de verdeling van

de kosten en baten in de keten. Hoe machtiger een actor is, des te groter de kans dat de incentivestructuur voor deze actor gunstig is.

2.3.2 *Vertrouwen*

Ketens benadrukken samenwerkingsverbanden tussen organisaties. Iedere organisatie levert verschillende producten, diensten en informatie. Als gevolg hiervan is iedere organisatie deelnemer aan vele ketens. Soms is deelname onvermijdelijk of zelfs verplicht. Vaak is er enigszins keuze aan welke keten men kan deelnemen. En er is altijd de keuze om zich al of niet volledig voor een keten in te zetten. Daarom is de incentivestructuur in een keten van groot belang voor organisaties. Een logische vraag is '*what's in it for me?'* In een complexe keten is deze vraag niet altijd eenvoudig te beantwoorden. Het kan in verschillende aspecten zitten, zoals directe besparingen, het betreden van een nieuwe markt, het aanknopen van relaties, het verbeteren van het imago, etc. Dergelijke aspecten worden afgewogen tegen de inkomsten die er waren geweest als de organisatie niet aan de keten had deelgenomen.

Er zijn verschillende soorten kosten verbonden aan deelname aan ketens:

- Geld (contributies)
- Transactiekosten (tijd gespendeerd aan afstemming tussen schakels)
- Opgave van autonomie

Om een keten met meerdere schakels en stromen goed te laten functioneren is een vorm van standaardisatie nodig. Consequentie van standaardisatie is de opgave van autonomie.

De machtsbalans is van groot belang voor ketendeelname. Het is immers de vraag ten behoeve van wie een organisatie bovengenoemde kosten zou willen 'betalen'. Voor wie wordt autonomie opgegeven? Ten dienste van wie worden de (transactie)kosten betaald? Indien het antwoord op deze vragen telkens wijst op een andere (machtige) organisatie, dan is ketendeelname niet waarschijnlijk. Met andere woorden: er is vertrouwen nodig dat de opgave van autonomie leidt tot een gunstige en eerlijke verhouding van kosten en baten. Dat vertrouwen is een voorwaarde om (volledig) aan ketens deel te nemen. Zonder het vertrouwen van de verschillende schakels in een gezamenlijk positief en redelijk verdeeld resultaat zullen ketens niet kunnen overleven. Op basis van Van Dalen (2000) maken we een onderscheid tussen twee vormen van vertrouwen.

- Georganiseerd vertrouwen. Dit is de meeste zichtbare vorm van vertrouwen. Het is vastgelegd in prijsafspraken, contracten, formele regels en procedures en certificering. De hardheid en het formele karakter van de afspraken vormen de basis van het vertrouwen dat de ketensamenwerking goed zal verlopen. Organisatorisch vertrouwen faciliteert het toetreden tot ketens. Het geeft garanties zonder dat partijen al ervaring met elkaar hebben gehad.
- Emergent vertrouwen. Dit type vertrouwen ontstaat gedurende samenwerking. Feitelijke ervaringen met het gedrag van ketenpartners kan het onderlinge vertrouwen versterken. Worden afspraken nagekomen? Heeft de partner vergelijkbare ideeën over het nakomen van plichten en het benutten van rechten?

Deze vormen sluiten elkaar overigens niet uit. Door formele maatregelen is er bijvoorbeeld voldoende zekerheid om een afhankelijkheid aan te gaan. Doordat er geleverd wordt, ontstaat vervolgens meer 'emergent' vertrouwen. De ene vorm van vertrouwen kan zo de andere faciliteren (Das & Teng, 1998).

Zowel macht als vertrouwen zijn veranderlijk. Emergent vertrouwen kan sterk afnemen als een partner zich niet loyaal aan de keten gedraagt. Gedragsveranderingen kunnen om verschillende redenen ontstaan:

- Personeelswisselingen
- Voortschrijdend inzicht en ervaringen
- Trade-offs met deelname aan andere ketens
- Ketenintegratie

Veranderlijkheid betreft dus zowel de deelnemende partijen als de inhoudelijke aspecten van ketens. Dit betekent dat er af en toe nieuwe problemen of kansen kunnen ontstaan en dat nieuwe actoren zich presenteren die zich bij het probleem of de oplossing betrokken voelen (Grijpink, 2000). Door middel van wijzigingen kunnen problemen of kansen worden geadresseerd, hierover meer in hoofdstuk 4 (Het besturingsvraagstuk van keteninformatiesystemen).

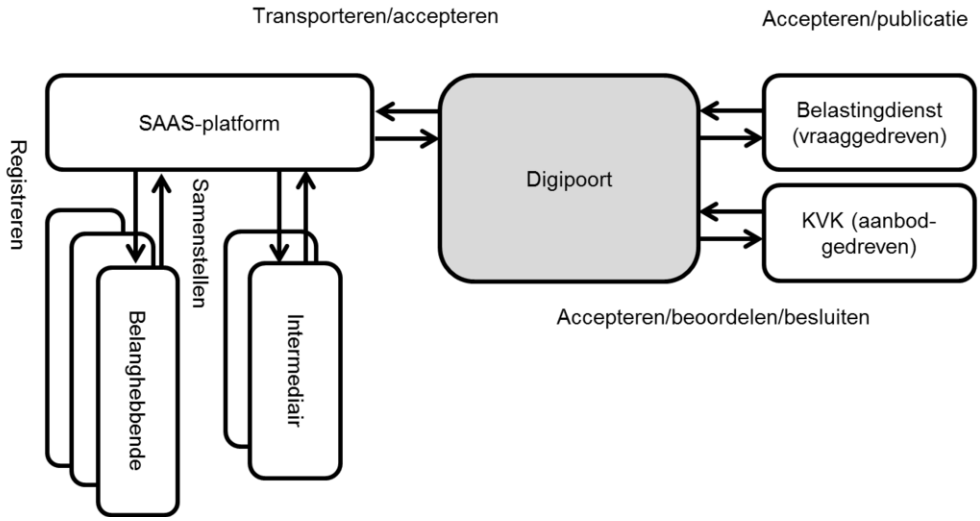
2.4 Informatieketens in de praktijk

Eerder zagen wij een eenvoudige weergave van een verantwoordingsketen. In de praktijk proberen de partijen binnen een verantwoordingsketen deze keten zo kosteneffectief als mogelijk in te richten. In de Inleiding is uitgelegd waarom in een informatieketen automatisering voor de hand ligt. Hierdoor ontstaat er binnen de keten een afhankelijkheid van de softwareleverancier. Bij de SBR verantwoordingsketens wordt het vervaardigen van verantwoordingen daarnaast vaak uitgevoerd door specialisten op een bepaald domein (belastingconsulent, accountant) en is dus sprake van uitbesteding aan de kant van de verantwoordende organisatie. Voor ongeveer 30.000 ondernemingen in Nederland geldt dat zij met betrekking tot de jaarrekening wettelijk verplicht zijn een accountantsverklaring (een controle verklaring) te deponeren. Hier wordt het beoordelen van de verantwoordingsinformatie verplicht door een onafhankelijke deskundige gedaan.

Kijken we naar de fiscale verantwoordingspraktijk dan zien we veel verschijningsvormen van de verantwoordingsketen. We hebben deze pluriformiteit in de verantwoordingsketens besproken in de Inleiding. Bij de meest eenvoudige keten logt een belanghebbende in op het portaal van de Belastingdienst en voert daar de OB aangifte in (handmatig). Dit is de praktijk voor de meeste ZZP-ers. Een groot deel van de ondernemingen levert vanuit een administratiepakket system-to-system (S2S) direct informatie aan bij de Belastingdienst. Veel organisaties roepen voor de opgaven en aangiftes hulp in van de belastingconsulent (intermediair). Waarbij dit voor de aangifte VpB/IB meer gemeengoed is dan voor de aangiftes OB, omdat het bij deze laatste vaak om relatief eenvoudige aangiftes gaat.

Onderstaand is een voorbeeld van een 'complexe' verantwoordingsketen weergegeven die in het SBR-domein voorkomt. Verschillende intermediairs maken in dit

voorbeeld gebruik van een gedeeld SaaS-platform (met boekhoud- en rapportagefunctionaliteit). Hun klanten dienen hier op aan te sluiten. De intermediair gebruikt het platform om met de registratie (de handelingen t.a.v. de administratie, de boekhouding) door de klant mee te kijken en deze te ondersteunen om tot goede verantwoordingsinformatie te komen. Vanuit het SaaS-platform wordt opgestelde verantwoordingsinformatie getransporteerd naar de Kamers van Koophandel of de Belastingdienst, via een tussenschakel van de overheid, Digipoort. In figuur 2.4 is alleen het aanleverproces opgenomen.



Figuur 2.4 – Voorbeeld van een aanbod- en vraaggedreven keten

In de bovenstaande keten zien we interessante aspecten uit de ketentheorie terugkomen, waaronder:

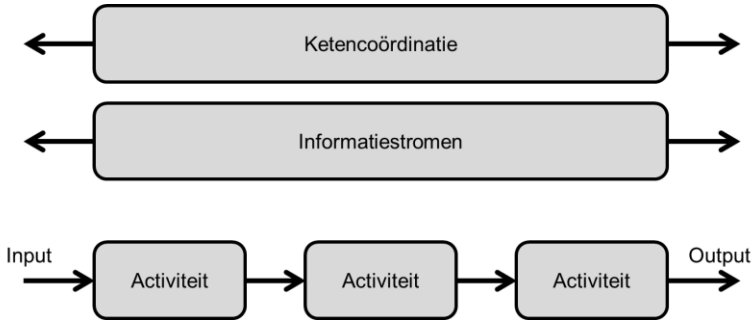
- Vraag gedreven: Het is overduidelijk de Belastingdienst die de eisen stelt aan de fiscale verantwoordingsinformatie. Op verschillende manieren beïnvloedt zij voorgaande schakels om de kwaliteit van informatie te garanderen.
- Aanbod gedreven: De belanghebbende (aanbodkant) is verantwoordelijk voor de inhoud en kwaliteit van de verantwoording, op basis van de verschillende eisen aan de jaarrekening die in de wet zijn vastgelegd. Ook de intermediair kan hier een deel van de verantwoordelijkheid op zich nemen. Er ligt voor de kwaliteitsborging van dit type verantwoordingsinformatie echter ook een belangrijke verantwoordelijkheid bij de Raad voor de Jaarverslaggeving (RJ). De Stichting voor de Jaarverslaggeving heeft als doel de kwaliteit van de externe verslaggeving van niet-beursgenoteerde organisaties en bedrijven in Nederland te bevorderen. Het uitvoerend orgaan van de Stichting is de RJ. De RJ is statutair belast met het autonoom opstellen en publiceren van stellige uitspraken en aanbevelingen (de Richtlijnen), alsmede het geven van adviezen. De RJ bestaat uit vertegenwoordigers van (1) de verschaffers, (2) de gebruikers en (3) de controleurs van financiële verslaggeving. (www.rjnet.nl).

- Verticale desintegratie: Waar Belastingdienst en intermediair in het verleden zelf de geautomatiseerde verwerking voor hun rekening namen, zijn nu respectievelijk de leverancier van Digipoort en de SaaS-leverancier hier gedeeltelijk operationeel voor verantwoordelijk.
- Horizontale collaboratie: Intermediairs en uitvragende partijen maken elk gebruik van gedeelde leveranciers voor geautomatiseerde gegevensverwerking.
- Verticale collaboratie: Intermediairs en de SaaS-leverancier werken intensief samen om het registratie- en samenstelproces te optimaliseren.
- Verstrengeling: de jaarrekeningketen en de fiscale keten raken enigszins verstrengeld. Het meest concrete voorbeeld is de Wet Samenval uit 2008 die kleine rechtspersonen de mogelijkheid biedt om de jaarrekening op te stellen op basis van de fiscale grondslagen die ook van toepassing zijn bij de aangifte voor de vennootschapsbelasting.
- Incentivestructuur: Standaardisatie in de verantwoordingsketens biedt mogelijkheden die in het verleden niet kostenefficiënt waren. De SaaS-leverancier biedt met zijn oplossing ondernemers (belanghebbenden) de mogelijkheid gemakkelijker zelf te registreren, een deel van de samenstelling gebeurt voortaan geautomatiseerd en tevens neemt de techniek de intermediair werk uit handen. Tot slot maakt standaardisatie het voor ketenpartijen gemakkelijker om te wisselen van ketenpartners. Het lijkt een mooie business case. De domeinverstrengeling kan leiden tot meer concurrentie tussen softwareleveranciers uit verschillende domeinen en nieuwe leveranciers zullen hun intrede doen. Bovendien raakt de intermediair in de nieuwe keten een deel van de (registratie/samenstel) werkzaamheden kwijt. Voor de intermediairs en automatiseerders betekent dit wel dat zij moeten investeren om de innovatie te realiseren, en daarmee bovendien in een competitiever speelveld terecht komen.
- Zachte variabelen: Registeraccountants (RA) en Accountants Administratieconsulenten (AA) zijn bij wet geregelde beroepen. Dit geldt niet voor de belastingconsulenten. Dit alles bepaalt de mate waarin partijen georganiseerd zijn, de machtspositie die zij hebben verworven en het vertrouwen of wantrouwen dat men in de loop der tijd heeft kunnen opdoen. Denk hierbij bijvoorbeeld aan de boekhoudschandalen aan het begin van het millennium die een herijking van het accountantsstelsel teweeg hebben gebracht. Momenteel zijn de machtsverhoudingen en vertrouwensrelaties aan het verschuiven, waardoor er nieuwe ketens ontstaan.

Macht en vertrouwen zijn essentiële verklaringen voor gedrag in ketens. Ze zijn echter ook moeilijk grijpbaar. Dit bemoeilijkt de analyse, maar ook de ketencoördinatie. Daarover gaat de volgende paragraaf.

2.5 Ketencoördinatie

Ketencoördinatie gaat over het bewaken van de aansluiting van de activiteiten op elkaar. Onderstaand schema van De Wit c.s. (2000) geeft weer dat ketencoördinatie op een meer beleidsmatig (of bestuurlijk) niveau loopt. Het gaat *over* activiteiten en informatiestromen, maar maakt er geen deel van uit.



Figuur 2.5 – Relatie tussen ketencoördinatie, informatiestromen en activiteiten

Voorgaande maakt al duidelijk dat ketencoördinatie niet waardeneutraal is. Voor zover er een optimaal ketenresultaat valt te bereiken door optimale coördinatie, is het sterk de vraag of dit ook daadwerkelijk bereikt wordt. Een optimaal ketenresultaat, bijvoorbeeld vanuit de optiek van de eindgebruiker, hoeft immers geen optimaal resultaat te zijn voor andere actoren. Dit betekent dat de vraag 'wie coördineert' van belang is. Machtige actoren kunnen ketencoördinatie en daarmee het ketenresultaat sterk beïnvloeden.

Het zij opgemerkt dat ketencoördinatie zelden een activiteit is van een enkele persoon, maar een groepsproces waarbij een ketencoördinator een belangrijke, doch faciliterende rol heeft. Het centrale coördinatieprobleem bij ketens is dat het ketenproduct slechts wordt gerealiseerd als alle partijen goed samenwerken (Grijpink, 2000). Die partijen moeten de activiteiten immers goed uitvoeren. Grijpink geeft aan dat goede samenwerking nog wel eens stukloopt op de complexiteit van ketens. Doelstellingen van partijen zijn vaak diffuus en tegenstrijdig, mede vanwege verschillen van mening over ketendoelstellingen. Er is vervolgens niet altijd een overkoepelend gezag dat beslissingen kan doordrukken.

De mate waarin ketencoördinatie nodig is, verschilt per keten. In sommige gevallen vindt er een natuurlijke samenwerking plaats, in andere gevallen is samenwerking meer afgedwongen. De Wit c.s. (2000) onderscheiden vier gradaties van ketencoördinatie, afhankelijk van de mate waarin een keten wordt aanvaard:

- Zelforganisatie
- Actieve coördinatie in estafettevorm: dus coördinatie over twee schakels
- Geformaliseerde coördinatie: overkoepelend, schriftelijk zichtbaar
- Strategische coördinatie: betrokken partijen krijgen de bevoegdheid en verantwoordelijkheid om de strategische koers van de gehele keten uit te zetten en te bewaken.

Deze opsomming suggereert al dat er verschillende instrumenten bestaan voor ketencoördinatie. Van Dalen (2000) noemt er zes:

- (Prijs)afspraken
- Contracten en overeenkomsten
- Autoriteit
- Formele regels en procedures (zoals ook standaardisatie)

- Integratie- en verbindingsrollen (makelaars, serviceproviders, coördinatie-organen)
- ICT-toepassingen

Dit zijn de tools voor ketencoördinatie. Het kernprobleem (vanuit een politiek perspectief) gaat echter niet over de tools, maar over de bereidheid van organisaties om samen te werken. Naarmate ketens complexer worden is er steeds minder vaak een bovengeschikte die eenvoudig regels kan opleggen. We hebben over machtsverschillen gesproken en tegelijkertijd betwijfeld of er van effectieve ketensamenwerking sprake kan zijn als kosten en baten te oneerlijk verdeeld worden. Daarvoor is vertrouwen te belangrijk.

Als de natuurlijke ketenleider ontbreekt, dient de coördinatie – de ketenregie – op een andere wijze tot stand te komen. Een metafoor uit het theater suggereert dat er een regisseur is die met aanwijzingen ketenpartners motiveert om zich op een collectief gewenste manier te gedragen. Grote vraag is vervolgens hoe binnen een complexe keten de regiefunctie moet worden ingericht. Hiervoor dient rekening gehouden te worden met de volgende aspecten:

- Onafhankelijkheid: Als er weinig vertrouwen is tussen ketenpartners, dan is voldoende onafhankelijkheid van de ketenregisseur gewenst, zodat deze niet de schijn heeft om enkele partijen te bevoordelen.
- Deskundigheid: Deskundigheid bij informatisering is schaars, hetgeen een groot potentieel probleem is. Omdat ook in informatieketens macht van groot belang is, moet de regisseur zowel bestuurlijke als inhoudelijke kwaliteiten hebben!
- Niveau: De regiefunctie moet verankerd zijn in alle lagen. Regie op een te laag niveau brengt gezagsproblemen met zich mee. Wanneer regie op een te hoog niveau is verankerd, dan kan er een technisch deskundigheidsprobleem ontstaan. Beide problemen zijn ondermijnend voor de acceptatie van sturing door de regisseur. Een regisseur kan investeren in contacten met onafhankelijke technische deskundigen door wie deze zich laat voeden. In het geval er veel ongelijkheid binnen een keten is (zoals bij een publiek-private keten) is een overkoepelende raad denkbaar.
- Incentives: 'Regie' kan een garantie zijn voor stroperige processen. Zeker als een keten complex is en de prikkels om mee te doen niet eenduidig zijn.[6] In zo'n geval is het raadzaam om een organisatie regievoerder te maken die belang heeft bij voortgang en realisatie van het ketenresultaat. Met andere woorden: 'Regie moet worden gevoerd door hen die zelf de pudding moeten eten'. Probleem is wel dat zij het niet zullen laten de keten en het ketenresultaat naar hun hand te zetten. Dit hoeft geen groot probleem te zijn voor de keten, als de regisseur de partners mee weet te krijgen. Dit kan wel een probleem zijn als concepten van de samenwerking hergebruikt moeten worden. Immers, in een andere keten zullen de specificaties die door de regisseur zijn gemaakt wellicht minder passen.

[6] Juist in deze omstandigheden is regie nodig, maar ook complex.

2.6 Ketencoördinatie en SBR

Middels het SBR Programma wil de overheid verantwoordingsketens meer vanuit het perspectief van de ondernemer inrichten. Hierdoor ontstaan er nieuwe afhankelijkheden tussen ketens die onderling nogal verschillen. De fiscale verantwoordingsketen is minder complex en kent helderdere afstemmingslijnen dan de jaarrekeningketen.

De Belastingdienst is de feitelijke machthebber binnen de fiscale informatieketen. Iedereen erkent het belang van het eindproduct. Zij heeft dan ook ruime bevoegdheden om de keten haar wil op te leggen. De Belastingdienst is volledig verankerd binnen het ministerie van Financiën en de keten heeft de facto te maken met een centraal gezag. De Belastingdienst heeft een lange traditie van afstemming met de aanleverketen, daar zij partijen maximaal de gelegenheid wil bieden om aan hun verplichtingen te voldoen en omdat zij de uitvoering van de belastingwetgeving zo kosteneffectief als mogelijk wil laten verlopen. Deze afstemming bevindt zich op verschillende lagen, zo zijn er het Becon-overleg en het Digicom-overleg. Het Becon-overleg is het overleg tussen de organisaties van belastingadviseurs en de Belastingdienst. Besproken worden praktische zaken uit het dagelijks verkeer tussen Belastingdienst en belastingadviseur. Het Digicom-overleg is een voorportaal van het Becon-overleg waar het gaat om digitale ontwikkelingen. De Belastingdienst vindt het verder zo belangrijk dat er in het digitale berichtenverkeer zo min mogelijk uitval ontstaat, dat zij softwareontwikkelaars ondersteunt bij het ontwikkelen en testen van de software. Deze ondersteuning, evenals periodieke overleggen, is ondergebracht bij de Unit Ondersteuning Software Ontwikkelaars (OSWO) van het bedrijfsonderdeel Belastingdienst/Centrale Administratie.

In het jaarrekeningendomein is er sprake van een diffuser beeld. Op het eerste gezicht lijkt het logisch om de Kamer van Koophandel binnen deze keten dezelfde positie toe te kennen als de Belastingdienst binnen de fiscale keten. Dit doet echter geen recht aan de werkelijkheid. De Kamer van Koophandel valt als uitvoeringsorganisatie onder toezicht van het Ministerie van Economische zaken, Landbouw en Innovatie, maar kent op dit niveau een zwakke verankering. Zo bepaalt de Sociaal-Economische Raad welke regionale ondernemers-, werkgevers- en werknemersorganisaties de bestuursleden van een regionale Kamer van Koophandel mogen benoemen. Bovendien ontplooit de Kamer van Koophandel naast haar publieke taken ook private activiteiten, waardoor er ten aanzien van verschillende taken verschillende belangen (deels publiek/deel economisch) spelen. Verder valt de wetgeving die de Kamer uitvoert in het kader van de deponering van de jaarrekening onder de verantwoordelijkheid van het ministerie van Veiligheid en Justitie. De opdracht van de Kamer van Koophandel beperkt zich hierbij tot het publiceren van de aangeleverde jaarrekening. Zij heeft geen handhavende bevoegdheden wanneer partijen niet aanleveren. Deze zijn belegd bij de Economische Controledienst die onderdeel uitmaakt van de FIOD. In de praktijk blijkt dat deze handhaving overigens geen prioriteit heeft. Zoals eerder is aangegeven, is naast de KvK de Raad voor de Jaarverslaggeving een belangrijke machtsfactor waar het gaat om eisen (richtlijnen) die aan het ketenproduct (de jaarrekening) worden gesteld. Zij ziet vooralsnog echter geen taak voor zichzelf weggelegd om positie te nemen in de technische operationalisatie van de

richtlijnen. Kwesties ten aanzien van de ontwikkeling van de jaarrekeningketen blijven dan ook lang liggen. Zo heeft het NIVRA (thans NBA) in 2007 al de stelling ingenomen dat de huidige accountantsverklaring niet kan worden gebruikt bij een jaarrekening in XBRL-formaat. Op dit moment werkt de NBA aan een oplossing om een accountantsverklaring bij een XBRL bestand af te geven.

Een belanghebbende heeft met beide verantwoordingsketens te maken. Zijn administratie vormt immers de bron voor de verschillende verantwoordingsrapportages. In de ideale SBR-keten stelt de belanghebbende vanuit deze bron op eenvoudige wijze de benodigde verantwoordingsinformatie samen en stuurt deze op eenduidige wijze naar de betreffende uitvragende partij.

Afstemming tussen de uitvragende partijen is hierbij noodzakelijk:

- Uitvragende partijen moeten op eenduidige wijze hun informatievraag definiëren en kenbaar maken. Dit vraagt om begripseenduidigheid. Wanneer beide partijen exact hetzelfde willen weten, is het handig dat zij hiervoor hetzelfde woord gebruiken.
- Zij dienen een standaard taal te gebruiken om hun informatiebehoefte voor software domeinonafhankelijk en interpretabel te maken.
- Zij dienen op basis van dezelfde standaarden een (technische) koppeling voor berichtenverkeer te gebruiken.
- Zij dienen dezelfde feedbackstructuur te hanteren (statusinformatie). Een marktpartij wil weten wanneer deze aan zijn verantwoordingsplicht heeft voldaan, zo niet welke fouten deze heeft gemaakt. Dit is een stuk gemakkelijker wanneer alle uitvragende partijen dit op eenduidige wijze communiceren.
- Zij dienen hun releasemanagement op elkaar af te stemmen en hun 'afstemming' met de private partijen uit de aanleverketen op elkaar aan te laten sluiten. Wanneer één rapportageketen een jaar eerder overgaat op een nieuwe vorm van authenticatie (partijen hebben een nieuw 'paspoort' nodig), is dit erg onhandig voor bedrijven die aan meerdere uitvragende partijen aanleveren.

Doordat de publieke uitvragende partijen gebruik maken van een gedeelde dienstverlener en een generieke infrastructuur en er naast conceptuele ook sprake van fysieke verstrengeling is, dienen uitvragende partijen voor de geïntegreerde informatieketens afstemming te zoeken over:

- Onderhoud en doorontwikkeling
- Bekostiging

Waar de Belastingdienst ten aanzien van het elektronisch berichtenverkeer in het verleden betrekkelijk autonoom kon optreden dient zij nu af te stemmen met de Kamers van Koophandel (en andere SBR-partners zoals het CBS en de Minister van EZ) en hun gemeenschappelijke dienstverlener Logius. Deze afstemming gebeurt vanaf 2011 op basis van onder meer een gezamenlijk jaarplan, begroting, dienstenbeschrijving. Er is een SBR-stuurgroep; een projectleidersoverleg en er zijn diverse inhoudelijke werkgroepen. Ook vindt afstemming met de markt plaats (publiek-privaat). In hoofdstuk 9 (Governance en beheer) gaan we hier verder op in. Voor dit hoofdstuk

is het nog relevant enkele aspecten te benoemen uit de casus SBR waar het bestuur van deze verstrengelde keten in de afstemming mee te maken heeft:

- De Kamer van Koophandel en het CBS kunnen – gezien hun beperktere schaal – minder bijdragen aan de SBR-afstemming. Het risico bestaat dat zij ondervertegenwoordigd raken in de besluitvorming/inrichting. Dit kan negatief uitwerken voor het draagvlak binnen hun eigen organisatie.
- De Belastingdienst en het CBS kunnen autonoom de Nederlandse Taxonomie vaststellen als adequaat gegevensmodel voor aangifte/opgave. Voor de Kamers van Koophandel is het – door het push-karakter van de keten – onduidelijker hoe aan de Nederlandse Taxonomie legitimiteit kan worden verschaft. Hierdoor bestaat het risico dat er vragen worden gesteld bij de status van Nederlandse Taxonomie in haar geheel.
- De Belastingdienst heeft anders dan de Kamers van Koophandel en CBS al een system-to-system kanaal (BAPI) ingericht. Dit betekent legacy voor alle fiscale ketenpartners. Hierdoor kunnen inrichtingkeuzes een substantieel andere impact hebben op de fiscale keten (namelijk technisch oud → technisch nieuw vs. papier oud → technisch nieuw). In combinatie met haar natuurlijke macht, bestaat hier het risico dat de keteninrichting suboptimaal geschiedt in het licht van een 'greenfield' – dus nog geen technische inrichting – benadering.
- Naast publieke uitvragende partijen bestaan er ook private uitvragende partijen (zoals drie grootbanken). Deze kunnen gebruik maken van het begrippenkader van de Nederlandse Taxonomie. Daarnaast kunnen zij zich voor hun voorzieningen (Taxonomie) committeren aan de hiervoor opgestelde architecturen. Dit roept de vraag op in welke mate zij invloed uit mogen oefenen op de vormgeving van deze architecturen en op welke wijze zij betrokken worden bij het wijzigingsbeheer van bijvoorbeeld de begrippen van de Nederlandse Taxonomie, maar ook van proces en techniek.
- Binnen SBR wordt ook gebruik gemaakt van standaarden waar de deelnemers van SBR slechts zeer beperkt invloed op hebben. Dit gaat om de open standaarden als XBRL 2.1, maar geldt bijvoorbeeld ook voor de koppelvlakken en het PKIoverheid stelsel. Vanuit de SBR-governance moet nagedacht worden hoe met deze ketenafhankelijkheden om te gaan.
- Er zijn steeds meer domeinen (zowel publiek als privaat) die gebruik willen maken van SBR. Hierdoor neemt de ketenverstrengeling toe. De vraag ontstaat op welke wijze deze partijen gezamenlijk tot een effectieve en efficiënte afstemming kunnen komen.
- Naast de verantwoordingsketens worden onderdelen en standaarden uit het SBR-concept toegepast bij andere type informatie-uitwisseling, waaronder elektronisch bestellen en factureren. Doordat hier deels dezelfde bedrijven en dezelfde softwareleveranciers bij betrokken zijn, ontstaat er geheel nieuwe (conceptuele) afhankelijkheid wat nieuwe afstemmingsvraagstukken met zich mee kan brengen.

2.7 Afsluiting

Dit hoofdstuk gaf een overzicht van ketentheorie en een politiek perspectief op ketens en ketencoördinatie. Vanuit dit perspectief is te zien dat de structuur van de keten van belang is voor de machtsbalans erbinnen. Ook interactie met andere ketens beïnvloedt de manier waarop actoren in ketens beslissingen naar hun hand kunnen zetten. Vertrouwen is een voorwaarde voor ketensamenwerking. Vertrouwen vormt een belangrijke opgave voor ketencoördinatie. Echter, ketencoördinatie is geen waardenvrij begrip. Dat komt omdat coördinatie van grote invloed is op de verdeling van kosten en baten in de keten. In het geval van Standard Business Reporting is standaardisatie een belangrijk coördinatiemechanisme. Belangrijke vragen zijn wie zal moeten investeren om de standaarden te ontwikkelen en/of te volgen en wie daar baat bij heeft. Dergelijke vragen zijn niet eenvoudig te beantwoorden wegens de ingewikkelde structuren en onderlinge verstrengeling van de SBR-ketens: er zijn veel verschillende actoren met verschillende belangen. In hoofdstuk 3 gaan we nader in op de uitdagingen en aangrijpingspunten voor verandermanagement in ketens.

3 Verandermanagement in informatieketens

3.1 Het verandervraagstuk

In het vorige hoofdstuk zijn we ingegaan op de complexiteit van informatieketens en het ketencoördinatievraagstuk. Nu gaan we in op de verandering van informatieketens en de manier waarop deze veranderingen gemanaged kunnen worden. Dit hoofdstuk is geschreven vanuit het perspectief van 'het verandermanagement'. Hierbij kan gedacht worden aan een persoon – de verandermanager – of aan een (permanent) ingerichte veranderorganisatie (programma of afdeling) waar meerdere personen onderdeel van uit maken. Het hoofdstuk biedt inzicht in:

- De uitdagingen waar het verandermanagement bij de herinrichting van informatieketens mee te maken heeft.
- De bestaande veranderstrategieën en sturingsinstrumenten die het management kan toepassen bij de verandering van informatieketens en het concept van acceptatie van veranderingen.

Ook in dit hoofdstuk vormt de publiek/private informatieketen met een wettelijke grondslag het voornaamste object van onderzoek. In het hoofdstuk wordt de theoretische basis gelegd voor hoofdstuk 4 dat ingaat op het besturen van wijzigingen.

3.2 Uitdagingen voor het verandermanagement

Bij het herinrichten van informatieketens krijgt het verandermanagement te maken met diverse uitdagingen die onder te verdelen zijn in twee samenhangende categorieën, te weten:

- De intrinsieke weerbarstigheid van informatieketens
- Het gedrag van betrokken partijen

De volgende paragrafen verduidelijken de bovenstaande categorieën.

3.2.1 *De intrinsieke weerbarstigheid van informatieketens*

In hoofdstuk 2 hebben we een aantal eigenschappen van deze ketens aangestipt, die het veranderen ervan bemoeilijken:

- Ketens bestaan uit meerdere actoren, die verschillende belangen kunnen hebben. Bovendien hebben ketenpartijen verschillende ICT- architecturen die niet zonder meer op elkaar hoeven te passen. Het overkoepelend ketenbelang hoeft dan ook niet overeen te komen met individuele belangen van ketenpartners.
- Er is veel dynamiek, in verschillende opzichten. Allereerst is de operatie dynamisch: informatie stroomt in miljarden bits en bytes per seconde van de ene organisatie naar de andere organisatie. Bovendien is de technologie dynamisch: voortschrijdend inzicht is aan de orde van de dag. Regelmatig zijn er nieuwe kansen en net zo vaak updates voor gebruikers. Tenslotte is de organisatie dynamisch: de structuur van de keten kan veranderen (zoals het aantal partijen binnen schakels, of het aantal selecterende of allocerende schakels) en tenslotte is de machtsbalans tussen actoren dynamisch.

Schekkerman (2000) voegt hier nog twee uitdagingen voor verandermanagement aan toe:

- Afhankelijkheid: Hoe meer bedrijfsprocessen door inter-organisatorische informatiesystemen worden overgenomen, hoe afhankelijker organisaties of schakels in een keten van dit systeem worden. Deze afhankelijkheid vereist hogere eisen aan verschillende aspecten, zoals continuïteit, beschikbaarheid, betrouwbaarheid en beveiliging. Verandering brengt risico's met zich mee die de afhankelijke partijen als onacceptabel kunnen beschouwen. Het mitigeren van deze risico's (door bijvoorbeeld een parallelle infrastructuur op te zetten) kan forse kosten met zich meebrengen. In de Inleiding (hoofdstuk 1) is deze afhankelijkheid expliciet genoemd als consequentie van de overgang naar S2S-integratie en gedeelde diensten.
- Ontstane complexiteit: Wijziging van een informatiesysteem of standaard kan grote gevolgen hebben voor partijen. Zij hadden andere systemen, andere definities, toegespitst op hun organisatie. Ook is het mogelijk dat hun systemen misschien niet zo op de organisatie waren toegespitst, maar dat de organisatie er dermate aan gewend is geraakt dat verandering een forste desinvestering zou betekenen. Niet alleen systemen hoeven aangepast te worden, mensen moeten getraind en opgeleid worden en nieuwe organisatieprocedures en routines kunnen nodig zijn. Er moet met andere woorden (semantische, technische, organisatorische) interoperabiliteit gecreëerd worden (zoals ook besproken in de Inleiding).

Deze karakteristieken leiden tot velerlei eisen aan informatieketens, waarbij de eisen, belangen en verwachtingen per actor verschillend kunnen zijn. Het werk van een verandermanager is aldus uitdagend, getuige bovenstaande eigenschappen van informatieketens.

3.2.2 *Strategisch gedrag*

De belangrijkste moeilijkheid voor het verandermanagement is echter nog niet genoemd. Dat is de weerbarstigheid van het gedrag van de vele betrokken actoren. Het gedrag van de betrokken actoren is te begrijpen vanuit bovenstaande eigenschappen van informatieketens. Dat gedrag is echter niet altijd wenselijk voor een verandermanager, die immers maar één van de actoren is.

Het idee om standaarden te introduceren voor het leveren van informatie aan overheden kan voor alle 'typen' actoren een aantrekkelijke gedachte zijn:

- Wanneer gegevens gemakkelijk uit te wisselen zijn, is de drempel voor het toepassen van bepaalde software lager: softwareleveranciers kunnen zich onderscheiden op functionaliteit en kwaliteit.
- Informatieleverende partijen kunnen efficiëntie winst verwachten (één leercurve, één koppelvlak) en worden minder afhankelijk van een softwareleverancier.
- Betrokken overheidspartijen krijgen hogere kwaliteit gegevens (onder meer doordat er minder conversies nodig zijn) en krijgen de beschikking over een flexibelere infrastructuur.
- Standaardisatie biedt de mogelijkheid voor intensiever hergebruik van (IT)diensten, wat de kosten voor IT en expertise omlaag kan brengen.
- Flexibiliteit: nieuwe spelers die de standaarden gebruiken, kunnen makkelijk toegevoegd worden.
- Duurzaamheid: doordat standaarden niet continue veranderen, kunnen investeringen in standaarden over langere periode afgeschreven worden.

Dit zijn potentiële voordelen. Het is echter niet zeker of deze voordelen door iedereen benut kunnen worden. De bovengenoemde complexiteiten komen – met als voorbeeld SBR – als volgt tot uiting:

- In veel sectoren liggen gegevens bij verschillende organisaties opgeslagen, die met behulp van verschillende definities tot informatie worden verwerkt. Ordening brengen in deze gegevens en informatie levert (efficiëntie)winst op. Sterker nog, dit levert dermate veel winst op dat er een markt kan ontstaan in het ordenen van informatie. In de agrosector zijn er bijvoorbeeld verschillende partijen (met name intermediairs) die een database beheren en geld verdienen aan het ordenen ervan. SBR is voor deze dienstverleners een bedreiging.
- Wanneer partijen hun gegevens in een pakket met onderliggende database hebben opgeslagen en het lastig is deze gegevens te exporteren in een vorm die voor de concurrerende pakketten makkelijk te importeren is, dan vormt dit een belemmering om van softwareleverancier te wisselen. Juist in verantwoordingsketens waar de beschikbaarheid van historische gegevens tot minimaal 5 jaar relevant is, kan deze zogenaamde '*vendor lock in'* voor de

leverancier een belangrijk concurrentievoordeel bieden. Meer interoperabiliteit doet dit voordeel voor de leverancier teniet.

- Het betekent nogal wat om voorloper te zijn. Informatieleverende partijen die als eerste SBR omarmen lopen het gevaar veel te moeten investeren en daar relatief weinig voor terug te krijgen. De winsten worden immers uiteindelijk verdeeld over alle gebruikers en het concurrentievoordeel is dan beperkt. Dit terwijl de backoffice moet worden gereorganiseerd op basis van de standaarden die aan het begin gedefinieerd zijn. Omdat de standaarden gedurende het project zullen veranderen, mede onder invloed van de kinderziektes die in de nieuwe operationele ketens zullen bestaan, zal er door die partijen vaker gereorganiseerd moeten worden. '*First movers advantage*' en een positief imago zijn voordelen voor voorlopers, maar deze voordelen zijn lastig te managen en te kapitaliseren.
- Door introductie van nieuwe ICT-toepassingen vindt een verschuiving van verantwoordelijkheden plaats in de keten, welke direct invloed heeft op de kernwaarden (gedeelde waarden binnen de organisatie) van betrokkenen. De projecten hebben invloed op de positie van de betrokken partijen in de waardeketen. Bij SBR gaat het om een veranderende rol van de intermediairs en de softwaremarkt. Een dergelijke verandering wordt door het merendeel van de bedrijven in eerste instantie als bedreigend ervaren. Slechts een klein aantal bedrijven ervaart het direct als kans. Te weinig inzicht in en begrip voor de kernwaarden en belangen van partijen is gevaarlijk voor verandermanagement. ICT raakt de kernprocessen van organisaties, waardoor partijen in eerste instantie niet mee willen werken. De medewerking van deze partijen is echter essentieel om tot een brede adoptie van de verandering te komen (Janssen et al., 2010).

Actoren zullen om deze redenen zich niet altijd volledig inzetten voor nieuwe systemen en projecten als SBR. Volledige inzet zou voor de verandermanager wenselijk zijn. Het is echter voor veel actoren aantrekkelijker om zich strategisch te gedragen. Veel voorkomende vormen van strategisch gedrag zijn dan ook:

- '*Wait and see*': Informatieleveranciers, softwareleveranciers en intermediairs die veel belangstelling tonen voor ontwikkelingen en ook participeren in werkgroepen en bijeenkomsten die vanuit de overheid worden georganiseerd. Maar die vervolgens wachten met echte investeringen, totdat duidelijk is dat SBR een voldongen feit is.
- '*Free riding*': Informatieleveranciers die wachten tot de belangrijkste investeringen zijn gedaan en de standaarden gestabiliseerd, en pas daarna instappen. De free rider profiteert zo van de investeringen die anderen hebben moeten doen. De angst voor een concurrentienadeel ten opzichte van de free rider, weerhoudt partijen ervan investeringen te doen.

Janssen et al. (2010) hebben in een onderzoek, dat gericht was op de ICT-ondersteuning van de omgevingsvergunning, geconstateerd dat het concept 'strategisch gedrag' zich kan vertalen in heel concrete problemen. Zij hebben over deze projecten onder meer het volgende geconcludeerd:

1. Wetgeving, beleid en techniek raken dermate vervlochten, waardoor vertraging in de ene sfeer ook vertraging in de andere sfeer betekent. Er ontstaat

een '*catch 22*-situatie', waarbij zij die technologie moeten adopteren wachten tot de wetgeving er is en wetgeving uitblijft omdat organisaties er technisch nog niet klaar voor zijn.
2. Het ambitieniveau verandert voortdurend en kan gedurende het project blijven stijgen, waardoor het project te complex wordt. Onder invloed van bestuurlijke wensen en beloftes van softwareleveranciers kan het ambitieniveau te groot worden, waardoor het project eindeloos wordt.
3. Het blijkt lastig in het veranderproject integraal zowel te focussen op de technologie, als de business en het verkrijgen van draagvlak, waardoor het hoofddoel uit het oog verdwijnt. Subdoelen (technologie, de organisatie of het verkrijgen van draagvlak) dreigen hoofddoel te worden.
4. Er is weerstand bij partijen die zich aangetast voelen in hun kernwaarden door de ingrijpende veranderingen in de rollen en processen van partijen in de gehele keten. Weerstand verloopt vervolgens via lobby en de bestuurlijke gremia, die een behoorlijke blokkademacht kunnen vormen voor het gehele proces.

Eind 2009 ondervond het verandermanagement van SBR hinder van bovengenoemde punten 2 tot en met 4. Punt 1 werd als risico erkend. Er is door betrokkenen fors in het programma ingegrepen teneinde de ontstane impasse te doorbreken. De gemaakte keuzes hebben het programma een positieve impuls gegeven. Onderstaand een overzicht van de belangrijkste maatregelen die genomen zijn om genoemde problemen weg te nemen of te voorkomen:

- Ten aanzien van punt 1 is er een werkgroep compliance, waarin juristen van de verschillende betrokken publieke partijen vertegenwoordigd waren. Deze juristen hebben als taak gekregen alle ontwikkel-, implementatie- en wijzigingsambities (technisch/inhoudelijk) te toetsen op juridische haalbaarheid. De wet bleek zelden belemmerend voor het realiseren van de behoefte, mits er aan bepaalde randvoorwaarden werd voldaan. Denk hierbij aan het volgen van de juiste procedure, het tijdig openbaar maken van bepaalde stukken. De wijze waarop het gevoerde beleid publiek werd gemaakt (communicatie over de uitvoering naar de verschillende stakeholders), bleek steeds een belangrijke voorwaarde voor compliance. Kritische succesfactor voor een werkgroep compliance is een goede samenwerking tussen juristen die kennis hebben van techniek en technici die gevoel hebben voor wetgeving en beleid. Een werkgroepvorm kan hierbij helpen, omdat juristen en technici in een vroeg stadium, parallel aan de vele ontwikkelingen, gecommitteerd worden aan SBR. Zij zullen door deze commitment geneigd zijn naar de technische en juridische mogelijkheden te gaan zoeken en niet naar de onmogelijkheden. In hoofdstuk 5 (I-Processen) wordt nader ingegaan op de rol van (proces)compliance.
- Ten aanzien van punt 2 is de volgende constatering relevant. Het Nederlandse Taxonomie Project (de voorloper van SBR) startte initieel met het op eenduidige wijze opslaan van de gegevensdefinities en de gegevensbehoefte van Centraal Bureau voor de Statistiek, de Kamer van Koophandel en de Belastingdienst. Dit project kreeg al gauw te maken met 'aanvullende' ambities, waaronder:

    - Gedeelde ICT-voorzieningen binnen de overheid (wat leidde tot Digipoort)
    - Nieuwe vormen van toezicht (koppeling met 'horizontaal toezicht' van de Belastingdienst, waaronder de implementatie van de verkorte winstaangifte, zie hoofdstuk 1)
    - Inhoudelijke zekerheid voorin de keten door toepassing van Simplified Validation Rules (SVR)
    - Business to business toepassing van SBR

  Vanaf begin 2010 is de focus vanuit de overheid komen te liggen op de implementatie van de basale onderdelen voor een verantwoordingsketen. Dit betekent dat de koppeling tussen SBR en horizontaal toezicht vanaf dat moment minder aandacht heeft gekregen. De validatie tegen SVR-regels is uit de gemeenschappelijke voorziening gehaald. Met alle betrokken partijen is vervolgens gefocust op het realiseren van een stabiele verantwoordingsketen (en dan met name aanleveren bij de overheid). Nu deze basisvoorziening gereed is komen sommige punten weer terug op de agenda, maar deze kunnen nu op een stabiel fundament leunen.
- De betrokken partijen realiseerden zich dat de invloed van de overheid op één van de belangrijkste beleidsdoelen waarvoor SBR in het leven geroepen was – administratieve lastenvermindering – beperkt was. Brede adoptie door de markt is hiervoor namelijk noodzakelijk. De weg naar adoptie is in stukjes gehakt, waarbij in 2010 eerst aangetoond moest worden dat er een geloofwaardige SBR-aanleverketen te realiseren was. Er is door de betrokken publieke organisaties een gezamenlijke roadmap opgesteld voor opschaling van gebruik en er zijn voor iedere partner in SBR projectleiders aangesteld, die verantwoordelijk waren voor het realiseren van een werkende keten. Deze projectleiders keken over de pijlers (techniek, organisatieverandering en draagvlak) heen en zorgden ervoor dat er inderdaad een geloofwaardige oplossing werd ingericht. Deze keten heeft bestuurders voldoende vertrouwen gegeven voor de volgende stap: het voorgenomen besluit om vanaf 2013 voor de verschillende stromen verantwoordingsinformatie SBR als enige methode voor system-to-system verantwoording gefaseerd open te stellen. Dit voorgenomen besluit geeft een enorme impuls aan marktadoptie en hiermee komt de oorspronkelijke beleidsdoelstelling weer in zicht.
- Er is in 2010 vanuit SBR een marktbewerkingstrategie gevolgd waarin veel meer ruimte is voor partijen die (vanuit welke waarde dan ook) niet op SBR zitten te wachten. De programmacommunicatie is begin 2010 van toon veranderd. Van 'u bent gek als u dit niet snapt' naar 'wij zijn blij als u met ons mee wilt doen'. Verder zijn er vanaf dat moment regiodagen voor belanghebbenden georganiseerd, waar tegenstanders en criticasters uitgebreid de ruimte krijgen om hun vragen te stellen. Het programma heeft een veel opener karakter gekregen, waardoor het 'wij' (voorlopers) tegen 'zij' (conservatieven) gevoel is afgenomen. Dit heeft geleid tot een veel minder gepolariseerd speelveld, wat het programma ten goede is gekomen.

Het definiëren en implementeren van een gebalanceerd pakket van maatregelen teneinde de problemen rond een ketenverandering het hoofd te bieden, is geen sinecure. Zeker wanneer bovenstaande problemen zich tegelijkertijd voordoen op een wijze

die zelden volledig te voorzien is, kan de neiging bestaan ad hoc te reageren. Projecten krijgen dan een sfeer van 'incident-management'. Ook hierdoor kan de gebruiker, en het programmadoel, grotendeels uit beeld geraken (Janssen c.s., 2010). Binnen SBR is dit probleem erkend en is een bestuurlijk programmamanager aangesteld die als opdracht had het programma weer 'saai' te maken en dus uit de incidentensfeer te halen.

Voor iedere keten-in-verandering geldt dat het verandermanagement moet kunnen omgaan met de beschreven uitdagingen. Met name zal ze moeten anticiperen op vormen van strategisch gedrag. De volgende paragraaf gaat in op de strategieën waarmee het verandermanagement een verandering kan benaderen.

3.3 Veranderstrategieën

Het is moeilijk om verandermanagement te realiseren. Met name doordat iedere informatieketen verschillend en veranderlijk is. Iedere aanbeveling is dan ook contextafhankelijk. Wat voor het ene verandermanagement werkt, hoeft niet voor het andere verandermanagement te werken. Er zijn dan ook geen absolute, algemeen geldende aanbevelingen. Wel kunnen we hier vanuit de literatuur over verandermanagement een aantal strategieën voor verandermanagers aangeven en uitwerken. We onderscheiden vier veranderstrategieën. De eerste twee zijn complementair aan elkaar, namelijk direct verandermanagement en procesmanagement. De andere twee strategieën zijn het veranderen van ketencondities en dilemmamanagement. Het is altijd aan het verandermanagement zelf om de voor hen meest aansprekende strategie verder in te vullen, waarbij mix-vormen (sequentieel of voor onderdelen) mogelijk zijn.

3.3.1 *Direct verandermanagement*

Hoofdvraag vanuit direct verandermanagement is hoe een organisatie van situatie A naar situatie B moet komen. Beide situaties zijn al gedefinieerd. Het is dus duidelijk wat het vertrekpunt is en wat het doel van de verandering is. Literatuur over verandermanagement is wijd verbreid in de organisatiekunde, maar niet altijd toegespitst op (informatie)ketens. Wel kunnen de meeste principes ervan worden doorvertaald naar ketens, omdat zowel organisaties als ketens bestaan uit verschillende actoren met verschillende belangen.

Agterhorst en Thaens (2000) adresseren een belangrijk aspect waar organisatiekundigen mee worstelen, namelijk weerstand tegen verandering. De genoemde strategieën bij SBR geven al aan dat dergelijke weerstand ook bij informatieketens bestaat. Zij refereren aan de zogenaamde 'veranderformule' van Dannemiller en Jacobs (1992). De veranderformule gaat er van uit dat een aantal factoren van belang is voor de wijze waarop de veranderingen kunnen worden gerealiseerd.

D x V x F > R

Waarbij D = dissatisfaction, V = vision, F = first steps en R = resistance.

Weerstand (resistance) staat centraal in deze formule. Agterhorst en Thaens stellen dat tegenover deze weerstand een gedeelde noodzaak om te veranderen, een gemeenschappelijk gedragen beeld over de toekomst en overeenstemming over de eerste stappen voor een succesvolle verandering nodig zijn.

De vraag is uiteraard hoe een dergelijke bereidheid om te veranderen – ofwel acceptatie, hoofdstuk 4 gaat verder in op dit concept- te organiseren valt. Van Amelsvoort (1996) onderscheidt verschillende benaderingen van organisatieverandering. We gaan ze allemaal even na, om zo een gevoel te geven voor het brede arsenaal aan mogelijkheden:

- De expertbenadering. Het toekomstbeeld wordt hier ontworpen door experts. Dit zijn deskundigen op het gebied van organisatiekunde. Resultaat is een plan, een architectuur of een ketenstructuur, dat vervolgens geïmplementeerd moet worden.
- De brede bottom-up benadering. De experts worden in deze benadering vervangen door medewerkers van een organisatie (of de keten). Zij hebben gebruikerskennis en kennen de huidige taakafbakeningen beter. Hierna wordt het ontwerp geïmplementeerd.
- De deblokkadebenadering. Deze benadering problematiseert niet wie veranderingen moeten ontwerpen, maar op basis waarvan dat moet gebeuren. De deblokkadebenadering gaat uit van het wegnemen van blokkades. Blokkades zijn één of meerdere ernstige problemen die dwars door de organisatie (of keten) gevoeld worden. Een beperkte multidisciplinaire projectgroep ontwikkelt een probleemanalyse en werkt blokkades weg. Het oplossen van problemen wordt zo de aanleiding tot organisatieverandering.
- De blauwdrukbenadering. Deze benadering stelt het proces van verandering centraal. De benadering gaat uit van een organisatieherontwerp aan de hand van een strakke indeling in fasen, die één voor één sequentieel moeten worden doorlopen. Deze methode komt in de ICT veel voor. Denk bijvoorbeeld aan het dwingende SAP blue print model voor de invoering van ERP-systemen.
- De grof-fijncyclus impliceert een geavanceerder proces. Een kleine groep maakt een grof ontwerp, waarop management en medewerkers gezamenlijk het grove ontwerp gaan verfijnen.
- De netwerkbenadering gaat uit van een netwerk van actoren waarbinnen de visie op de toekomstige organisatie (of keten) wordt ontwikkeld en verspreid. Hier wordt de structuur van de organisatie (of keten) losgelaten ten gunste van een veel losser, informeler verband tussen ontwerpers, die experts, managers of medewerkers kunnen zijn.

Essentie van direct verandermanagement blijft dat een verandering van A naar B wordt gerealiseerd, waarbij zowel A als B bekend zijn. In de praktijk zijn A en B echter niet altijd gegeven. Met name wanneer veel actoren een rol spelen en allemaal andere doelen nastreven, staan zowel A als B nogal eens ter discussie. De volgende veranderstrategie gaat er van uit dat A en B niet gegeven zijn en is daarom complementair aan direct verandermanagement.

3.3.2 *Procesmanagement*

Procesbenaderingen van verandering zijn momenteel populair. Veel mensen krijgen expliciet de functie van 'procesmanager' opgespeld. Zij houden zich veel bezig met interactie met andere actoren, al of niet georganiseerd in allerlei stuur- en werkgroepen en interactieve ontwerpsessies. De opkomst van 'procesmanagers' betekent een erkenning van het feit dat veranderingen vaak langdurige processen zijn, die meer behelzen dan het maken van een ontwerp op de tekentafel dat vervolgens top-down overnacht wordt geïmplementeerd. Vele actoren willen hun zegje doen en met hun deskundigheid een bijdrage leveren. Dat is vanuit het perspectief van een verandermanager ook nuttig, zelfs noodzakelijk voor acceptatie door partijen, een breder draagvlak en een rijk ontwerp. Desalniettemin is een erkenning dat processen lang duren en 'gemanaged' moeten worden geen garantie voor een soepel lopend proces. Een verklaring hiervoor kan gevonden worden in de verschillen in opvatting over wat het doel van een proces kan zijn.

Procesmanagement betekent niet 'alles open maken'
Een veel voorkomend misverstand over procesmanagement is dat het eenvoudigweg zou gaan over het betrekken van zo veel mogelijk stakeholders bij beslissingen. Een naïef soort procesmanagement kan vanuit deze gedachte ontstaan: alles wordt open gemaakt. De agenda is open, het proces is open, er is toegang voor iedereen en de uitkomst hangt af van de inbreng van alle partijen. Een soort onzichtbare hand zou leiden tot de beste oplossing. Een dergelijk naïef procesmanagement leidt onherroepelijk tot langdurige 'Poolse landdagen'. Voor zover er een oplossing komt, dan is de kans vervolgens groot dat deze oplossing een bestuurlijk compromis is dat de toets van deskundigen niet kan doorstaan.

Uit procesmanagement als veranderstrategie zijn twee sturingsinstrumenten af te leiden: directe en indirecte procesmanagement (Bruijn, Heuvelhof, & Veld, 2008). Processturing geldt hier als synoniem voor procesmanagement. We komen hier later op terug.

Grofweg is te stellen dat hoe hoger de bestuurlijke complexiteit, des te meer het verandermanagement is aangewezen op procesmanagement als veranderstrategie. Een directere benadering gaat er vanuit dat actoren zich binnen een proces laten dirigeren naar een tevoren gewenste uitkomst. Bij een hoge bestuurlijke complexiteit is een dergelijke veronderstelling niet realistisch.

3.3.3 *Intermezzo: direct verandermanagement versus procesmanagement*

Benaderingen van procesmanagement kunnen onder condities effectief zijn. Een gevoel voor dergelijke condities krijgen we uit studies naar verandermanagement, bijvoorbeeld een studie naar de ontwikkeling en implementatie van shared service centers (De Bruijn c.s., 2004). De invoering van shared service centers bij de Rijksoverheid (het project P-direct) is een publiek project met efficiëntie als doelstelling. Het concept beloofde efficiëntie, maar ook hier moest aan stevige randvoorwaarden in de informatieketen worden voldaan, alvorens de belofte kon worden ingelost. Op basis van interviews met betrokkenen onderscheidt de studie twee belangrijke variabelen van verandermanagement: het ambitieniveau van het project ('groots en meeslepend' of 'klein en wendbaar') en implementatiestrategieën. Met betrekking tot de laatste variabele zijn twee extremen voor implementatie uit de interviews gededuceerd:

Verleidingen van direct verandermanagement
In de praktijk blijkt een business case gebaseerd op een direct verandermanagement aanpak gemakkelijker aan bestuurders (budgethouders) te verkopen. Uitgaand van een gegeven eindsituatie kan op basis van back-casting een ogenschijnlijk 'zekere' inschatting van tijd, geld en middelen gegeven worden. Wanneer de einduitkomst niet bekend is, is men afhankelijk van forecasting en zelfs meerdere scenario's. De onderbouwing van de business case en go/no-go scenario's neemt in dit geval in complexiteit toe. Bestuurders houden over het algemeen niet van open einden in hun begroting en zijn minder geneigd hierin te investeren. Sponsoren van de verandering (en de projectleiders) kunnen bij complexe trajecten in de verleiding komen tegen beter weten in de business case te baseren op een direct veranderproject. Bestuurders kunnen in de verleiding komen tegen beter weten in met de voorgestelde aanpak akkoord te gaan.

1. **Big bang.** De verandering kent een hoog ambitieniveau ('groots en meeslepend') en implementatie geschiedt als een project. Deze vorm zal met name hen met een technische oriëntatie aanspreken. Er wordt centraal een beste oplossing ontwikkeld, die ongeacht de bestaande systemen (en dus radicaal) wordt geïmplementeerd. Alvorens tot implementatie over kan worden gegaan, zullen wel eerst alle systemen en het management op orde moeten zijn (eerst het huis op orde). Als zodanig is implementatie als project te vergelijken met 'direct verandermanagement'. Zowel A (het huis is op orde) als B (de beste oplossing) zijn bekend. De invoering wordt low profile georganiseerd, zodat de omgeving weinig invloed op het project heeft.

2. **Zachte dwang.** De voorziene verandering kent een laag ambitieniveau ('klein en wendbaar') en implementatie geschiedt als een proces. Het suggereert het tegenovergestelde van de 'big bang'. De implementatie staat meer open voor wensen vanuit de decentrale gelederen van de organisatie, de ketenpartners en de bestaande systemen, die hier vaak de achtergrond van vormen.

In tabel 3.1 zijn deze twee extreme implementatiestrategieën samengevat.

Tabel 3.1 – Twee extremen voor verandermanagement

	Big Bang (direct verandermanagement)	**Zachte dwang (procesmanagement)**
Besluitvorming	Centraal	Decentraal
Invoering	Radicaal	Stapsgewijs
Timing	'Eerst huis op orde'	'Over the wall engineering'
Management verwachtingen	Gesloten	Open

In ieder proces is behoefte aan closure: een moment dat er een eenduidige beslissing valt. Het is aan het procesmanagement om aan deze behoefte te voldoen. Het suggereert het combineren van de extreme verandermanagementstijlen uit voornoemde studie naar shared service centers. Een 'big bang' en 'zachte dwang' zullen op enigerlei wijze moeten worden gecombineerd, zodat een proces niet alleen open genoeg is om belangen en kennis van partijen te benutten, maar ook (technische) expertise en regie hun plaats krijgen. De Bruijn c.s. (2008) spreken van het combineren en alterneren van coöperatie en *command and control* (zie ook: Koffijberg, 2005). Hier ligt een van de belangrijkste uitdagingen voor het procesmanagement: hoe closure te organiseren? Wanneer worden hiërarchische interventies geaccepteerd? Dit is niet op papier voor te schrijven, maar is onderwerp van ervaring en intuïtie bij een procesmanager.

De vraag is hoe beide managementstijlen zijn te combineren en te alterneren. Een 'big bang' doet geen recht aan de bestuurlijke complexiteit en dynamiek (lees: strategisch gedrag) in ketens, maar de procesbenadering leidt niet tot 'closure' en kan als zodanig niet functioneren in een omgeving dat randvoorwaarden (zoals budget en deadlines) oplegt. Hoe kan het beste van beide werelden worden benut? Drie voorbeelden van combinaties zijn denkbaar (zie bijv. Bharosa et al., 2011; Koffijberg, 2005):

1. Hiërarchische interventie en ruimte laten. Een 'engineering approach' geeft regie, maar is kwetsbaar als de belangen van actoren geen recht is gedaan. Weerstand kan problematisch zijn als deze belangen bij actoren horen die essentieel zijn voor het realiseren van de verandering. Bovendien kan een engineering approach moeilijk omgaan met voortschrijdend inzicht van de actoren die erdoor worden aangestuurd. Ruimte laten kan hun weerstand matigen en hun deskundigheid benutten. Een voorbeeld van 'ruimte laten' is sturen op output in plaats van op processen. Tijd, kosten en kwaliteitsstandaarden worden strikt geformuleerd en gehandhaafd, maar de manier waarop actoren binnen deze randvoorwaarden opereren staat open voor discussie en decentrale besluitvorming.
2. Timing en hiërarchie. Processen in informatieketens kunnen veel tijd in beslag nemen. Binnen de looptijd van dergelijke processen kunnen problemen en oplossingen verschijnen en verdwijnen, voorkeuren komen en gaan en politieke druk opkomen en verminderen. Dit suggereert dat er een tijd is voor hiërarchische interventie en een tijd voor coöperatie en tolerantie voor diversiteit. Wanneer is de tijd voor hiërarchische interventie aangebroken? Wanneer is hiërarchie legitiem genoeg, zodat deze wordt geaccepteerd? Voorwaarden hiervoor kunnen zijn: een sterke urgentie bij alle partijen om

tot een beslissing te komen, een eerdere oprechte, maar mislukte poging om middels coöperatie tot een oplossing te komen en een situatie waarin een grote meerderheid na een intensief proces over de streep is getrokken. In het laatste geval zal de procesmanager gelegitimeerd zijn de kleine minderheid te bewegen in te stemmen en eventueel hiervoor te compenseren.

3. Hiërarchisch opleggen van een proces. Dit is een versie van 'hiërarchische interventie en ruimte laten', die top-down implementatie van besluitvormingsregels behelst. Dergelijke regels kunnen bijvoorbeeld gaan over de vraag wie er participeert in besluitvorming en welke rol technisch deskundigen in het proces hebben. Binnen dergelijke regels kan er ruimte gelaten worden voor een meer agile benadering (Boehm, 2002).

Het moge duidelijk zijn dat procesmanagement vele vormen kan aannemen en geen kant-en-klare oplossing voor alle kwalen is. Het vergt het voortdurend balanceren tussen hiërarchie en coöperatie. De balans hiertussen hangt sterk af van de condities waaronder de verandering plaats moet vinden. Grofweg kunnen we wel stellen dat het belang van procesmanagement stijgt met het ambitieniveau van een veranderstraject. Immers, hoe hoger het ambitieniveau, hoe groter de technische en bestuurlijke complexiteit. We hebben echter ook gezien dat hiërarchie pas wordt geaccepteerd bij een sterk urgentiegevoel bij alle partijen om tot een beslissing te komen. Dit is niet in alle complexe trajecten het geval. Het SBR Programma heeft in 2010 geconstateerd dat er een geloofwaardige oplossing operationeel was (bewezen technologie), maar dat er nog geen sprake was van een gelijkwaardig substituut met bestaande wijzen van verantwoording doordat:

- de SBR keten een beperktere functionaliteit bood (bijvoorbeeld geen eMededelenkanaal en geen mogelijkheid voor het aanleveren van een samenstelverklaring);
- de SBR keten beperktere kwaliteit kon bieden (kleinere service-organisatie).

Doordat het aantal gebruikers van SBR een stuk kleiner was dan het aantal gebruikers van de alternatieve kanalen, voelden betrokken actoren weinig urgentie voor een investering in SBR. Met de mededeling dat de bestaande wegen de komende jaren uitgefaseerd gaan worden, hebben bestuurders de urgentie weten te creëren om de benodigde sprong in kwaliteit te realiseren. Partijen 'moeten' SBR als aanleverkanaal nu wel serieus nemen.

3.3.4 *Veranderen van ketencondities*

Een derde veranderstrategie noemen we het 'veranderen van ketencondities'. Dit hoofdstuk begon met een aantal weerbarstige eigenschappen van informatieketens. Deze kunnen een directe verantwoordingsstrategie dwarsbomen.

Soms zijn de condities te slecht om een directe veranderstrategie door te voeren. In een dergelijk geval is een indirecte veranderstrategie het hoogste haalbare. Deze omhelst minimaal twee stappen. De eerste stap is het verbeteren van de condities waarin verandering plaats moet vinden. De tweede stap is het doorvoeren van de verandering. Dit idee is al oud. Kurt Lewin (1951), één van de pioniers van de veranderkunde, ontwikkelde drie stappen, met de concepten *unfreeze – move – freeze*. Unfreeze

staat voor het voorbereiden van medewerkers van een organisatie op een verandering. De geesten worden 'ontdooit', ofwel klaargemaakt voor een verandering. De move is de verandering zelf en de freeze is de internalisatie van de verandering.

De concepten van Lewin zijn sterk toegespitst op weerstand van individuele medewerkers in een organisatie. De processen die hij beschrijft verlopen anders dan de processen van verandering in informatieketens. Het idee van het beïnvloeden van de omstandigheden voor verandering is echter wel van toepassing. We werken twee beïnvloedingsvormen uit:

- Verandering van de ketenstructuur
- Strategisch communiceren

3.3.4.1 Verandering van de ketenstructuur

In het vorige hoofdstuk hebben we aangegeven dat de ketenstructuur de machtsbalans binnen een keten kan bepalen. Verandering in de ketenstructuur kan dan ook leiden tot een verandering in de machtsbalans. De machtsbalans kan verandering accepteren en ondersteunen of blokkeren. Wanneer het laatste het geval is, dan is direct verandermanagement waarschijnlijk niet effectief. Via de ketenstructuur kunnen de condities voor verandermanagement wellicht worden verbeterd.

De Bruijn en Ten Heuvelhof (1995) beschrijven enkele strategische opties voor de verandering van de ketenstructuur. We lichten er drie uit en passen ze toe op de SBR-casus.

- Het sluiten van allianties met zwakke, selecterende of divergerende schakels. Deze schakels bepalen immers het procesverloop in grote mate. Het aangaan van allianties met deze schakels biedt de beste beheersmogelijkheden. Dit kan in de SBR-casus bijvoorbeeld relevant zijn bij het kiezen van een sector. Welke organisaties integreren de meeste gegevens? Dat zijn de organisaties waarmee overeenstemming over standaarden moet worden bereikt. Vanuit het SBR Programma is intensief ingezet op allianties met voorlopende intermediairs en hun softwareleveranciers.
- Het beheersen van meerdere schakels in de keten. Zo kan het procesverloop beter worden beïnvloed. In de SBR-casus kan dat bijvoorbeeld door softwareontwikkeling zelf ter hand te nemen. Hier is binnen SBR overigens tot nu toe terughoudend mee omgegaan.
- Het verbeteren van de interfaces tussen schakels in de keten. Dat kan door bijvoorbeeld de interactie tussen de schakels te faciliteren. In het geval van SBR zijn verschillende expertgroepen opgericht, waarbij ook de dialoog tussen (private) ketenpartners gestimuleerd wordt.

3.3.4.2 Strategisch communiceren

Bij strategische communicatie zet je communicatie binnen en buiten het programma in teneinde het perspectief van actoren op de verandering te beïnvloeden. Je let hierbij bijvoorbeeld sterk op de connotatie die al aan begrippen kleeft. Het spreken over ketens, is hier een voorbeeld van.

Ketens zijn moeilijk zichtbaar. Feitelijk zijn ze alleen zichtbaar op papier. Dat wil zeggen dat het eigenlijk 'maar' gedachtenconstructies zijn. Een metafoor voor processen zoals die verlopen. Of voor processen zoals die volgens een specifieke partij zouden moeten verlopen. Het gaat wel om een heel krachtige metafoor: iedereen kan zich er heel snel iets bij voorstellen. Ingewikkelde processen zijn met deze metafoor relatief gemakkelijk uit te leggen aan hen die zich er inhoudelijk minder in hebben verdiept, zoals sommige bestuurders. Deze kracht kan ook tevens de zwakte zijn: het beeld van een keten kan al snel andere processen, die niet tot de keten behoren, naar de achtergrond doen verdwijnen (Duivenboden, Twist, & Veldhuizen, 2000). We zien, bij wijze van spreken, alleen de keten nog. Of de metafoor van de keten een kracht of een zwakte is, hangt uiteraard ook af van de vraag hoe de metafoor gebruikt wordt in de communicatie.

Er is de laatste jaren veel aandacht in de economische en bestuurskundige literatuur over het bewust beïnvloeden van keuzes door anderen middels strategische communicatie. Thaler en Sunstein (2008) spreken van *nudging*. In de Nederlandstalige literatuur wordt van *framing* gesproken (Bruijn, 2011; Korsten, 1988). De wijze waarop een probleem of een oplossing in taal wordt uitgedrukt (ofwel geframed) bepaalt in hoge mate de beslissing. Het duiden van een probleem of een oplossing (hetzij van jezelf, hetzij van een ander) is daarmee van het grootste belang, en een belangrijk instrument voor indirecte sturing.

In het politiek-maatschappelijke debat zijn veel voorbeelden van framing en hun invloed op beslissingen te vinden. Een mooi voorbeeld is de succesvolle actie van WakkerDier om vleesproducten van de bio-industrie 'kiloknallers' te noemen. Een ander voorbeeld van framing is het duiden van energiebesparingen. Een eerste campagne luidt "*Als u energiebesparende maatregelen neemt, dan bespaart u 350 euro*". Een tweede campagne luidt "*Als u geen energiebesparende maatregelen neemt, dan kost u dat 350 euro*". Onderzoek heeft uitgewezen dat de tweede campagne veel effectiever is dan de eerste.[7]

SBR is bijvoorbeeld politiek verkocht als 'administratieve lastenverlichting voor het bedrijfsleven', terwijl het er zeker ook om gaat de uitvoeringslasten aan de publieke kant te verminderen en de kwaliteit van gegevens te verhogen. Een ander voorbeeld is de beeldvorming rondom het elektronisch patiëntendossier. Dit is eigenlijk niet één dossier, maar een infrastructuur voor het uitwisselen van medische gegevens tussen medische professionals. Het dossier is virtueel. Het zou kunnen dat de term patiëntendossier veel sneller zorgen oproept over de vertrouwelijkheid van de gegevens (privacy) dan wanneer hetzelfde systeem was gebracht als communicatieoplossing om samenwerking tussen artsen, en tussen artsen en apothekers te bevorderen en zo fouten te voorkomen. In dat geval zou wellicht de betrouwbaarheid van de gegevens op de voorgrond hebben gestaan en niet de vertrouwelijkheid.

Er is ook een andere kant van framing. Zeker binnen de publieke context kunnen bepaalde termen of mantra's 'politiek besmet' zijn, uit de mode raken of juist ineens

[7] Het voorbeeld is overgenomen van Thaler and Sunstein (2008:40)

heel populair worden. Zo is het begrip 'pilot' bij bepaalde directies een tijd lang sterk uit de gratie geweest. In plaats daarvan werden begrippen als 'praktijktoets' en 'experiment' gehanteerd.

3.3.5 *Dilemmamanagement*

De hiervoor besproken veranderstrategieën onderkennen de contextafhankelijkheid van de verandering wel, maar integreren ze niet of nauwelijks in hun aanbevelingen waardoor zij toch min of meer de vorm van een vast recept krijgen. Van Twist c.s. (1998) daarentegen zetten juist de context centraal. Zij stellen voor "*in dilemma's te denken*" bij organisatieverandering. Zij presenteren een methodiek van organisatieverandering, die verandermanagers handvatten geeft om zelf de juiste mix te bepalen. Een dilemma is een keuze tussen twee concurrerende waarden, die allebei zowel positieve als negatieve implicaties hebben (zie ook Quinn, 1998). Een keuze voor een van beide heeft dus altijd zowel voordelen als nadelen. Een voorbeeld: top-down veranderen of bottom-up veranderen? Top-down veranderen heeft als voordeel dat de door de initiator gewenste verandering wordt doorgevoerd. Over deze verandering is waarschijnlijk goed nagedacht of er is een sterke politieke wil om die verandering door te voeren. De verandering is vaak eenduidig en goed te begrijpen vanuit de initiator.

Een nadeel van top-down verandering is de mogelijke weerstand ertegen. Zij die de veranderingen moeten ondergaan zijn vaak deskundig over hun eigen werk en hebben daar een mening over. Zij voelen zich niet gekend in de verandering en kunnen zich tegen de verandering verzetten. Vaak is dat succesvol bij complexe organisaties of ketens, omdat de macht in een dergelijke keten verdeeld is. Denk bijvoorbeeld ook aan lange besluitvormingsprocessen bij grote infrastructuurprojecten zoals de A4 door Midden-Delfland, sterk vertraagd door tegenstanders en hun juridische procedures.

Bottom-up verandering heeft juist draagvlak als voordeel. Dit minimaliseert niet alleen het verzet, maar benut ook de kennis die over de keten verspreid is.
Nadeel is echter de lange duur van bottom-up veranderen en de vaak zouteloze compromissen die er het resultaat van zijn.

Tabel 3.2 –Voor en nadelen van top-down en bottom-up verandering

	Top-down	**Bottom-up**
Voordelen	-Voor initiator gewenste verandering -Eenduidigheid	-Draagvlak -Benutten van kennis
Nadelen	-Weerstand -Vertragingen	-Lange duur ontwikkeling -Zouteloze compromissen

Van Twist c.s. (1998) stellen dat het onderkennen van dilemma's essentieel is voor goed verandermanagement. Dilemma's maken oplossingen namelijk contextgevoelig. Ze laten de weerbarstigheid van problemen en oplossingen zien in complexe organisaties (en ketens). Er is dan ook geen goede of foute beslissing, hoogstens een goede of foute in een specifieke context.

Zonder het onderkennen van dilemma's is er het gevaar dat organisaties (en ketens) op lange termijn telkens van keuze verschieten: er ontstaat een cyclisch proces dat als volgt verloopt (Eeten, Bruijn, Voort, & Bueren, 2000):

- Het verandermanagement kiest optie X wegens de voordelen ervan.
- De nadelen van optie X manifesteren zich na enige tijd.
- De voordelen van optie Y lonken.
- Er volgt een reorganisatie ten gunste van optie Y.
- De nadelen van optie Y manifesteren zich na enige tijd.
- De voordelen van optie X lonken.
  Etc.

Overigens zijn wij van mening dat het veranderen van de benadering gaandeweg een verandertraject niet per se slecht hoeft te zijn, mits het maar bewust gebeurt. Het is hierbij de kunst om een arrangement te vinden dat de voordelen van de beide opties benut en de nadelen vermijdt. Voorbeelden van dergelijke arrangementen zijn:

- De keuze gevoelig maken voor tijd: een bottom-up verandering initiëren, maar na een vastgestelde tijd het resultaat ervan top-down implementeren.
- De keuze gevoelig maken voor reikwijdte van de keten: een analyse maken van de keten; op basis hiervan een selectie maken met wie bottom-up een verandering moet worden ontwikkeld; voor de overigen top-down veranderen.
- De keuze gevoelig maken voor detailniveau: top-down een verandering initiëren, maar hierin ruimte overlaten voor partijen om de verandering bottom-up gestalte te geven. Dit kan betrekking hebben op het ontwerp (zoals de 'grof fijn cyclus' van Van Amelsvoort), maar ook op het implementatieproces.

Ter verduidelijking van het 'denken in dilemma's' geven we een zestal voorbeelden van dilemma's die bij het veranderen van informatieketens een rol spelen, onderverdeeld in strategische, tactische en operationele dilemma's.

3.3.5.1 Strategische dilemma's

Een hoog of laag ambitieniveau voor het verandertraject?
Wat is het ambitieniveau? Op basis van deze beslissing kunnen onderliggende vragen worden beantwoord, zoals:

- Hoeveel actoren wil het verandermanagement bedienen? Hoe meer actoren, hoe meer wensen, hoe moeilijker standaardisatie. Veel actoren past bij een (soms te) hoog ambitieniveau. Te weinig actoren leidt niet tot de gewenste adoptie en schaalgrootte om representatief te zijn voor de rest van de sector. Eenzelfde mechanisme geldt voor de grootte van actoren: het niet betrekken van grote, machtige actoren kan standaardisatie vergemakkelijken, maar opschaling bemoeilijken.
- Over welk soort informatie moet het gaan? Als het om informatie diep in de bedrijfsprocessen gaat, dan getuigt dat van een hoog ambitieniveau. Deze informatie is namelijk sterk veranderlijk en daarom moeilijk te standaardi-

seren. Als het bijvoorbeeld 'slechts' gaat om sterk geaggregeerde, bedrijfseconomische gegevens van een gehele sector over een lange termijn, dan getuigt dat van een lager ambitieniveau.

- Op welke wijze wordt ICT geïmplementeerd? Op een *door-to-door* wijze of wordt het ook tot in de bedrijfssystemen doorgevoerd? Bij de eerste manier zijn veelal minder voordelen te behalen, maar zijn de consequenties voor de organisaties vaak ook minder. In het laatste geval zijn meer voordelen te halen, maar zijn de vereiste veranderingen ook groter en complexer.
- Worden bestaande standaarden gebruikt of worden nieuwe 'standaarden' ontwikkeld? Het eerste is een veilige manier waarop bestaande standaarden gebruikt kunnen worden. De vraag is of deze bestaande standaarden ver genoeg gaan om de beoogde voordelen te bereiken. Bij het ontwikkelen van nieuwe standaarden wordt een zeker risico aangegaan. Deze moeten niet alleen ontwikkeld worden, met alle complexiteit en additionele activiteiten van dien, de vraag is ook of al deze standaarden door de markt geadopteerd zullen gaan worden of dat de keten zich later zal moeten aanpassen aan een nieuwe standaard.

Feitelijk geldt hier het dilemma of het een 'groots en meeslepend' verandertraject moet worden of een 'klein en wendbaar' traject (Bruijn, Wagenaar, Voort, & Wendel de Joode, 2004). De voor- en nadelen volgen uit deze voorstelling van zaken: een hoog ambitieniveau heeft een hogere faalkans en is weinig flexibel, maar als het succesvol wordt ingevoerd dan zijn de efficiencywinsten waarschijnlijk talrijk en fors. Een laag ambitieniveau geeft een wendbaarder traject, met meer mogelijkheden door te leren middels '*trial and error*'. Het is echter de vraag of realisatie van de verandering een einde is of het begin van nog een lange reeks volgende projecten. De efficiencywinst zal in ieder geval bescheiden zijn. Weening (2006) formuleerde het zo: "*alles of niets*" of "*niets meer en niets minder*".

Een brede of smalle scope van het verandertraject?
De scope van een verandertraject bepaalt wat tot het verandertraject gerekend mag worden en wat niet. Bij afbakeningen van de scope kan het gaan over de tijdspanne waarin de verandering moet worden vormgegeven en uitgevoerd, maar het kan ook gaan over de hoeveelheid actoren (of schakels) die door de verandering geraakt zullen worden. Over het algemeen geldt dat een brede scope de attentie van velen kan trekken, waardoor het verandertraject geld kan genereren van bestuurders en omgeving en waardoor ook de kwaliteit van het verandertraject kan verbeteren. Attentie van velen geeft immers ook kansen voor het benutten van hun deskundigheid. Beheersbaarheidsproblemen vormen echter een groot nadeel van een brede scope. Een grote hoeveelheid actoren over een lange tijd is niet gemakkelijk aan te sturen. Bovendien wordt het op den duur onduidelijk wat bij het verandertraject hoort en wat niet, wat de beheersbaarheid ook niet ten goede komt.

3.3.5.2 Tactische dilemma's

Richten op early adopters of volgers?
Met early adopters is het mogelijk om veel te leren over hoe de nieuwe keten het beste ingericht kan worden. Bovendien kunnen zij bij succes als voorbeeld dienen voor anderen. Het te veel richten (of: een eenzijdige focus) op deze groep heeft echter

als gevaar dat de volgers feitelijk achterblijvers worden. Ofwel kunnen zij het tempo niet volgen, omdat er te veel wordt gelet op hen die toch al geïnteresseerd en kundig waren, ofwel zien zij er na verloop van tijd toch geen brood in (zie het strategisch gedrag, met name '*wait and see'* en *'free riding'*). Er ontstaat een wij-zij gevoel, met als risico dat binnen de early adopters het contact met de 'stroperige' realiteit wordt verloren, waarbij er sprake kan zijn van groupthink (Janis, 1972). Het richten op volgers garandeert dat de groep gebruikers bij elkaar blijft. Nadeel is echter dat het ambitieniveau slechts zo hoog wordt als de langzaamste volger. Het risico bestaat dat er op die manier weinig wordt geïnnoveerd.

Zelf ontwikkelen of softwareleveranciers laten doen?
Het ontwikkelen van software is kennisintensief en het lijkt logisch ontwikkeling uit te besteden aan hiertoe gespecialiseerde softwareontwikkelaars en -leveranciers. 'Leveranciersdominantie' ligt echter op de loer, namelijk het gevaar dat softwareleveranciers hun kennispositie kunnen benutten om de transactie met de klant naar hun hand te zetten. Er ontstaat een eenzijdige afhankelijkheidsrelatie met de leverancier. Een klassiek voorbeeld van 'leveranciersdominantie' is de verkoop van een gebruikte auto aan een klant die de technische kennis mist om het product te beoordelen.

Bij SBR bestaat er een dergelijke eenzijdige afhankelijkheidsrelatie tussen softwareleveranciers en sommige intermediairs. Het gevaar is dat softwareleveranciers niet overgaan op SBR, waardoor intermediairs niet in SBR kunnen aanleveren. Zelf hebben intermediairs meestal niet de capaciteit om software te ontwikkelen. Dit kan de SBR-organisatie ondervangen door ontwikkeling zelf ter hand te nemen, bijvoorbeeld middels open source software. Leveranciersdominantie wordt zo voorkomen. Nadeel is dat de deskundigheid van softwareleveranciers wel eens gemist kan worden. Bovendien verzorgt fiscale software niet enkel rapportagefunctionaliteit, maar ook workflow, termijnbewaking, koppeling met fiscale kennis en koppeling met andere software – veel van deze functionaliteiten worden vooralsnog niet in open source software ondersteund. Een fundamentele onderliggende vraag voor de overheid hierbij is bovendien wat zij zelf moet doen en wat moet worden overgelaten aan de markt.

3.3.5.3 Operationele dilemma's

Reduceren of uitbreiden van alternatieven van aanlevering?
Aanleveren van informatie kan via verschillende kanalen (zoals SBR, het ondernemersportaal, pdf of e-mail). Voor standaardisatie is het van belang dat het aantal formats beperkt blijft. Algemener geldt dat hoe hoger het detailniveau van standaarden, des te meer efficiencywinst er te behalen valt. Nadeel is dat een hoog detailniveau (ofwel een sterke reductie van opties) de hoge investeringen in de back office sterk naar voren haalt in de tijd. De informatieleverende partijen worden voor het blok gezet: nu diep investeren of tegenwerken (door bijvoorbeeld lobby tot en met het parlementaire niveau). Dit vormt een politiek risico. Zolang er meerdere substituten voor aanlevering blijven, zal de weerstand beperkter zijn. Het wordt dan evenwel wel een stuk lastiger om de belofte tot efficiency gestand te doen. Dit voorbeeld laat zien dat de wijze waarop met een operationeel dilemma wordt omgegaan – hoeveel aanleverkanalen worden er opengesteld – grote consequenties kan hebben voor een programma als SBR.

Blijven vernieuwen of bevriezen van de interfaces?
Nieuwe technische mogelijkheden zullen er altijd zijn. Het is aantrekkelijk om te blijven vernieuwen en de nieuwe mogelijkheden te benutten. Ook hier ligt efficiencywinst in het verschiet, maar is het onduidelijk wanneer en door wie de winst kan worden genoten. Een argument voor de tegenhanger is de mogelijkheden voor gebruik van het bereikte bij andere sectoren (ofwel 'hergebruik'). Hergebruik maakt investeringen van de overheid rendabeler.

3.3.6 *Dimensies van verandering*

Voorgaande lijst met veranderstrategieën is niet uitputtend. Er zijn verschillende varianten extra te noemen. Uit de lijst is wel een aantal belangrijke dimensies te deduceren, die relevant zijn voor ketenverandering. Op basis van deze dimensies kunnen verandermanagers zelf allerlei varianten bedenken:

- Dimensie 1. Top-down of bottom-up veranderen?
  Wordt de verandering geïnitieerd door een enkele partij namens de partij die zich als 'top' afficheert? Of wordt ingezet op ideeën voor verandering bij medewerkers c.q. niet-initiërende actoren in de keten?
- Dimensie 2. Vraag- of aanbodgedreven?
  Een voorbeeld van vraaggedreven veranderingen wordt vertegenwoordigd door de 'deblokkadebenadering' bij direct verandermanagement. Er is een breed gedragen probleem dat veel partijen opgelost willen zien. Een aanbodgedreven verandering is bijvoorbeeld geïnspireerd door nieuwe (bijvoorbeeld technologische) mogelijkheden, waarvan nog niet iedereen zich bewust is. In die situatie is er nog nauwelijks een vraag, maar zijn er wel mogelijkheden vanuit de aanbodkant.
- Dimensie 3. Inhoudelijk of procesmatig veranderen?
  Sommige benaderingen gaan uit van een ontwerp door deskundigen (hetzij experts, hetzij medewerkers). Dat moet vervolgens conform ontwerp worden geïmplementeerd. Andere benaderingen benadrukken eerder het proces waarbinnen veranderingen gestalte moeten krijgen. Binnen zo'n proces worden ideeën voor veranderingen bedacht, die van tevoren niet bedacht zouden kunnen zijn, zo is de theorie. Van tevoren is er dan minder sprake van een inhoudelijk ontwerp, maar het inhoudelijke ontwerp wordt gedurende een proces geleidelijk ontwikkeld.
- Dimensie 4. Veranderen van resultaat of veranderen van condities?
  Veranderen van A naar B kan als zowel A als B bekend zijn en de condities om B te behalen gunstig zijn. Veel vormen van procesmanagement, *framing* en het veranderen van de ketenstructuur zijn echter niet gericht op het behalen van B, maar het verbeteren van condities om veranderingen door te voeren. Er wordt eerst gewerkt aan voorwaarden voor verandering. Voorwaarden kunnen gelegen zijn in de ketenstructuur, in onderling vertrouwen of zelfs in taalgebruik.
- Dimensie 5: Probleemgestuurd of oplossingsgestuurd?
  Dilemmamanagement gaat dieper in op de keuzerichtingen voor ketenherinrichting. B is als het ware het probleem in plaats van de ster in het oosten. In tegenstelling tot direct verandermanagement en het veranderen van ketencondities wordt B als een probleem gezien en niet als een op voorhand

bekende oplossing. Een goede strategie is als het ware in het probleem besloten. De andere twee benaderingen zijn meer oplossingsgericht: probleemformulering wordt hierin gezien als een gepasseerd station.

Een benadering kan zo een configuratie zijn van keuzes op de dimensies. Zo kan verandermanagement oplossingsgestuurd, inhoudelijk, aanbodgedreven en top-down zijn, inhoudelijk, vraaggedreven, bottom-up, gericht op condities zijn, etc. Het is aan het verandermanagement zich bewust te zijn van de positie die zij op de verschillende dimensies inneemt en welke voor- en nadelen hieraan kleven.

3.4 Sturingsinstrumenten

Sturingsinstrumenten zijn de werkstructuren aan de hand waarvan een verandering wordt aangestuurd. Het gaat hier om middelen die ingezet kunnen worden om de partijen in de keten te bewegen of aan te zetten iets te doen of iets na te laten. Er is in het verandermanagement een verschuiving zichtbaar geworden van het gebruik van meer klassieke hiërarchische instrumenten (denk aan het top-down verplichten binnen een bestaande organisatie) naar meer interactieve benaderingen, waarin het accent ligt op de betrokkenheid van meerdere partijen en de min of meer gezamenlijke verandermechanismen. De Bruijn en Ten Heuvelhof (1994) hebben het over de zogenaamde 'tweede generatie instrumenten'. Een instrument van de tweede generatie kan worden omschreven als een instrument dat de barrières verdisconteert die een gebruiker in haar veranderactiviteiten ontmoet (Ibid., p.13). Het gaat dan om de maatschappelijke pluriformiteit, de geslotenheid en autonomie van betrokken actoren en om de interdependenties tussen actoren, zowel publieke als private. We bespreken vier van deze tweede generatie-sturingsinstrumenten, die in onze praktijkvisie meestal bij ketenveranderingen worden gebruikt:

- Procedures
- Projecten
- Programma's
- Processturing

Bovenstaande sturingsinstrumenten verschillen op een aantal punten. Een overzicht hiervan wordt in tabel 3.3 gegeven en vervolgens uitgediept.

Tabel 3.3 – Overzicht van sturingsinstrumenten

	Doel	Kenmerkend	Druk	Processen
Procedureel	Onderhoud	Afhandelend	Efficiëntie	Star
	Bedrijfsresultaat	Methodisch gebonden	Zorgvuldigheid	Uitgebalanceerd
	Service levels	Repetitief	Functioneren van de keten	Quality control points
Project	Vernieuwing	Realiserend	Resultaat onzekerheid	Flexibel
	Performance/ Business case	Tijdsgebonden	Tijdigheid	Resultaatgericht
	Acceptatiecriteria	Uniek	Integratie met de keten	Fases
Programma	Heroriëntatie	Inrichtend	Organisatorische onzekerheid	Open
	Positie/Voortbestaan	Verandering gebonden	Sunk costs (costs in brede zin)	Verandering gericht
	Blauwdruk/Visie	Onomkeerbaar	Verandering van de keten	Plateaus
Processturing	Agendering	Richtend	Maatschappelijke onzekerheid	Open
	Draagvlak creatie	Verbinding gebonden	Veranderbehoefte	Kennis gericht
	Collectief leren	Conceptueel	Positioneren	Ronden

3.4.1 *Procedures*

Het eerste sturingsinstrument dat vaak bij ketenveranderingen wordt toegepast is de procedure. Een procedure is een zeer specifieke beschrijving van een proces dat doorlopen dient te worden of een middel dat ingezet kan worden voor de realisatie van een specifiek doel. Dit is het meest rigide en directieve sturingsinstrument in de tabel. Het doel is om op een zo efficiënte en effectief mogelijke manier een verandering door te voeren. Uitgangspunt hier is dat er al duidelijke en concrete afspraken op ketenniveau zijn gemaakt over het toepassen van de procedure. Om ruis en verkeerde informatie te voorkomen is het noodzakelijk de procedures zo concreet mogelijk te maken. Procedures zijn meestal beproefd en gebaseerd op ervaringen. Een procedure kan alleen worden vastgelegd als er duidelijkheid bestaat over het effect van een handeling of product op een specifieke variabele. Dit sturingsinstrument is '*off the shelf*' te gebruiken en bevat veelal een bijsluiter – een gedetailleerde beschrijving van de logica (oorzaak en gevolg), de stappen die gevolgd dienen te worden en de mogelijke bijwerkingen.

3.4.2 *Projecten*

Het tweede sturingsinstrument dat vaak bij ketenveranderingen wordt toegepast is het project. Een project is een niet-routinematige, niet-herhaalbare, eenmalige activiteit met een begin en eind, een duidelijk omschreven doel en afzonderlijke doelstellingen m.b.t. prestaties, kosten en tijdsduur, waaraan bepaalde risico's zijn verbonden. De identificatie van risico's is belangrijk, aangezien er nog enige onzekerheid bestaat over de doelen en middelen. Dit sturingsinstrument biedt ten opzichte

van een procedure meer vrijheidsgraden voor de uitvoering. Vijf aannames over projecten zijn (Hedeman, Vis van Heems, & Fredriksz, 2009):

1. Projecten worden uitgevoerd in een beheerste omgeving.
2. Een project is pas succesvol als alle betrokken partijen tevreden zijn met het projectresultaat (en daarbij hebben vaak de gebruikers de meeste invloed op de mening van de andere partijen).
3. Succesvolle projecten zijn *'business driven'*.
4. Samenwerking tussen alle bij het project betrokken partijen leidt tot meer succesvolle projecten.
5. Wat werkt wordt door de praktijk bepaald.

3.4.3 *Programma's*

Het derde sturingsinstrument dat vaak bij ketenveranderingen wordt toegepast is het programma. Hedeman & Vis van Heemst (2011) definiëren een programma als *"het geheel van samenhangende projecten en activiteiten in een tijdelijke organisatie om een of meer van te voren gedefinieerde doelstellingen te realiseren die van strategisch belang zijn" (p.163).*

Twee punten vallen op in deze definitie: (1) het gaat om meerdere projecten en (2) het gaat om het realiseren van strategische doelstellingen. We lichten beide punten toe.

Ten eerste gaat het om meerdere, samenhangende projecten. Over het algemeen zijn de resultaten van meerdere samenhangende projecten nodig om de programmadoelstellingen te kunnen realiseren. De doorlooptijd van een programma is hierdoor langer dan van de afzonderlijke projecten. De afhankelijkheid van de projectresultaten maakt het lastig om vooraf te bepalen wanneer een programma zal eindigen. Hierdoor zullen betrokkenen een afweging moeten maken in hoeverre de investeringen in de ketenverandering de daarmee op te brengen baten nog rechtvaardigen.

Een tweede punt dat opvalt is de scope – programma's concentreren zich rond strategische doelstellingen. Deze worden meestal vastgelegd in een visiedocument en vertaald in een blauwdruk voor de SOLL-situatie. Zoals we eerder in dit hoofdstuk hebben beschreven gaat de realisatie van strategische doelstellingen vaak gepaard met ingrijpende veranderingen in de keten. Dit betekent dat verschillende verandergrootheden worden geraakt gedurende de looptijd van een programma.

3.4.4 *Processturing*

Processturing is van een andere orde dan de eerder beschreven programma's, projecten en procedures. Processturing kent als uitgangspunt dat vele actoren belangen hebben bij een issue en dat zij allen hun eigen probleempercepties en (deel)oplossingen hebben. Processturing wil in principe recht doen aan deze belangenconstellatie en verschillende percepties. Partijen zijn immers toch tot elkaar veroordeeld. Binnen processturing kan onderscheid worden gemaakt tussen twee vormen: directe en indirecte processturing.

Directe processturing is een sturingsinstrument om actoren te beïnvloeden in een tevoren vastgestelde richting. Actoren moeten, vanuit het perspectief van het verandermanagement, worden geleid van huidige situatie A naar gewenste situatie B. Het organiseren van interactieve processen is hiertoe slechts een middel. De processen zijn nodig om bij wijze van spreken aan actoren uit te leggen waarom B een gewenste situatie is.

Indirecte processturing is een sturingsinstrument om actoren rijp te maken voor verandering, zonder dat een einddoel duidelijk is vastgesteld. Processturing is erop gericht een proces te ontwerpen en te managen, dat die actoren met hun problemen en hun oplossingen laat interacteren en tot nieuwe, gemeenschappelijke problemen en oplossingen laat komen. De Bruijn c.s. (2008) wijzen op belangrijke leereffecten van processen. Door interactie leren actoren over zowel de inhoud van een probleem als over het gedrag van andere actoren. Bovendien hebben interactieve processen de kwaliteit om actoren met elkaar te verbinden. Een goed georganiseerd proces kan leiden tot vertrouwen tussen actoren en een blijvend commitment om een probleem op te lossen.

Het einddoel wordt gedurende het proces geleidelijk vastgesteld. Aldus is een proces tot op zekere hoogte doelzoekend. Dit kost in veel gevallen de nodige tijd, uitgebreid onderzoek, en het werk van velen voordat er van een probleem gesproken kan worden dat in termen van handelingsopties, preferenties en keuzes kan worden bediscussieerd. Deze dynamische verhouding tussen problemen, oplossingen en actoren en de kans dat deze op het juiste moment op de juiste wijze aan elkaar worden gekoppeld, is op theoretisch niveau beeldend beschreven. Bekend is de metafoor van de '*Garbage can'* om de wisselwerking tussen problemen, oplossingen en actoren te beschrijven (Cohen, March, & Olsen, 1972). Volgens dit model deponeren actoren hun problemen en oplossingen, op de momenten die voor hen opportuun zijn, in de 'vuilnisbak' van een lopend besluitvormingsproces. Voor verandering is cruciaal dat de actoren combineerbare oplossingen en problemen op eenzelfde moment in dezelfde vuilnisbak deponeren. Dan wordt een koppeling mogelijk en ontstaan er belangrijke kansen voor sturing.

3.5 Acceptatie van veranderingen

3.5.1 *Het concept acceptatie*

Acceptatie definiëren wij als de *aantoonbare bereidheid van een ketenpartij*[8] *om een verandering te steunen en te realiseren*. Acceptatie is geen vanzelfsprekendheid, als gevolg van het feit dat veranderingen in informatieketens plaatsvinden in een dynamische, multi-actor context. Daaruit volgend kunnen mogelijke oorzaken voor het gebrek aan acceptatie zijn:

[8] Vaak wordt acceptatie op het niveau van de individuen bepaald. Aangezien we binnen deze context van ketenpartijen spreken – die in een bestuur worden vertegenwoordigd door een individu – hebben we het over de acceptatie door een ketenpartij.

- Ketenpartijen verschillen in de organisatiedoelen die zij hebben. Vanuit hun optimale doelbereiking zullen ketenpartijen verschillende voorkeuren hebben ten aanzien van een verandering.
- Ketenpartijen kunnen verschillen in startpositie (de A-situatie), bijvoorbeeld in de mate waarin zij geautomatiseerd werken. Daardoor kan de impact van de verandering – en daaruit volgende voorkeuren – verschillen.
- Het kan zijn dat een ketenpartij kosten moeten maken om de verandering te implementeren, terwijl de baten vallen bij een andere ketenpartij.

Indien één of meerdere ketenpartijen de verandering niet accepteren (bijvoorbeeld vanwege één van de bovengenoemde oorzaken) kan het wenselijk zijn om de acceptatie te bevorderen. De verschillende veranderstrategieën en sturingsinstrumenten beschreven in het hoofdstuk zijn hier feitelijk allemaal op gericht.

Veel factoren beïnvloeden acceptatie. Denk bijvoorbeeld aan factoren die zien op de eigenschappen van de verandering zoals voordelen voor de ketenpartij, interoperabiliteit, experimenteerbaarheid en omkeerbaarheid (Rogers, 2003). Maar ook factoren als gepercipieerde risico's, vertrouwen (in het gremium en sturingsinstrument) en communicatie over verandering kunnen hier een rol spelen (Clark, Cavanaugh, Brown, & Sambamurthy, 1997). Door de invloed van deze factoren, die verschillen bij elke verandering, kan het lastig zijn om erachter te komen hoe acceptatie bevorderd kan worden.

Op basis van literatuur werken we een denkraam uit dat kan worden gebruikt om de condities voor acceptatie tastbaar (grijpbaar) en inzichtelijk te maken. Gedurende de verandering kan het denkraam helpen om de oorzaak achter gebrek aan acceptatie te achterhalen.

3.5.2 *Denkraam rondom acceptatie*

Merchant en Van der Stede (2003) onderscheiden drie beheers- en bestuurbaarheidsproblemen, te weten gebrek aan richting ('weten', of 'kennen'), gebrek aan competentie ('kunnen') en gebrek aan motivatie ('willen'). Dit onderscheid passen we toe op een verandering van een informatieketen.

Tabel 3.4 –Kennen-kunnen-willen toegepast op de inschatting die een ketenpartij maakt over een voorgestelde verandering

	Definitie
Kennen	De mate waarin de ketenpartij zekerheid heeft over de interne voorwaarden en impact van de implementatie van de voorgestelde verandering in de eigen context.
Kunnen	De mate waarin de ketenpartij overtuigd is competenties en middelen ter beschikking te hebben om de verandering te implementeren.
Willen	De mate waarin de ketenpartij overtuigd is dat de voorgestelde verandering bijdraagt aan het kosteneffectief behalen van de door de ketenpartij gestelde doelen.

De ketenpartij baseert zich op het 'kennen' bij het inschatten van het 'kunnen' en het 'willen'. Voor het 'kunnen' geldt dat met name het gebrek aan competenties en middelen blokkades kunnen vormen om de verandering te realiseren. Het 'willen' is de belangrijkste drijvende kracht achter de acceptatie. De overtuiging dat de verande-

ring een sterkere bijdrage levert aan de gestelde doelen zal leiden tot een hoge acceptatie. De inschatting of overtuiging dat een verandering juist tegengesteld is aan de doelen, zal leiden tot een lage acceptatie. Metselaar & Cozijnsen (2005) spreken in dit kader ook wel van veranderingsbereidheid.
Bij de dialoog over de verandering (en acceptatie) kan dit denkraam worden ingezet om de oorzaak achter gebrek aan acceptatie te achterhalen.

Besturingsproblemen volgens Merchant en Van der Stede (2003):

1. Gebrek aan richting (kennen): gebrek aan kennis over het 'wat' en het noodzakelijke 'hoe'.
2. Gebrek aan competenties (kunnen): kan voortvloeien uit een tekortschieten in kennis, ervaring of vaardigheden, maar kan ook zijn oorsprong vinden buiten de persoon, bijvoorbeeld in een gebrek aan operationele informatie.
3. Gebrek aan motivatie (willen): om organisatieleden de gewenste prestatie te laten leveren dienen zij daartoe en motivatie te hebben.

Het object van verandering kan betrekking hebben op een veelheid aan dimensies. Denk bijvoorbeeld aan processen, techniek, organisatie (structuur, cultuur) of afspraken over samenwerking. Een ketenpartij die een voorgestelde verandering niet accepteert kan inzichtelijk maken welke dimensie(s) van een verandering zij de verandering niet accepteert. Langs het kennen-kunnen-willen kan de ketenpartij inzichtelijk maken of de impact voor de verandering in de eigen context niet helder is, of zij niet denken over de benodigde competenties en of middelen te beschikken, en/of dat zij niet gemotiveerd zijn om de verandering door te voeren.

Afhankelijk van wat de oorzaak van gebrek aan acceptatie is, zijn er verschillende benaderingen om acceptatie te bevorderen. Te denken valt aan het wegnemen van blokkades door het ondersteunen van partijen of juist het motiveren van partijen. In hoofdstuk 4 zullen we enkele voorbeelden zien van de toepassing van dergelijke benaderingen bij het doorvoeren van bepaalde typen veranderingen.

3.6 Afsluiting

Dit hoofdstuk biedt inzicht in de complexiteit van verandering in ketens. Kenmerkend is dat, gezien de afhankelijkheden en verschillende belangen in ketens bij veranderingen, het niet onwaarschijnlijk is dat één of meerdere actoren weerstand hebben tegen de verandering. Hierdoor kan de algemene acceptatie van de verandering een uitdaging zijn.

We weten dat acceptatie belangrijk is, maar hebben tot dusver nog weinig gezegd over wat er geaccepteerd moet worden (veranderobject), welke factoren invloed hebben op acceptatie en welke besturingsvorm je hierbij nodig hebt. Hoofdstuk 4 (Het besturingsvraagstuk van keteninformatiesystemen) gaat dieper in op deze aspecten.

4 Het besturingsvraagstuk van keteninformatiesystemen

4.1 Inleiding

De voorgaande hoofdstukken bieden inzicht in keteninformatiesystemen en afhankelijkheden. Met name wanneer er wijzigingen in een keten moeten worden doorgevoerd, worden deze afhankelijkheden manifest. Keteninformatiesystemen hebben voortdurend met wijzigingen te maken. Wijzigingen in keteninformatiesystemen (we nemen SBR als voorbeeld) kunnen uiteenlopen van het upgraden van de software bij de gedeelde dienstverlener of het implementeren van een nieuwe versie van de taxonomie tot de implementatie van SBR bouwblokken[9] in een nog niet geïntegreerde verantwoordingsketen. Wijzigingen kunnen verschillende actoren raken en moeten

[9] Hoofdstuk 1 bevat een overzicht van de SBR bouwblokken.

bestuurd worden. Het bepalen wie (welke ketenactoren) een wijziging in een keteninformatiesysteem op welke manier (veranderstrategie en sturingsinstrument) moet besturen, noemen we het besturingsvraagstuk.

Het steeds juist beantwoorden van het besturingsvraagstuk is een substantieel onderdeel gebleken van de opgave waar de betrokkenen bij SBR mee te maken hadden. Ook in andere informatieketens loopt men tegen de complexiteit van het besturingsvraagstuk aan. Het doel van dit hoofdstuk is om lezers, die met wijzigingen in ketens te maken hebben, een handvat te bieden voor het beantwoorden van het besturingsvraagstuk.

Onlosmakelijk verbonden met het besturingsvraagstuk is het begrip governance. Afspraken over wie er op welke manier betrokken zijn bij een wijziging zijn onderdeel van de governance. Daar waar het gaat om een organisatie-overstijgend besturingssysteem, spreken wij over de ketengovernance. In principe geeft een toereikende ketengovernance voor zoveel mogelijk wijzigingen antwoord op het besturingsvraagstuk.

Als we in de literatuur op zoek gaan naar kennis en begrip over het besturingsvraagstuk, dan valt op dat een integrale behandeling van het vraagstuk ontbreekt. Een substantieel deel van de literatuur gaat over het besturen van wijzigingen in informatiesystemen (zie bijv. Thiadens, 2008), maar niet over ketens. Literatuur over keteninformatiesering (Grijpink, 2010) en ketenmanagement (Duivenboden et al., 2000) scherpt de geest, maar biedt geen concrete aanwijzingen waaruit we kunnen opmaken welke afspraken er zouden moeten zijn omtrent wijzigingen. Best practices voor IT-governance zijn waardevol, maar gaan er vaak vanuit dat de wie-vraag (wie zijn betrokken bij het besturen van de wijziging) al beantwoord is.

Teneinde actoren die met wijzingen in ketens te maken hebben een handvat te bieden voor beantwoording van het besturingsvraagstuk, beschrijft dit hoofdstuk achtereenvolgens:

1. Wat het object van wijziging binnen keteninformatiesystemen is. Wat bij deze theoretische beschouwing opvalt, is het tweedimensionale karakter van wijzigingen. Bij een wijziging verdienen zowel de dimensie technologie als governance aandacht. We (h)erkennen vaak alleen de technologische wijziging, niet de eventuele wijziging van de ketengovernance (§ 4.2).
2. Twee essentiële vragen in het licht van besturing van wijzigingen. We komen erachter dat de bekendheid van de situatie nádat de wijziging is doorgevoerd (de B-situatie) en de dimensies waarop de wijziging betrekking heeft (technologie en/of ketengovernance) bepalend zijn voor de besturing van de wijziging (§ 4.3). Nieuwsgierige lezers kunnen alvast een blik werpen op figuur 4.3.
3. Het besturingsvraagstuk voor wijzigingen waarvoor de B-situatie bekend is. We behandelen vier typologieën (§ 4.4).
4. Het besturingsvraagstuk voor wijzigingen waarvoor de B-situatie niet bekend is. Het besturingsvraagstuk is lastig (zo niet onmogelijk) te beantwoorden. We behandelen drie scenario's (§ 4.5).

Bovenstaande punten vormen de indeling van de rest van dit hoofdstuk. We werken toe naar een handvat. Kanttekening hierbij is dat dit hoofdstuk niet beschrijft hoe de ketengovernance in SBR er nu uitziet. Dat gebeurt in hoofdstuk 9.

Tot slot is het van belang dat we vanwege de leesbaarheid enkele begrippen vooraf kort definiëren. Onder de besturing van de wijziging verstaan we de ketenactoren die betrokken zijn bij de wijziging en de manier waarop zij de wijziging besturen. Onder het besturen van de wijziging verstaan we de activiteiten die ketenactoren uitvoeren in het kader van de besturing. De bekende oneliner die het begrip besturen tot leven brengt, is "*steering, not rowing*" (Osborne & Gaebler, 1992). Ten slotte verstaan we onder het bestuur de ketenactoren die de wijziging besturen.

4.2 De relatie tussen governance en technologie

Er is veel onderzoek gedaan naar afhankelijkheden binnen systemen in het algemeen en informatiesystemen in het bijzonder. Eén van de theorieën die hieruit voorkomt is de contingentietheorie (Donaldson, 2001; Galbraith, 1973; Gresov, 1989). Centraal binnen deze theorie staat het identificeren van contingenten – factoren die fluïde zijn en elkaar beïnvloeden. Twee contingenten binnen informatiesystemen zijn governance en technologie[10] (Brooks, 2006; Sambamurthy & Zmud, 1999). De volgende paragrafen zoomen in op governance en technologie als afzonderlijke aspecten. Daarna staan we stil bij de samenhang tussen beide begrippen.

4.2.1 *Governance*

Governance is een populair begrip. Zowel in de Nederlands- als Engelstalige literatuur wordt steeds vaker naar deze term gegrepen om een uiteenlopend spectrum van handelingen en structuren te duiden. Politici, bestuurders, managers, architecten, auditors en anderen zijn allemaal dol op dit begrip. Het leent zich zowel voor verwijzing naar 'het probleem' (bad governance) als de oplossing (good governance). In de bestuurskundige literatuur wordt soms de term governance – in plaats van government – gebruikt om te benadrukken dat de overheid opereert in een multi-level en multi-actor krachtenveld, waarin het afhankelijk is van meerdere partijen voor de realisatie van doelstellingen (Rhodes, 1996).

Het begrip lijkt een brede reikwijdte te hebben. Door de sterke intuïtieve aantrekkingskracht, worden nauwkeurige definities zelden nodig geacht (Lee, 2003). Aangezien we in dit boek vaker terugvallen op dit begrip, is het zaak dat we deze wat preciezer definiëren. De aanpak die we hiervoor volgen is pragmatisch: we kijken eerst naar enkele definities uit de literatuur (zowel binnen als tussen organisaties) en kiezen een definitie die bij de context van dit hoofdstuk (informatieketens) past. We slaan de verkenning van de literatuur over governance in de organisatorische context niet over, omdat:

[10] Soms wordt er verwezen naar de architectuur (blauwdruk) van de technologie. Echter, ook kan worden verwezen naar de architectuur van de governance (zie bijv. Gulati & Singh, 1998). In beide gevallen gaat het om een verwijzing naar het ontwerp. Wanneer we specifiek verwijzen naar het ontwerp van de governance of technologie, zullen we spreken over de 'architectuur'.

- De literatuur over governance binnen organisaties meer inzicht geeft in de functie van governance, waar de literatuur over governance in de interorganisatorische context juist de nadruk legt op de complexiteit van governance.
- Er gewoonweg nog weinig onderzoek verricht is naar governance in een interorganisatorische context in relatie tot informatiesystemen (Pardo, Gil-Garcia, & Burke, 2008).

We kunnen uiteraard niet in één hoofdstuk alle relevante aspecten van governance belichten. Voor een bredere uiteenzetting van governance kunt u onder meer Brown & Grant (2005), Lee (2003) en Stoker (1998) raadplegen.

Enkele definities van governance in ketens

- "*Governance implies arrangements in which public as well as private actors aim at solving problems or create societal opportunities, and aim at the care for the societal institutions within which these governing activities take place*." Kooiman (2000: p. 139)
- "*Governance refers to the solutions that individuals and organizations devise for problems of coordination*". Markus & Bui (2012: p. 164)

We beginnen bij de literatuur over governance binnen een organisatie. Ook hier zijn er veel domeinen en definities te onderscheiden. Aangezien we binnen de context van keteninformatiesystemen schrijven en later iets over de relatie tussen governance en technologie willen zeggen, zoeken we in de hoek van 'information system/technologie governance'. Het onderzoek van Peter Weill en Jeanne Ross van MIT op dit gebied wordt hierbij vaak geciteerd. Hun onderzoek onder 250 bedrijven in 23 landen concludeert dat governance cruciaal is om voordelen uit (IT) investeringen te behalen. Sterker nog, top presterende bedrijven onderscheiden zich door een zorgvuldig vormgegeven governance (Weill & Ross, 2005). Weill (2004) hanteert de volgende definitie voor IT governance: *"specifying the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT"* (p. 3). Deze definitie benadrukt twee dingen:

1. Het specificeren (in afspraken vastleggen) van taken en bevoegdheden is belangrijk.
2. Governance moet 'gewenst gedrag' stimuleren.

Weill verruimt deze definitie door een vergelijking met de term IT Management: "*IT governance is not about what specific decisions are made. That is management. Rather, governance is about systematically determining who makes each type of decision (a decision right), who has input to a decision (an input right) and how these people (or groups) are held accountable for their role*" (p. 3).
Volgens Weill en Ross geeft een effectieve governance antwoord op de volgende vragen omtrent de beslissingsbevoegdheden:

- Welke beslissingen moeten genomen worden om te zorgen voor effectief gebruik en management van (ICT) voorzieningen?
- Wie moet deze beslissingen nemen?
- Hoe moeten deze beslissingen genomen worden en op welke wijze worden zij bewaakt?

Beantwoording van deze vragen gebeurt langs afstemmings-/interactieprocessen. Het resultaat hiervan is een verdeling/allocatie van besluitvormingsbevoegdheden.

Deze bevoegdheden kunnen deels worden geëxpliciteerd aan de hand van een organisatiestructuur (Mintzberg, 1992). De term organisatiestructuur kan hier verwarring scheppen, aangezien het ook om de structuur van een programma of project kan gaan. Essentieel is de verdeling die in een structuur (of architectuur) te vangen is. Sambamurty & Zmud (1999) voegen op basis van praktijkvoorbeelden hieraan toe dat de meest efficiënte en effectieve verdeling van beslissingsbevoegdheden niet ad-hoc, maar conform bepaalde 'governance arrangements', oftewel afspraken, plaatsvindt. Deze afspraken bevatten de collectieve kennis, normen en voorkeuren van de actoren over hoe de verdeling tot stand komt en veranderd kan worden.

Ook in een interorganisatorsche (multi-actor) omgeving spelen bovenstaande vragen over beslissingsbevoegdheden en zijn afspraken nodig. Actoren zijn dan niet per se alleen belanghebbenden (stakeholders) binnen de organisatie, maar gedelegeerde functionarissen vanuit verschillende organisaties die onderdeel vormen van een keteninformatiesysteem. In de literatuur over governance in een multi-actor omgeving wordt in definities voor het begrip governance vaak veel nadruk gelegd op het gezamenlijk/collectief oplossen van problemen (zie kader). Het begrip probleem is hier een wat nauwe en wellicht negatieve focus. Governance gaat namelijk ook over beslissingen omtrent hardware en software, prioriteiten, planningen en bekostiging en omvat afspraken over het doorvoeren van wijzigingen.

Over de scope van governance stellen Markus en Bui (2012, p. 164): "*governance can address both mundane operational coordination (e.g., how open source software developers 'check in' new code) and high-level strategic coordination (e.g., where investment capital will come from, who owns the intellectual property, and the role of board members and senior executives in IT decision making).*" Hiertussen bestaan allerlei agendapunten, zoals prestaties, middelen, risico's, compliance, value delivery en alignment (National Computing Centre, 2005). En dit allemaal in een situatie waarin verschillende – wederzijds afhankelijke – partijen aanwezig zijn.

Kortom: ketengovernance is nodig voor het collectief oplossen van diverse vraagstukken en omvat afspraken over hoe beslissingen in de vraagstukken moeten worden genomen. De afspraken tussen partijen kunnen informeel/ongedocumenteerd zijn of formeel/ gedocumenteerd. In het eerste geval kan worden gesproken van een virtueel ketenbestuur, in het laatste van een reëel ketenbestuur (Wit, Rademakers, & Brouwer, 2000).

Rekening houdend met de observaties tot dusver, definiëren we ketengovernance als *de afspraken tussen partijen over wie er op welke manier betrokken zijn bij beslissingen ten aanzien van aspecten*[11] *die bepalend zijn voor de afhankelijkheidsrelatie binnen de keten.*

[11] Onderdelen van een keteninformatiesysteem die meerdere partijen raken, zoals de Nederlandse Taxonomie, overige ketenspecificaties op berichtenniveau, processpecificaties en de configuratie van koppelvlakservices.

In de inleiding van dit hoofdstuk hebben we van een aantal begrippen aangegeven op welke manier we ze hanteren. We kunnen nu de verbinding leggen tussen deze begrippen en ketengovernance. Het besturingsvraagstuk – het bepalen wie (welke ketenactoren) een wijziging in een keteninformatiesysteem op welke manier (veranderstrategie en sturingsinstrument) moeten besturen – betreft in wezen het vaststellen van de ketengovernance voor de wijziging. Het besturen van de wijziging (de activiteiten) kan worden beschouwd als de ketengovernance in werking.

Een dominant vraagstuk bij keteninformatiesystemen is het omgaan met wijzigingen (Markus & Bui, 2012; Sutanto, Kankanhalli, Tay, Raman, & Tan, 2009; Van der Aa, 2009). We hebben dit in de inleiding geïntroduceerd als het besturingsvraagstuk van keteninformatiesystemen. Om dit vraagstuk te kunnen adresseren is het van belang dat we eerst een tweede contingent binnen keteninformatiesystemen – technologie – onder de loep nemen.

4.2.2 *Technologie*

De vraag – wat is technologie? – is veelvuldig gesteld en uiteenlopend beantwoord. We verkennen eerst de definitie van technologie in het algemeen. Wat precies wel en wat niet onder technologie valt, is een terugkomend debat in de wetenschappelijke literatuur (zie bijv. Berg, 1998; Lamb & Kling, 2003). Dit manifesteert zich in verschillende 'scholen' die elk een andere opvatting hebben over technologie. Aanhangers van het 'technologisch determinisme' beschouwen technologie als een exogene en autonome ontwikkeling die organisaties en relaties afdwingt en determineert (Fleck & Howells, 2001). Zij hanteren een smalle en reductionistische kijk op technologie en geloven in de kracht van de technologie en de daarmee samenhangende (industriële) rationalisering (Zuurmond, 1994). Technologie als 'een verzameling technieken' is – zoals we zullen zien – een te smalle definitie. Aan de andere kant hanteren aanhangers van de 'structuration theory' (Brooks, 1997; Orlikowski, 1992) namelijk een brede en holistische kijk, waarin nadrukkelijk wordt verwezen naar de 'pervasiveness of technology' – de vervlechting tussen technologie en sociale/politieke structuren en processen. Deze school stelt dat technologie pas betekenis krijgt wanneer we de interactie met de mens in beschouwing nemen. Onderstaand citaat onderbouwt deze stelling:

"Technology is the product of human action, while it also assumes structural properties. That is, technology is physically constructed by actors working in a given social context, and technology is socially constructed by actors through the different meanings they attach to it and the various features they emphasize and use. However, it is also the case that once developed and deployed, technology tends to become reified and institutionalized, losing its connection with the human agents that constructed it or gave it meaning, and it appears to be part of the objective, structural properties of the organizations" (Orlikowski, 1992, p. 406).

Het lastige aan dit debat is dat we het niet hebben over één technologie die vijftig jaar geleden bedacht is en daarna is doorontwikkeld, maar over een accumulatie van technologieën waarvan de ene al decennia oud is en de andere nog maar net het daglicht heeft gezien.

Figuur 4.1 – Technologie kan van smal tot breed gedefinieerd worden

Dit hoofdstuk gaat niet nog een debat voeren over wat nou wel of juist niet onder technologie valt. Hiervoor verwijzen wij u naar de zojuist geciteerde literatuur. Voor de opbouw van ons betoog is het echter wel prettig als we een stipulatieve definitie bieden die aanknopingspunten bevat voor wat wij in dit hoofdstuk als technologie beschouwen. Onze ervaring met ketenveranderingen positioneert ons hierbij in de richting van de structuration theory stroming waarin een brede blik op technologie wordt aangeraden om zodoende valkuilen en essentiële factoren voor succes niet te overzien (Bruijn & Herder, 2009). Implementatie van technologie mislukt wanneer er geen rekening wordt gehouden met niet-technologische factoren – zoals ervaring met de technologie, kennis van de werking en toepassing – zo luidt meestal de verklaring (Bauer & Herder, 2009; Clegg, 2000).

Er bestaat een zekere mate van subjectiviteit in technologie (Fountain, 2001). Technologie is binnen een organisatie of keten niet een absoluut objectief gegeven. Technologie wordt vanuit een zeker normen- en waardenpatroon gepercipieerd. Bijvoorbeeld het perspectief van de functie of publieke taak van een overheid die opdracht geeft tot het (door)ontwikkelen of toepassen van een technologie. Het krijgt betekenis (wordt geconstrueerd) binnen dat perspectief.

Tegen deze achtergrond willen we technologie breed definiëren als *het totaal van praktische en theoretische kennis, vakmanschap, procedures, ervaring met falen en succes en technische hulpmiddelen die toegepast worden bij het oplossen van een probleem of het uitvoeren van een specifieke functie, teneinde een bepaald doel te behalen.*

4.2.3 *Fit*

Eerder hebben we twee contingenten van een keteninformatiesysteem behandeld: ketengovernance en technologie. Zoals gezegd beïnvloeden contingenten elkaar. Hoe dit gebeurt en wat de relatie is tussen die twee aspecten, willen we hier uitwerken. Hiervoor blijven we binnen het theoretische kader van de contingentietheorie en benaderen de relatie tussen de contigenten door middel van het concept ‘fit’.

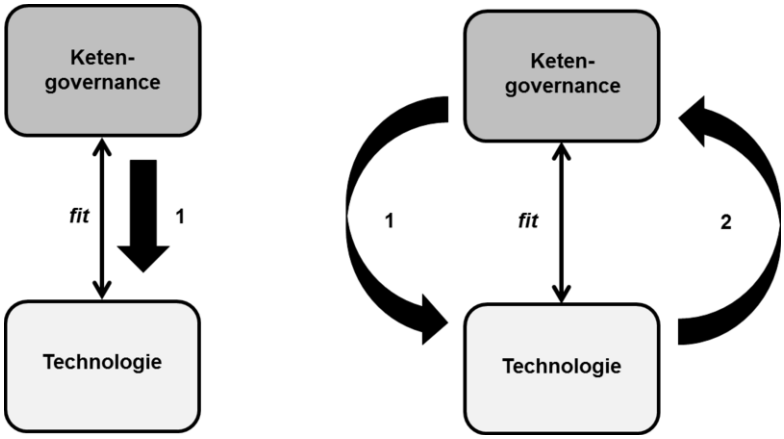
Fit is een concept om de interactie tussen twee contingenten te onderzoeken. Nadler and Tushman (1980) geven de volgende, algemene definitie voor fit: *"the degree to which the needs, demands, goals, objectives and/or structure of one component are consistent with the needs, demands, goals, objectives and/or structure of another component"*. In deze definitie staat componenten synoniem voor contingenten.

Waarom is een fit belangrijk? Er is veel onderzoek gedaan naar wat een fit is en waartussen een fit nodig is (Galbraith, 1973; Gresov, 1989; Mintzberg, 1992). Onderzoek (Gresov, 1989) waarin de fit tussen governance en technologie is onderzocht laat weinig ruimte voor twijfel: een fit tussen governance en technologie is cruciaal en een 'misfit' leidt tot problemen. Dit kan zich uiten aan de output-zijde van de organisatie, door bijvoorbeeld een lagere effectiviteit, verlaagde efficiëntie of ontevredenheid bij de gebruikers van de technologie. Maar het kan zich ook uiten in het mislukken van implementatie van nieuwe functionaliteit of grotere overhead. Om de problemen bij een misfit te voorkomen hebben we in de jaren negentig een flinke groei gezien van concepten en raamwerken die moeten helpen bij het vinden van een fit. Het vinden van een fit wordt in het Engels ook wel alignment (afstemming) genoemd. Bekende alignment modellen zijn het strategic alignment model (Henderson & Venkatraman, 1993) en het negenvlaksmodel (Maes, 2003).

Wat opvalt in de literatuur is dat het vinden van een fit geen eenmalige exercitie, maar een continu proces is. Het behouden van een fit in informatiesystemen is een permanente uitdaging. Bij wijzigingen moet er rekening worden gehouden met het vinden van een fit. Een wijziging kan betekenen dat de technologie er in de nieuwe situatie anders uit komt te zien.

4.2.4 *Wijziging van technologie betekent soms wijziging van ketengovernance*

Met name in hoofdstuk twee komt naar voren dat technologische wijzigingen impact kunnen hebben op de afhankelijkheden die binnen een keten bestaan. In dat geval is de kans groot dat de fit tussen de bestaande ketengovernance en de nieuwe technologie onder druk komt te staan. Voor een efficiënte besturing van de nieuwe 'versie' van het keteninformatiesysteem zijn dan hoogstwaarschijnlijk ook aanpassingen in de ketengovernance noodzakelijk. Ook uit de literatuur blijkt dat succesvolle ketens en netwerken zich onderscheiden van minder succesvolle door hun ketengovernance tijdig aan te passen aan de stand van de technologie (Markus & Bui, 2012; Provan & Kenis, 2007; Tiwana, Konsynski, & Bush, 2010). Een wijziging in de technologie van een keteninformatiesysteem kan derhalve tevens een aanpassing van de ketengovernance behoeven (Brooks, 2006). In figuur 4.2 is de samenhang tussen ketengovernance en technologie versimpeld weergegeven. In het linker figuur ontstaat vanuit de ketengovernance een wijzigingsbehoefte in de technologie. In de rechter figuur zien we dezelfde situatie, waarin de wijziging in de technologie op zijn beurt om een wijziging in de ketengovernance vraagt.



Figuur 4.2 – Een wijziging kan betrekking hebben op de technologie (links), maar als gevolg van het streven naar de fit daarmee tevens een wijziging in de ketengovernance behoeven (rechts)

Gezien de bovenstaande wisselwerking tussen technologie en ketengovernance conceptualiseren wij het object van wijziging – het keteninformatiesysteem – langs twee dimensies: technologie en ketengovernance. Soms verandert alleen de technologie of alleen de ketengovernance, maar een wijziging kan ook betrekking hebben op beide dimensies. We lichten dit toe aan de hand van een voorbeeld uit SBR. Het gebruik van shared services van Logius door de betrokken overheden betrof een wijziging in de technologie. Door het gebruik van shared services vormde Logius een nieuwe schakel in de keten. Hierdoor ontstonden nieuwe en andere afhankelijkheden tussen partijen. Afhankelijkheden tussen partijen worden bestuurd door middel van afspraken (Malone & Crowston, 1994). Naarmate er sprake is van sterkere horizontale collaboratie en verticale integratie (door samen te werken met een gedeelde dienstverlener), zijn dit soort afspraken meer van belang. Derhalve wijzigde bij de introductie van shared services niet alleen de technologie, maar tevens de ketengovernance.

Merk op dat het streven naar de fit ons ook aanwijzingen geeft over de kenmerken van een toereikende ketengovernance. In de inleiding is aangegeven dat informatieketens met pluriforme actoren en informatiestromen voor gedeelde voorzieningen een flexibele technologie behoeven. Als gevolg van het streven naar de fit, volgt hieruit dat er een bijpassende flexibiliteit in de ketengovernance aanwezig dient te zijn. Tevens hebben we waargenomen dat het streven naar de fit een voortdurend proces is (alignment). Dit vraagt om een periodieke evaluatie om vast te stellen of de ketengovernance blijvend toereikend is.

4.3 De wijziging nader beschouwd

In de vorige paragraaf is beschreven dat een wijziging betrekking kan hebben op twee dimensies: technologie en governance. In navolging van hoofdstuk 3 (Verandermanagement in informatieketens), beschouwen we de wijziging als een verandering van situatie A naar situatie B. Overigens wordt in de context van (keten)informatiesystemen ook wel gebruikgemaakt van de termen IST en SOLL.
Het doorvoeren van de wijziging vraagt om besturing. In de inleiding van dit hoofdstuk is reeds aangegeven dat er een antwoord moet worden gevormd op de vraag wie (welke ketenactoren) een wijziging op welke manier besturen. Dit is het besturingsvraagstuk. We stellen twee essentiële vragen over de wijziging die bepalend zijn voor de besturing van de wijziging.

De eerste vraag is: “Hoe ziet het beeld van de B-situatie eruit?” Volgend uit § 4.2, heeft dit beeld zowel betrekking op de technologie als op de ketengovernance. Technologie hebben we breed gedefinieerd. Daarbij spelen zaken als de toekomstige praktische en theoretische kennis en technische hulpmiddelen (denk daarbij aan benodigde applicaties, infrastructuur, functionaliteit, architectuur en specificaties) een rol. Voor de ketengovernance betreft de B-situatie de toekomstige afspraken tussen partijen over wie er op welke manier betrokken zijn bij beslissingen ten aanzien van aspecten die bepalend zijn voor de afhankelijkheidsrelatie binnen de keten. Al dan niet is de B-situatie bekend. Met ‘B is bekend’ bedoelen we dat er 1) een helder beeld bestaat over de technologie die gebruikt gaat worden, 2) dat er een helder beeld bestaat over de bijbehorende toekomstige ketengovernance en 3) dat de verschillende ketenpartijen dezelfde voorstelling hebben van dit beeld.

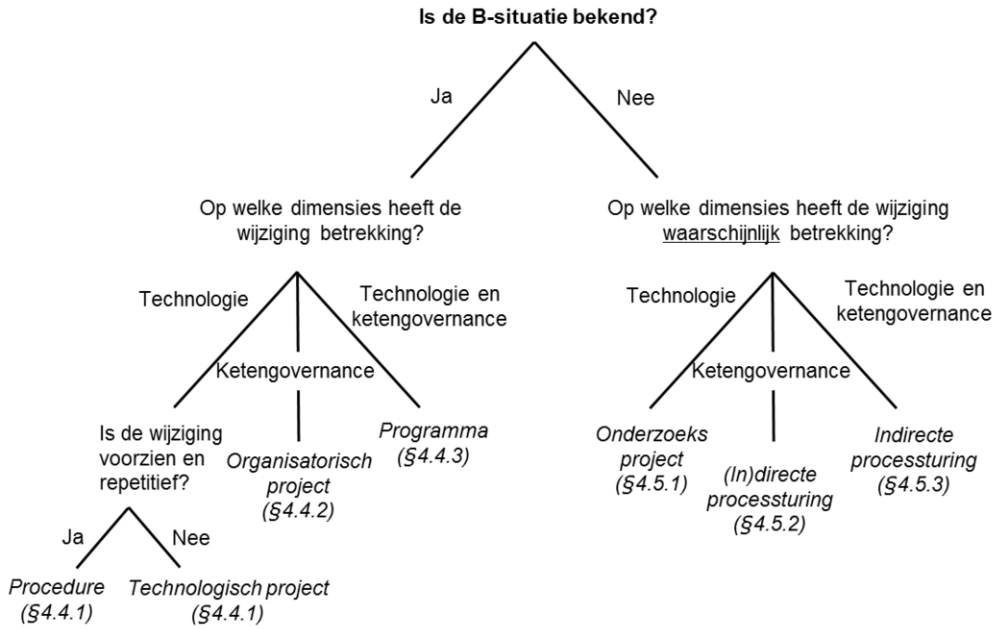
De tweede vraag is: “Op welke ketenpartijen heeft de wijziging betrekking?” Over het algemeen zal een wijziging binnen een keteninformatiesysteem niet betrekking hebben op alle aspecten van het systeem. Daarbij hoeft een wijziging in een aspect niet alle ketenpartijen te raken. Voor het besturen van de wijziging zijn de actoren nodig die geraakt worden door de wijziging. Daarbij dient de ketengovernance in de B-situatie in ieder geval in de besturing van de wijziging weerspiegeld te worden. Merk de grote afhankelijkheid op tussen de vraag ‘hoe ziet B eruit?’ en het antwoord op het besturingsvraagstuk. Immers, wanneer B niet bekend is, is het lastig vast te stellen wie door de wijziging geraakt wordt.

In het licht van de bovenstaande twee vragen valt het volgende op. Als er sprake is van een situatie waarin B bekend is, dan valt er gemakkelijk antwoord te geven op bovenstaande twee vragen. Het is bekend welke partijen er geraakt worden door de wijziging. Zij zijn in ieder geval betrokken bij het besturen van de wijziging. Ook is – met kennis van de huidige situatie – de opgave om de wijziging te implementeren inzichtelijk te maken. Doordat de technologie in de B-situatie bekend is, kan iedere partij die wordt geraakt door de wijziging een impactanalyse opstellen. Als de B-situatie bekend is, dan hoeft het beantwoorden van het besturingsvraagstuk dus zeker geen complexe aangelegenheid te zijn.

Echter, als er geen sprake is van een bekende B-situatie, dan is het vinden van een antwoord op de tweede essentiële vraag – op welke ketenpartijen heeft de wijziging

betrekking? – een stuk problematischer. Het is immers niet duidelijk welke ketenpartijen in de B-situatie met elkaar te maken gaan krijgen. In afwezigheid van een bekende B-situatie is het lastig om mogelijk betrokken ketenpartijen zekerheid te geven over de mate waarin de B-situatie bepaalde problemen in het keteninformatiesysteem oplost, en dus om hen te motiveren de wijziging te besturen. In deze situatie is het beantwoorden van het besturingsvraagstuk een zeer complexe – zo niet onmogelijke – aangelegenheid.

Wij maken bij de indeling van wijzigingen in relatie tot de besturing van wijzigingen daarom onderscheid tussen twee typologieën: de eerste typologie wordt gekenmerkt door bekendheid van de B-situatie. We zullen zien dat voor deze typologie het besturingsvraagstuk goed te beantwoorden is. Bij de tweede typologie is er geen sprake van een bekende B-situatie. Omdat een duidelijk beeld van de B-situatie, de betrokken partijen en de weg ernaartoe ontbreekt, is het beantwoorden van het besturingsvraagstuk in dit soort gevallen lastig. Deze tweedeling vormt het topje van een boomstructuur waar wij wijzigingen mee indelen. We zullen zien dat het tweede relevante onderscheid in relatie tot de besturing van wijzigingen een eigenschap van de wijziging betreft die we al eerder zijn tegengekomen in dit hoofdstuk, te weten in § 4.2. In deze paragraaf is beschreven dat een wijziging gevolgen kan hebben voor twee dimensies, te weten technologie en/of ketengovernance. Ten slotte kan het voor de besturing van sommige wijzigingen bepalend zijn of de wijziging voorzien en repetitief is. Zo komen we tot de boomstructuur in figuur 4.3.



Figuur 4.3 – De onderverdeling van wijzigingen langs drie vragen die bepalend zijn voor de besturing van wijzigingen

Wat opvalt aan de boomstructuur is dat, wanneer er geen sprake is van een bekende B-situatie, de dimensies waarop de wijziging betrekking heeft niet met zekerheid zijn vast te stellen. Immers, doordat de B-situatie nog niet bekend is, bestaan er gedurende het wijzigingstraject nog aanzienlijke vrijheidsgraden. Als gevolg van het streven naar de fit tussen technologie en ketengovernance kan men er gedurende een wijziging in de technologie achter komen dat er tevens een wijziging in de ketengovernance nodig is. Op een gelijke wijze kan men er gedurende een wijziging in de ketengovernance achter komen dat een wijziging in de technologie noodzakelijk is. Derhalve zeggen we dat de wijziging waarschijnlijk betrekking heeft op de genoemde dimensies.

Met de onderverdeling van wijzigingen langs vragen die bepalend zijn voor de besturing van een ketenverandering bieden we een handvat voor het beantwoorden van het besturingsvraagstuk. De volgende paragrafen werken achtereenvolgens elk van de takken van de boomstructuur uit. In § 4.4 behandelen we de typologie die gekenmerkt wordt door een bekende B-situatie. Voor wijzigingen die vallen onder de typologie die gekenmerkt wordt door onbekendheid van de B-situatie – dit zijn de drie scenario's weergegeven aan de rechterkant van de boomstructuur – valt niet altijd antwoord te geven op het besturingsvraagstuk. We gaan meer verkennend te werk en geven aanwijzingen. Dit doen we in § 4.5. In beide volgende paragrafen werken we toe naar antwoorden op het besturingsvraagstuk. Daarnaast spelen bij een wijziging ook het acceptatievraagstuk en het implementatievraagstuk. Daar gaan we bewust minder op in, maar zullen er bij de verschillende wijzigingen toch iets over zeggen.

4.4 Het besturingsvraagstuk voor wijzigingen met een bekende B-situatie

In de vorige paragraaf is geconcludeerd dat er in relatie tot de besturing van wijzigingen onderscheid dient te worden gemaakt in wijzigingen waarvoor de B-situatie bekend is en wijzigingen waarvoor dit niet het geval is. In deze paragraaf staat het besturen van wijzigingen die vallen onder de eerste typologie – B is bekend – centraal. Deze paragraaf behandelt het besturingsvraagstuk voor wijzigingen die vallen onder deze typologie. Voor deze wijzigingen is een aantal aandachtspunten relevant.

Ten eerste zijn binnen een keteninformatiesysteem verschillende onderdelen (bouwstenen) te onderkennen. Met name bij een wijziging die betrekking heeft op de technologie dienen ketenactoren bij de impactanalyse nauwkeurig vast te stellen op welke onderdelen van het informatiesysteem de wijziging betrekking heeft. Ten tweede maken we in dit hoofdstuk onderscheid tussen wijzigingen die betrekking hebben op de technologie of op de ketengovernance of beide. Zo logisch als het op papier klinkt, zo lastig kan het zijn om in de praktijk hiervan bewust te zijn. Gedurende de fasen van het traject van een technologische wijziging (zeker als er nog flinke aanpassingen in de wijziging optreden) is het van belang dat ketenactoren voortdurend herijken of de ketengovernance ongewijzigd blijft. Bij het wijzigen van de ketengovernance is herijking op vergelijkbare wijze van belang. Ten derde is het behouden van een fit tussen technologie en ketengovernance (zie § 4.2) onder ver-

anderende omstandigheden makkelijker als partijen zich aan bepaalde architectuurprincipes houden (Bharosa & Janssen, 2010; Dickerson & Mavris, 2010). Principes beperken namelijk de ontwerp/veranderingskeuzen van partijen tot een ontwerpruimte waarin wijzigingen 'veilig' zijn en geen schade kunnen aanrichten aan de werking van een systeem (Clegg, 2000). Dit betekent dat een wijziging in overeenstemming dient te zijn met de opgestelde principes. Principes kunnen worden opgevat als regels die voortkomen uit de collectieve overtuiging van partijen op basis van opgedane ervaring. Het is een speciale klasse afspraken die zelden verandert en voor alle ketens, schakels en stromen geldig is. In deel B gaan we hier verder op in.

De behandeling van de wijzigingen bestaat uit een beschrijving van de passende veranderstrategie, het geschikte sturingsinstrument en een beschrijving van de betrokkenheid van ketenactoren. Ook gaan we in op acceptatie. We grijpen zoveel mogelijk terug op hoofdstuk 3 (Verandermanagement in informatieketens). We passen de daar uitgewerkte criteria voor sturingsinstrumenten en veranderstrategieën toe op de kenmerken van de wijzigingen en leiden daaruit een passende veranderstrategie en geschikt sturingsinstrument af. Tevens geven we voorbeelden van het betreffende type wijziging vanuit SBR. Achtereenvolgens worden behandeld: een voorziene en repetitieve wijziging in de technologie, een onvoorziene en/of laagfrequente wijziging in de technologie, een wijziging in de ketengovernance en een wijziging in de technologie en in de ketengovernance. We sluiten deze paragraaf af met enkele algemene aandachtspunten die gelden voor wijzigingen waarvoor de B-situatie bekend is.

4.4.1 *Voorziene en repetitieve wijziging in de technologie*

Kenmerkend aan wijzigingen binnen deze typologie is dat de wijziging uitsluitend betrekking heeft op de technologie, dat de wijziging is voorzien (denk hierbij in termen van frequentie, moment en impact) en dat de wijziging repetitief van aard is.

Een voorbeeld van een voorziene en repetitieve wijziging is de jaarlijkse wijziging van de Nederlandse Taxonomie (NT). De overheidspartijen in SBR brengen elk jaar een nieuwe versie van de NT uit met daarin actuele uit te vragen gegevens en gegevensdefinities, bijvoorbeeld aangepast als gevolg van wijzigingen in wet- en regelgeving.

De actoren die de wijziging besturen, passen de veranderstrategie van direct verandermanagement toe. Ze willen de keten van situatie A naar situatie B brengen, beide situaties zijn bekend. Zij kunnen de blauwdrukbenadering en waar nodig de deblokkadebenadering gebruiken. In hoofdstuk 3 zijn de directe veranderstrategieën nader toegelicht.

Wijzigingen die voorzien worden, dienen door middel van een procedure te worden doorgevoerd. Een procedure bevat zeer concrete afspraken over het proces dat doorlopen dient te worden om een bepaald resultaat te bewerkstelligen. Daardoor waarborgt een procedure – mits goed ingericht uiteraard – een efficiënte afhandeling van de wijziging. In hoofdstuk 3 zijn de kenmerken van dit sturingsinstrument verder uiteengezet.

Welke ketenactoren op welke manier betrokken zijn bij de wijziging is voorafgaand aan de wijziging reeds vastgelegd in de procedure. Bij voorziene technologische wijzigingen zullen in ieder geval functionarissen van het operationeel niveau betrokken zijn, en hoogstwaarschijnlijk ook personen van het tactisch niveau. De verdeling van taken, verantwoordelijkheden en bevoegdheden is vastgelegd in de procedure. De procedure is belegd in 'de lijnorganisatie'. Als er geen sprake is van escalatie bij het doorlopen van de procedure, valt te verwachten dat er vanuit het strategisch niveau geen betrokkenheid is bij het doorvoeren van de wijziging. De expertise van betrokken actoren zal met name liggen op het technologisch vlak. Denk daarbij bijvoorbeeld aan IT-servicemanagers, technisch beheerders, applicatiebeheerders, gegevensarchitecten, procesarchitecten en/of informatiebeveiligers, eventueel begeleid door een change coördinator.

Zodra B bekend is, kunnen acceptatie en implementatie min of meer sequentieel en conform procedure verlopen. Een 'change' proces, zoals bekend is uit best practices als ITIL, kan hierbij een goede leidraad zijn. De mate van complexiteit van acceptatie en implementatie en de duur van dit traject heeft te maken met de impact van de wijziging. Omdat het gaat om een voorziene en repetitieve wijziging, zijn partijen als het goed is hierop ingesteld en is er baat bij een degelijke, maar standaard afwikkeling. De actoren die de wijziging besturen, kunnen – als onderdeel van hun dagelijkse werk – conform procedure werken aan het verkrijgen van acceptatie en de uiteindelijke implementatie van de wijziging besturen. Zodra er voldoende acceptatie bestaat (in het gremium dat als change advisory board functioneert), kunnen de partijen overgaan tot implementatie. Wanneer de verantwoordelijke functionarissen niet binnen een redelijk gestelde termijn tot acceptatie kunnen komen, ligt er een basis om te onderzoeken waar de schoen wringt en hierbij maatregelen te nemen om de drempels weg te nemen. In dat geval wordt er via de lijn geëscaleerd. De vraag die dan direct gesteld moet worden is waarom het type wijziging niet past binnen de verwachting van partijen of waarom zij niet bereid zijn de impact te dragen. Waarschijnlijk is er meer aan de hand waar de bekende partijen op hoger niveau met elkaar over om tafel moeten.

4.4.2 *Onvoorziene en/of laagfrequente wijziging in de technologie*

Kenmerkend aan wijzigingen binnen deze typologie is dat de wijziging uitsluitend betrekking heeft op de technologie en dat de wijziging onvoorzien en/of eenmalig is.

Een voorbeeld van een laagfrequente technologische wijziging is de vervanging van de certificaten waar Digipoort voor de systemen van aanleverende en uitvragende partijen mee te herkennen is. Doordat beveiligingsstandaarden in ontwikkeling zijn, kan er na verloop van tijd aanleiding zijn om certificaten te vervangen. Zo zijn een aantal jaar geleden projectmatig de SHA-1 certificaten vervangen door SHA-2 certificaten. Een ander voorbeeld is de overgang naar een dimensionele taxonomie. Deze wijziging kwam voort uit het besluit om de XBRL dimensions specificatie, een module van de internationale XBRL specificatie, toe te passen ten behoeve van de Nederlandse Taxonomie. De reden voor deze verandering was dat uitvragende partijen de behoefte hadden aan de mogelijkheid om bepaalde elementen van de uitvraag exacter te specificeren, bijvoorbeeld een uitsplitsing van omzet naar regio en product. Met deze wijziging werd de taxonomie voortaan dimensioneel opgebouwd.

De actoren die de wijziging besturen, passen de veranderstrategie van direct verandermanagement toe. Ze willen de keten van situatie A naar situatie B brengen, waarbij beide situaties bekend zijn. Zij kunnen de blauwdrukbenadering en waar nodig de deblokkadebenadering gebruiken.

Wijzigingen die vallen onder deze typologie dienen te worden afgehandeld met behulp van een technisch project. Een project is een eenmalige, tijdelijke activiteit, gericht op het realiseren van een duidelijk omschreven doel. Het is een maatwerk-instrument, specifiek vormgegeven voor de betreffende wijziging waar bij de inrichting vrijheidsgraden noodzakelijk zijn. In hoofdstuk 3 zijn de kenmerken van dit sturingsinstrument nader uiteengezet.

De ketenpartijen waarop de wijziging betrekking heeft, worden betrokken bij het besturen van de wijziging. Bij een technisch project wordt de verdeling van de taken, verantwoordelijkheden en bevoegdheden op maat gemaakt. Afhankelijk van de partijen die worden geraakt door de wijziging, wordt de projectgovernance ingericht. De projectgovernance blijft binnen de kaders van de huidige ketengovernance. De bestaande ketenafhankelijkheden veranderen niet bij dit type wijziging. Het project wordt aangestuurd door een stuurgroep en uitgevoerd door een projectteam. In de stuurgroep is het tactisch dan wel het strategisch niveau vertegenwoordigd. In het projectteam is het operationeel niveau en waarschijnlijk ook het tactisch niveau betrokken. De expertise van het projectteam ligt met name op technologisch vlak. Denk hierbij aan: IT-servicemanagers, technisch beheerders, applicatiebeheerders, gegevensarchitecten, procesarchitecten en/of informatiebeveiligers, eventueel begeleid door een change coördinator dan wel project manager.

Doordat de wijziging niet is voorzien, is er grote kans dat deze in eerste instantie stuit op een gebrek aan acceptatie. Zeker wanneer de reikwijdte van de implementatie breder is dan de verantwoordingsketen waar het probleem ligt. Het is aan het projectteam om gericht met dit acceptatieprobleem aan de slag te gaan. Zij dienen op zoek te gaan naar de specifieke belemmeringen op het gebied van kennen, kunnen en willen bij de betrokken ketenpartners en bekijken hoe zij voldoende draagvlak kunnen krijgen voor de wijziging. Het projectteam moet begrijpen waar de grenzen van haar bevoegdheden liggen, maar wel breder onderzoek durven te doen. Soms kan er op twee gewenste wijzigingen een ‘uitruil’ tussen partijen plaatsvinden om een stap in ieders belang te kunnen maken. Een voorstel voor een dergelijke tactische stap moet door het projectteam met het probleem-overstijgende besturingsniveau besproken worden. Door tijdens de acceptatiefase al goed na te denken over de implementatiefase, die volgt zodra acceptatie is verkregen, kunnen partijen – bijvoorbeeld door het bieden van goede ondersteuning bij implementatie – eerder over de streep getrokken worden. Wanneer acceptatie van de wijziging uitblijft, moet het projectteam niet te lang wachten met het teruggeven van haar opdracht aan de stuurgroep en haar vragen een weg te kiezen om uit de ontstane impasse te kunnen komen. Het kan blijken dat de voorgestelde B niet de oplossing is en B kan dan niet meer als bekend gezien worden.

4.4.3 *Wijziging in de ketengovernance*

Kenmerkend aan wijzigingen binnen deze typologie is dat de wijziging uitsluitend betrekking heeft op de ketengovernance. Een wijziging in uitsluitend de ketengovernance kan optreden als gevolg van externe invloeden (bijvoorbeeld de roep om reorganisatie) of om een betere fit te bereiken tussen de technologie en de ketengovernance (zie § 4.2). Daarom kenmerkt dit soort wijzigingen zich door eenmaligheid, uniciteit en gerichtheid op een specifiek resultaat.

Ten tijde van schrijven is een actueel voorbeeld van dit type wijziging de verandering van SBR van programma naar een afdeling (lijnactiviteit) van Logius. Er is reeds een blauwdruk aanwezig die als bekende B kan worden gezien. De technologie die SBR ketens toepassen verandert niet. Wel worden er nieuwe overlegvormen ingericht, waarbij uitvragende partijen, Logius en de leverancier van Logius bij elkaar komen; er zijn meer gestandaardiseerde documenten met afspraken tussen partijen en er is intensievere betrokkenheid van de professionals uit de lijn van Logius bij de bestaande SBR gremia.

Direct verandermanagement en waar nodig het veranderen van ketencondities zijn passende veranderstrategieën. Bij direct verandermanagement kunnen verschillende benaderingen worden toegepast, zoals de expertbenadering en de deblokkadebenadering. Het veranderen van ketencondities kan plaatsvinden door bijvoorbeeld strategische communicatie en het sluiten van allianties. In hoofdstuk 3 zijn deze veranderstrategieën nader toegelicht.

Gezien het eenmalige, vernieuwende en tijdsgebonden karakter van een wijziging als deze, zou een dergelijke wijziging door middel van een organisatorisch project moeten worden bestuurd, eventueel aangevuld door directe processturing. In hoofdstuk 3 zijn de kenmerken van deze sturingsinstrumenten uiteengezet.
Bij een organisatorisch project wordt de verdeling van de taken, verantwoordelijkheden en bevoegdheden op maat gemaakt. Doordat de bestaande ketenafhankelijkheden wijzigen, dient de ketengovernance in de B-situatie (en met name de partijen die daarbij betrokken zijn) in de besturing van de wijziging voldoende weerspiegeld te worden. Met andere woorden: het zijn naast de actoren die afscheid nemen ook de actoren die in de toekomstige situatie met elkaar te maken krijgen die de wijziging gaan besturen. Ten opzichte van de A-situatie, kan het zijn dat er geen verandering is van de ketenpartijen die betrokken zijn, maar dat zij wel andere taken, verantwoordelijkheden en bevoegdheden krijgen. Ook is het mogelijk dat er nieuwe ketenpartijen toetreden of wegvallen.

Het project wordt aangestuurd door een stuurgroep en uitgevoerd door een projectteam. In de stuurgroep is vermoedelijk het strategisch niveau, maar in ieder geval het tactisch niveau vertegenwoordigd. In het projectteam is het tactisch niveau en mogelijk ook het operationeel niveau betrokken. De expertise van te betrekken functionarissen ligt op het gebied van ketengovernance en organisatieadvies. Denk hierbij aan governance deskundigen, de enterprise architect, beleids- en organisatieadviseurs.

Acceptatie en implementatie worden het snelst bereikt door via de nieuwe rollen te gaan opereren en hier vanuit een tijdelijke projectstructuur op te reflecteren. Het is bij een organisatorische wijziging wel van belang dat partijen en personen geschikt zijn voor de nieuwe rol die zij gaan spelen. Waar het gaat over rollen die cruciaal zijn in de ketensamenwerking is dit een gedeeld probleem. Partijen zullen op het juiste niveau met elkaar over competenties in gesprek moeten. Dit is niet altijd gemakkelijk en vraagt om tact. Omdat het kan gaan om individuen, moet hier zorgvuldig en op gepaste wijze mee omgegaan worden.

4.4.4 *Wijziging in de technologie en in de ketengovernance*

Kenmerkend aan wijzigingen binnen deze typologie is dat de wijziging zowel betrekking heeft op de technologie als de governance. Dit is het geval voor verbredingsketens, waarin de generieke bouwblokken worden toegepast in het verantwoordingsproces naar publieke of private partijen (wijziging in de technologie). Dit betekent dat ook deze partij als nieuwe actor betrokken raakt bij SBR (ketengovernance). Hoofdstuk 10 gaat uitgebreid in op verbreding.

Direct verandermanagement en waar nodig het veranderen van ketencondities zijn passende veranderstrategieën. Geschikte benaderingen bij de genoemde veranderstrategie zijn de expertbenadering en de brede bottom-up benadering.

Een programma is een geschikt sturingsinstrument voor dit type wijziging. Een programma bestaat uit meerdere samenhangende projecten. In hoofdstuk 3 is al beschreven dat een programma voor verandering van de keten kan worden ingezet. In een verbredingstraject gaat het bijvoorbeeld om een project om een taxonomie voor het domein te ontwikkelen en een project om de processen bij verantwoordende partijen en bij de ontvangers aan te passen. Daarnaast zal de deelname van de nieuwe ketenpartij in de SBR gremia moeten worden gerealiseerd. Naast de wijziging in de technologie en de wijziging in de ketengovernance, dient tevens de fit tussen de technologie en de ketengovernance in de B-situatie gewaarborgd te worden.

Directe processturing zou een aanvullend instrument kunnen zijn om alle betrokken organisaties en verantwoordelijke functionarissen mee te nemen in de wijziging naar de B-situatie.

Bij een programma wordt de verdeling van de taken, verantwoordelijkheden en bevoegdheden op maat gemaakt. Omdat de bestaande ketenafhankelijkheden wijzigen, is het van belang om te borgen dat de nieuwe ketengovernance (en met name de partijen die daarbij betrokken zijn) in de besturing van de wijziging weerspiegeld wordt. Het programma wordt aangestuurd door een stuurgroep, waarin per definitie het strategisch niveau vertegenwoordigd is (Hedeman & Vis van Heemst, 2011). In het programmateam kan het strategisch, tactisch en operationeel niveau betrokken zijn. De betrokkenheid van strategisch en tactisch niveau is van belang met het oog op de nodige input ten aanzien van de ketengovernance. Daarnaast moet er expertise op het gebied van technologie worden ingebracht. Voorbeelden van deze experts zijn benoemd in de voorgaande twee paragrafen. Ter aanvulling kan er gebruik worden gemaakt van programmamanagers en verandermanagers.

Acceptatie en implementatie zijn onderdeel van de deelprojecten van het programma, met dien verstande dat weerstand uit het ene project kan gaan interfereren met een ander project. Partijen die moeite hebben met de nieuwe governance kunnen bezwaren uiten over de techniek, omdat zij bijvoorbeeld de kans groter achten dat zij daar hun gelijk halen. Het is aan het programmamanagement dergelijke problemen 'af te pellen' en de werkelijke weerstand te achterhalen. Het is van belang dat leden van de stuurgroep zich voldoende verdiepen in zowel de technische als de organisatorische component. Anders wordt het heel lastig om problemen die interfereren te begrijpen en te sturen op de acceptatie. Voor de implementatie geldt dat er afhankelijkheden bestaan tussen de verschillende projecten. Wanneer één van de projecten 'stokt', om wat voor reden dan ook, kan het noodzakelijk zijn aanpassingen te doen in het andere project. Grote valkuil is een te scherpe focus op techniek om vervolgens de organisatorische component niet tot een *closure* te laten komen. Het kan een strategie zijn de geaccepteerde techniek te implementeren om zo een acceptatie van de nieuwe governance te forceren, maar dit kan grote risico's met zich meebrengen.

4.5 Aanwijzingen voor wijzigingen waar de B-situatie niet bekend is

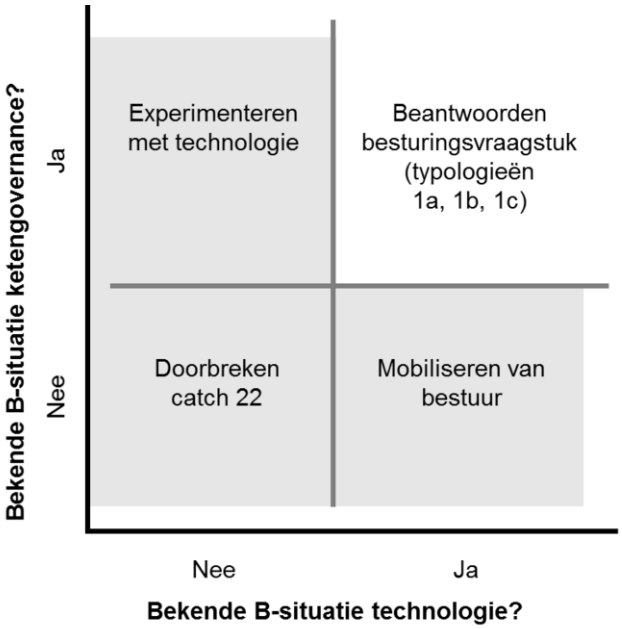
In de vorige paragraaf is het besturingsvraagstuk voor wijzigingen waarvoor de B-situatie bekend is behandeld. In deze paragraaf verkennen we het besturingsvraagstuk voor vragen waarbij geen sprake is van een bekende B-situatie. Wederom kan er sprake zijn van een voorgestelde wijziging in de technologie, in de ketengovernance of de technologie en de ketengovernance. Ook wanneer bij aanvang van een wijziging wordt verondersteld dat de wijziging uitsluitend betrekking heeft op de technologie, is dit niet met zekerheid vast te stellen. Een onvoorzien technologisch aspect kan immers nog onvoorziene afhankelijkheden met zich meebrengen. Uitgaande van de noodzaak voor een fit tussen technologie en ketengovernance kan men er gedurende het traject dus achter komen dat er tevens een wijziging in de ketengovernance nodig is als gevolg van de uiteindelijke wijziging in de technologie. Hetzelfde gaat op voor een wijziging in de ketengovernance die uiteindelijk tevens een wijziging in de technologie blijkt te vereisen. Derhalve zeggen we dat de wijziging waarschijnlijk betrekking heeft op de technologie, de ketengovernance of beide.

Zoals reeds in § 4.3 is beschreven, kan de besturing van een wijziging waarvoor de B-situatie niet bekend is lastig zijn. We komen in een grijs gebied (zie figuur 4.4) en moeten voorzichtiger omgaan met het aandragen van aanwijzingen. We verkennen de besturing van wijzigingen die vallen onder deze typologie en bieden vanuit de ervaringen binnen de SBR-casus aanwijzingen voor besturing bij drie scenario's.

In het eerste scenario is er een wijziging in de technologie en waarschijnlijk niet in de ketengovernance, waarbij onze suggestie is om binnen een onderzoeksproject een technologisch experiment uit te voeren. In het tweede scenario is er een wijziging in de ketengovernance en waarschijnlijk niet in de technologie, waarbij onze suggestie is om het bestuur te mobiliseren. In het derde scenario is er een wijziging die waarschijnlijk betrekking heeft op zowel de technologie als de ketengovernance, waarbij

onze suggestie is om de catch 22 (eerst ketengovernance of eerst technologie wijzigen) te doorbreken. Dit lichten we straks uitgebreid toe.

De relatie tussen de beschreven scenario's en de typologieën die besproken zijn in de vorige paragraaf is weergegeven in onderstaande figuur.



Figuur 4.4 – Relatie tussen de besproken scenario's en typologieën van wijzigingen

Hierna worden de verschillende scenario's in het grijze gebied toegelicht.

4.5.1 *Technologisch onderzoeksproject*

Kenmerkend aan wijzigingen binnen dit scenario is dat de wijziging waarschijnlijk uitsluitend betrekking heeft op de technologie, waarbij de B-situatie voor de technologie niet helder en gedeeld is. De ketenpartijen gaan ervan uit dat de wijziging geen betrekking heeft op de ketengovernance.

Een voorbeeld is een opgemerkte zwakte in de gebruikte beveiligingsprotocollen voor de koppelvlakken. De ketenpartijen die gebruikmaken van de koppelvlakken dienen om tafel te gaan voor een oplossing. Deze partijen dienen te onderzoeken door middel van welke technologie het beveiligingslek gedicht kan worden.
Van de wijzigingen die gekenmerkt worden door een onbekende B-situatie, zijn wijzigingen die alleen betrekking lijken te hebben op de technologie de meest bestuurbare. Een belangrijke constatering is immers dat de governance in de B-situatie bekend lijkt te zijn. Daarmee kan, in ieder geval bij aanvang, het bestuur voor de wijziging worden bepaald. Er dient in ieder geval meer inzicht verkregen te worden in de toe te passen technologie.

Gedurende het onderzoeksproject is het een blijvend aandachtspunt om vast te stellen of de ketengovernance niet wijzigt en of er een helder en gedeeld beeld blijft bestaan over de governance. Het is lastig om een essentiële eigenschap te noemen wanneer er in de B-situatie geen sprake meer is van een helder en gedeeld beeld van de ketengovernance. Zo kan – met betrekking tot de wijziging – een combinatie van meerdere van de volgende signalen erop wijzen dat er geen sprake meer is van een helder en gedeeld beeld van de B ketengovernance:

- De dialoog omtrent de ketengovernance wordt gekenmerkt door dynamiek.
- Ketenpartijen die actief betrokken zijn in het huidige bestuur zien de relevantie daarvan niet in of stellen hun betrokkenheid ter discussie.
- Ketenpartijen die niet betrokken zijn beroeren zich en zoeken naar manieren om invloed uit te oefenen.
- Het lukt niet of nauwelijks om tot besluiten te komen, omdat een gezamenlijk verantwoordelijkheidsgevoel of urgentie lijkt te ontbreken.
- Er ontstaat externe druk om het bestuur aan te passen.

Let erop dat ieder van de bovenstaande signalen ook veroorzaakt kan worden door tal van andere factoren. Het oordeel of er geen sprake meer is van een helder en gedeeld beeld van de ketengovernance is dus sterk afhankelijk van de context. Enige voorzichtigheid bij de interpretatie van deze signalen is derhalve op zijn plaats.

Tijdens het onderzoeksproject moeten partijen zich realiseren dat zij de basis aan het leggen zijn voor een wijziging die geaccepteerd en geïmplementeerd moet worden. Kenmerk van een goede uitkomst is dat er al een zeker zicht is op de mate waarin actoren de oplossing accepteren en op de implementeerbaarheid van de oplossing. Dit kunnen criteria zijn waar alternatieve B-situaties op beoordeeld worden. Het project kan, door deze componenten in het onderzoek mee te nemen en stakeholders te consulteren, in deze ronde reeds bijdragen aan de acceptatie en implementatiefase, die volgt zodra B bekend is.

4.5.2 *Mobiliseren van besturing*

Kenmerkend aan wijzigingen binnen dit scenario is dat de wijziging waarschijnlijk uitsluitend betrekking heeft op de ketengovernance, waarbij de B-situatie voor de ketengovernance niet bekend is. Er bestaat wel een helder en gedeeld beeld over de huidige technologie, welke – naar verwachting – niet zal wijzigen in de B-situatie.

In de literatuur staat deze situatie bekend als 'institutional void'. Hajer (2003) definieert dit als "*there are no clear rules and norms according to which politics is to be conducted and policy measures are to be agreed upon. To be more precise, there are no generally accepted rules and norms according to which policy making and politics is to be conducted*" (p. 607).

Vertaald naar deze context betekent bovenstaande dat een wijziging plaatsvindt in een situatie waarbij er nog geen afspraken zijn over hoe er in de B-situatie bestuurd gaat worden (ketengovernance). Instutional void komt vaak voor bij de vorming of (totale) herziening van samenwerkingsverbanden (ketens en netwerken).

Een voorbeeld is de decentralisatie van rijksoverheidstaken naar gemeenten op het terrein van ondersteuning (Wmo), participatie en jeugdzorg. Dit behelst een omvangrijke wijziging van de ketengovernance in deze ketens. De technologische voorzieningen die worden ingezet voor de uitvoering van de verschillende wetten die hier op toezien (denk aan systemen waarin uitkeringen worden bijgehouden), hoeven op zich niet gewijzigd te worden om de decentralisatie mogelijk te maken. Daarmee is overigens niet uitgesloten dat de noodzaak tot een wijziging volgt uit aanpassingen van wetten die tegelijk met de decentralisatie worden doorgevoerd. Het is bekend dat de gemeenten verantwoordelijk worden voor de uitvoering van taken, maar er lijken nog geen (concrete) afspraken over de betrokkenheid van de ketenpartijen bij beslissingen te zijn. Bijvoorbeeld hoe gemeenten samen gaan werken met andere gemeenten en zorgverleners en hoe deze samenwerking resulteert in taken ten aanzien van het keteninformatiesysteem.

De belangrijkste constatering is dat de technologie in de A- en B-situatie bekend is. Een partij die de technologie breder wil gaan inzetten en de benodigde steun onder partijen wil mobiliseren, kan gaan lobbyen en 'verkopen'. In de literatuur wordt dit ook als '*mobilization coordination*' beschreven (Ven & Walker, 1984). Het betreft activiteiten die in gang worden gezet door een 'enkele actor' die een bepaald doel heeft, waarvoor de steun, samenwerking, of middelen van een aantal andere organisaties nodig is. Dit komt overeen met wat we in hoofdstuk 3 hebben behandeld onder de noemer directe processturing.

We kunnen ook in deze verandervorm spreken over de eerste acceptatie- en implementatieronde (waar partijen organisch met elkaar in onderzoek zijn) en de tweede acceptatie- en implementatieronde. De eerste ronde verloopt volledig integraal met het onderzoek naar hoe B eruit moet komen te zien. Partijen wijzen transitiemanagers aan die voorstellen uitwerken en die middels een lobby acceptatie voor hun vorm proberen te krijgen. Via trial and error moet er langzaam een gewenste B ontstaan. Naarmate B meer bekend wordt, zoeken partijen elkaar al op langs de lijnen van B en is de eerste implementatieslag geslagen. Zodra er een basis ligt en helder is waar men naartoe wil, kan het programma verder geformaliseerd worden. Voor deze acceptatie- en implementatieronde geldt een meer gerichte en sequentiële besturing.

4.5.3 *Doorbreken catch 22*

Kenmerkend aan wijzigingen binnen dit scenario is dat de B-situatie zowel voor de technologie als voor de ketengovernance niet bekend is, maar de wijziging waarschijnlijk betrekking heeft op beide dimensies. Binnen deze typologie is er sprake van een institutional void en technologische onzekerheid. De wijziging vertoont grote gelijkenissen met wat in de literatuur bekend staat als '*wicked problems*' (Churchman, 1967), oftewel ongetemde problemen.

In een rapport over de 'lerende overheid' heeft de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) een kritische bespreking gewijd aan het functioneren van de overheid bij de oplossing van maatschappelijke vraagstukken (WRR, 2006). Het rapport benadrukt dat de problemen waarmee de overheid geconfronteerd wordt, zich in veel gevallen niet zomaar lenen voor directe besturing. De raad spreekt van ongetemde problemen, waarbij nog veel onduidelijk is over de aard van het probleem, de

middelen die beschikbaar zijn voor de oplossing, en de doelen die daarbij zouden moeten worden nagestreefd. Bovendien zijn de meeste van deze problemen met veel wetenschappelijke onzekerheid omgeven: er is een tekort aan gevalideerde kennis.

Een kenmerk van ongetemde problemen is de '*catch 22*'. Catch 22 is een term, afkomstig uit de roman Catch-22 van Joseph Heller (1961), waarmee een situatie wordt beschreven waarin een individu twee acties dient te verwezenlijken die wederzijds afhankelijk zijn, waarbij de ene actie dient te starten wanneer de andere is voltooid en vice versa. Met betrekking tot een wijziging houdt de catch 22 het volgende in: een wijziging waarvoor de technologie in de B-situatie nog niet bekend is, vraagt om het besturen van de wijziging door de in de B ketengovernance betrokken ketenpartijen, teneinde toe te werken naar een bekende technologie. Echter, de potentiële ketenpartijen in de B ketengovernance vragen om een bekende B technologie, om gemotiveerd het bestuur in te kunnen richten. Het probleem van de wederzijdse afhankelijkheid is dat er zowel voor de besturing van de wijziging als de technologie niet toegewerkt kan worden naar een bekende B-situatie.

Nieuwe technologische ontwikkelingen – bijvoorbeeld op het gebied van informatie- en communicatietechnologie – zijn in onze samenleving een belangrijke bron van ongetemde problemen (Hoppe, 2010). Wanneer nieuwe ontwikkelingen zich aandienen is er vaak nog veel onzekerheid over de mogelijkheden van de technologie en ontbreekt het aan overeenstemming over de beoordeling daarvan. Dit was bijvoorbeeld in hoge mate het geval bij de (bestuurlijke) wens voor het uitwisselen van patiëntgegevens tussen zorgverleners. Bij aanvang viel ook SBR binnen dit scenario.

Concrete richtlijnen voor ongetemde problemen zien we niet in de als zodanig voorhanden zijnde literatuur. De WRR gaat bijvoorbeeld in haar rapport vooral in op de consequenties van dit soort problemen voor de politieke besluitvorming. Politiek omgaan met ongetemde problemen is volgens de raad geen zaak van voortvarende besluitvorming, maar vraagt om het stimuleren van maatschappelijke leerprocessen. Dat vereist de inzet van een verscheidenheid aan betrokkenen, juist ook buiten de overheid zelf, om uit te vinden hoe het probleem er precies uit ziet en kaders te ontdekken waarin over een kwestie beslist kan worden.

In retroperspectief vertoonde SBR bij aanvang grote gelijkenissen met ongetemde problemen. Er was sprake van een wens tot wijziging, maar geen zicht op de uiteindelijke wijze waarop de diverse ketenpartijen betrokken moesten worden (de ketengovernance). Er lag al vrij snel een visie op de technologie en een schets van de architectuur. De technologie in de B-situatie was echter nog niet bekend. Deze situatie komt overeen met de catch 22 zoals hierboven is beschreven.

Binnen SBR is de catch 22 doorbroken door toe te werken naar een bekende B-situatie voor de technologie. Ofwel, eerst richting geloofwaardig (stabiel) gebruik en pas daarna grootschalig en domeinoverstijgend gebruik. De Belastingdienst heeft de business case voor generiek toepasbare system-to-system uitwisseling weten uit te leggen en hiervoor middelen weten vrij te maken. Partijen in de verantwoordingsketen initieerden aanvankelijk enkele (losse) projecten (NTP) en programma's (GEIN) om gezamenlijk de nadere (technische) specificaties vast te stellen. Standaarden waren

deels al aanwezig. Vervolgens werd het SBR Programma opgetuigd voor verdere ontwikkeling en implementatie van bouwstenen. Hieronder vielen ook projecten waarin experimenten (proof of concept) centraal stonden. Een beperkt aantal ketenactoren van wat uiteindelijk de B ketengovernance zou worden, is blijvend in staat geweest om mogelijkheden te creëren om de ontwikkeling in technologie voort te zetten, óók in afwezigheid van de uiteindelijke besturing.

Parallel aan dit meerjarige traject – dat in afwezigheid van de uiteindelijke besturing geen eenvoudige opgave is – richt een beperkt aantal ketenactoren van wat het uiteindelijke bestuur zou worden zich stapsgewijs op de realisatie van een intensievere en meer opdrachtgestuurde samenwerking en besturing. Daarmee kwamen partijen stapsgewijs tot uitgebreidere afspraken over hoe zij in de B-situatie zouden gaan besturen. Naarmate de technologie volwassener werd, verschoof de uitdaging naar het mobiliseren en inrichten van het bestuur, zoals in § 4.5.2 beschreven. Door de ketengovernance op bepalende momenten stap voor stap verder te brengen, werd de institutional void opgevuld.

Voor wijzigingen die gelijkenissen vertonen met ongetemde problemen kunnen we vanuit SBR met enige voorzichtigheid een aanwijzing meegeven: ketenpartijen lijken meerdere wegen af te kunnen leggen om vanuit een scenario waarin B zowel voor de technologie als de ketengovernance niet bekend is, toe te werken naar een scenario waarin dit wel het geval is. Binnen SBR is dit gelukt door de focus te houden op de ontwikkeling van de technologie, waarbij het noodzakelijk is alle ontstane obstakels in afwezigheid van een (A en B) ketengovernance (en dus een weerspiegeling hiervan in de besturing van de wijziging) te overwinnen. Een alternatieve methode lijkt te zijn om in een vroeg stadium de ketengovernance in de B-situatie (tijdelijk) vast te stellen, waardoor een afgebakende groep van partijen verantwoordelijk wordt gemaakt om tot een technologische oplossing te komen. Uiteraard is ook dit niet eenvoudig, niet in de laatste plaats, omdat het vraagt om een prominente en daadkrachtige rol voor de overheid of andere betrokken partijen. Een iteratieve aanpak tussen de twee uitersten lijkt ook mogelijk, zolang ketenpartijen maar voortdurend blijven werken aan ofwel het verder ontwikkelen van de technologie ofwel het optuigen van de ketengovernance in de B-situatie. Het ontbreken van een focus op één van beide dimensies (ofwel: een poging om de technologie en de ketengovernance gelijktijdig en in samenhang verder te brengen) zal waarschijnlijk leiden tot stagnatie.

Voor acceptatie en implementatie geldt dat dit in sterke mate iteratief geschiedt. Er zijn verschillende implementatie- en acceptatierondes nodig, waarin steeds opnieuw de puzzel moet worden gelegd. Voorlopers implementeren alvast, werken ondertussen aan acceptatie door anderen, die door de eerste implementaties bevorderd wordt, en vervolgens kan de besturing daarop aangepast worden. Het is hierbij van belang dat betrokkenen blijven herijken. B kan immers sterk veranderen in dit proces. Een roadmap op hoofdlijnen kan hierbij als belangrijk richtpunt blijven gelden. Tijdens het traject kunnen de partijen die eerder hebben geïmplementeerd te maken krijgen met teleurstellingen als B sterk veranderd is ten opzichte van datgene wat zij destijds geaccepteerd en geïmplementeerd hebben. Bijvoorbeeld wanneer zij de baten van de B-situatie hebben overschat, of andere relevante punten (bijvoorbeeld verplichtingen in de nieuwe ketengovernance) zich niet hebben beseft.

4.5.4 *Discussie*

In dit hoofdstuk hebben we ons gericht op het vormen van een handvat voor het beantwoorden van het besturingsvraagstuk, daarbij beseffende dat een veelheid aan thema's links blijven liggen. Eén hoofdstuk leent zich er ook niet voor om het besturingsvraagstuk volledig en uitdiepend te onderzoeken. Door een viertal kanttekeningen aan de bijdrage te benoemen, solliciteren we naar meer bijdragen op dit gebied.

Ten eerste hebben we het besturingsvraagstuk vooral beschouwd vanuit de contingentietheorie. Dit hebben we gedaan om nadruk te kunnen leggen op twee belangrijke contigenten en de relatie (fit) hiertussen. Jacobson (2009) geeft aan dat ook andere theorieën (waaronder de transactiekostentheorie en de agency theorie) waardevolle inzichten bieden op governance kwesties. Binnen de kaders van de contingentietheorie is het mogelijk om naar meerdere contigenten binnen systemen te kijken. We hebben in dit hoofdstuk twee contigenten een centrale rol gegeven: governance en technologie. Contingenten als leiderschap, informatieposities, cultuur en competenties van betrokkenen zijn, gezien de focus van dit hoofdstuk, nauwelijks uitgediept.

Ten tweede baseerden we het aangereikte handvat grotendeels op één casus (SBR). Meerdere casussen zouden een verrijkt handvat kunnen opleveren.
Ten derde zijn we beperkt ingegaan op de benodigde competenties van managers en bestuurders. Zonder kennis van deze competenties is de 'wie-vraag' moeilijker te beantwoorden.

Ten vierde is de koppeling tussen de kenmerken van een wijziging en criteria voor toepassing van een sturingsinstrument, of een veranderstrategie en de bijpassende betrokkenheid van actoren op basis van hoofdstuk 3, deels op de praktijk gebaseerd maar ook deels theoretisch. Nader onderzoek en aanvullende praktijkervaring zal verder kunnen uitwijzen hoe toereikend een bepaald instrument of bepaalde strategie is voor het besturen van de verschillende wijzigingen.

Vanuit deze kanttekeningen bezien vormt dit hoofdstuk naast een handreiking voor bestuurders ook een uitnodiging naar onderzoekers om het besturingsvraagstuk bij keteninformatiesystemen verder te ontleden en te onderzoeken. Rekening houdend met de toename van keteninformatiesystemen, en daarmee ook het aantal te besturen wijzigingen in informatieketens, kunnen we met vertrouwen stellen dat meer onderzoek – het liefst uitgekristalliseerd in aanvullende handvatten – van harte welkom is.

4.6 Afsluiting

In de inleiding van dit hoofdstuk introduceren we het besturingsvraagstuk van keteninformatiesystemen: het bepalen wie (welke ketenactoren) een wijziging op welke manier (veranderstrategie en sturingsinstrument) moeten besturen. Als we op zoek gaan naar kennis en begrip over het besturingsvraagstuk in de literatuur over keteninformatiesystemen, dan valt op dat een integrale behandeling van het vraagstuk ontbreekt.

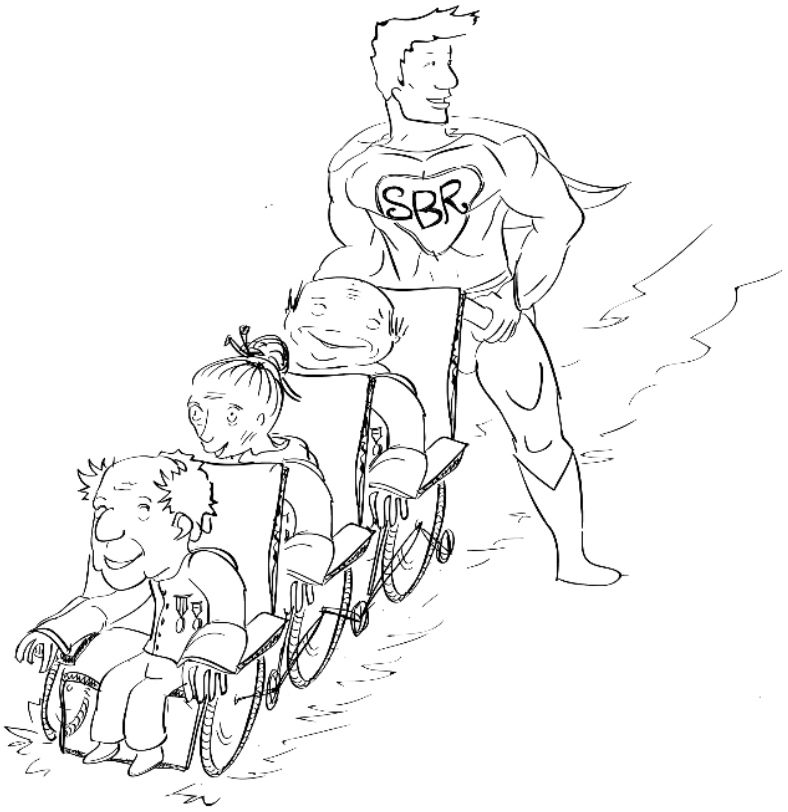
In dit hoofdstuk komen we – met de bovenstaande discussiepunten in acht nemend – tot een handvat bij het beantwoorden van het besturingsvraagstuk. Voor het besturen van een wijziging is het bepalend of ten eerste de B-situatie bekend is (ja/nee), en ten tweede op welke dimensie de wijziging betrekking heeft (technologie en/of ketengovernance). Ook kan meespelen of een wijziging voorzien en repetitief is (ja/nee). Zo maken we een onderverdeling in totaal vier typologieën en drie scenario's van wijzigingen. Voor vier typologieën van wijzigingen (daar waar B bekend is) behandelen we het besturingsvraagstuk door de betrokkenheid van ketenactoren te beschrijven en aan te geven welke veranderstrategie en welk sturingsinstrument geschikt zijn. Voor drie scenario's van wijzigingen (daar waar B onbekend is) geven we aanwijzingen.

Tijdens ons onderzoek naar het besturingsvraagstuk hebben we de SBR casus gebruikt. Hierdoor is verder inzicht verkregen in de opgave waar de betrokken partijen binnen SBR mee te maken hebben. Binnen SBR was er al vrij snel een visie op de technologie en een schets van de architectuur. De technologie in de B-situatie was echter nog onbekend, hetzelfde gold voor de B ketengovernance. In Wunderbare Reisen zu Wasser und zu Lande: Feldzüge und lustige Abenteuer des Freiherrn von Münchhausen (Bürger, 1923) valt te lezen dat Baron von Münchhausen zichzelf redt van een vrijwel zekere dood in het moeras door op eigen kracht zichzelf aan zijn haren uit het moeras te trekken. Het volksverhaal staat symbool voor het vinden van een oplossing voor een vrijwel onmogelijke opgave, in afwezigheid van een externe handreiking. In de context van keteninformatiesystemen zien we dat de externe handreiking – in de vorm van hulp die besturing biedt – niet altijd aanwezig is, ook op momenten wanneer dit juist het hardst nodig is. Binnen SBR is deze opgave overwonnen, doordat een beperkt aantal ketenactoren van wat uiteindelijk de B ketengovernance zou worden, blijvend mogelijkheden wisten te creëren om de ontwikkeling in technologie voort te zetten, óók in afwezigheid van de uiteindelijke besturing. Bovendien richten zij zich stapsgewijs op de realisatie van intensievere en meer opdrachtgestuurde samenwerking en de uiteindelijke besturing.

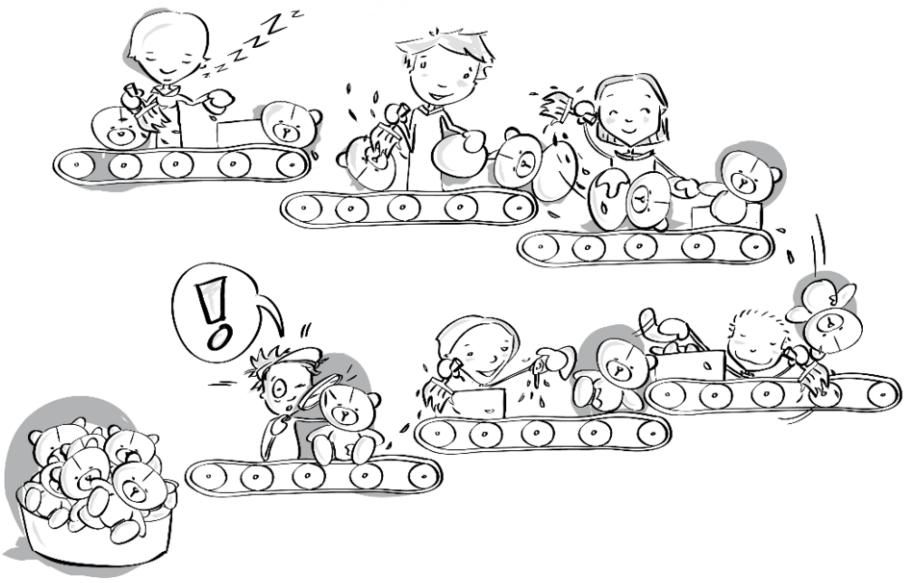
Met dit hoofdstuk sluiten we deel A – SBR als opgave – af. Tijdens ons onderzoek naar het besturingsvraagstuk zijn we een aantal relevante punten tegengekomen voor deel B. Er is nogal wat gezegd over wat een goede ketengovernance is. Onder andere komt naar voren dat een goede ketengovernance antwoord geeft op hoe er met wijzigingen binnen de informatieketen wordt omgegaan en dat de ketengovernance een fit dient te hebben met de technologie. Merk op dat in hoofdstuk 1 is aangegeven dat informatieketens met pluriforme actoren/informatiestromen een flexi-

bele technologie behoeven, met als gevolg dat – om deze fit te behouden – de ketengovernance tevens flexibel dient te zijn. Bovendien is het noodzakelijk om periodiek de ketengovernance te evalueren om vast te stellen of deze toereikend is. Ook is er aangegeven dat wijzigingen in lijn dienen te zijn met de principes die zijn afgesproken. Ook voor SBR zijn deze principes afgesproken, teneinde de technologie blijvend flexibel en schaalbaar te houden. In deel B gaan we nader in op hoe de ketengovernance er binnen SBR uitziet.

Deel B – SBR als oplossing



5 I-Processen



5.1 Het containerbegrip ‘processen’ verder geconcretiseerd

Dit hoofdstuk gaat over de processpecificaties als bouwblok van de SBR oplossing. We gaan eerst in op het containerbegrip ‘processen’. Daarbinnen kunnen we een specifieke categorie onderscheiden: informatieverwerkingsprocessen, in de literatuur ook wel informatieprocessen genoemd (i-processen). We bespreken de kenmerken van het werken met i-processen. Vervolgens zoomen we in op SBR. In de context van SBR voert een gedeelde dienstverlener bepaalde onderdelen van de i-processen voor de uitwisseling en verwerking van verantwoordingsinformatie uit.

In dit hoofdstuk willen wij de personen die met de herinrichting van informatieketens te maken krijgen, handvatten bieden om het abstracte fenomeen ‘i-processen’ op een gerichte wijze toe te passen bij het ontwerpen van informatieketens. Hierbij

beginnen wij met de algemene karakteristieken van processen, waarna wij SBR gebruiken als casus om duidelijk te maken hoe deze algemeenheden op een systematische wijze om te zetten zijn naar een specifieke en gestructureerde procesimplementatie en procesbeheer. Bijzondere aandacht gaat uit naar de gestandaardiseerde procesonderdelen van SBR gericht op informatieverwerking. Het subject van de SBR i-processen is de XBRL-instance (zie voor nadere toelichting hoofdstuk 6 - Gegevens). Deze generieke i-processen worden dankzij de generieke procesinfrastructuur, (Digipoort) die zorgt voor S2S-integratie, met name geautomatiseerd afgehandeld. De specificaties voor de i-processen zijn net als de berichtspecificaties definiërend voor de services en de onderliggende techniek die uitvoering geven aan de i-processen. Deze componenten worden los van elkaar onderhouden en gewijzigd, maar hangen wel nauw met elkaar samen. Het hoofdstuk over de technische inrichting van SBR (hoofdstuk 7) maakt deze samenhang nog duidelijker zichtbaar. Tot slot geldt dat er op het gebied van procesautomatisering rondom deze i-processen nog een aantal vraagstukken open staat en ontwikkelingen lopen die het noemen waard zijn.

Samenvattend beantwoordt dit hoofdstuk de volgende zeven vragen, die de inhoudsopgave van dit hoofdstuk vormen:

1. Wat is een proces?
2. Wat is een goed proces?
3. Welke managementfilosofieën over procesverbetering zijn er?
4. Hoe onderhoud je een goed proces?
5. Welke tooling en methoden kunnen we gebruiken voor ontwerp en onderhoud?
6. Wat zijn specifieke eisen aan SBR i-processen?
7. Welke relevante vraagstukken en ontwikkelingen zijn er rond i-processen?

5.2 Wat is een proces?

De eenvoudige definitie van een proces is: een geordende set van taken met een vastgesteld doel. Het idee proces is breed toepasbaar. In de praktijk heeft deze brede toepasbaarheid positieve en negatieve effecten. Positief is dat het idee processen een generieke formule biedt die toepasbaar is op veel verschillende vakgebieden, waardoor er veel literatuur voorhanden is over de wijze waarop processen ingericht en beheerst kunnen worden. Er zijn verschillende theorieën die van toepassing zijn op praktisch alle processen: van het bereiden van een maaltijd tot het afhandelen van een XBRL-instance. Een negatief effect van het hoge abstractieniveau van het begrip proces is dat iedere praktijksituatie nog een specifieke vertaling van het processenbegrip vereist (van globale opzet naar werking). Deze slag is moeilijk en wordt niet altijd gemaakt. Hierdoor blijft men hangen in algemeenheden, het niveau 'waar alles nog klopt'. Een voorbeeld hiervan is dat het standaard ITIL-changemanagement proces is overgenomen, terwijl er niet kritisch gekeken is of deze invulling voor de specifieke situatie wel de handigste is. Hierdoor komen uit de beschrijving geen richtlijnen naar voren hoe het management dient te handelen bij verschillen van inzicht. Een ander effect is het te eenzijdig richten op de 'happy flow' – vaak beschreven in algemene voorbeelden en zonder met uitzonderingen rekening te houden. Dit terwijl de kwaliteit van een proces in de praktijk juist bepaald wordt door de wijze waarop

het de uitzonderingen weet te beperken en hoe het de impact van uitzonderingen weet te minimaliseren.

Het lezen van dit boek kun je ook zien als een proces, waarbij een aantal stappen wordt doorlopen met een vastgesteld doel. Het boek moet gevonden en geopend worden, waarna de volgende stap het daadwerkelijke lezen is. Processen worden in de bedrijfskundige en organisatiekundige literatuur vaak gezien als taken die in de tijd uitgevoerd worden (Davenport, 1993). Davenport and Short (1990) definiëren een proces als "*a set of logically related tasks performed to achieve a defined business outcome for a particular customer or market*". Terwijl Hammer and Champy (1993, p. 53) een proces definiëren als "*a collection of activities that takes one or more kinds of input and creates an output that is of value to the customer. A business process has a goal and is affected by events occurring in the external world or in other processes*". Deze definitie is gericht op het transformeren van input middels activiteiten in output. Door het uitvoeren van de individuele taken en te bekijken welke taak samenhangt met een andere taak wordt een procesbeschrijving gecreëerd. Taken krijgen input van voorgaande taken en creëren output die als input kan dienen voor de taken die daarna komen. Het gaat bij processen dus niet om de afzonderlijke individuele taken, maar juist de verbanden tussen de verschillende taken en de relaties met input en output leveren de toegevoegde waarde van de procesbeschrijving.

Een andere definitie van een proces is *"a lateral or horizontal organizational form, that encapsulates the interdependence of tasks, roles and people, departments and functions required to provide a customer with a product or service"* (Earl, 1994, p. 13). Deze definitie neemt een organisatorische invalshoek en richt zich op taken, rollen en de mensen die de taken uitvoeren. Een organisatie kan verschillende rollen bevatten, waarbij een actor een persoon is die vanuit een rol een bepaalde taak uitvoert. Personen kunnen meerdere taken en rollen uitvoeren. Een rol verwijst op abstract niveau naar wat een persoon moet doen zonder in de specifieke functies en taken te treden. Het is dus een abstracte manier van kijken naar het uit te voeren werk.

Weske (2007, p. 5) definieert een proces als "*a set of activities that are performed in coordination in an organizational and technical environment. These activities jointly realise a business goal*". Zijn definitie geeft aandacht aan de omgeving die bestaat uit socio-technische aspecten en aan het organisatiedoel van het proces. Dit laatste is belangrijk, omdat met het doel ook de voorwaarden waaraan een proces moet voldoen duidelijker worden. Als het doel verandert of verschuift, kan dit ook gevolgen hebben voor de inrichting van het proces. Waar het doel ingaat op de wat-vraag, gaan processen in op de hoe-vraag. Processen beschrijven *hoe* een keten of organisatie het wat (haar doel) verwezenlijkt.

In tabel 5.1 zijn de elementen van processen opgesomd. Het zijn de actoren die taken uitvoeren. Actoren kunnen zowel menselijk (een persoon of een team) dan wel geautomatiseerd (software) zijn in het geval van een elektronische taak. Bij het uitvoeren van processen worden resources gebruikt, bijvoorbeeld de tijd die een persoon besteedt aan een taak of de tijd die een server nodig heeft om een activiteit af te ronden.

Daarbij is relevant of taken geautomatiseerd worden uitgevoerd. In informatieketens worden typisch veel taken geautomatiseerd uitgevoerd. Een specifiek type taak in processen is de beslissing. Een beslissing vereist dat de actor de bijbehorende beslissing mag nemen. De omgeving heeft invloed op de uitvoering van het proces, voorbeelden hiervan zijn dat de geleverde informatie niet compleet of incorrect is en dat mensen ziek kunnen zijn. Verstoringen komen vaak voort uit de omgeving die in meer of mindere mate beïnvloed kan worden. Bij Six Sigma (zie § 5.4.8) gaat het met name om het reduceren van verstoringen.

Tabel 5.1 – Elementen van processen

Proceselementen	Beschrijving
Actor	Diegene die of datgene wat een bepaalde processtap uitvoert.
Resources (bronnen)	Datgene wat nodig is om de taak uit te voeren, hetgeen zowel betrekking kan hebben op een handmatige of geautomatiseerde taak. Bij de eerste wordt de tijd en energie van de actor gebruikt, bij de tweede gaat het bijvoorbeeld om de processing capaciteit van hardware.
Input	Datgene wat nodig is om de eerste taak in een proces te starten of wat uit voorgaande taken meegenomen wordt om een opvolgende taak uit te voeren. Vaak betreft dit informatie en beslissingen uit voorgaande stappen.
Taak (transformatie)	De taak die input tot output transformeert.
Beslissing	Een specifieke taak waarbij een besluit wordt genomen.
Taakuitvoering	De wijze waarop een taak uitgevoerd wordt (elektronisch, handmatig, etc.).
Omgeving	De omgeving beïnvloedt het proces en kan effect hebben op het verloop en daarmee de voorspelbaarheid van het verloop van het proces.
Output	Het resultaat van de taak die gebruikt kan worden als input voor volgende taken.
Doel	Een proces is doelgericht in de zin dat door de uitvoering van verschillende taken een bepaalde uitkomst nagestreefd wordt.
Proceseigenaar	Degene die verantwoordelijk is voor het verloop, beheer en de verbetering van het proces van begin tot einde.
Procesbeheersing en -aansturing	De procesaansturing zorgt ervoor dat na het aflopen van een taak de volgende taak gestart wordt en dat als er ongeregeldheden zijn, zoals taken die te lang duren, er wordt ingegrepen.

Naast het uitvoeren van taken en het nemen van een beslissing zijn er voor de procesbeheersing en –aansturing vaak proceseigenaren aangesteld. Waar actoren voor een bepaalde taak verantwoordelijk zijn en een afdelingshoofd voor de taken binnen haar afdeling, wordt van een proceseigenaar verwacht dat hij het grotere plaatje in de gaten houdt en zorgt dat het proces van begin tot einde soepel verloopt en verbeterd wordt indien nodig. Een proces loopt vaak door meerdere organisatorische eenheden heen. Dit kunnen afdelingen zijn of zelfs verschillende organisaties betreffen. Het wordt als een goed organisatieprincipe gezien om voor elk proces binnen de organisatie ook proceseigenaren aan te wijzen. De proceseigenaar kan dan zorgen dat er mechanismen zijn om processen goed te doen lopen en te evalueren en te verbeteren.

5.2.1 *Procesclassificaties*

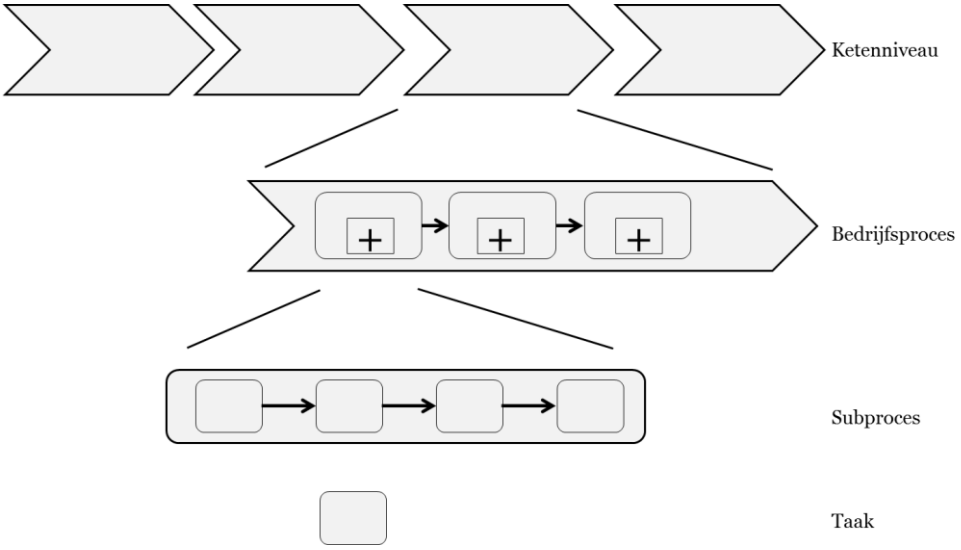
Processen zijn op verschillende wijzen te classificeren, waaronder de scheiding tussen:

- Fysieke- en informatieprocessen
- Primaire, sturende, ondersteunende en strategieprocessen
- Keten-, bedrijfs- en subprocessen
- Processen met een lage of hoge automatiseringsgraad
- Processen die vaak of incidenteel voorkomen
- Gestructureerde of ongestructureerde processen

We associëren processen vaak met fysieke en operationele processen. In dit hoofdstuk gaan we verder echter alleen in op i-processen (informatie(verwerkings)processen) en laten we de fysieke processen voor wat ze zijn. Wel kan een aantal van de theorieën die we bespreken ook worden toegepast op fysieke processen. Zoals in hoofdstuk 2 besproken, is dit een wezenlijk verschil. Waar fysieke processen vaak direct zichtbaar zijn, is het bij i-processen veelal lastig of zelfs onmogelijk om deze met het blote oog te zien. Naast de operationele processen zijn er ook ondersteunende processen. Denk bijvoorbeeld aan financiële, human resource management (HRM), richtinggevende, management- en veranderingsprocessen (Armistead, Pritchard, & Machin, 1999).

Vanuit het systeemperspectief wordt er vaak onderscheid gemaakt tussen primaire, sturende of beherende en ondersteunende processen (Weske, 2007). Primaire processen zijn de processen waarop de keten drijft. Als die wegvallen, dan valt de keten stil. Sturende of beheerprocessen zijn nodig om de primaire processen aan te sturen. Dit kan op kortere of langere termijn zijn. Ondersteunende processen zorgen ervoor dat de primaire processen doorgang kunnen vinden, bijvoorbeeld door het aannemen van personeel. Hiernaast zijn er nog de strategieprocessen, gericht op het ontwikkelen en uitvoeren van strategieën.

Een andere indeling van processen is de indeling naar aggregatieniveau. Een proces is van hoog naar laag te demonteren in kleinere delen. Deze decompositie in fijnmazige delen is belangrijk, omdat verschillende actoren geïnteresseerd zijn in verschillende niveaus en elk niveau zijn eigen vraagstukken kent. Een organisatorische eenheid die een proces uitvoert, kan als een schakel in een keten van processen gezien worden.



Figuur 5.1 – Decompositie van ketens in taken

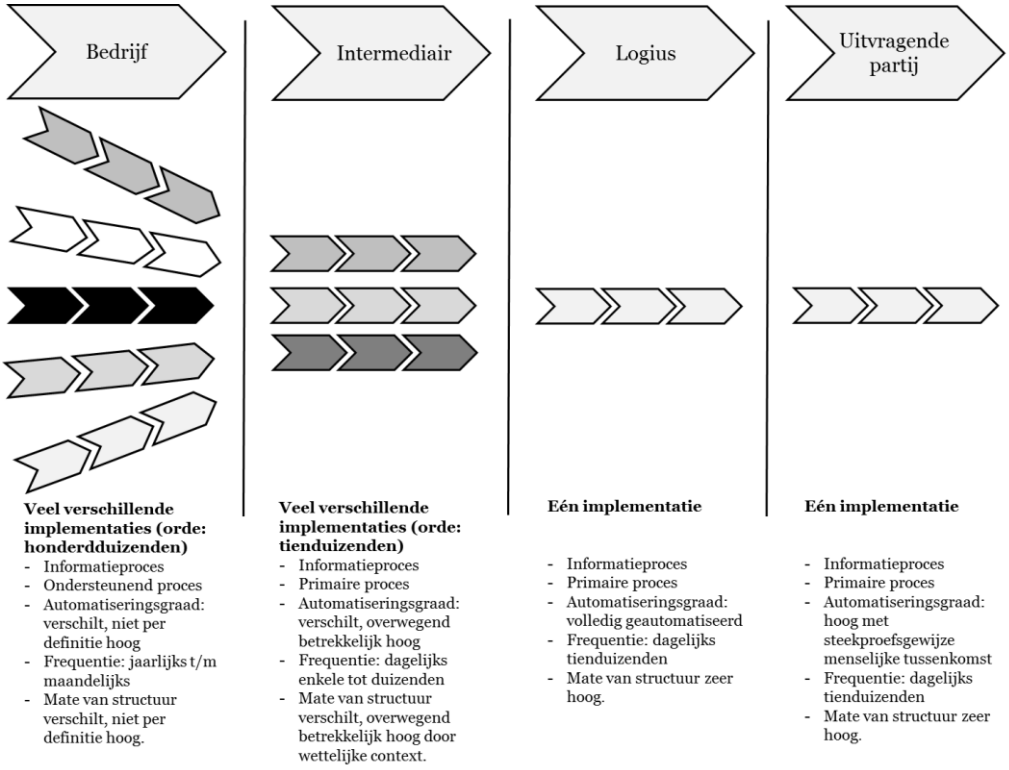
Een andere nuttige indeling van processen is naar het niveau van automatisering. Sommige processen zijn volledig geautomatiseerd en kunnen daardoor grote volumes snel afhandelen. Andere processen vereisen echter menselijk activiteiten, al is het alleen maar voor de besluitvorming of de afweging van conflicterende regels. Gestructureerde i-processen met hoge volumes lenen zich het beste voor automatisering en het behalen van schaal- en efficiëntievoordelen.

De mate van herhaling van een proces is een volgende indeling. Een investering in processen die veel gebruikt worden, loont meer. Bij hoge volumes is het belangrijk om een hoge efficiëntie te hebben, waarbij dit met incidentele processen minder nodig is.

Een laatste belangrijke classificatie van processen is de mate waarin ze gestructureerd zijn. Goed gedefinieerde en gestandaardiseerde processen zijn vaak betrouwbaar en bewezen en leiden tot een voorspelbare uitkomst. Niet-gestructureerde processen zijn moeilijk te volgen en kunnen onverwachte uitkomstmogelijkheden hebben. De meeste strategieprocessen vallen onder de laatste categorie. Bij semi-gestructureerde processen is vaak op hoog abstractieniveau de volgorde duidelijk (bijvoorbeeld aanvraag, informatie verzamelen, besluitvorming en communiceren), maar kunnen de specifieke taken op velerlei manieren ingevuld worden.

In de SBR-verantwoordingsketens vinden we processen met verschillende classificaties terug. Binnen een bedrijf is de verantwoording te karakteriseren als een ondersteunend proces dat enkele malen per jaar uitgevoerd wordt en dat niet per se geautomatiseerd of gestructureerd hoeft te verlopen (denk aan de bekende schoenendoos in het kader van de belastingaangifte). Bij Logius komen echter miljoenen berichten per jaar langs en daarom is het Logius-proces te karakteriseren als een primair pro-

ces dat volledig geautomatiseerd dient te zijn. Het onderstaande figuur geeft de proceskarakteristieken voor de verschillende schakels binnen één verantwoordingsketen weer.



Figuur 5.2 – Proceskarakteristieken voor de verschillende schakels binnen één verantwoordingsketen

5.2.2 *Procesharmonisatie bij SBR*

Het bestaan van intermediairs in verantwoordingsketens is voor een deel te verklaren uit het streven naar kosteneffectiviteit. Voor het samenstellen van bijvoorbeeld een goede aangifte of een financieel jaarverslag is specialistische kennis nodig. Een ondernemer heeft deze kennis niet standaard in huis en voor het beperkt aantal keren dat deze kennis vereist is, zegt de kerncompetentie theorie dat het handig is deze taken uit te besteden aan een specialist (Drejer, 2002). Deze specialist (in dit geval een intermediair) heeft meerdere klanten en handelt hetzelfde proces dus veel vaker af. Hierdoor loont het voor intermediairs te investeren in structurering en automatisering van het proces. De totale verantwoordingsketen kan hierdoor kwalitatief beter worden en de totale transactiekosten kunnen daardoor omlaag gaan. Met SBR standaardiseren verschillende uitvragende partijen de wijze waarop zij verantwoordingsinformatie aangeleverd willen krijgen. Ondernemers en intermediairs kunnen hierdoor voor verschillende soorten verantwoording procesonderdelen verder harmoniseren. Dit betekent nog grotere volumes over hetzelfde proces, dus nog meer

schaalvoordelen en lonende investeringen in verdere automatisering. Op basis van de XBRL-taxonomie kunnen uit één administratie geautomatiseerd meerdere verantwoordingsrapportages gegenereerd worden. Hier komt de slogan '*store once, report many*' vandaan. Dit principe zorgt ervoor dat in de verantwoordingsketen nog een verdere procesintegratie mogelijk is. De uitvragende partijen kunnen, op dezelfde wijze als Logius, de afhandeling van verschillende informatieverwerkingsprocessen geautomatiseerd laten uitvoeren. Ook hier zorgt de taxonomie ervoor dat één component (validatieservice) toepasbaar is op verschillende inhoud. In de praktijk zie je dat anno 2011 deze integratie langzaam maar zeker vorm begint te krijgen. Er zijn enkele grote accountantskantoren die voor verschillende verantwoordingsprocessen de benodigde processtandaardisatie hebben doorgevoerd.

5.2.3 *Black box, white box*

Wanneer er verschillende processen in een keten gekoppeld zijn, kunnen betrokken actoren op verschillende wijzen naar elkaars schakels kijken. Bij een black box perspectief zijn partijen naast hun eigen proces alleen geïnteresseerd in de interfaces, de koppelvlakken, tussen de voorafgaande en opvolgende schakels. Hoe het proces in een opvolgende schakel eruitziet doet er niet toe, als deze maar op basis van de gevraagde input de verwachte output levert. Bij een white box perspectief ontrafelen de actoren elkanders processen tot het laagste niveau. Beide aanpakken hebben voor- en nadelen.

Voordeel van de black box benadering is een lage ketencoördinatielast. Hier tegenover staat wel een risico van keten suboptimalisatie. Partijen kunnen ongemerkt activiteiten dubbel uitvoeren. Verder kunnen zaken als end-to-end beveiliging minder aandacht krijgen. Ketenpartners richten zich bij deze benadering immers alleen op degene met wie ze direct contact hebben en niet op degenen die verderop in de keten zitten. Een zwakke schakel kan hiermee alle investeringen in beveiliging van de overige schakels teniet doen. Het tegenovergestelde kan zich ook voordoen, namelijk dat iedere schakel veel investeert in beveiligingsmaatregelen op het koppelvlak, terwijl dit eigenlijk, gezien bepaalde procescontroles in verdere schakels, niet nodig is. Wel moet opgemerkt worden dat schakels vanuit beveiligings- of concurrentieperspectief gedwongen kunnen zijn tot een black box benadering. Bij een white box benadering is er een mogelijkheid processen meer lean in te richten. Dubbelingen in activiteiten vallen eerder op. Tevens kunnen controles beter op elkaar afgestemd worden. Het belangrijkste nadeel van de white box benadering is de hoge participatiekosten (partijen moeten zich in elkaars processen verdiepen) en het risico om tijdens de afstemming te ver in detail te treden en de grote lijnen uit het oog te verliezen. Bij een grey box benadering zie je dat partijen op essentiële punten naar elkaar transparant zijn. Bij de overige zaken wordt een meer gesloten (black box) benadering gehanteerd door te focussen op de input en output.

Binnen een SBR verantwoordingsketen zien we in de expertgroep processen en techniek een grey box benadering. De verschillende ketenpartners bespreken de wijze waarop zij omgaan met zaken als end-to-end beveiliging. Hierbij zijn er in de keten wel verschillende black box relaties en white box relaties te onderkennen. Allereerst zijn de uitvragende partijen geïnteresseerd in het detailniveau van de processen die Logius afhandelt. Dit is logisch daar zij zeer afhankelijk zijn van deze partij. Logius

moet een zekere mate van inzicht in de processen van de uitvragende partijen hebben en de ontwikkelingen daarbinnen. Dit om in te kunnen schatten welke impact wijzigingen kunnen hebben op het ketenproces en wat er van Logius verwacht wordt. De wijze waarop intermediairs en ondernemingen werken, verschilt nogal en is dientengevolge in veel mindere mate transparant. Waarbij wel geldt dat een aanzienlijk deel van de intermediairs (bijvoorbeeld RA/AA) vanuit de beroepsvereniging waarbij zij aangesloten zijn, gedwongen zijn conform bepaalde procesvoorschriften te werken.

Logius geeft inzicht in de processen door middel van het beschikbaar stellen van processpecificaties, één van de bouwblokken van SBR. Een processpecificatie is een beschrijving van de wijze waarop de uitvragende partij de aangeboden of aan te bieden gegevens wil verwerken, ofwel een beschrijving van het informatieverwerkingsproces. Naast het inzicht in de wijze waarop processen door schakels zijn beschreven of ingericht (opzet en bestaan), kunnen partijen ook geïnteresseerd zijn in de vraag of een schakel inderdaad werkt zoals men verwacht. In het geval van bijvoorbeeld Logius is het handig hier een onafhankelijke deskundige partij een verklaring over af te laten geven. Wanneer de zogenaamde third party mededeling een goede reikwijdte heeft, kan een organisatie aan alle relevante schakels in één keer verantwoording afleggen. De verantwoording van Logius ziet er, kort door de bocht, als volgt uit:

- Logius handelt de overeengekomen processen conform de processpecificaties af. Deze beschrijvingen gaan in op het niveau van het subproces (zie figuur 5.1).
- Logius heeft maatregelen genomen (technisch en procedureel) om de overeengekomen service levels met voldoende mate van zekerheid te kunnen garanderen.

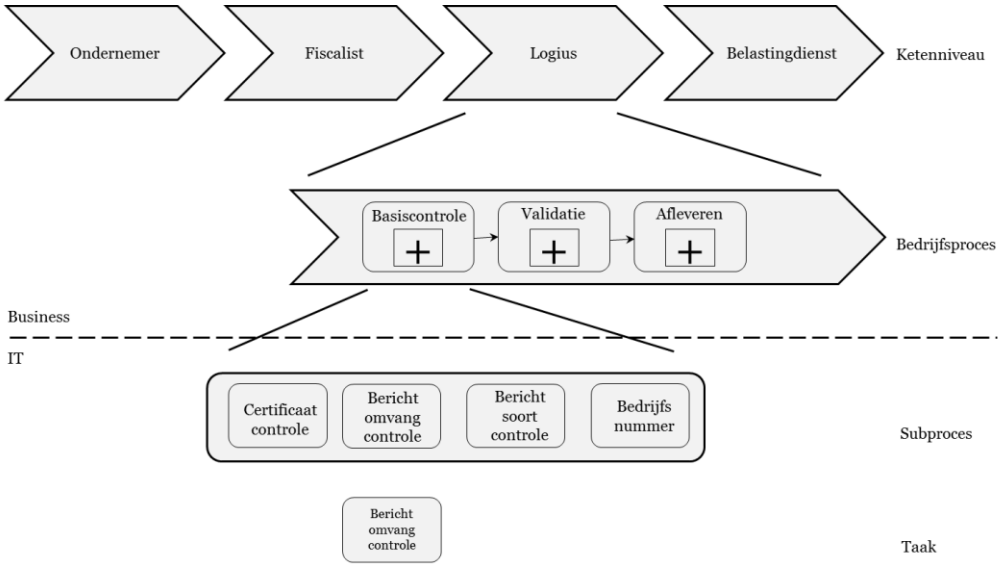
Er is een trend gaande waarin organisaties van ketenpartners verwachten dat zij een proactieve houding hebben en dat zij belanghebbenden op de hoogte stellen wanneer er fouten gemaakt zijn in het proces. Overheidsinitiatieven als horizontaal toezicht sluiten hierbij aan.

In de film Fight Club geeft één van de hoofdpersonen een cynische voorstelling van een autofabrikant die zuiver vanuit het financiële perspectief van de eigen schakel bepaalt hoe het met productiefouten omgaat:
"*A new car built by my company leaves somewhere traveling at 60 mph. The rear differential locks up. The car crashes and burns with everyone trapped inside. Now, should we initiate a recall? Take the number of vehicles in the field, A, multiply by the probable rate of failure, B, multiply by the average out-of-court settlement, C. A times B times C equals X. If X is less than the cost of a recall, we don't do one*."
Dit zwarte scenario staat haaks op de trend waarin ketens vanuit het ketenbelang en vanuit meer zachte waarden zoals bijvoorbeeld milieu, consumentenveiligheid en dierenwelzijn met elkaar spreken over hoe een probleem binnen een schakel aan te pakken.

5.2.4 *Van Business- naar IT-proces*

I-processen vormen over het algemeen een concept waarbinnen de mensen van zowel de IT als de business elkaar vinden en worden gebruikt om de technologie aan

ketenprocessen te verbinden. Figuur 5.3 laat schematisch zien dat bij SBR de business kan gaan over het ketenniveau en het bedrijfsproces. De onderkant is het speelveld van IT, dat de generieke processen doorvertaalt in uitvoerbare subprocessen en taken. Daarmee functioneren processen veelal als spil tussen IT aanbod en organisatiebehoefte. Zowel de IT als de business kunnen over processen praten en begrijpen deze, alhoewel het abstractieniveau verschilt en ze naar andere zaken kijken. Zwart-wit gesteld: de bedrijfskant denkt in termen van hoe waarde te creëren en wat nodig is en de IT-kant denkt in termen van hoe dit technisch te realiseren valt. Zij bepalen welke taken automatisch afgehandeld kunnen worden en welke technologie hiervoor nodig is.



Figuur 5.3 – Van business- naar IT-proces binnen SBR

5.3 Wat is een goed proces?

Een goed proces zorgt ervoor dat het doel, dat met de uitvoering van het proces is beoogd, ook daadwerkelijk behaald wordt. Vaak gaat het erom de vooraf gedefinieerde output tegen zo min mogelijk tijd, geld en middelen te realiseren. Dit lijken eenvoudig vast te stellen indicatoren, maar de werkelijkheid is complexer:

- Tijd, geld, kwaliteit en middelen kunnen concurrerende eisen zijn. De doorlooptijd kan groter worden naarmate de kostenefficiëntie toeneemt.
- De beoordeling kan verschillen bij het toepassen van de indicatoren op het proces of op de totale context. Gaat het om een efficiënte keten, een efficiënte schakel of een efficiënt bedrijf?
- Focus op efficiëntie kan conflicteren met menselijke waarden. De taakdiepte of taakbreedte is bepalend voor de motivatie van de personen die het proces moeten uitvoeren. Denk hierbij aan het verzet bij de spoorwegen tegen het ‘rondje om de kerk’.

- Bij repeterende processen gaat het altijd om gemiddelden en spreiding. Hier zullen bijvoorbeeld de volgende afwegingen een rol spelen: een gemiddeld snelle doorlooptijd, maar met een grote spreiding, heeft als gevolg dat er soms een lange doorlooptijd optreedt. Het alternatief is gemiddeld een iets minder snelle doorlooptijd, maar met amper spreiding en daardoor minder negatieve uitschieters.
- Beveiliging en/of bescherming van het algemeen belang of de consument vragen om maatregelen die het proces minder efficiënt maken. Een complexe authenticatie (verplicht een complex wachtwoord bij inloggen en het gebruik van een token) maakt het werk omslachtiger, maar veiliger. De verplichte controle van de accountant op de jaarrekening maakt het proces complexer, maar geeft zekerheid aan het maatschappelijk verkeer.
- Soms is het uitvoeren van het proces een doel op zich. Het gaat hier vaak om spelprocessen (de puzzel werd niet opgelost, de wedstrijd werd verloren, maar het proces was leuk).

Organisaties zullen de kwaliteit van processen beoordelen langs hun eigen waarden, waarbij zij zich in meer of mindere mate aangesproken voelen door onderstaande concurrerende uitersten (gebaseerd op Cameron, & Quinn, 2006):

- Een goed proces bestaat uit een dynamische en vernieuwende werkwijze.
- Een goed proces bestaat uit een efficiënte en gestructureerde werkwijze.
- Een goed proces bestaat uit een werkwijze die sterk aansluit bij de behoefte van de markt.
- Een goed proces bestaat uit de (vanuit menselijk perspectief) meest harmonieuze werkwijze.

Bij procesontwerpen binnen SBR is er een spanning tussen architecten die in de eerste plaats affiniteit hebben met efficiëntie en architecten die juist het dienstbaar zijn aan de 'klant' in het ontwerp vooropstellen. Hier speelt vanzelfsprekend de spanning tussen een intern gerichte, maar efficiënte (kleine) overheid en de extern gerichte, servicegerichte overheid. Valkuil van de op efficiëntie gerichte architect is vervreemding van de praktijk, waardoor de overheid wellicht efficiënt opereert, maar de private ketenpartners alleen via kostbare constructies aan de eisen van de overheid kunnen voldoen. De gepercipieerde last, en hiermee het beeld van de overheid, blijft in dit geval groot. Valkuil van de dienstgerichte architect is dat deze alle voorkomende behoeften in de markt wil bedienen, wat het proces aan de kant van de overheid (of over de gehele keten) nodeloos complex en kostbaar maakt. Wanneer 99% van de betrokken private ketenpartners te maken krijgt met een 'lastiger' proces, met als achterliggende reden dat de overige 1% van de bedrijven geen aanpassingen hoeft te doen, kunnen hier vragen bij gesteld worden. Met name omdat voor de overheid geldt dat de interne procesafhandeling in dit soort gevallen een stuk kostbaarder wordt. Binnen SBR houden de architecten elkaar, mede door de werkwijze van duidelijke uitgangspunten vooraf en de timebox benadering, in evenwicht. De inrichting van de governance is erop gericht om het gehele end-to-end ketenproces in ogenschouw te nemen. Tevens is er binnen SBR veel aandacht voor het definiëren van doelgroepen en deze, wanneer nodig, afzonderlijk te behandelen, in plaats van hen door één proces te voeren. De uitzondering krijgt dan te maken met een heel eigen

proces. Dit is klantvriendelijk, maar kan ten koste gaan van de efficiëntie. Hergebruik is daarbij essentieel. Een grey box benadering wordt dan gebruikt waarbij de partijen op essentiële punten naar elkaar transparant zijn, maar zich bij overige zaken alleen op de input en output richten.

Een definitie van een goed proces is dus niet zonder meer te geven, maar er zijn voldoende aangrijpingspunten om gestructureerd met proceskwaliteit om te gaan. Onderstaande lijst is een niet uitputtend rijtje van proceseigenschappen die de procesanalist in zijn ontwerp of beoordeling mee kan nemen. Afhankelijk van de context zoekt de procesanalist naar het gewenste optimum. Vooral wanneer een proces op één van de punten slecht tot zeer slecht scoort, dient hier een heel goede motivatie voor te zijn.

- Een proces dient een duidelijk doel.
- Een proces is zo eenvoudig mogelijk.
- Een proces levert minimale defecten, minimale uitval.
- De effecten van uitzonderingen op de 'main stream performance' zijn maximaal beperkt.
- Een proces is uitvoerbaar.
- Een proces is schaalbaar.
- Een proces is bestuurbaar en controleerbaar.
- Een proces bevat geen activiteiten die geen waarde bijdragen.
- Een proces heeft een minimale hoeveelheid afval.
- Een proces voldoet aan de waarden van de organisatie.
- Een proces sluit maximaal aan bij de strategie en het beleid van de organisatie.
- Een proces voldoet aan wet- en regelgeving.
- Een proces heeft een eigenaar.
- Een proces is communiceerbaar.
- Een proces heeft duidelijke prestatieverwachtingen.

Relevant te noemen is het verschil tussen uitval, afval en verspilling. Uitval heeft betrekking op eind- of tussenproducten die afgekeurd worden. Afval zijn grondstoffen die tijdens productie verloren gaan en verspilling betekent dat er meer grondstoffen gebruikt worden dan volgens de norm is toegestaan. Een bericht met verantwoordingsinformatie dat door een uitvragende partij niet beoordeeld kan worden omdat er essentiële gegevens missen, kunnen we zien als uitval. ICT (geautomatiseerde controles) maakt het bij uitstek mogelijk om dit soort onnodige uitval te beperken.

Afval lijkt op het eerste gezicht een probleem dat zich met name toespitst op de fysieke ketens. Ieder geslacht dier levert een hoeveelheid risicomateriaal op dat vernietigd moet worden. Waar vroeger het afval bij voorkeur 'gestort' werd, kwam de politicus Lansink in 1979 met het volgende rijtje:[12]

[12] 'De ladder van Lansink', zie: http://nl.wikipedia.org/wiki/Ladder_van_Lansink

- Preventie
- Hergebruik (recyclen)
- Verbranden
- Storten

Later is dit rijtje verfijnd en is onder andere de categorie 'nuttig toepassen' toegevoegd. Op grote productieaantallen is de hoeveelheid afval goed te voorspellen. Er is steeds meer aandacht voor duurzame ICT.[13] Het afval in de informatieketen bestaat onder andere uit de energie die niet omgezet wordt in dataverwerking, maar in (ongebruikte) warmte. Door gebruik van andere materialen, bijvoorbeeld bio-based polymere glasvezel, kan het energieverbruik in datatransmissie tot 15 keer verminderd worden. Tevens kunnen afvalstoffen uit andere ketens, zoals mest en gft-afval, als materiaal (vervanger van olie en koper) in de ICT nuttig toegepast worden. De warmte die servers uitstralen kan gebruikt worden voor de verwarming van het kantoor van het datacenter.

5.4 Welke managementfilosofieën over procesverbetering zijn er?

Er zijn altijd processen te vinden die voor verbetering vatbaar zijn. Een externe prikkel vormt over het algemeen de aanleiding voor de herziening. Er moet bezuinigd worden, concurrenten hebben een kortere levertijd, het bedrijf heeft een nieuwe richtlijn voor informatiebeveiliging, een bedrijf wil zich profileren op duurzaamheid, een organisatie heeft te maken gehad met een groot incident waardoor er verantwoordingsinformatie verloren is gegaan etc. In principe is het goed wanneer een organisatie processen voor een specifieke verbetering tegen het licht houdt. Risico is echter wel dat de scope van de verbetering beperkt is en de verbetering niet plaatsvindt in het kader van concurrerende kwaliteitseisen aan het proces. In de loop der tijd kunnen hierdoor perverse effecten ontstaan. Aan de andere kant kan bij een bredere scope 'het betere' de vijand worden van 'het goede'. Een organisatie gaat dan van implementatie naar implementatie, terwijl juist in de verbouwingsperiode een bedrijf niet maximaal kosteneffectief opereert. Procesverbetering heeft dus heel wat voeten in de aarde en heeft al decennia de aandacht op zich weten te vestigen. In de loop van de tijd zijn er verschillende stromingen geweest die het procesdenken centraal gesteld hebben. Het procesdenken komt voort uit het industriële tijdperk, toen productieprocessen geautomatiseerd werden. In de loop van de tijd zijn deze werkwijzen ook vertaald naar de dienstensector en vanuit deze sector worden ze ook meer en meer binnen de overheid gebruikt. Veel van deze stromingen zijn gebaseerd op managementfilosofieën die bepaalde uitgangspunten als basis hebben. In dit boek werpen we een genuanceerde blik op een aantal van deze managementfilosofieën door de basisconcepten te beschrijven. Wij passen ze waar mogelijk toe op SBR.

[13] Zie ook: www.greenict.org

5.4.1 *Business Process Re-engineering*

Business Process Re-engineering (BPR) is een managementfilosofie die ervan uitgaat dat, om grote verbeteringen in organisaties teweeg te brengen, een fundamentele en radicale herstructurering van bedrijfsprocessen vereist is. De automatisering dient de herontworpen processen te ondersteunen. Tijdens de opkomst van de BPR managementfilosofie zijn er velerlei procesinrichtingsprincipes ontwikkeld. Een aantal hiervan is als universeel aan te merken (zie bv. O'Neill & Sohal, 1999; Weerakkody & Dhillon, 2008). Hammer bracht in 1990 de volgende principes te berde:

1. Organiseer rondom resultaten en uitkomsten in plaats van rondom taken. Dit kan tot gevolg hebben dat verschillende taken bij elkaar worden gevoegd. Het principe stelt dat samenhangende informatie die benodigd is voor een resultaat in één hand blijft.
2. Zorg dat degenen die de uitkomst van een proces moeten gebruiken ook het proces uitvoeren. Hierdoor worden de uitvoerders zelf verantwoordelijk voor een goede output en bij slechte output voelen zij zelf de pijn: lijdensdruk lijdt tot verbetering.
3. Zorg dat de informatieverwerkingsprocessen zo dicht mogelijk bij het werk worden geplaatst waar de informatie vandaan komt. Op deze manier worden zaken logisch bij elkaar geclusterd.
4. Behandel geografisch verspreide bronnen alsof deze op één punt zijn. Zo wordt vermeden om in termen van hier en daar te denken.
5. Verbind parallelle activiteiten met elkaar in plaats van de resultaten te integreren. Zo worden eventuele fouten bij het integreren van de uitkomsten van verschillende taken voorkomen.
6. Leg de besluitvorming daar waar ook het werk wordt uitgevoerd. De logica is dat degenen die het werk uitvoeren ook de meeste kennis hebben om een beslissing te nemen.
7. Zorg dat de checks en controles in het proces ingebakken zitten in de taken van het werk dat wordt uitgevoerd. Checks en controles moeten zo min mogelijk tot overhead leiden en zo dicht mogelijk bij de taken zitten waarop deze betrekking hebben, om te zorgen dat de lijnen kort zijn.
8. Zorg dat de informatie slechts één keer bij de bron verzameld wordt. Door de bron te gebruiken wordt voorkomen dat informatie vervormd raakt of dat onnodig fouten gemaakt worden.

Hammer en Champy (1993) hebben later nog twee additionele principes toegevoegd:

9. Processen kunnen verschillende varianten en versies hebben om klantgericht te worden.
10. Een casemanager moet zorgen voor een eenduidig contactpunt voor klanten, zodat zij niet van het kastje naar de muur gestuurd worden.

In het SBR-domein zien we de toepassing van enkele principes in het inrichtingsproces op verschillende niveaus terug:

Principe 1: Organiseer rondom resultaten en uitkomsten
De aansluitondersteuning binnen SBR is belegd bij één partij (accountmanagement), die verstand heeft van:

- de business (accountancy, fiscale wetgeving);
- gegevens, het creëren van een XBRL-instance;
- processen, de wijze waarop verantwoordingsinformatie door de overheid behandeld wordt;
- techniek, het gebruik van beveiligingscertificaten en webservices.

De accountmanagers zijn hierdoor in staat een partij te ondersteunen tot het moment dat het gewenste resultaat is bereikt: een softwareleverancier is in staat op basis van brondata een instance te creëren die valide is en weet deze via Digipoort (de generieke infrastructuur van de overheid) aan te leveren. Het is overigens belangrijk op te merken dat het hier gaat om toepassing in het inrichtingsproces en niet in het verantwoordingsproces.

Principe 3: Zorg dat de informatieverwerkingsprocessen zo dicht mogelijk bij het werk worden geplaatst waar de informatie vandaan komt. De softwaremarkt (boekhoudingspaketten, rapportagetools) maakt het mogelijk dat bedrijven (met hulp van de software) zelf hun boekhouding kunnen voeren en de accountant met name meekijkt. De befaamde schoenendoos met bonnetjes verdwijnt zo langzamerhand. Dit maakt het mogelijk om bepaalde taken al vroeg in de keten in te bouwen.

Principe 7: Zorg dat de checks en controles in het proces ingebakken zitten in de taken van het werk dat wordt uitgevoerd. SBR ondersteunt de trend dat softwareleveranciers steeds meer controles in de administratie- en rapportagesoftware inbouwen. Met de taxonomie kan zonder interpretatie getoetst worden aan de rapportageregels. Digipoort koppelt gefaseerd terug over opeenvolgende validaties. Hierdoor is een partij direct op de hoogte wanneer een bericht niet aan de acceptatie-eisen voldoet.

Principe 8: Zorg dat de informatie slechts één keer bij de bron verzameld wordt. 'Gegevens bij de bron' - '*store once, report to many*' - vormt feitelijk het fundament onder SBR. Een bedrijf kan vanuit één administratie aan de verschillende uitvragende partijen verantwoorden.

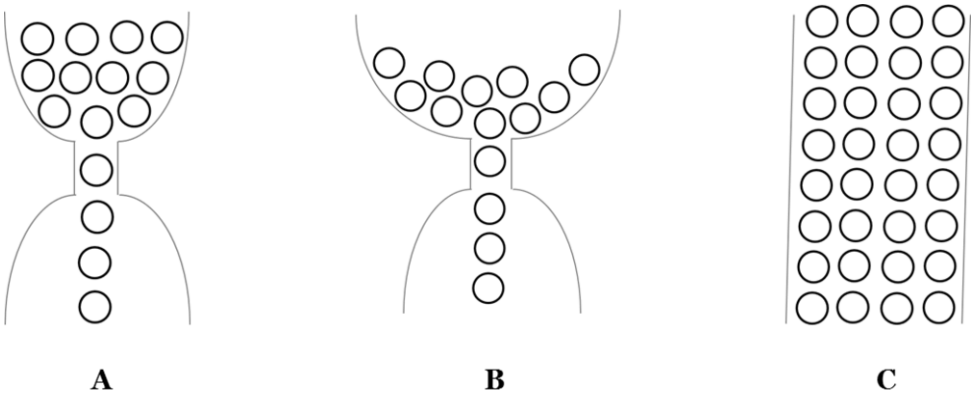
Principe 10: Een casemanager moet zorgen voor een eenduidig contactpunt voor klanten. Er bestaan al financiële adviseurs die recent zijn gaan werken met een relatiemanager, die voor hen de contacten onderhoudt met klanten. Zo hoeven de accountants en fiscalisten dat zelf niet meer te doen.

Ook de principes van Hammer kunnen in een ontwerp concurreren en de procesanalist zal hierin een balans moeten zoeken.

5.4.2 *Theory of Constraints*

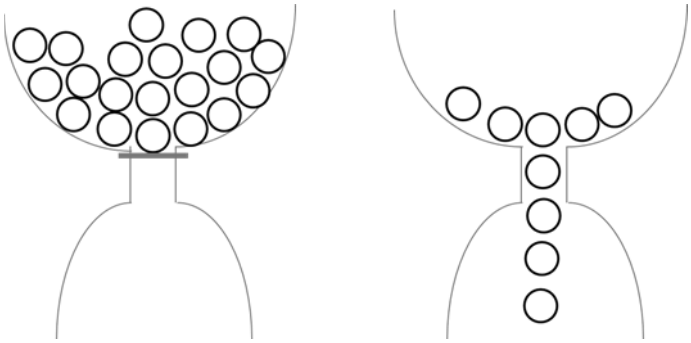
De Theory of Constraints (ToC) stelt dat een proces afhangt van de flessenhals (bottleneck) die het gehele proces vertraagt, en dat een keten dus zo sterk is als de zwakste schakel (Goldratt, 1997; Goldratt & Cox, 1984). De bottleneck is de beperking (constraint), waarvan de prestatie van het gehele proces afhangt. Het idee van ToC is dat alleen als de bottleneck verbeterd wordt de gehele keten beter zal presteren, zoals in figuur 5.4 visueel gemaakt is. Situatie 'a' laat de flessenhals zien. In situatie 'b' is de

doorlooptijd van het proces, ondanks de capaciteitstoename voor de flessenhals, gelijk aan die van situatie 'a'. Pas bij het opheffen van de bottleneck neemt de doorstroom na de hals toe. Deze schakel of taak moet dan ook het doel van de verbeteringsacties zijn. Als de zwakste schakel verbeterd is, dan is er weer een ander zwakke schakel die daarna verbeterd moet worden. Er blijft altijd een bottleneck over. Het idee is dat al het andere ondergeschikt moet worden gemaakt aan deze bottleneck om het proces te kunnen verbeteren.



Figuur 5.4 – a. Visualisatie van bottleneck, b. procesverbetering, maar niet de bottleneck verbeterd en c. zonder een bottleneck

Met oog op de ToC is het gebruik van buffers en wachtrijen van belang. Wanneer de bottleneck stilvalt, ontstaat er immers direct een 'gat' in de aanvoer, terwijl een tijdelijke opstopping in het proces vóór de bottleneck nog ingelopen kan worden. Dit is zichtbaar gemaakt in figuur 5.5.



Figuur 5.5 – Bij het falen van de bottleneck valt er direct een blijvend gat in de productie. Dit geldt niet wanneer de aanvoer voor de flessenhals tijdelijk stopt. Zolang de buffer niet leeg is, gaat de productie door.

De buffers zorgen er verder voor dat variatie vermindert. Het gebruik van buffers gaat tegen de principes van lean in, die zulke buffers als verspilling zien. Hoewel opslag in de ICT-keten minder kostbaar is dan in de fysieke keten, betekenen voorraden

soms wel extra opslag van vertrouwelijke informatie. De benodigde beveiligingsmaatregelen kunnen hierbij kostbaar zijn en ook introduceert het een extra risicopunt van waaruit informatie te stelen is.

Het principe van ToC wordt vaak zichtbaar in ziekenhuizen, waar de specialisten schaars en duur zijn en de procesbeheersing er primair is om ervoor te zorgen dat deze specialisten continu bezig blijven. Dit heeft als gevolg dat er veel mensen in de wachtruimte zitten, wat haaks staat op het nog te behandelen concept van Straight Through Processing. Voor het verbeteren volgens ToC kan men feitelijk de volgende stappen doorlopen (Goldratt, 1997):

1. Formuleer het precieze doel van het proces.
2. Identificeer de beperkingen (de taak die de andere taken ophoudt).
3. Zorg dat optimaal gebruik wordt gemaakt van de bottleneck door de beperkingen rondom te identificeren. Hiervoor kunnen buffers en wiskundige planningsmethodieken worden gebruikt.
4. Alle andere taken en activiteiten worden ten dienste gesteld van de bottleneck (korte termijn planning).
5. Verbeter de beperkingen en zorg dat de bottleneck opgelost wordt (langere termijn verandering).
6. Start weer bij het begin.

Hoewel ToC in de eerste plaats richtlijnen geeft voor het verbeteren van doorlooptijd en efficiëntie, kan het idee van ToC als een managementfilosofie worden beschouwd. Deze redenering kan ver doorgevoerd worden. Niet alleen kunnen er bottlenecks qua tijd zijn, maar een bottleneck kan ook de taak zijn die de hoogste kans op falen heeft, de taak die de meeste mankracht vergt of de taken die het meeste geld kosten. Binnen SBR is het met name de taak van de expertgroep processen & techniek om bottlenecks in de keten te identificeren en te benoemen. De werkgroep processen & techniek (bestaande uit publieke uitvragers en Logius) identificeert bottlenecks in de publieke schakels van de SBR keten. Binnen de SBR-processen zijn er de afgelopen jaren verschillende bottlenecks geïdentificeerd. Wij bespreken er vier:

1. De validatieservice in Digipoort
2. De koppeling tussen Digipoort en de uitvragende partijen
3. Het verplichte gebruik van een Autorisatie Service Provider (AuSP)
4. De distributie van certificaten in het kader van verplichtstelling

Digipoort is de generieke infrastructuur, beheerd door Logius, de gedeelde dienstverlener van de overheidspartijen in SBR. De meest archetypische bottleneck is de validatieservice in Digipoort. Deze service valideert een instance (XBRL-bericht met verantwoordingsinformatie) tegen de Nederlandse Taxonomie. Hiervoor is het nodig dat de validator op basis van het endpoint in de instance met de taxonomie het juiste validatie-'schema' genereert. Waar het gaat om verwerkingscapaciteit is de validatieservice de klassieke bottleneck. Vooral wanneer de validator op hetzelfde moment een groot aantal verschillende type instances (verantwoordingsinformatie zoals bijvoorbeeld de jaarrekening, OB-opgave, VPB-aangifte, etc.) aangeboden krijgt, neemt de verwerkingstijd per bericht snel toe. De SBR oplossing voorziet daarom in ontkoppeling tussen aanlevering en verwerking binnen Digipoort (losse koppelvlak-

services en verwerkingsservices). Deze ontkoppeling maakt het mogelijk voor de validator om een buffer aan te leggen, waarmee mogelijk procesfalen in tijden van piekbelasting voorkomen wordt. Met een robuust proces als resultaat.

Een andere bottleneck betrof de koppeling tussen Digipoort en de uitvragende partijen. Wanneer een uitvragende partij een klein moment (langer dan twee minuten) niet bereikbaar was, kreeg een aanleverende partij in het oorspronkelijke proces een technische foutmelding. Dit betekende dat de aanleverende partij een bericht opnieuw moest aanbieden op een later tijdstip. Ook hier legde de ontkoppeling tussen aanlevering bij Digipoort en verwerking/aflevering aan de uitvragende partij de basis voor verbetering. Met de ontkoppeling waren de genoemde problemen echter niet direct van de baan. Binnen Digipoort moeten eerst de benodigde bufferfunctionaliteiten worden ingericht. Bovendien moeten de uitvragende partijen aansluiten op een koppelvlak, waarmee een bericht opnieuw aan hen aangeboden kan worden.

Een bottleneck van een andere orde betrof de verplichte toepassing van een AuSP bij berichtenaanlevering. In de oorspronkelijke situatie moesten aanleverende partijen gebruik maken van een commerciële AuSP, die zekerheid gaf over de bevoegdheid van de aanleverende partij om voor de belanghebbende partij verantwoordingsinformatie aan te leveren. De aanleverende partij (bijvoorbeeld de belastingconsulent) moest hiertoe bij de AuSP aantonen dat deze door de belanghebbende partij (het bedrijf) gemachtigd was om belastingzaken af te handelen. Deze relatie werd opgenomen in een register dat bij aanlevering door de Digipoort gecontroleerd werd. De AuSP werd om diverse redenen als bottleneck of zelfs als roadblock ervaren:

- De markt van AuSPs was niet volwassen. Hierdoor was er weinig keuze en het registratieproces van machtigingen werd als inefficiënt beschouwd. Met name de doorlooptijd voor aansluiting op SBR werd bepaald door de doorlooptijd van dit proces.
- De intermediairs hebben in de substituten (bijvoorbeeld BAPI) niet te maken met commerciële AuSPs. Dit betekent dat zij de rekening die gepaard gaat met registratie van machtigingen als lastenverzwaring ervoeren.
- Er was slechts een beperkt normenkader voor de AuSP rol. Voor toetreding of toezicht was niets ingesteld. Hierdoor ontstonden vragen over de effectiviteit van het mechanisme.
- Intermediairs willen in hun dienstverlening de afhankelijkheid van derden beperken. Bij een verstoring in de AuSP kon een intermediair geen berichten afleveren.
- Het gewin bij het onbevoegd insturen van belastingaangifte is beperkt. Tevens krijgt de belanghebbende de aanslag altijd nog op papier, waarmee onjuiste opgaven/aangiften achteraf opgemerkt worden. Bij een goed authenticatiemechanisme is de onbevoegd handelende partij dan alsnog op te sporen.

Hoofdstuk 8 (Beveiliging van informatieketens) gaat uitgebreid in op de problematiek rond authenticatie/autorisatie. Voor nu is het voldoende om aan te geven dat er een aantal maatregelen is genomen om de bottleneck te verhelpen:

- Het gebruik van een sterker authenticatiemechanisme, te weten PKIoverheidscertificaten is verplicht gesteld.

- Het gebruik van de AuSP zelf is optioneel gemaakt.
- Statusinformatie over een aanlevering is alleen op te vragen door de partij die de aanlevering doet.

In 2012 was de distributie van de PKIoverheid certificaten te kenschetsen als een openstaande bottleneck. Voor system-to-system verkeer was er bijna geen andere optie voor authenticatie dan te werken met certificaten. Er was in Nederland slechts een beperkt aantal partijen dat conform het PKIoverheid stelsel certificaten uitgeeft. Desalniettemin moesten alle partijen die per 2013 IB/VPB aangiftes system-to-system wilden aanbieden bij de Belastingdienst beschikken over een dergelijk certificaat. Het gaat om ongeveer 11.000 partijen. Bovendien had de Diginotar affaire in het najaar van 2011 pijnlijk duidelijk gemaakt wat er gebeurt wanneer een zogenaamde Certificate Service Provider niet meer als vertrouwd aangemerkt kan worden. SBR heeft veel aandacht besteed aan het tijdig wegruimen van deze bottleneck voor de aansluiting.

(Type) beperkingen kunnen dus gerelateerd zijn aan apparatuur, mensen, beleid en wetgeving. Een voorbeeld van een beperking gerelateerd aan apparatuur is dat een keten niet meer werkt als de elektronische verbindingen niet meer beschikbaar zijn of als een server uitvalt. Deze bottlenecks (zwakste schakels) moeten geïdentificeerd worden en er moeten alternatieven zijn om te voorkomen dat het gehele proces vastloopt. Bij een goed ingerichte informatieketen ligt de zwakste schakel veelal bij het invoeren en verzamelen van de data.

5.4.3 *Lean Six Sigma*

Vanuit Japan komt in de jaren tachtig van vorige eeuw het Total Quality Management (TQM) op. Deze managementfilosofie is gericht op het continu verbeteren van de processen. Sinds het begin van deze eeuw heeft in de dienstenindustrie de Lean Six Sigma (LSS) methode zijn intrede gedaan, die eerder met name in de productie-industrie gebruikt werd. LSS is een versmelting van twee verschillende methoden. Lean richt zich op het creëren van waarde en het tegengaan van verspilling en Six Sigma op het minimaliseren van de interne en externe variatie.

De 'lean process' verbetering komt vanuit Toyota en Taiichi Ohno en is gericht op het tegengaan van verspilling (Ohno, 1988). Op grote schaal kreeg het bekendheid door het boek 'The machine that changed the world' (Womack, Roos, & Jones, 1990). Activiteiten die personeelsinzet, tijd of geld nodig hebben en geen waarde hebben voor het proces of de klant moeten verwijderd worden. Lean kent een strategisch perspectief gericht op het begrijpen van waarde (value) en een operationeel deel gericht op het tegengaan ver verspilling (Hines, Holweg, & Rich, 2004).

5.4.4 *Lean kernprincipes*

Womack et al. (1990) hebben de volgende vijf kernprincipes van lean geïdentificeerd:

1. Value: het specificeren van de waarde vanuit het gezichtspunt van de eindgebruiker.

2. Value Stream: het identificeren van de waardestroom door het identificeren van de taken voor elke productfamilie en het elimineren van taken die geen waarde toevoegen.
3. Flow: het inrichten van workflows. Zorgen voor een geïntegreerde en strakke workflow, zodat het product snel doorstroomt naar de klant.
4. Pull: trekken, de klanten waarde laten toevoegen voor de volgende klanten.
5. Perfection: perfectie, de cyclus herhalen en verbeteren door het proces transparant te maken en verspilling tegen te gaan.

In een Value Stream Analyse (VSA) wordt nagegaan welke taken waarde toevoegen om zo overbodige taken te identificeren. Een VSA wordt visueel vormgegeven om zo ook de processen en organisatiedoelen te communiceren en om de relatie tussen processen en beheersing aan te geven. Voor het maken van deze analyses zijn er allerlei procesmodelleringsmethoden. De keuze vereist wel het maken van een afweging op welk detailniveau de modellering zal plaatsvinden. Tegenwoordig wordt steeds vaker Business Process Model Notation (BPMN) gebuikt, voor zowel procesmodellering als uitvoering. In § 5.5.4 - BPMN als procesmodelleringstechniek voor ontwerp en onderhoud - gaan we uitgebreid in op procesmodellering met behulp van BPMN.

Bij het toepassen van lean in de publiek/private keten is het nodig stil te staan bij het bijzondere karakter van deze ketens. Door de wettelijke verplichting is het 'bedrijf', de aanleverende partij, een gedwongen gebruiker van de verantwoordingsprocessen. De uitvragende partij is vanwege een wettelijke taak gedwongen informatie uit te vragen en te verwerken. Deze verplichtingen vertroebelen de push/pull afwegingen. De samenleving betaalt via belastingen de uitvragende partij en stelt via de parlementaire democratie de eisen aan de verantwoording. Wanneer het gaat om het specificeren van de waarde voor de eindgebruiker is het maar de vraag wie de eindgebruiker is. Meer gegevens maakt het leven van de uitvragende partij gemakkelijker, maar verhoogt de last van de ondernemer. Veel omvangrijke rapportages kunnen de handhaving verbeteren, wat in het belang is van de samenleving. De verhoogde kosten, die wellicht leiden tot meer belastingen, kunnen de samenleving weer minder blij maken. Hier maakt uiteindelijk de politiek een trade-off: wie betaalt de rekening van de procesafhandeling? Richten we het proces zo in dat het prijzig is voor de uitvragende partij, maar gemakkelijk voor de aanleverende partij? Het Landbouw Economisch Instituut (LEI), één van de verbredingspartijen van SBR, vergoedt uit algemene middelen een deel van de kosten van de intermediair om gegevens bij bedrijven te verzamelen en aan te leveren. In dat geval betaalt de samenleving als geheel. Andersom kan de last ook bij het bedrijf gelegd worden. In dat geval betaalt slechts een deel van de samenleving. Het mooiste is natuurlijk een procesverbetering waarin de lasten als geheel worden teruggebracht. Dit is het ketenperspectief waar SBR voor staat. Desalniettemin is het goed om voorafgaand aan het (her)ontwerp van processen duidelijk de uitgangspunten van de waardebeoordeling vast te stellen met de ketenpartners.

5.4.5 *Verspilling*

Naast het creëren van waarde is de andere basisgedachte achter lean het tegengaan van verspilling. Overbodige activiteiten of activiteiten die geen waarde toevoegen moeten worden beschouwd als verspilling. Gebaseerd op het werk van Ohno (1988)

geven Womack and Jones (1996) acht vormen van verspilling, te weten: overproductie, wachten, transporteren, extra processing, voorraad, gebrekkige inrichting, onvolledige bezetting en defecten. Alles waarvoor extra handelingen nodig zijn, zoals het omgaan met problemen en defecten wordt als verspilling gezien. Voor de dienstensector zijn deze acht basisvormen vertaald naar tien vormen van verspilling (Bonaccorsi, Carmignani, & Zammori, 2011).

1. Defecten: typfouten, invoerfouten, verloren bestanden, verloren of beschadigde data. Womack and Jones (1996) zien alles wat niet aan de eisen van de klant voldoet als een defect.
2. Duplicatie: het overtypen van data, gebruik van meerdere handtekeningen, onnodig veel rapporteren en onnodige vragen moeten beantwoorden.
3. Incorrecte of onvolledig informatie: het zoeken naar de juiste informatie, onnodige kopieën van informatie bewaren.
4. Geen gebruiker(klant)focus: klantonvriendelijk, niet kennen van de klant, onbeleefdheid, niet luisteren.
5. Overcapaciteit en -productie: rapportages maken die niemand leest, uitdraaien van papieren kopieën, afleveren van papier voordat het nodig is, activiteiten om defecten te herstellen.
6. Onduidelijke communicatie: incorrecte informatie, geen gebruik van standaardformaten, onduidelijke workflow.
7. Informatiebeweging en -transport: onnodige verzending, niet duidelijk waar informatie naartoe moet, waarvoor informatie gebruikt gaat worden, het moeten uitzoeken wat de volgende taak is waarvoor de informatie gebruikt wordt etc.
8. Onderbezetting: moeten wachten, te veel bureaucratie, beperkte bevoegdheid om zaken te doen.
9. Variatie: gebrek aan procedures en processen om met uitzonderingen om te gaan, geen standaardformaten, normen en verwachtingen niet gedefinieerd.
10. Wachten en vertragingen: wachten op toestemming, server down time en het wachten op aanvoer van gegevens.

Veel verspilling geeft aan dat een proces niet goed beheerst wordt. Zelfs zaken als een helpdesk worden binnen lean als verspilling gezien, omdat de helpdesk zaken afhandelt waarmee in het proces niet goed wordt omgegaan. Een druk bezette helpdesk is een indicatie voor een proces dat niet goed op orde is. De bovenstaande lijst kan als een checklist fungeren. SBR omarmt impliciet veel van deze principes. Onderstaand per principe een vraagstuk dat speelt of speelde in het SBR-domein:

1. Defecten. Zoals eerder gesteld, maakt SBR het gemakkelijker en efficiënter voor softwareleveranciers om controles voorin het proces uit te voeren. Dit verkleint de kans op fouten. De SBR convictie compliance by design is gericht op het voorkomen van defecten door onjuiste input of afhandeling technisch onmogelijk te maken.
2. Duplicatie. Binnen de SBR processen worden verschillende validaties nog redundant uitgevoerd. Als het goed is, valideert de softwareleverancier tegen de XBRL-taxonomie. Digipoort doet dit vervolgens nogmaals en uiteindelijk zijn er uitvragende partijen die deze check nog een keer in hun eigen validatie meenemen. Het is de verwachting dat bij voortdurende procesoptimalisatie - en een volwassen wordende keten - de redundancy in deze controles zal afnemen.

3. Incorrecte of onvolledig informatie. Logius is de gedeelde dienstverlener van de overheid (onder meer) binnen het verantwoordingsdomein. Zoals al uit 2. blijkt en eerder besproken is, zullen uitvragende partijen gezien hun afhankelijkheid van Logius bepaalde taken (zoals het bewaren van stukken) in eerste instantie dubbel inrichten. Waar het gaat om het minimaliseren van kopieën heeft de werkgroep processen/techniek in 2011 stap voor stap een ketenvisie ontwikkeld op het zekerstellen, herinjecteren, herafleveren en heraanbieden van berichten door Digipoort. Het opslaan van kopieën blijft in het kader van de Archiefwet en het beleid van de overheid onvermijdelijk, maar zal - op basis van deze visie - gaandeweg over de keten heen worden geminimaliseerd en nog maar op één plaats gebeuren.
4. Geen gebruiker(klant)focus. Het SBR Programma heeft met haar vele publiek/private organen, en op basis van de expertise van de Belastingdienst op dit gebied, veel geïnvesteerd in het kennen van alle gebruikers/klanten rond de SBR dienstverlening.
5. Overcapaciteit en –productie. Bij het inrichten van het eMededelenproces, dat in 2011 is ontworpen, is voor de verstrekking van de Service Bericht Aanslag (SBA) door de Belastingdienst rekening gehouden met het feit dat lang niet iedere belanghebbende een dienstverlener aanwijst die een dergelijk bericht mag ontvangen. Voordat de Belastingdienst de elektronische kopie genereert, bekijkt zij bij een abonnementenregister of er interesse in de SBA is. Bij geen interesse maakt zij geen SBA aan.
6. Onduidelijke communicatie. Een van de kernpunten van SBR is het verbeteren van de communicatie door standaardisatie op verschillende niveaus, waaronder het procesniveau. Het voorgeschreven gebruik van BPMN voor in ieder geval de generieke onderdelen is hier een voorbeeld van.
7. Informatiebeweging en –transport. Kijken we naar de processen, dan zien we nog steeds de druk op Logius om betrekkelijk veel verschillende informatie op transportniveau mee te geven aan de uitvragende partij. Dit, omdat het 'weleens handig zou kunnen zijn' voor analyses of bij incidenten. Deze behoefte is niet onlogisch gezien het huidige volwassenheidsstadium van SBR (zie ook punt 2 en 3). Ook hier is het de verwachting dat architecten in de publieke keten gaandeweg scherpere criteria zullen formuleren over welke informatie inderdaad geleverd moet worden en welke als ballast kan worden aangemerkt.
8. Onderbezetting. De bureaucratie rond SBR werd onder andere ervaren bij het eerder genoemde gebruik van AuSPs, die daarom nu bijna niet meer worden gebruikt.
9. Variatie. In 2010/2011, op weg naar geloofwaardig gebruik, werd het probleem van ontbrekende procedures voor uitzonderingen opgelost, doordat de projectleiders van Logius en de uitvragende partijen elkaar direct konden vinden, op de hoogte werden gehouden van incidenten en een goede relatie onderhielden met de lijn. Dit kan bij kleine volumes. Vanaf 2011 is er veel energie gestoken in het maken van heldere afspraken en procedures over hoe de ketenpartners 'gestructureerd' met incidenten om kunnen gaan. Dit in het licht van de naderende toename in volumes.
10. Wachten en vertragingen. In voorgaande onderdelen van het hoofdstuk is al uitgebreid ingegaan op de problematiek rond bottlenecks, ontkoppeling en

buffers om downtime en onnodig wachten te voorkomen. Het spreekt voor zich dat dit gepaste aandacht heeft vanuit de SBR ketenpartners.

5.4.6 *Tijdigheid*

Onder het begrip 'lean' vallen allerlei zaken, zoals Total Productive Maintenance (TPM), cellular manufacturing, Single-Minute Exchange of Die (SMED), Mixed Model Production (MMP), Just-in-time (JIT), en Straight Through Processing (STP). Alleen deze laatste twee zullen we bespreken, omdat deze relevant zijn voor i-processen. Just-in-time (JIT) is het principe dat vraag en aanbod op elkaar afgestemd zijn. Pas op het moment dat iets daadwerkelijk nodig is, wordt het geleverd. Dit heeft als voordeel dat er geen voorraden of buffers aangehouden hoeven te worden. Voor informatieketens betekent het dat informatie niet lokaal opgeslagen wordt, maar beschikbaar komt zodra deze informatie nodig is. Dat bespaart duplicatie van data of onnodig over en weer pompen van data. Het nadeel van een JIT-filosofie is, dat elke ontwrichting of verstoring leidt tot het blokkeren en daarmee stoppen van het gehele proces. Er leven in het domein van de verantwoording gedachten over het toepassen van JIT. In het geval van toepassing zal een uitvragende partij pas bij een controlebehoefte aanvullende gegevens opvragen bij een bedrijf. Dit is een interessante gedachte, maar sluit niet aan bij de bestaande convicties van SBR en de mal waarin het bestuursrecht en de verantwoordingswetten zijn gegoten. Enerzijds zullen er daarom nog heel wat vraagstukken opgelost moeten worden om de JIT-convictie los te laten op het system-to-system verwerken van verantwoordingsinformatie. Anderzijds maken bouwstenen binnen SBR en opkomende technologieën en de toepassing in andere domeinen, dat deze optie technisch steeds reëler wordt. Het JIT-principe staat daarom goed voorgesorteerd om deel uit te gaan maken van de nieuwe redesign golf in de verantwoordingsketen.

Straight Through Processing (STP) is een principe waarbij zaken direct afgehandeld worden. Een voorbeeld in de financiële industrie kan het aanvragen van een kredietofferte zijn, waarbij meteen alle activiteiten worden uitgevoerd en een antwoord binnen enkele seconden of minuten gegeven wordt. Een ander voorbeeld is de situatie bij een helpdesk, waar een probleem meteen wordt opgelost in plaats van slechts te analyseren. Deze voorbeelden laten zien dat het voor het invoeren van STP belangrijk is om zoveel mogelijk activiteiten automatisch te laten verwerken. Bij STP wordt geen of zo min mogelijk gebruik gemaakt van buffers, maar worden alle taken meteen afgehandeld. Ook batchgewijze aanpak is uit den boze. Het te ver doorvoeren van dit principe kan tot gevolg hebben dat de efficiëntievoordelen van batchgewijs verwerken niet meer gezien worden. Zo is al aan de orde geweest dat de processen binnen SBR oorspronkelijk zonder buffers (dus conform STP) waren opgezet, maar dat dit toch teveel uitval met zich mee bracht. STP wordt vaak ingevoerd voor goed gestandaardiseerde processen, waarna het principe langzaam uitgebreid wordt naar moeilijkere processen. Voor geautomatiseerde i-processen geldt, dat STP makkelijker te realiseren is naarmate de aantallen geleidelijker over de tijd verdeeld zijn. Zie in dit licht ook de beschrijving over de performance van de validatieservice. De ketenkarakteristieken en de wettelijke eisen bepalen in welke mate de spreiding in aanvoer te minimaliseren valt. De aangifte van de omzetbelasting kenmerkt zich door een relatief hoge frequentie (voor de meeste ondernemers geldt één aangifte per

kwartaal), betrekkelijk veel verschillende softwarepakketten, veel zelfaangevers en een harde - strakke - deadline, namelijk de laatste dag van de maand opvolgend aan de betreffende aangifteperiode. Het gevolg is een grote piek in aanleveringen richting het einde van de maand. Belastingconsulenten kunnen voor hun klanten uitstel aanvragen voor de inkomstenbelasting en de vennootschapsbelasting. Vooral de aangifte voor de vennootschapsbelasting wordt overwegend door intermediairs opgesteld. De normaal geldende deadline van 1 april van het opvolgende jaar verschuift in dat geval naar 1 mei van het jaar daarop. De belastingconsulent dient evenwel over het totaal aantal aangiften het schema te volgen dat is weergegeven in figuur 5.6. Op deze wijze zorgt de Belastingdienst dat berichten meer gelijkmatig worden aangeleverd.

Tijdens de uitstelperiode moet u de aangiften inleveren volgens het inleverschema dat u hebt ontvangen. In dit schema staat hoeveel aangiften u voor het einde van iedere inleverperiode minimaal moet inleveren. Dit aantal aangiften is gebaseerd op de percentages in de tabel.

Tot en met	*Totaal percentage*	*Totaal aantal aangiften*
Mei/juni/juli/augustus	30%	
September	38,75%	
Oktober	47,50%	
November	56,25%	
December	65%	
Januari	73,75%	
Februari	82,50%	
Maart	91,25%	
April	100%	

Figuur 5.6 – Uit de folder van de Belastingdienst: uitstelregeling voor belastingconsulenten

5.4.7 *Complexiteitsreductie*

Een belangrijke strategie binnen lean is de reductie van complexiteit. Deze strategie is nodig, omdat door de tijd heen verschillende personen aan de processen sleutelen, waardoor deze processen steeds gecompliceerder worden. Een hoge complexiteit leidt gemakkelijk tot fouten en is moeilijker beheersbaar. Niemand heeft meer het overzicht of weet precies hoe het proces in elkaar zit. Daar staat tegenover dat een lagere technische en bestuurlijke complexiteit eenvoudiger te begrijpen is en daarmee ook minder gevoelig voor fouten. Organisaties kunnen daardoor ook meer agile worden, omdat een proces makkelijker aan te passen is. Primair kijkend naar de informatieketen wordt complexiteit gevormd door de:

- Hoeveelheid taken
- Hoeveelheid overdrachtspunten
- Iteraties tussen taken en feedback loops

Meestal is het aantal overdrachtspunten gelijk aan het aantal taken plus één extra. Een simpele kansberekeningformule kan laten zien wat het effect van het aantal taken, overdrachtspunten en feedback loops is. Neem aan:

T – aantal taken
O – aantal overdrachtspunten
X - de kans dat een taak de volledige uitkomst geeft
Y – de kans dat een overdracht volledig goed gaat

De betrouwbaarheid van het proces (P) (kans dat het proces goed werkt) is dan
$P = X^T Y^O$

Dit is een vereenvoudigde berekening gestoeld op een aantal aannames. In de praktijk zullen er vaak afhankelijkheden tussen taken zijn en kunnen er feedback loops zijn om fouten te herstellen. Middels simulatie kan dit voor een specifieke situatie berekend worden.

Tabel 5.2 – Gevolgen van fouten op een proces

	T (aantal taken)	O (aantal overdrachtspunten)	X (de kans dat een taak de volledige uitkomst geeft)	Y (de kans dat een overdracht volledig goed gaat)	$P = X^T Y^O$ (betrouwbaarheid)
Situatie 1	5	6	0,95	0,99	0,73
	5	6	0,95	0,95	0,57
	5	6	0,95	0,9	0,41
Situatie 2	10	11	0,95	0,99	0,54
	10	11	0,95	0,95	0,34
	10	11	0,95	0,9	0,19

De tabel laat zien dat als overdrachtspunten een hogere betrouwbaarheid hebben het gehele proces, in iedere situatie, ook veel betrouwbaarder wordt. Hetzelfde geldt voor taken. Het verschil tussen de twee verschillende situaties laat zien, dat als het aantal taken en het aantal overdrachtspunten toeneemt de betrouwbaarheid aanzienlijk omlaag gaat. Dit laat intuïtief zien, dat het belangrijk is om zo min mogelijk taken en overdrachtspunten te hebben en om de complexiteit van een proces zo laag mogelijk te houden. Eerder bespraken wij al de trade-offs die hierbij in het kader van procesvereenvoudiging bij SBR spelen.

5.4.8 *Reduceren van variatie*

Het voorgaande toont al aan dat de zorg voor het zo goed mogelijk laten functioneren van taken de basis vormt voor een foutloos (functionerend) proces. Six Sigma is gericht op het reduceren van variatie door metingen en statistische analyse. Een Six Sigma proces kenmerkt zich door 99.99966% goed, dit betekent minder dan 3,4 fouten op de miljoen. Dit is extreem goed en onwaarschijnlijk voor processen waarin mensen deelnemen. Daar waar computers geautomatiseerde processen uitvoeren is dit wel realistisch, alhoewel niet vergeten moet worden dat daar ook wel eens iets

fout kan gaan. Denk hierbij aan servers die vastlopen of gereset moeten worden. Binnen de overdracht van data in computers zijn daarom mechanismen ingebouwd om te contoleren of data correct zijn overgedragen en wordt overgegaan op het opnieuw versturen als fouten gesignaleerd worden.

Een belangrijk idee is, dat, voordat de analyse begint, ambitieuze doelen worden gesteld. Zonder het proces te kennen, kunnen de verwachtingen aan de prestatie van het proces gesteld worden (zie § 5.3 (Wat is een goed proces?)). Six Sigma projecten volgen de Plan-Do-Check-Act (PDCA) cyclus van Deming (Womack & Jones, 1996). Er zijn twee methoden: DMAIC voor projecten die huidige processen verbeteren en DMADV voor nieuwe producten en processen. DMAIC bestaat uit de volgende vijf fasen (Feo & Bar-El, 2002):

1. Definieer het probleem.
2. Meten van de kernaspecten en het verzamelen van data.
3. Analyseren van data en verifiëren van oorzaak-gevolg relaties. Wat zijn de oorzaken van de fouten in het proces? Welke factoren hebben hier invloed op? Uiteindelijk moeten de wezenlijke oorzaken boven water komen.
4. Improve (verbeteren) van het huidige proces met technieken zoals experimenten, poka yoke (dit is een combinatie van vermijd (yokeru) en fouten (poka) door te zorgen dat taken niet fout uitgevoerd kunnen worden, standaardisatie etc.)
5. Controle door elke afwijking te meten, te corrigeren en te zorgen dat deze niet meer voorkomt.

En bij DMADV worden de laatste twee activiteiten vervangen door de hiernavolgende twee activiteiten:

4. Design, dat voldoet aan de klantverwachtingen.
5. Verifiëren van de prestatie van het ontwerp en de mate waarin het aan de klantbehoeften voldoet.

Om dit te realiseren zijn allerlei methoden, technieken en tools voorhanden, zoals in onderstaande tabel te zien is. Het behandelen van al deze technieken gaat buiten het bestek van dit boek. Desalniettemin is het belangrijk deze technieken te benoemen, omdat ze nuttig kunnen zijn voor het analyseren en verbeteren van processen.

Tabel 5.3 – Overzicht Six Sigma strategieën, principes, tools en technieken (Feo & Bar-El, 2002)

Six Sigma business strategies and principles	Six Sigma tools and techniques
• Project management Statistical process control • Knowledge discovery • Process control planning • Data collection tools and techniques • Variability reduction • Belt system (Master, Black, Green, Yellow) • DMAIC process • Change management tools	• Data-based decision making Process capability analysis Measurement system analysis • Design of experiments • Robust design • Quality function deployment • Failure mode and effects analysis • Regression analysis • Analysis of means and variances • Hypothesis testing • Root cause analysis • Process mapping

5.5 Hoe onderhoud je een goed proces?

Een proces moet eerst ontwikkeld worden, waarna dit onderhouden moet worden (continous improvement). Ontwikkelen kan via radicale of incrementele benaderingen. Onderhoud kan voortkomen door ontwikkelingen, het meten van prestatie-indicatoren of door spontane verbeteracties. Onderhouden van processen vereist veel afstemming tussen de ketenpartners. Allereerst moeten alle structurele veranderingen en nieuwe ontwikkelingen goed gecommuniceerd worden naar elkaar. Soms is het moeilijk om vooraf de effecten van een verandering op andere ketenpartners in te schatten. Ook bij verwachte veranderingen van volumes is het verstandig om dit door te geven, zodat de anders spelers hierop voorbereid zijn.

5.5.1 *Procesontwikkelingsaanpakken*

Procesveranderingsaanpakken hebben zich in de loop van de tijd ontwikkeld. Business Process Re-engineering (BPR) kwam op in het begin van de jaren negentig en heeft als doel om processen radicaal te verbeteren (Hammer & Champy, 1993), terwijl later de Total Quality Management (TQM) stroming het procesdenken omarmde.

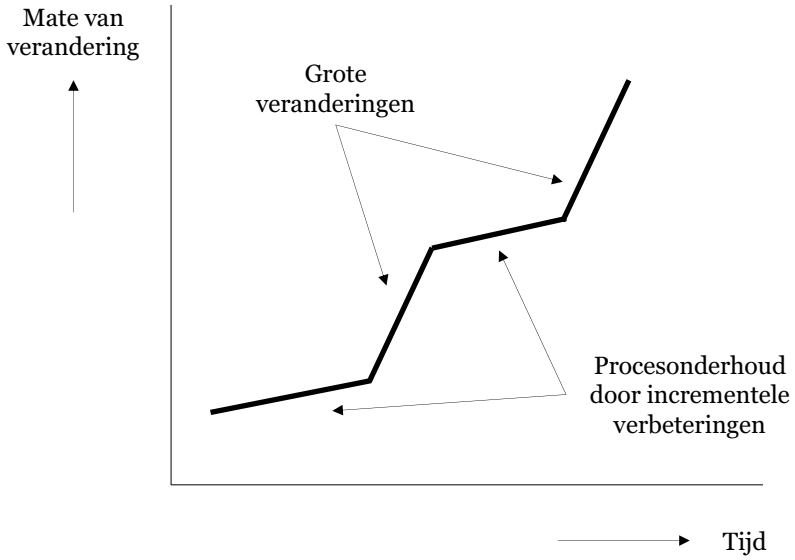
De basisgedachte van BPR is dat niet naar bestaande processen gekeken moet worden, omdat dan teveel op het bestaande gericht gaat worden en mogelijke betere oplossingen genegeerd worden. Bij BPR wordt het te bereiken doel als uitgangspunt genomen en worden de nieuwe processen op een leeg vel ontworpen (‘*blank sheet of paper*’). De basisgedachte is dat alleen door radicale veranderingen substantiële voordelen verkregen worden (Kim, Pan, & Pan, 2007; O’Donnell & Timonen, 2003). Teng et al. (1994, p. 9) definiëren BPR als “*the critical analysis and radical redesign of existing business processes to achieve breakthrough improvements in performance measures*”. Karakteristieken van BPR zijn fundamentele en radicale veranderingen, die tot verbeteringen moeten leiden, en waarbij het procesdenken centraal staat.

BPR leidde echter niet tot de verwachte voordelen in de praktijk en veel van de BPR projecten mislukten. BPR wordt bekritiseerd om zijn lage slagingskans (Earl, 1994). Met name het radicale en revolutionaire element leidt niet tot het gewenste succes. Dit neemt niet weg dat BPR wel tot succes kan leiden en dat soms minder van wat we kunnen en meer vanuit wat we willen, het gewenste, uitgegaan moet worden. Tegenwoordig wordt BPR minder met radicaal en revolutionair geassocieerd en veel meer met het procesdenken. Om de associatie met de negatieve aspecten te vermijden, worden ook andere termen zoals business engineering en proces innovatie gebruikt om het procesdenken mee aan te duiden. Het succes van BPR is kritisch afhankelijk van het gebruik van BPR technieken en middelen (Kettinger, Teng, & Guha, 1997; O'Neill & Sohal, 1999; Wastell, White, & Kawalek, 1994). Kettinger et al. (1997) geven een overzicht van 72 technieken, die vaak in BPR gebruikt worden. Deze technieken zijn gerelateerd aan tools, zoals Quality Function Deployment (QFD), procesmodelleren, brainstormen, simulatie, regels specificeren, database ontwerpen en procesmetingen. Een aantal van deze technieken valt typisch onder het begrip 'lean'.

Zoals gesteld heeft BPR een hoge faalkans. Daarom wordt het hier tegenover Total Quality Management (TQM) gezet, dat zich richt op het incrementeel verbeteren van bedrijfsprocessen (Carr & Johansson, 1995; Davenport, 1993; O'Neill & Sohal, 1999). Uit de TQM benadering komt Lean Six Sigma (LSS) voort, dat de elementen van lean en van Six Sigma combineert.

Net als op BPR is er ook op TQM en LSS kritiek (Hines et al (2004). Deze benaderingen houden geen of te weinig rekening met de verschillende typen organisatie en kunnen niet omgaan met verschillen tussen processen en organisatie. Bovendien leggen ze geen relatie tussen het strategische niveau en de inrichting van processen. Hiernaast is er de kritiek dat er te weinig aandacht is voor de menselijke aspecten en dat er te veel wordt gefocust op de operationele processen. Door dit laatste aspect wordt het strategisch niveau uit het oog verloren.

Beide benaderingen zijn complementair en ze zullen elkaar opvolgen in de tijd (O'Neill & Sohal, 1999). Bij grote procesveranderingen worden de fundamentele uitgangspunten waar een systeem op gebaseerd is niet meer gedragen en zijn de technologische mogelijkheden zodanig anders dat enkel procesverbetering niet (meer) loont. Een radicale herziening van het fundamentele ontwerp is in zo'n geval noodzakelijk: van een koets maak je nooit meer een goede auto. Het is beter om in zo'n geval een nieuwe blauwdruk te maken. Een andere situatie is de fase waarin SBR zich nu bevindt: een fase waarin geen grote veranderingen meer optreden. De aandacht is de laatste jaren gegaan naar het continu verfijnen van de i-processen om ze nog beter op de eisen en wensen van informatie-aanleveraars en -afnemers aan te laten sluiten. Dit gebeurt incrementeel en geleidelijk. Figuur 5.7 laat schematisch de verschillen zien tussen de grootte van de veranderingen.



Figuur 5.7 – De complementariteit van BPR en TQM (gebaseerd op Dervitsiotis, 1998)

Onderstaande tabel plaatst de afgelopen en komende fase van SBR (en haar voorganger NTP) in het licht van BPR en TQM/LSS, waarbij de verwachting is dat SBR de komende jaren steeds meer zal opereren conform TQM/LSS veranderaanpak.

Tabel 5.4 – Karakteristieken van de aanpakken voor procesverandering

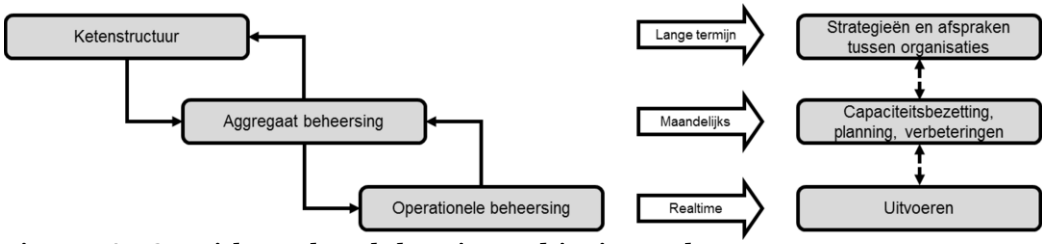
Karakteristieken	BPR	TQM/LSS	NTP/SBR 2006 t/m 2012	SBR 2013 e.v.
Verandermethode	Radicaal	Incrementeel	Radicaal	Incrementeel
Focus	'blank sheet of paper'	Huidige praktijk	'blank sheet of paper'	Nieuwe praktijk
Frequentie	Éénmalig	Continu	Enkele iterates	Continu
Scope	Breed, herzien van functies	Beperkt gericht op bepaalde functies	Breed	Steeds meer gericht op bepaalde functies
Participatie	Top-down	Bottom-up	Middle out (combinatie van top-down en bottom-up)	Middle out
Risico's	Groot	Beperkt	Groot	Nemen af
Betekenis van IT	Centraal	Beperkt	Centraal	Blijft gelijk
Hulpmiddelen	Methoden en technieken	Medewerkers, empowerment met tools	Medewerkers, methoden en technieken	Medewerkers, methoden en technieken en empowerment met tools
Type verandering	Structuur, cultuur	Processen	Structuur, cultuur	Processen

5.5.2 *Onderhoud in keteninrichting en uitvoering*

Het onderhouden en beheersen van de processen in een keten vereist dat organisaties op elkaar ingespeeld zijn en duidelijke afspraken over elkaars verwachtingen gemaakt hebben. Dit kunnen verwachtingen zijn over de langere termijn (wat te doen bij een verandering) of over de korte termijn (‘*Houston, we have a problem*’). Ketenbeheersing vindt niet plaats in isolement, maar vaak in samenspraak tussen afdelingen of organisaties die samen ketens vormen. Dit betekent dat de planning ook in deze context plaats moet vinden.

Figuur 5.8 geeft een overzicht van een beheersing in ketens. De ketenstructuur heeft betrekking op de lange termijn en bestaat uit de invulling van strategieën en afspraken die gemaakt zijn om de keten te laten functioneren. De ketenstructuur staat relatief vast en veranderingen daarvan vereisen vaak onderhandelingen tussen partners en het implementeren van deze veranderingen door middel van een geschikte sturingsvorm. Aggregaat-beheersing is een periodieke planning om ervoor te zorgen dat de beschikbare capaciteit toereikend is en om kleinere procesverbeteringen door te voeren. Een voorbeeld kan zijn dat in bepaalde periodes pieken worden verwacht, omdat relatief veel berichten aangeleverd worden. Ook het doorvoeren van verbeteringen binnen de ketenstructuur valt onder aggregaat-beheersing. Dit kan door het vervangen van een technische bouwsteen door een verbeterde bouwsteen, zonder dat de interface verandert. Ook vinden hier besluiten plaats rondom het (tijdelijk) dichtdoen of openzetten van een poort voor bepaalde berichten.

Operationele beheersing betreft het daadwerkelijk uitvoeren en ingrijpen indien nodig. Het behelst het monitoren van de uitvoering van de keten en ingrijpen in de ketenstructuur volgens de gemaakte afspraken als de keten niet functioneert, bijvoorbeeld omdat een systeem uit de lucht is, er een beveiligingsprobleem is of er vertragingen optreden. Indien nodig moeten er controles zijn opgenomen in de processen om te kijken of het doel behaald wordt en om de juiste, betrouwbare, tijdige en continue werking van processen te waarborgen en waar nodig te kunnen bijsturen. Dit laatste gaat tegen het principe van de lean managementfilosofie in, waarin controles als verspilling worden gezien en het proces zelfsturend moet zijn. Controles zijn echter wel nodig, omdat het anders fout kan gaan zonder dat het opgemerkt wordt.



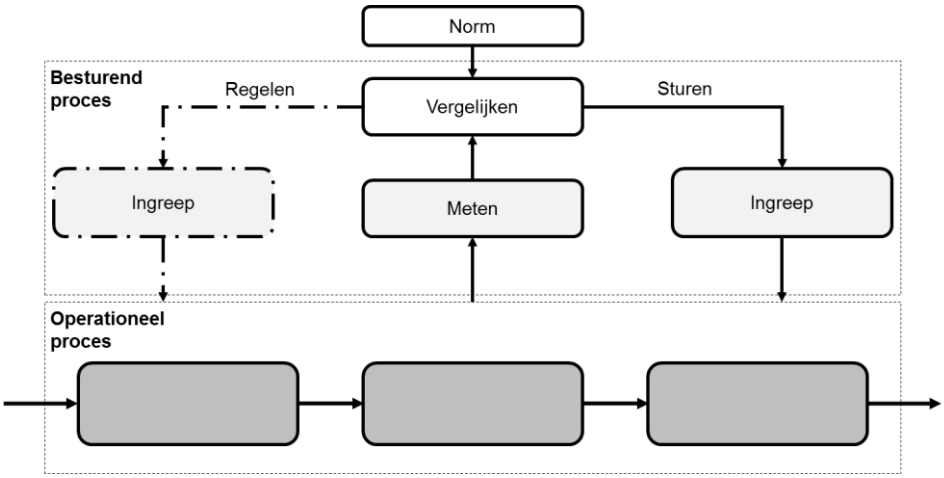
Figuur 5.8 – Overzicht van ketenbeheersing op drie niveaus: ketenstructuur, aggregaatbeheersing en operationele beheersing

De pijlen tussen de drie niveaus geven aan dat deze elkaar beïnvloeden. Een calamiteit op het operationele beheersingsniveau kan opgeschaald worden naar ketenniveau en daar wijzigingen tot gevolg hebben.

5.5.3 *Beheersing en prestatiemeting van processen*

Het bepalen van prestatie-indicatoren voor processen is van belang om de organisatiestrategie door te vertalen naar meetbare grootheden voor processen, voor het continu evalueren van de uitvoering van processen en bijsturing, en voor het initiëren en starten van ingrijpende veranderingsprocessen. In een keten kunnen de prestatie-indicatoren gebruikt worden om de ketenpartners te laten zien dat men in control is.

We zien in figuur 5.9 het principe van een besturend proces, dat het operationele proces meet en op grond van een vergelijking met voorgedefinieerde normen een ingreep kan doen. We zien in deze figuur twee soorten ingrepen, een sturende en een regelende ingreep. De sturende ingreep (feed forward) grijpt vooruit in het proces in. Dit is hetzelfde wat een automobilist doet tijdens het autorijden. De regelende ingreep grijpt terug in het proces in en is met stippellijnen weergegeven in de figuur. Om te zorgen dat een regelende ingreep niet te laat plaatsvindt (er zijn bijvoorbeeld al klachten), dienen daarvoor de normen hoger gelegd te worden.



Figuur 5.9 –Besturend proces met sturende ingreep en regelende ingreep

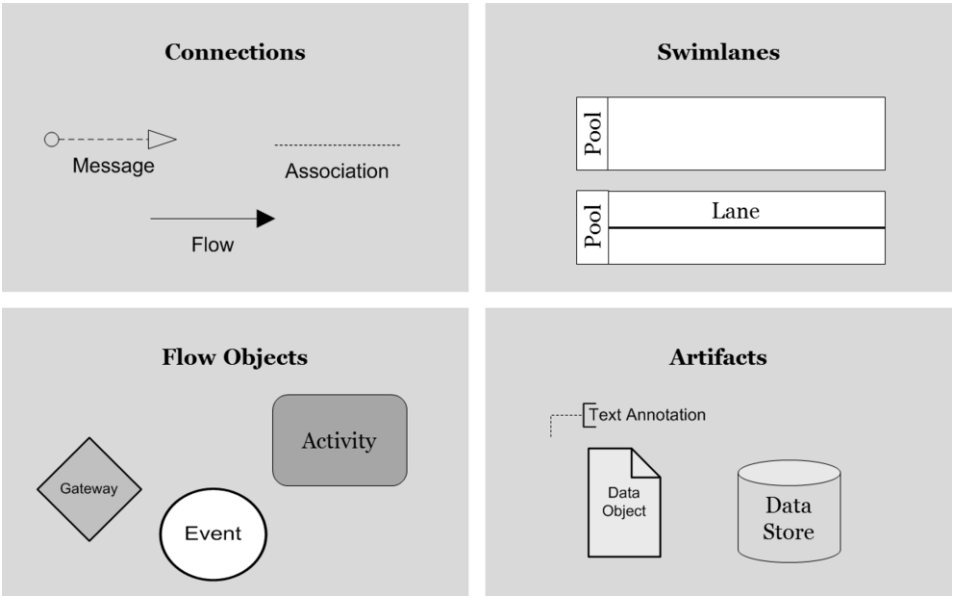
Het aansturen van processen vindt doorgaans plaats middels software. Vanuit een technisch perspectief wordt dit vaak ondersteund door Web Service Orchestratie software die de uitvoering van processen volgt, ook een type BPM software. Deze software maakt het mogelijk om de uitvoering van processen continu te bekijken. Het overzicht en de status van processen kunnen bekeken worden. Bovendien kan ingesteld worden dat als een proces te lang duurt, alerts verstuurd worden en ook zijn alerts mogelijk als services niet beschikbaar zijn. Ingrepen kunnen geautomatiseerd zijn, maar ook kan naar beheerders een bericht worden verstuurd. Bij het monitoren moet niet alleen naar klassieke procesmetrieken als doorlooptijd en kosten gekeken worden.

5.5.4 *BPMN als procesmodelleringstechniek voor ontwerp en onderhoud*

Eén van de eisen aan de SBR oplossing komt voort uit de behoefte aan eenduidige procesbeschrijvingen (processpecificaties): de i-processen moeten worden beschreven met behulp van een processtandaard. De Business Process Modellering Notation (BPMN) is een open visuele standaard voor modellering van processen en biedt eenduidige symbolen en constructen om processen in kaart te brengen (White & Miers, 2008). Dit resulteert in eenvoudige en communicatieve modellen (Vergidis et al., 2008). In de Nederlandse overheidsarchitectuur (NORA) wordt BPMN als de standaard voor het analyseren van bedrijfsprocessen gezien. BPMN biedt publieke ketenpartners een uniforme 'taal' voor het inzichtelijk maken van een proces. Hoewel er verschillende standaarden voor procesmodellering zijn, schrijft SBR, in ieder geval waar het gaat om processen, het gebruik van BPMN voor. De Object Management Group (OMG) is verantwoordelijk voor het onderhoud van BPMN. BPMN wordt door diverse software leveranciers ondersteund. Initieel is BPMN gebaseerd op de activiteitendiagrammen van Unified Modelling Language (UML). De kracht van BPMN is dat zowel activiteiten als services gemodelleerd kunnen worden, waardoor BPMN gemakkelijk te vertalen is in geautomatiseerd af te handelen processen. In BPMN 2.0 heeft er een verschuiving plaatsgevonden van BPMN als primair een visuele taal voor het modelleren van processen naar een taal die ook direct uitgevoerd kan worden (Chinosi & Trombetta, 2012). Het ideaal is dat een proces gemodelleerd kan worden en meteen ook geïmplementeerd.

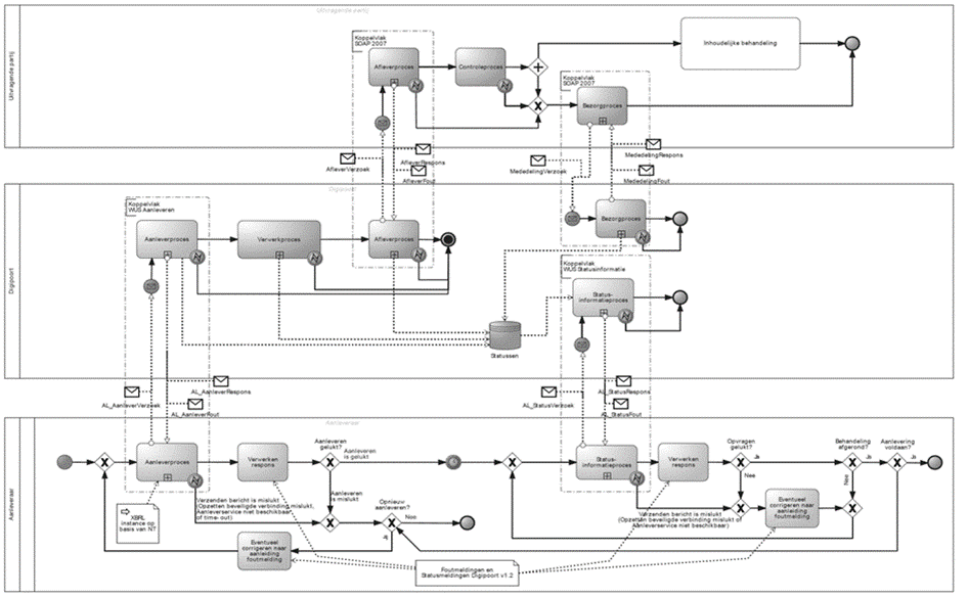
BPMN gebruikt 'swim lanes' om naar de actoren te verwijzen die taken uitvoeren, zoals in figuur 5.10 te zien is. Cirkels laten het begin en einde van gebeurtenissen zien (events) en de rechthoeken met ronde hoeken beschrijven de taken of subprocessen (activities). Ruiten worden gebruikt om de beslissingen aan te duiden (gateways). Hiernaast zijn er pijlen om de gebeurtenissen, activiteiten en beslissingen met elkaar te verbinden. Tenslotte is er een aantal objecten (artifacts) waarmee kan worden aangegeven welke data gebruikt worden, welke elementen bij elkaar horen of om toelichtende informatie te geven. Samengevat zijn de vier basiselementen van BPMN:

1. Stroom objecten (Gebeurtenissen, Activiteiten en Poorten)
2. Verbindende objecten (Sequentiestroom, Berichten stroom of Associatie)
3. Swim lanes (pool en lanes)
4. Artefacten (Data Objecten, Groepen en Aantekeningen)



Figuur 5.10 – Basis BPMN elementen

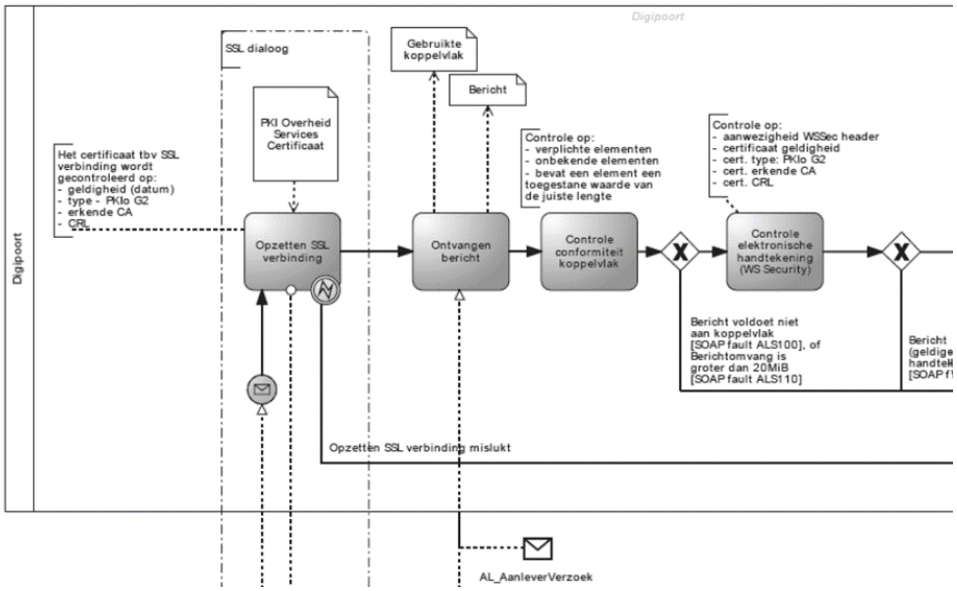
BPMN leent zich bij uitstek voor het in kaart brengen van ketenprocessen, omdat de processen van ketenpartners in swim lanes ondergebracht kunnen worden, waardoor processen gekoppeld kunnen worden aan verantwoordelijkheden. De interacties tussen organisaties kunnen beschreven worden door services (veelal webservices), waarbij de modelleur het aggregatieniveau kiest waarop een service weer verder wordt uitgewerkt. Hiermee kan de verbinding worden gelegd tussen ketenniveau, bedrijfsniveau, subprocesniveau en taakniveau. In figuur 5.11 is een ketenproces van SBR weergegeven, waarbij de onderstaande pool de aanleverende partij betreft, de middelste pool het proces weergeeft dat bij Logius wordt afgehandeld en de bovenste pool de acceptatie door de uitvragende partij beschrijft.



Figuur 5.11 – Voorbeeld van een BPMN diagram van een SBR keten

In de figuur zijn de verschillende bedrijfsprocessen weergegeven die in de keten te onderscheiden zijn. Deze zijn afzonderlijk weer verder uitgewerkt. De kunst is om te bepalen op welk niveau van abstractie en detail processen bekeken moeten worden en hoe dit weer te geven in een model. Veel modelleurs beperken zich tot de typische scenario's (happy flow) en werken modellen niet ver genoeg uit om ze ook uitvoerbaar te maken. Op globaal niveau blijven kan nuttig zijn om een overzicht te maken, makkelijk te communiceren en zelfs ook om lean principes toe te kunnen passen. Degene die het proces implementeert, moet echter alle details weten; wat zijn de alternatieven en hoe wordt het uitgevoerd.

Een risico is dat alles wat niet gemodelleerd is, naar het inzicht van de programmeur wordt ingericht. Bij het modelleren moeten beslissingen op grond van expliciete afwegingen gemaakt worden en moeten ontwerpkeuzen zichtbaar worden gemaakt. In het kader van SBR worden de onderdelen die Logius afhandelt in grote mate van detail beschreven. Figuur 5.12 zoomt in op de aanleverservice en de gedetailleerde taken.



Figuur 5.12 – Inzoomen op de aanleverservice

5.5.5 *BPMN leesbaarheidsprincipes*

BPMN is een visuele standaard, daarom is het belangrijk om te zorgen dat modellen die in BMPN gemaakt worden ook makkelijk leesbaar zijn. Dit is des te belangrijker omdat verschillende analisten van hetzelfde proces tot verschillende procesinrichtingsvoorstellen kunnen komen. Dit betekent dat ook eenzelfde proces op verschillende manieren gemodelleerd en ingericht kan worden. Principes en richtlijnen kunnen de modelleur en analist helpen om te zorgen dat de modellen beter op elkaar gaan lijken, resulterend in meer uniformiteit en standaardisatie. Binnen SBR zijn de modellen leesbaar gehouden door de volgende richtlijnen te volgen:

- Gebruik decomposities (subprocessen) wanneer taken samenhangen (zie figuur 5.1) en zorg voor maximaal 20 taken per proces. Kom je hierboven, definieer dan een nieuw proces waar dan de taken onder kunnen vallen.
- Zorg ervoor dat lijnen elkaar zo min mogelijk overlappen om processen leesbaar te houden (d.w.z. bij feedback loops en weer bij het begin beginnen).
- BPMN modellen moeten nog leesbaar zijn wanneer geprint of geprojecteerd op A4-formaat, om deze bespreekbaar te houden met de ketenpartners.
- Modelleer de volgorde van taken in de tijd zoveel mogelijk van links naar rechts (dus begin een taak links en eindig aan de rechterkant).
- Als er meerdere begin- of eindpunten zijn, gebruik dan verschillende namen om deze aan te duiden en verwarring hierover te voorkomen.
- Gebruik altijd een actief werkwoord om een taak aan te duiden en begin met dit werkwoord.
- Gebruik altijd hetzelfde type poort, gateway om een proces te splitsen en weer bij elkaar te brengen (join).

- Benoem bij gebruik van een XOR gateway (een gateway die splitst in alternatieve stromen) welke de standaard (default) en welke de conditionele stroom is en geef deze stromen verschillende namen.
- Visualiseer de samenwerking tussen actoren in verschillende pools middels ingoing en outgoing berichten.
- Gebruik hiërarchische decompositie (zie figuur 5.1), waarbij onderscheid wordt gemaakt tussen het ketenniveau en het organisatieniveau.
- Wanneer de uitkomst van een taak een specifiek product of een specifieke dienst is, visualiseer dit dan met een data object dat verbonden is middels een verbindend object. Op dezelfde wijze kan ook de input voor een activiteit gevisualiseerd worden. Wetgeving kan middels een data object gevisualiseerd worden.
- Een beslissing waar menselijk handelen aan te pas komt, moet gemodelleerd worden door een taak (beslissingsactiviteit), gevolgd door een ruit (gateway) om alternatieve paden mogelijk te maken.
- Gebruik geen aparte taak om te ontvangen of te versturen. Hiervoor kunnen de gebeurtenisobjecten gebruikt worden.
- Processen moeten altijd afgesloten worden met een end event om deadlock te vermijden.

Deze regels kunnen als richtlijnen bij het modelleren gebruikt worden om de leesbaarheid en communiceerbaarheid te verhogen. De leesbaarheid dient afgedwongen te worden door beheermaatregelen die ervoor zorgen dat verschillende procesmodellen aan de kwaliteitseisen voldoen, samenhangend en consistent zijn.

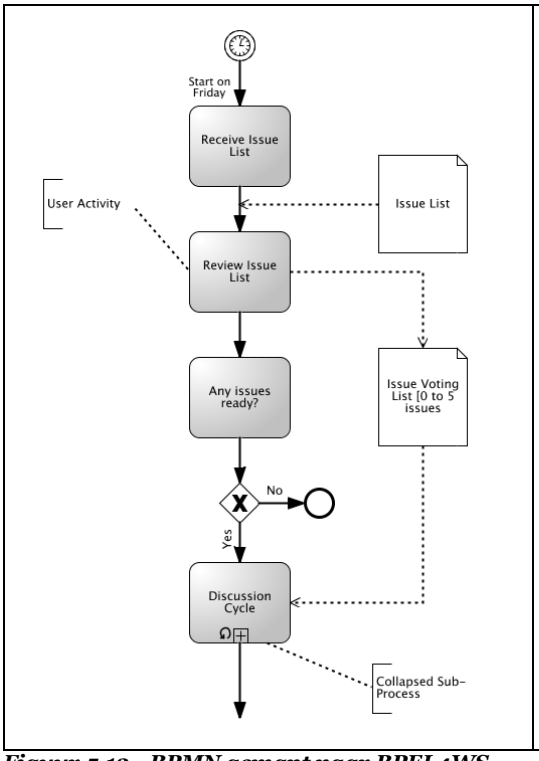
5.5.6 *Van proces naar uitvoering*

Nadat een proces gemodelleerd is in de visuele taal BPMN, is de volgende stap het daadwerkelijk uitvoeren van het proces. BPMN 2.0 maakt het mogelijk om een proces direct uit te voeren, maar vaak worden procesbeschrijvingen en de uitvoering uit elkaar getrokken. Voor het direct geautomatiseerd afhandelen kan het procesmodel naar een uitvoerbare code geëxporteerd worden. Hiervoor is de XML Process Definition Language (XPDL) ontwikkeld. Dit is een op XML gebaseerde taal om procesbeschrijvingen tussen BPM producten uit te wisselen. Deze taal is gestandaardiseerd en wordt onderhouden door de Workflow Management Coalition (WfMC).[14] XPDL slaat zowel de grafische informatie op als informatie over de uitvoering. Voor het uitvoeren van een proces wordt web service orchestratie gebruikt. Web service orchestratie is een onderdeel van de web services stack, gericht op het afstemmen van verschillende web services. Hierbij vindt procesuitvoering plaatst door middel van aanroepen van web services. Web service orchestratie richt zich dus op het specificeren van de logica achter de tijdsvolgordelijke aanroepen van verschillende web services. Het beschrijft een proces vanuit het gezichtspunt van een bepaalde organisatie of afdeling en gaat niet op de interacties tussen afdelingen in. De de facto standaard voor orchestratie is BPEL4WS, de Business Process Execution Language for Web

[14] Zie: http://www.wfmc.org/

Services, vaak kortweg BPEL genoemd. BPEL is ontwikkeld door Microsoft, IBM en BEA, en verenigt twee oudere talen van Microsoft en IBM: XLANG en WSFL.

De nieuwste versie van BPEL4WS bevat proceslogica die traditioneel alleen in workflow talen aanwezig was. Zo biedt het ook de mogelijkheid om taken door mensen te laten uitvoeren. De grote voordelen van web service orchestratie ten opzichte van workflow zijn de uniforme en standaard manier van het aanroepen van processen en de applicaties middels web services. Dit maakt zaken als hergebruik en het snel en gemakkelijk aansluiten van nieuwe processen mogelijk. Een proces ontworpen in BPEL4WS kan idealiter in software van verschillende leveranciers afgespeeld worden. Met het verschijnen van BPMN 2.0 is vaak gesteld dat BPEL achterhaald is, maar velen zien BPEL nog steeds als de manier om processen uit te voeren (Chinosi & Trombetta, 2012). Direct uitvoeren van BPMN beschrijvingen is vaak niet mogelijk, omdat er nog verdere keuzes gemaakt dienen te worden. Het is echter de verwachting dat BPEL op termijn achterhaald zal zijn, als er betere doorvertalingen komen van BPMN modellering naar uitvoering. Dit wordt versterkt doordat BPMN 2.0 op een aantal fronten meer kan modelleren dan BPEL kan uitvoeren. Zo geeft BPMN 2.0 extra aandacht aan interacties en conversaties. Feitelijk zal het in vele situaties slechts van belang zijn dat de processen in BPMN gemodelleerd worden. Uitvoering kan op meerdere manieren plaatsvinden en is van de softwareleverancier afhankelijk. Door de relatie tussen BPMN en BPEL kan een proces gemapt worden, zoals te zien is in figuur 5.13.




```
<process name="EMailVotingProcess">
<!-- The Process data is defined first-->
 <sequence>
 <receive partnerLink="Internal“portType="tns:pro-
cessPort“ operation="receiveIssueList“ varia-
ble="processData“ createInstance="Yes"/>
 <invoke name="ReviewIssueList" partnerLink="In-
ternal“ portType="tns:internalPort" operation="sen-
dIssueList“ inputVariable="processData“ outputVaria-
ble="processData"/>
 <switch name="Anyissuesready">
 <!-- name="Yes" -->
 <case condition="bpws:getVariableProperty(Pro-
cessData,NumIssues)>0">
 <invoke name=“DiscussionCycle“ partnerLink="In-
ternal“ portType="tns:processPort" opera-
tion=“callDiscussionCycle“ inputVariable="pro-
cessData"/>
 <!– Other Activities not shown -->
 <!--name="No" -->
 </case>
 <otherwise>
 <empty/>
 </otherwise>
 </switch>
 </sequence>
</process>
```

Figuur 5.13 –BPMN gemapt naar BPEL4WS

Voor een werkende koppeling tussen BPMN en BPEL moeten aan de verschillende symbolen nog metadata toegevoegd worden. Hiervoor zijn diverse suites in gebruik. In een laboratoriumsetting zijn op deze wijze bijzonder flexibele infrastructuren te ontwikkelen. In de praktijk blijkt de afstand tussen de business en IT nog te groot om de programmeur te schrappen. Desalniettemin maakt het gebruik van BPMN, mede doordat de ruimte voor interpretatie verkleind wordt, de kloof tussen business en techniek een stuk kleiner.

5.6 Welke tooling en methoden zijn te gebruiken voor ontwerp en onderhoud?

5.6.1 *Software voor ondersteuning*

BPMN wordt door diverse softwareleveranciers ondersteund. Ondersteuning kan variëren van basisfunctionaliteit, om alleen processen grafisch te kunnen tekenen en visualiseren, tot complete suites, die kunnen helpen om de processen direct uit te voeren en te verbeteren. Voor een overzicht van implementaties zie http://www.bpmn.org. Op het internet zijn de leveranciers gemakkelijk te vinden. Bij functionele eisen aan de software valt te denken aan de volgende eisen:

- Grafische BPMN editor om eenvoudig processen te tekenen en aan te passen.
- Mogelijkheid om procesbouwstenen te definiëren die in meerdere processen hergebruikt kunnen worden.
- Rollen per gebruiker toewijzen voor onderhoud en ontwikkeling.
- Vertaling van proces naar datastructuur.
- Grafische UML editor om de datastructuur te editen.
- Processimulatie inclusief data importsupport en statistische ondersteuning.
- Procesdiagnose (wachtrijen, bottleneck identificatie etc., maar ook overeenkomsten tussen processen detecteren).
- Exportmogelijkheden (naar XPDL) of direct kunnen uitvoeren van de processen (in BPEL). Bij dit laatste komen nieuwe functionele eisen als connectie met webservices en grafische BPEL editor naar voren.
- Integratie met werkelijke werkstroomuitvoering en de Business Activity Monitor.

Naast deze functionele eisen kunnen er ook een groot aantal niet-functionele of kwaliteitseisen gesteld worden aan de software:

- Licentiekosten (per persoon) of open source
- Betrouwbaarheid van de leverancier
- Volwassenheid/stabiliteit van de software
- Regelmatige updates en forwards compatibel (i.v.m. nieuwe updates van standaarden als BPMN en BPEL)
- Trainings- en opleidingsmogelijkheden
- Bekendheid en gebruikersgroepen (i.v.m. beschikbare kennis)
- Aantal mensen dat tegelijk kan werken aan één model
- Schaalbaarheid en grootte modellen
- Lokaal installeren of gebruik van SaaS (Software as a Service) oplossing

Zowel grote softwareleveranciers als werkstroom- en applicatie-integratie leveranciers ondersteunen dit soort functionaliteit. Hierdoor is op de markt een groot scala aan oplossingen beschikbaar. Binnen SBR is een SaaS-oplossing geselecteerd, waarmee ketenpartners toegang kunnen krijgen tot de processen in uitvoering en in ontwerp. Momenteel werkt Logius aan de verdere ontwikkeling van dit processenlab, waarin een sterkere koppeling tussen weergave, executie en simulatie punt van aandacht is.

5.6.2 *Zwakten BPMN*

BPMN kent – mede door haar eenvoud – ook een aantal zwakten. Onderstaand de nadelen die binnen SBR worden ervaren.

- BPMN is een visuele standaard. Het uitwisselen van BPMN modellen tussen suites is soms lastig.
- Het beoordelen en reviewen van grote, complexe en meerlaagse modellen is soms lastig. Het beheer van modellen en consistentie tussen modellen is daardoor geen sinecure.
- BPMN heeft geen standaard voor het formuleren van 'complexe' business rules.
- BPMN geeft ruimte om hetzelfde probleem op verschillende wijzen te beschrijven, hierdoor is er - overeenkomstig de Nederlandse Taxonomie Architectuur - eigenlijk Nederlandse (BPMN) procesarchitectuur nodig.
- De directe conversie naar een executeerbare code blijkt in de praktijk nog lastig en er is nog relatief veel kennis van de procesengine nodig om de koppeling te maken.

5.7 Wat zijn specifieke eisen aan SBR i-processen?

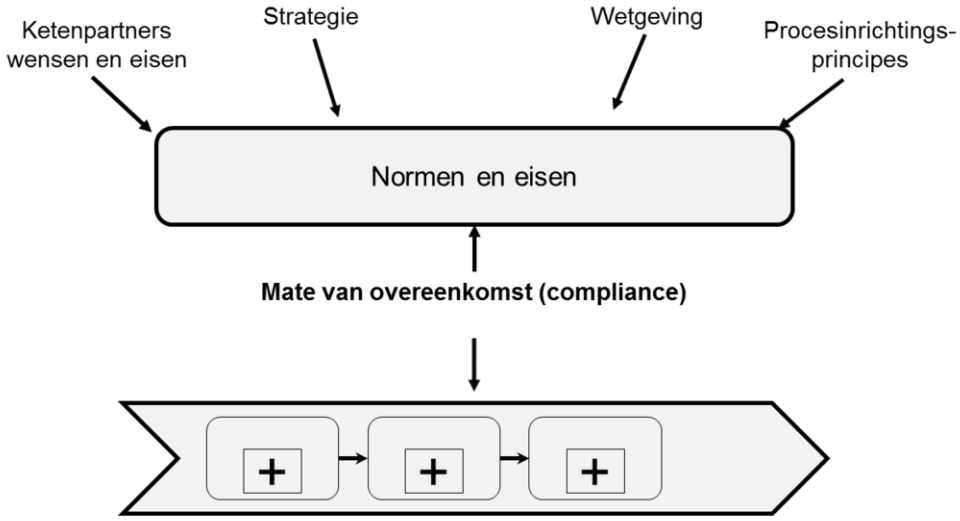
Een i-proces (informatieverwerkingsproces) bestaat uit een verzameling van taken die samen informatie verwerken. In het verantwoordingsdomein zijn de i-processen de processen van uitwisseling en verwerking (bijvoorbeeld het aanleveren en controleren van gegevens) van de door een verantwoordende partij aan een uitvragende partij aangeboden verantwoording (bijvoorbeeld de aangifte vennootschapsbelasting). Een deel daarvan wordt door de generieke procesinfrastructuur (Digipoort) uitgevoerd. We verkennen hier dit SBR-deel van de i-processen. Deze i-processen zijn opgebouwd uit losse services, koppelvlakservices en verwerkingsservices, waar we in hoofdstuk 7 dieper op ingaan.

Belangrijke eisen aan de SBR oplossing zijn dat de i-processen conform wettelijke kaders worden uitgevoerd, dat deze bij wijziging van de i-processen (of van de kaders zelf) deze conformiteit behouden en dat verschillende procesgangen (en daarmee verschillende normenkaders) onderhouden kunnen worden.

5.7.1 *Compliance: conformiteit met vooraf gedefinieerde normen*

Op basis van hun wettelijke taak zijn de uitvragende partijen verantwoordelijk voor de inrichting van de uitvraagprocessen. Het programma van eisen dat een uitvragende partij voor deze i-processen hanteert, kent een aantal bronnen. Allereerst is er

de wetgeving. Verder komen eisen bijvoorbeeld voort uit het regeringsbeleid, het algemene beleid van de uitvragende partij, de inrichtingsprincipes (convicties) die de uitvragende partij hanteert en wensen en eisen van ketenpartners. Zoals we eerder hebben gezien, kunnen deze eisen conflicteren. Dit geldt zelfs voor wettelijke eisen onderling. Het komt dan ook zelden voor dat een i-proces volledig tegemoetkomt aan alle eisen. Door van tevoren een integraal eisenkader op te stellen voor een i-proces, worden afwegingen vooraf inzichtelijk gemaakt. Bestuurders kunnen in dat geval architecten heldere uitgangspunten meegeven, die zij bij het ontwerp kunnen toepassen. In figuur 5.14 is de confrontatie tussen de normen en de i-processen in werking weergegeven. Compliance gaat over de mate waarin i-processen aansluiten bij vooraf gedefinieerde normen.



Figuur 5.14 – Bepalen mate van compliance: confrontatie tussen normen en i-processen in werking

5.7.2 *Vertalen van normen*

Binnen SBR is er een werkgroep die de generieke i-processen toetst aan de wettelijke normen voor de verantwoordingsprocessen. Deze werkgroep compliance toetst daarnaast de i-processen aan de eisen die gelden vanuit de semantische, syntactische en technische standaarden voor SBR. Logius voert de i-processen uit met behulp van de generieke procesinfrastructuur: Digipoort. Digipoort is een systeem van de overheid, beheerd en gebruikt in opdracht van de uitvragende bestuursorganisatie ten behoeve van het uitvoeren van de wettelijke taak of bevoegdheid van de uitvragende bestuursorganisatie. Logius kent geen bestuursbevoegdheden en daarom geldt Digipoort als verlengstuk van het bestuursorgaan. Hiermee zijn de eisen die een uitvragende partij stelt aan het uitvraagproces direct van toepassing op de i-processen die afgehandeld worden in de Digipoort. Het is dan ook de uitvragende partij die zich aan de afspraken omtrent SBR (de standaarden) conformeert.

Een aanduiding van Logius of Digipoort als postkamer of doorgeefluik is echter niet juist. Het is van belang vast te stellen dat Logius in de verantwoordingsketen initieel de volgende taken uitvoert:

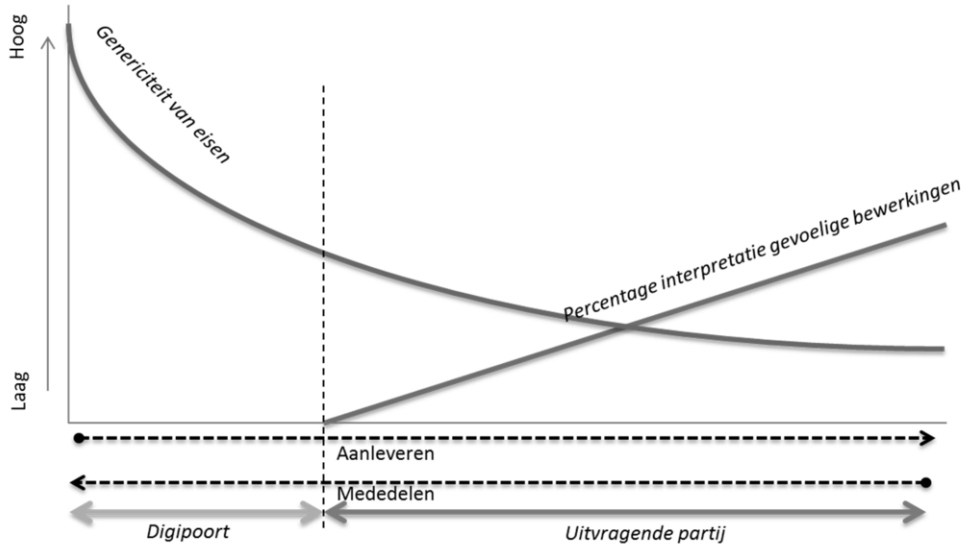
- Bevestigen van succesvolle aanlevering
- Verifiëren van de authenticiteit van het aangeleverde bericht en verifiëren van de identiteit, authenticiteit en autorisatie van de aanleverende partij
- Zekerstellen[15] en archiveren van aangeleverde berichten
- Controleren van instances op consistentie met rapportageregels, zolang deze regels beperkte (te verwaarlozen) ruimte voor interpretatie kennen
- Afleveren van berichten

Vanaf 2011 komen daar nog andere taken bij. Logius beheert dan in ieder geval tijdelijk het vertrouwde register waarin machtigingsrelaties zijn opgenomen in het kader van de Service Bericht Aanslag (SBA). Daarnaast biedt Logius een standaard eMededelenproces waarin mededelingen van uitvragende partijen, zoals SBA's, op een standaard wijze ter beschikking gesteld kunnen worden.
Kijken we naar de positie die Logius in de uitvraagprocessen heeft ingenomen, dan kan gesteld worden dat Logius:

- die taken afhandelt die in grote mate generiek zijn voor de verschillende verantwoordingsketens;
- de controles uitvoert op objectieve en eenduidig te communiceren criteria. De controles van Logius leiden tot beslissingen die objectiveerbaar te rechtvaardigen zijn op basis van de wet elektronisch bestuurlijk verkeer;
- een aanvullende rol speelt bij de formele terugkoppeling naar de aanleverende partij.

In figuur 5.15 is de positionering van Digipoort ten opzichte van de uitvragende partijen schematisch weergegeven. Achtereenvolgens bespreken wij een aantal relevante normen dat op dit deel van de i-processen betrekking heeft en maken wij inzichtelijk tot welke procesontwerpen deze normen geleid hebben. De teksten en analyses zijn in grote mate gebaseerd op materiaal dat aangereikt is door de werkgroep compliance en de werkgroep processen/techniek van SBR. De getoonde ontwerpvoorbeelden zijn afkomstig uit de meest recente SBR i-procesontwerpen. Voor een overzicht van de SBR-i-processen op hoofdlijnen verwijzen wij naar bijlage A1.

[15] Het tijdelijk bewaren van een bericht ten behoeve van het eventueel herstel van een proces.



Figuur 5.15 –Positionering Digipoort

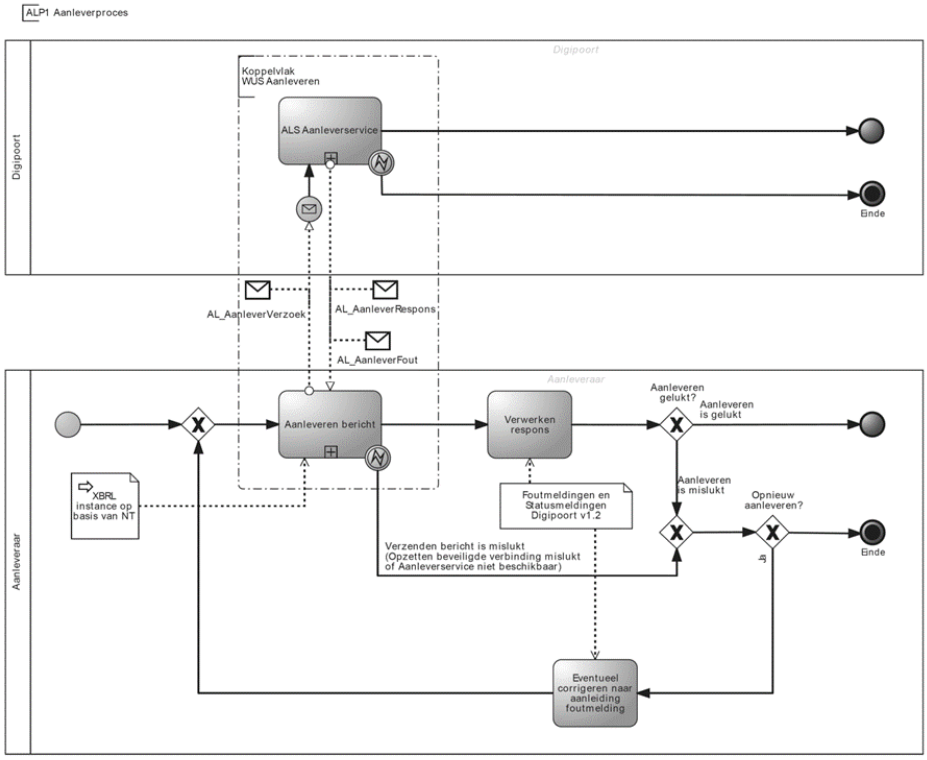
De verantwoordelijkheid over het bericht: ontvangstbevestiging Digipoort

Een aanleverende partij wil, los van de inhoud, in de eerste plaats weten wanneer hij ervan uit kan gaan dat de uitvragende partij een aangeleverd bericht ook daadwerkelijk ontvangen heeft. Bij een dispuut wil deze immers niet te horen krijgen dat de overheid 'helemaal niet bekend is met enige aanlevering'. Artikel 2:17 lid 2 Awb zegt hierover: "*Als tijdstip waarop een bericht door een bestuursorgaan elektronisch is ontvangen, geldt het tijdstip waarop het bericht zijn systeem voor gegevensverwerking heeft bereikt.*" Digipoort is in dit geval het systeem van gegevensverwerking. Het bedoelde tijdstip van ontvangst betreft het moment van 'technische' ontvangst. Dit zegt – op dat moment – nog niets over de verwerkbaarheid van het bericht. Hiermee wordt zowel de technische als de functionele verwerkbaarheid bedoeld, vast te stellen door controles op bijvoorbeeld betrouwbaarheid, vertrouwelijkheid en volledigheid en op de functionele inhoud van het bericht. Er kunnen nog handelingen van de aanleveraar worden verwacht indien het bericht niet daadwerkelijk verwerkbaar blijkt. Bijvoorbeeld in een systeem als Digipoort kan de verwerkbaarheid pas worden vastgesteld na een aantal controles ná het tijdstip van ontvangst. De wet (artikel 4:3a Awb) vereist een ontvangstbevestiging voor een elektronisch ingediende aanvraag.[16] Deze technische ontvangstbevestiging hoeft niet exact op het tijdstip van ontvangst te worden verzonden. De ontvangstbevestiging kan op een later moment worden gegeven, na een aantal noodzakelijke controles, door middel waarvan de technische verwerkbaarheid kan worden vastgesteld. De technische ontvangstbevestiging dient herleidbaar te zijn naar het bericht. De herleidbaarheid is van belang, omdat een aanleveraar meerdere berichten 'tegelijk' kan inzenden (inzending van meer dan één

[16] Algemeen wordt aangenomen dat dit geldt voor alle soorten elektronisch ingediende berichten, ook niet-aanvragen.

bericht voordat de bevestiging van de eerste is ontvangen). In geval van een fout bericht is het pas mogelijk om alleen dat bericht opnieuw in te zenden, indien kenbaar is in de foutmelding en/of bevestiging welk bericht het betreft. Anders zou de aanleveraar alles opnieuw moeten aanbieden. Een bestuursorgaan mag een bericht ook weigeren. Dit kan op basis van artikel 2:15 lid 2 en 3 Awb wanneer een bericht respectievelijk een aanvaarding zou leiden tot een onevenredige belasting voor het bestuursorgaan en wanneer de betrouwbaarheid of vertrouwelijkheid van dit bericht onvoldoende is gewaarborgd. Een goed voorbeeld hiervan is als de uitkomst van de verificatie van de autorisatie / bevoegdheid om het desbetreffende bericht aan te leveren negatief is. Op grond van artikel 2:15 lid 3 en lid 4 Awb is het bestuursorgaan verplicht om deze weigering mede te delen.

Bovenstaande normen gelden voor de volledige berichtenstroom van de SBR i-processen, zowel de aangifteprocessen van de Belastingdienst als het deponeren van een jaarrekening bij de KvK of het aanleveren van statistische informatie bij het CBS. Deze set van eisen leidt tot het volgende ontwerp voor de aanleverservice van Digipoort.



Figuur 5.16 – Aanleverproces op hoofdlijnen

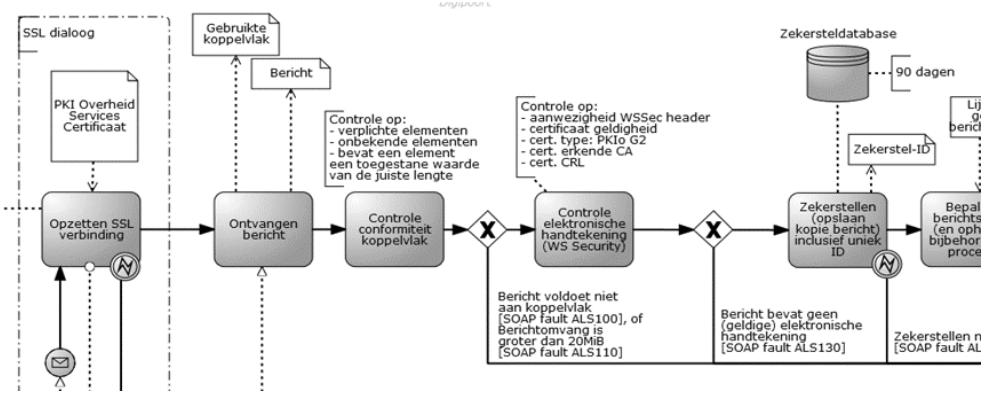
In de aanleverprocessen vindt er in één sessie één aanlevering plaats bij de aanleverservice. De aanleverende partij heeft de mogelijkheid een eigen aanleverkenmerk

met het bericht mee te geven. De aanlevering levert altijd een aanleverfout of een technische ontvangstresponse op.

In de aanleverservice vinden allereerst twee basiscontroles plaats, waarin vastgesteld wordt of een bericht:

- een correcte WS-securityheader heeft, zodat de betrouwbaarheid van het bericht voldoende geborgd is;
- een maximaal toegestane berichtomvang niet overschrijdt.

Beide onderdelen kunnen een foutmelding tot gevolg hebben. Deze foutmelding is in ieder geval te herleiden naar het bericht, doordat zij in dezelfde sessie als het bericht ontstaat. Zij verwijzen echter niet naar het meegegeven aanleverkenmerk, omdat Digipoort niet aan de slag gaat met een potentieel risicovol bericht. Hiermee kan een virus of denial of service attack voorkomen worden. De herleidbaarheid van de foutmelding naar het bericht dient in dit geval door de applicatie van de aanleveraar op 'sessieniveau' te worden gerealiseerd. Zijn deze controles echter goed doorlopen, dan wordt het bericht direct zekergesteld. In figuur 5.17 zijn de controles uit dit eerste deel van de aanleverservice weergegeven.



Figuur 5.17 – Initiële controles aanleverservice

Vervolgens vinden er binnen de aanleverservice nog diverse controles plaats die tot een formele weigering kunnen leiden. Dergelijke foutmeldingen verwijzen echter altijd naar het meegegeven kenmerk van de aanlevering. Hierdoor is de foutmelding op berichtniveau direct herleidbaar. Tevens is het bericht in originele vorm zekergesteld. Indien een dispuut ontstaat over een weigering of juist doorlevering kan in ieder geval tot 90 dagen het originele bericht opgevraagd worden.

Wanneer een bericht inderdaad verwerkbaar blijkt door Digipoort, volgt er een technische ontvangstresponse, een bericht met daarin zowel het door de aanleveraar opgenomen kenmerk als een door Digipoort toegekend proces ID. Met dit kenmerk is de verdere procesafhandeling van het bericht te volgen. Na de technische ontvangstresponse vinden er in de Digipoort en bij de uitvragende partij nog controles plaats die kunnen leiden tot het niet accepteren van het bericht voor verwerking. Een aanleverende partij die weet dat een bericht goed ontvangen is, dient vervolgens dus nog

wel vast te stellen of het uiteindelijk ook voor verwerking is geaccepteerd: functioneel verwerkbaar is. Dit doet de aanleveraar door bij Digipoort een nieuwe sessie te initieren om de statusinformatie over het bericht op te vragen.

Voldoen aan de vereiste formele aanleveractiviteiten: acceptatie voor verwerking
Het bericht moet voldoen aan de functionele eisen voor de betreffende verantwoording (gesteld in/op grond van domeinspecifieke wet- en regelgeving). Dit wordt vastgesteld door de uitvragende partij, met/na eventuele mogelijkheid tot herstel, en eventueel bevestigd (naar de aanleveraar) door deze partij, afhankelijk van diens interne processen. De Belastingdienst en de KvK hebben deze bevestiging bij een oudere versie van de procesinrichting als een aparte mededeling verstuurd. Bij de huidige procesinrichting krijgen partijen de statusinformatie over de verwerking bij de uitvragende partij via dezelfde statusinformatie service als de statusinformatie van de verwerking binnen Digipoort. De aanleverende partij kan het bericht volgen tot het een zogenaamde eindstatus heeft bereikt. De uitvragende partijen communiceren bij welke eindstatus een bericht geaccepteerd is voor verwerking. Het bericht is vanaf dit moment herstelbaar, met andere woorden: inhoudelijke onvolkomenheden moeten in principe kunnen worden aangevuld door de aanleveraar (4:5 lid 1 Awb).

Archiveren
De Archiefwet 1995 (Staatsblad 1995, 276) schrijft voor hoe een overheidsorganisatie om dient te gaan met gegevens die door haar zijn opgemaakt en ontvangen. Deze wet regelt onder meer de vorming, selectie, behoud en vernietiging van archiefbescheiden. In de Memorie van Toelichting van de Archiefwet 1995 (p.4) staat dat één van de belangrijkste doeleinden van het archiefbeleid het zorgvuldig en selectief bewaren van informatie is. Dit betekent dus dat niet alle informatie gearchiveerd dient te worden en dus niet alle informatie een archiefbescheiden is. Volgens de wet zijn onder meer archiefbescheiden: "*bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten*" (artikel 1 sub c Archiefwet 1995). Een aantal onderdelen van de Archiefwet is nader uitgewerkt in het Archiefbesluit (Staatsblad 1995, 671). Het Archiefbesluit is de voornaamste uitvoeringsregeling van de Archiefwet. Daarnaast is er de Archiefregeling (Staatscourant 2010, 70).

De Archiefregeling geeft in artikel 17 onder andere het volgende aan:
"*De zorgdrager zorgt ervoor dat van elk van de archiefbescheiden te allen tijde kan worden vastgesteld:*

a. *de inhoud, structuur en verschijningsvorm bij het ontvangen of opmaken ervan door het overheidsorgaan, een en ander voor zover deze aspecten kenbaar moesten zijn voor de uitvoering van het betreffende werkproces;*
b. *wanneer, door wie en uit hoofde van welke taak of werkproces het door het overheidsorgaan werd ontvangen of opgemaakt* [..];"

Vanaf het moment van het ontvangen van archiefbescheiden moeten dus de originele verschijningsvorm en de metadata (zoals het tijdstip van binnenkomst en de onder-

liggende taak of handeling) vastgelegd worden, zodat altijd de authenticiteit (de conformiteit met de oorspronkelijk vastgelegde versie) van de weergave van een bescheiden geverifieerd kan worden.[17]

Digipoort verwerkt het elektronische bericht. Zo is de inhoud van de elektronische envelop, de daadwerkelijke instance, in eerste instantie base64 gecodeerd. Teneinde het bericht te kunnen valideren is hier een decodering nodig. Bovendien vervangt Digipoort de originele WS-securityheader door een eigen WS-security header. Wanneer een aanleverende partij het idee heeft, dat de inhoud die verwerkt is niet aansluit bij de ingezonden inhoud, zal deze de behoefte hebben het originele door de overheid ontvangen bericht te toetsen aan het bericht dat in zijn beleving verwerkt had moeten worden. Artikel 17 uit de Archiefregeling schrijft voor dat de uitvragende partij hier inderdaad achteraf over moet kunnen beschikken. In figuur 5.17 is te zien hoe direct na de controle van de WS-security header het bericht wordt zekergesteld (tijdelijk bewaard ten behoeve van het eventueel herstel van een proces). Dit zekergestelde bericht is nog niet gemodificeerd en blijft in ieder geval 90 dagen bewaard. Voor de controle op de WS-security header is de authenticiteit van het bericht niet vast te stellen en zou opslaan een risico kunnen zijn. Wanneer uit de verdere verwerking van het bericht blijkt dat het gaat om een archiefbescheiden, plaatst Digipoort het zekergestelde (en originele) bericht in een tijdelijk archief. Dit tijdelijke archief kan gekoppeld worden met relevante decentrale archieven van uitvragende partijen.

Zekerstellen / Herinjectie
Een ander voordeel van het zekerstellen is dat het de overheid beter in staat stelt om haar verantwoordelijkheid voor het 'ontvangen' bericht te nemen. Herinjecteren is het opnieuw in het proces brengen van een bericht wanneer door een (technische) fout de verwerking gestopt is. De exacte inrichting van het herinjecteren ligt begin 2013 nog voor bij de werkgroep processen/techniek en de architecten van Logius. Wel zijn de volgende zaken duidelijk.

Het herinjecteren wordt gestart bij bepaalde technische fouten, waarvoor de aanleveraar in principe een technische fout als status zou krijgen. Indien herinjecteren lukt en het proces verloopt verder goed, dan krijgt de aanleveraar per aanleverstap de reguliere bevestiging van Digipoort. Indien het herinjecteren niet succesvol is, krijgt de aanleveraar - aan het einde van de sessie - alsnog de foutmelding van de service waar de technische fout optrad.

Juridisch gezien is het van belang dat:

- de aanleveraar per ommegaande een reactie (positief of negatief) krijgt op zijn aanlevering (de technische ontvangstbevestiging of foutmelding van de aanleverservice) (de Awb en beginselen van zorgvuldigheid, transparantie en rechtszekerheid);
- de aanleveraar via de statusservice een eventuele foutmelding teruggekoppeld krijgt en kan zien waar de fout optreedt (2:15 Awb);

[17] Zie ook http://www.archief.nl/informatiebeheer archiefvorming/authenticiteit/authenticiteit-vaststellen

- de aanleveraar in geval van een goed verlopen proces een bevestiging krijgt van de eindstatus met hierbij het tijdstip van de statusmelding.

Het primaire proces biedt hiervoor de benodigde functionaliteit. Omdat herinjecteren binnen het aanleverproces plaatsvindt, zijn deze belangrijke elementen ook bij de herinjectie geborgd. De juridische positie van de aanleveraar verandert met foutmelding of bevestiging, niet met herinjectie(pogingen). Wel worden alle statussen van een bericht, dus ook ten aanzien van herinjectie, teruggekoppeld aan de aanleveraar.

5.7.3 *Verschillende eisen aan de verantwoordingsprocessen*

Eén van de eisen aan de SBR oplossing was dat deze gestandaardiseerde i-processen moet kunnen verwerken, maar wel in meerdere en zelfs verschillende procesgangen. De reden hiervoor is dat per verantwoordingsstroom de gewenste servicelevels anders kunnen zijn en men te maken heeft met verschillende normen. De normen die wij hiervoor hebben besproken zijn vooral uit algemene wetgeving afkomstig. Maar er zijn ook eisen aan de i-processen en aan Digipoort ingegeven door de specifieke domeincontext. Dit is ook logisch, omdat algemene wetten vaak bepalingen kennen in de trant van 'voldoende voor het doel…'. Hiermee wordt de definitieve uitwerking direct afhankelijk van de context. Zoals in het hoofdstuk over beveiliging aan de orde zal komen, bepaalt bovendien de inrichting van het totale ketenproces in sterke mate de eisen die aan de Digipoort i-processen gesteld zullen worden. Verschillen die spelen binnen SBR hebben met name betrekking op kwalitatieve aspecten van de processen. Denk hierbij bijvoorbeeld aan:

- Hoe erg is het dat een i-proces tijdelijk niet beschikbaar is? Voor een aanlevering met een harde deadline en grote aantallen is dit vervelender dan voor processen met een gespreide deadline en minder grote aantallen. Ook wanneer er nog bruikbare alternatieve aanleverkanalen zijn, zal aan de beschikbaarheid van een i-proces een andere eis gesteld worden.
- Hoe erg is het dat de informatie niet vertrouwelijk behandeld wordt? Wanneer een stuk ingezonden wordt om openbaar te maken, is de vertrouwelijkheid minder een issue dan wanneer een stuk met concurrentiegevoelige informatie ingezonden wordt dat niet 'op straat' mag komen te liggen. Een belastingaangifte is in dit kader gevoeliger dan de jaarrekening.
- Hoe erg is het dat informatie niet authentiek blijkt? Hier geldt juist dat informatie die openbaar gemaakt wordt en waar veel partijen zich op baseren, lees de jaarrekening, bij een niet authentiek exemplaar tot meer problemen kan leiden dan een niet authentiek stuk, waardoor één partij te maken krijgt met een onjuiste beschikking. In dat geval zullen de uitvragende partij en de (vermeende) belanghebbende met elkaar onderzoeken hoe de niet authentieke informatie in de keten terecht is gekomen.

In de praktijk zien we dat de serviceniveau eisen die bij de generieke i-processen gehanteerd worden in grote mate overeenkomen met de eisen van de partij die het grootste belang heeft bij de borging. De uitvragende partij stelt op basis van de eigen context vast welke serviceniveaus voor een informatiestroom benodigd zijn. In de recente dienstenbeschrijving van Logius wordt onderscheid gemaakt tussen twee

verschillende serviceniveaus: baseline en operational excellence. Beide serviceniveaus voldoen functioneel aan de Wet elektronisch bestuurlijk verkeer. Het bieden van de keuze tussen twee serviceniveaus is efficiënter dan voor elk proces een uniek serviceniveau te bepalen. Als we de wetgeving als basis nemen, kunnen we stellen dat de berichtenstroom voldoende betrouwbaar dient te zijn. Voor sommige stromen is baseline voldoende (bijvoorbeeld de jaarrekening, waarbij een bedrijf één keer per jaar aanlevert en waar later aanleveren niet erg is). Voor andere stromen is operational excellence gewenst (bijvoorbeeld OB, omdat hier een boete volgt bij te late aanlevering). De uitgangspunten van de architectuur van de SBR oplossing –scheiding van functionaliteit en techniek en loosely coupled services die de i-processen uitvoeren – zijn van belang om met twee serviceniveaus te kunnen werken.

5.7.4 *Toetsen aan de normen*

Compliance Management gaat over het ontwerpen, inrichten, implementeren, beheren en verifiëren van en rapporteren over de mate van conformiteit aan de regels. Het is de rol van de (IT) auditor om te toetsen aan de normen en het geven van een oordeel daarover. Een auditor verzamelt hiervoor feitelijk data uit het verleden om te bekijken of een proces compliant is. In ketens is het toetsen niet eenvoudig, vanwege onder andere de vele betrokken partijen, de dynamiek van het i-proces en van IT systemen. Tevens moet er een organisatie zijn die de verantwoordelijkheid neemt om de compliance van de gehele keten te bezien en zich niet alleen richt op de eigen schakel. Hierdoor vereist het toetsen in ketens, waarbij vele organisaties betrokken zijn en het om zowel IT als organisatie gaat, veel meer kennis en inzicht bij auditors (zowel in de breedte als in de diepte), die niet per definitie voorhanden is. De ketenpartners kunnen de auditor helpen door:

- voor iedere stroom een integraal normenkader (juridisch, performance, beleid etc.) voor te ontwerpen i-processen op te stellen en te onderhouden;
- voldoende controles en monitoring in het i-proces in te bouwen. Een goede audit trail is onontbeerlijk.

5.8 Welke relevante vraagstukken en ontwikkelingen lopen er rond i-processen?

De ontwikkeling van procesmodellering heeft de kloof tussen procesmodelleren en -uitvoering de afgelopen jaren verkleind. De huidige talen worden steeds krachtiger om dit verschil te overbruggen. Het ideaal dat processen alleen gemodelleerd hoeven te worden en direct uitgevoerd kunnen worden, komt steeds dichterbij. De trend rond procesmodelering is dat volgordes niet meer vooraf vastgelegd en gedefinieerd worden, maar ter plekke worden bepaald.

5.8.1 *Dynamische processen*

Binnen SBR Digipoort geldt dat i-processen altijd vooraf gedefinieerd zijn en dat altijd op dezelfde volgorde de taken worden doorlopen. Dit hoeft echter helemaal niet het geval te zijn. Vanuit een dienstgerichte en effectieve benadering is er steeds meer behoefte om de gebruiker centraal te stellen en op grond van de vraag van uitvragende partijen een specifiek (en soms uniek) i-proces samen te stellen. Een i-proces op maat biedt meer waarde voor een uitvragende partij dan een i-proces gebaseerd

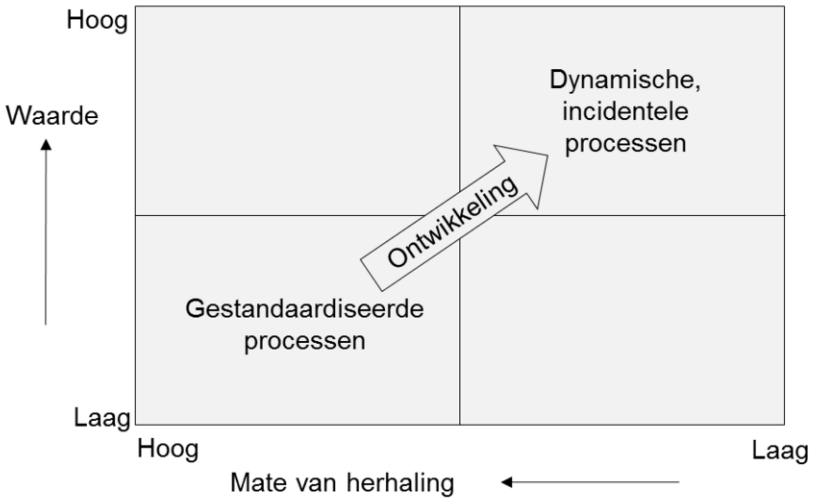
op het idee van 'one size fits all,' zoals in figuur 5.18 schematisch te zien is. In theorie betekent dit in meest extreme vorm, dat een uitvragende partij de verwerking volledig op het unieke geval toespitst. De mate van flexibilisering kan zelfs nog een stap verder gaan, waar pas bij de volgende stap bepaald wordt wanneer de voorgaande stap afgerond is en dat deze vervolgstap in principe volledig openstaat. Wanneer een persoon verantwoordelijk is voor de verwerking, valt hier wel iets bij voor te stellen. Een verantwoordingsrapport komt binnen en het valt deze persoon op dat de bedrijfsnaam een aantal keer fout geschreven is. Vervolgens kan deze persoon op het idee komen het geprinte logo te vergelijken met het logo op het internet. Wanneer dit niet goed overeen blijkt te komen, kan de verwerker bepalen een nader onderzoek in te stellen naar de authenticiteit van het stuk.

Er zijn verschillende redenen om een dergelijke risicogerichte benadering door computers te willen laten simuleren:
"*Usually such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends. Fraud cases are statistically analyzed to derive relationships among input data and values for certain key parameters in order to understand the various patterns of fraud. This knowledge of fraud trends is then iteratively taught to feed-forward neural networks, which can successfully identify similar fraud cases occurring in the future*."

Voor de verantwoordingsketens kan hierbij gedacht worden aan een validatieservice, die op basis van feedback uit de verwerking – welke berichten bleken (bewust) fout te zijn – berichten met een hoog risico op fraude kan detecteren. Het mooiste zou zijn, dat het lerende systeem tevens de meest logische vervolgstap voor controle van de vermeende misstap uitvoert. Dit zou bijvoorbeeld op basis van een trendanalyse gebaseerd op eerdere berichten van de belanghebbende kunnen geschieden.

De toepassing van dergelijke business intelligence in de geautomatiseerde keten heeft verregaande gevolgen en roept meteen vragen op. Het voordeel van vooraf gedefinieerde i-processen is, dat vooraf gecontroleerd kan worden of het proces werkt zoals bedoeld en er geen afwijkingen plaatsvinden (bijvoorbeeld: het i-proces blijft hangen bij een taak of bepaalde informatie is niet beschikbaar). Met dynamische i-processen is dat veel moeilijker en moet naar andere middelen gegrepen worden om te kunnen aantonen of een proces werkt. Dit kan door het testen van varianten, het uitvoeren van simulaties of door voor te schrijven dat een i-proces altijd minimaal bepaalde stappen bevat. Ook is het continu monitoren belangrijk, om zo'n afwijking in het i-proces tijdig te kunnen ontdekken.

Het is een fundamentele vraag of een gedeelde dienst in een publieke context, zoals Digipoort, dergelijke risicoanalyses moet uitvoeren of dat dit typisch iets is voor de backoffice van de uitvragende partij. Momenteel lijkt de technologie nog niet voorhanden om hier generieke services voor te bieden, hoewel er voorbeelden van succesvolle toepassingen bij creditcardmaatschappijen en banken bestaan. In de praktijk worden tussenvarianten bedacht van i-processen die deels vooraf gedefinieerd zijn (bijvoorbeeld de generieke stappen) en waarbij de specifieke stappen op verschillende wijzen uitgevoerd kunnen worden.



Figuur 5.18 –Van statische naar dynamische processen (gebaseerd op Gong, Janssen, Overbeek, & Zuurmond, 2009)

5.8.2 *Toepassing van business rules*

I-Processen kunnen worden aangepast in BPMN of BPEL, maar dit is een omslachtige manier van werken. Ook het modelleren van een proces met zeer veel varianten ligt niet voor de hand. Om de gewenste flexibiliteit te verkrijgen wordt vaak met bedrijfsregels (business rules) gewerkt. Een business rule is een compacte en eenvoudige verklaring, die een aantal belangrijke aspecten van een bedrijf vertegenwoordigt (Morgan, 2002). Door het vastleggen van de regels van een organisatie hoeven alleen deze regels veranderd te worden om de processen ook te veranderen. Feitelijk biedt een validatieservice die compliant is met de XBRL-module formula's de mogelijkheid om consistentiechecks op basis van business rules op objectniveau uit te voeren. Het is dan wel van belang te definiëren wat er met de uitkomst van de validatie gebeurt. De koppelvlakken van Digipoort bieden de mogelijkheid om aanvullende metadata (bijvoorbeeld een verwerkingsklasse) met de instance mee te geven. Het gebruik van formula validatie op betrekkelijk harde regels (zie hoofdstuk 6 – Gegevens), zoals de FRIS-regels, is organisatorisch en bestuursrechtelijk gemakkelijker te realiseren binnen Digipoort dan het gebruik van complexe regels voor risicoanalyses.

De incorporatie van bedrijfsregels binnen processen brengt enkele vraagstukken met zich mee:

- Ambiguïteit. Verschillende betrokkenen kunnen diverse interpretaties aan business rules geven. Dit wordt nog verder bemoeilijkt als de regels (deels) vanuit (meerdere) uitvragende partijen worden aangeleverd. Bij het tekenen van een proces is duidelijk hoe dit gaat verlopen, maar bij het gebruik van bedrijfsregels hoeft zulks niet het geval te zijn. Het beheer van regels is een aspect dat aandacht behoeft, zeker als de regels (deels) vanuit (meerdere) uitvragende partijen worden aangeleverd.

- Het feit dat de Simplified Validation Rules geen onderhouden standaard business rule taal is, was de reden dat de Belastingdienst het gebruik van de simplified validation rules door Digipoort niet accepteerde.
- Verschillende type bedrijfsregels. Er is niet zoiets als een 'bedrijfsregel'. Deze kunnen op verschillende niveaus voorkomen. De verschillende niveaus vragen om verschillende 'talen'.
- Vertaling. De overgang van 'een zinnetje in een wet' naar geautomatiseerde ondersteuning kan ontzettend groot zijn. Het veranderen van één woord in een wet kan een grote invloed hebben. Dit is afhankelijk van de interpretatie die eraan gegeven wordt. De gevolgen van de interpretatie zijn niet altijd direct zichtbaar bij bedrijfsregels.
- Eigenaarschap. Een proceseigenaar is relatief makkelijk aan te wijzen, maar wie eigenaar is van welke bedrijfsregel is onduidelijk. Ook wat te doen als bedrijfsregels conflicterend zijn.

Om bedrijfsregels in processen te ondersteunen is de Semantics of Business Vocabulary and Business Rules (SVBR) ontwikkeld, die door de Object Management Group (OMG) onderhouden wordt (www.omg.org/spec/SBVR/). SVBR is een declaratieve taal, die als basis dient voor het maken van diverse type bedrijfsregels. In de toekomst moet gekeken worden hoe deze optimaal gebruikt kan worden.

5.9 Afsluiting

Voor het ontwerp van i-processen zijn goede analysemethoden en technieken voorhanden. Er heeft al veel systematisch onderzoek plaatsgevonden en er zijn diverse principes gepubliceerd. Zo veel mogelijk wordt afgevangen in het proces zelf door het proces continu te verbeteren. Er is echter geen winnend recept te geven voor het creëren van een goed proces. Bij het ontwerp of herontwerp van processen dienen de betrokken architecten uit de gehele keten in staat te zijn de trade-offs te herkennen die spelen in het specifieke domein. Zeker wanneer dit een publiek/private keten betreft, zijn trade-offs legio en spelen allerlei belangen door elkaar, zoals dit in hoofdstuk 3 beschreven is. De keuze van decompositie van processen, of dat juist lean of ToC toegepast moet worden, zijn zaken waarbij trade-offs naar voren komen. Met name het vertalen van concepten naar de praktijk is vaak moeilijker dan gedacht (Wu, 2003). De SBR voorbeelden kunnen daarbij helpen, door als referentie te dienen. In de volgende hoofdstukken komen meer voorbeelden aan bod. In hoofdstuk 6 gaan we dieper in op gestandaardiseerde gegevensuitwisseling. In hoofdstuk 7 wordt de generieke procesinfrastructuur – Digipoort – ontleed. Logius heeft met Digipoort als gedeelde procesinfrastructuur een belangrijke positie in de i-processen voor verantwoording ingenomen. Logius moet de regie over de totstandkoming en onderhoud van generieke en op wet- en regelgeving aansluitende i-processen voeren en ervoor zorgen dat deze toepasbaar zijn voor de vele publieke partijen die met verantwoordingsinformatie te maken hebben. Door hierop aan te sluiten kunnen uitvragende partijen een deel van de complexiteit in de informatie-uitwisseling tussen bedrijven betrekkelijk eenvoudig adresseren.

6 Gegevens

6.1 Inleiding

Interpretatie, context, kennis, timing, uitspraak – het zijn allemaal factoren die de interpretatie van een begrip kunnen beïnvloeden. Dit geldt ook bij de uitwisseling en verwerking van gegevens binnen een keten. Als niet is afgesproken wat een begrip inhoudt, kan elke partij er een andere interpretatie van hebben. Hoewel dit soms onschuldig oogt, kan een verkeerde interpretatie van gegevens in informatieketens tot ongewenste consequenties leiden. Denk hierbij aan een bezoek van de belasting-inspecteur of een boete van de toezichthouder. Voor informatie-uitwisseling in een keten is het essentieel dat de betekenis van de uitgewisselde gegevens niet verloren

gaat gedurende het uitwisselingproces. De gegevens moeten verwerkbaar en begrijpelijk blijven voor de personen en applicaties.

Deze uitwisseling van informatie tussen organisaties wordt sterk beïnvloed door een tweetal nauw gerelateerde informatiekundige factoren: interoperabiliteit en standaardisatie. Het begrip 'interoperabiliteit' houdt in dat verschillende organisaties in een informatieketen in staat zijn om effectief met elkaar te communiceren en zodoende relevante informatie te kunnen uitwisselen. Het draait hierbij om de verbindingen die ontstaan tussen wederzijdse processen, applicaties en technische infrastructuren. Om deze verbinding in de praktijk tot stand te laten komen, zijn afspraken nodig tussen organisaties over de wijze van verbinden. Deze afspraken kunnen als standaarden voor de uitwisseling van informatie worden vastgesteld. Een standaard is over het algemeen een procedure, maat of technologie waarvan een groep mensen met elkaar heeft afgesproken dat ze deze zullen gebruiken (OSOSS, 2005).

Dit hoofdstuk beschrijft een bouwblok van de SBR-oplossing: berichtspecificaties. Het gaat verder in op gegevensstandaardisatie en gegevensuitwisseling en het belang hiervan voor de S2S-uitwisseling en gedeelde verwerking van verantwoordingsinformatie waar SBR voor staat. Hierbij is een nadere afbakening noodzakelijk. We hebben ons bij de afbakening laten leiden door de volgende overwegingen:

- Het hoofdstuk focust op het object van het informatieverwerkingsproces (i-proces) en niet het i-proces zelf. Dat object is een gegeven of gegevensset, bedoeld om uitgewisseld en/of verwerkt te worden. Het i-proces zelf, en de afhankelijkheid tussen gegevenssets en het inrichten en automatiseren van de keten worden in respectievelijk hoofdstuk 5 en 7 beschreven.
- Het hoofdstuk dient voldoende inhoud te geven aan de theoretische concepten – waaronder syntax, semantiek, normalisatie en taxonomie – die een rol spelen bij de interpretatie van gegevens door mens en computer.
- Het hoofdstuk dient de lezer inzicht te geven in de levenscyclus van gegevens en de afspraken die in het kader van SBR zijn gemaakt.

Tegen deze achtergrond hebben we ervoor gekozen om dit hoofdstuk te splitsen in drie delen:

- De behoefte aan eenduidige gegevensinterpretatie in ketens (6.2). We gaan daarbij in op het belang van semantiek voor eenduidige interpretatie door mens en computer.
- De literatuur omtrent relevante standaarden rond syntax en semantiek en ontwikkelingen (6.3).
- De concrete invulling van deze behoefte in het kader van SBR (6.4).

Het derde deel van dit hoofdstuk (6.4) besteedt bijzondere aandacht aan de wijze waarop de Nederlandse Taxonomie tot stand is gekomen. Deze beschrijving dient partijen die interesse hebben in de concepten achter SBR inzicht te bieden in welke aspecten een rol spelen bij de totstandkoming van een taxonomie. Hierbij geldt, dat er op het gebied van gegevens nog enkele ontwikkelingen lopen die noemenswaardig zijn. Voor dit laatste geldt dat enkele relevante ontwikkelingen de wijze van totstandkoming van een taxonomie kunnen gaan beïnvloeden. Deze ontwikkelingen worden ook beschreven.

Dit hoofdstuk wordt afgesloten met een reflectie op de bovenstaande vragen. Het thema 'gegevensbeheer' valt buiten de scope van dit hoofdstuk, maar hoofdstuk 9 (Governance en beheer) zal hier kort op ingaan. Tenslotte willen we de lezer wijzen op de relatief grote hoeveelheid van inhoudelijke begrippen die wordt gehanteerd in dit verdiepingshoofdstuk. Hoewel deze begrippen zoveel mogelijk worden toegelicht, verwijzen wij de lezer voor een bredere uiteenzetting hiervan naar andere publicaties. Hier wordt in de tekst kort naar verwezen.

6.2 De behoefte: eenduidige interpretatie van gegevens in ketens

Gegevens (data) is een generieke term, die voor verschillende interpretaties vatbaar is. Het is hierbij van belang om het onderscheid tussen gegevens en informatie helder te hebben. Volgens Ackoff (1989) zijn gegevens bewerkte of onbewerkte waarden die een organisatie registreert voor allerlei doeleinden, maar ze krijgen pas betekenis, vorm en meerwaarde als ze op het juiste moment, in de juiste vorm door de juiste persoon geïnterpreteerd kunnen worden. Vanaf het moment dat gegevens geïnterpreteerd worden, wordt het gezien als informatie. Interpreteerbaar duidt hier op (McGilvray, 2008):

- verwerkbaar: de mate waarin de gegevens tot de gewenste bedrijfstransacties of uitvoer zullen leiden;
- begrijpbaar: de mate van beschikbaarheid van documentatie en metadata om het bericht correct te kunnen interpreteren.

In het kader van dit hoofdstuk verstaan we onder gegevens de feiten of begrippen, weergegeven in de vorm die geschikt is voor het communiceren, interpreteren en verwerken tot informatie, hetzij door de mens, hetzij door automatische middelen, of door beide. Dat is niet vanzelfsprekend. Verschillende organisaties werken vaak met licht afwijkende definities voor begrippen, interpreteren begrippen net even anders en berekenen waarden volgens andere regels (Besselink, 2010). Naast deze semantische verschillen kan ook de syntax afwijken. Het formaat of de structuur kan bijvoorbeeld anders zijn voor de naam van een persoon (eerst achternaam of eerst voornaam), in het gegevensformaat (vier byte datavelden versus zes byte datavelden) of in codering van het geslacht (man-vrouw versus m-f versus 1-2). Voordat we dieper ingaan op de significantie van semantiek en syntax, is het goed als we eerst de rol van gegevens in elektronisch berichtenverkeer onder de loep nemen.

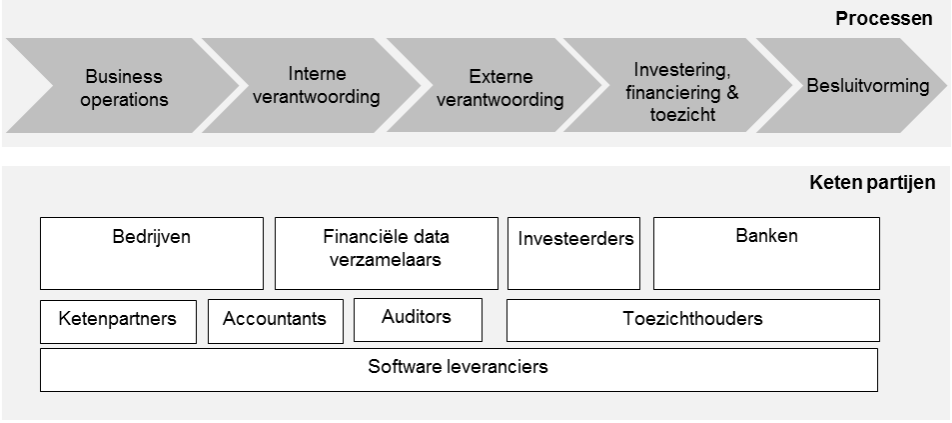
6.2.1 *De rol van gegevens in elektronisch berichtenverkeer*

Gegevens spelen een belangrijke rol in het berichtenverkeer tussen organisaties. Zij geven invulling aan de informatieverplichtingen die uitvragende partijen opleggen aan organisaties. Deze informatieverplichtingen vloeien voort uit een drietal perspectieven: het verantwoordingsperspectief, het transactieperspectief en het beleidsmatig perspectief. Deze perspectieven worden hieronder toegelicht:

1. Het verantwoordingsperspectief legt informatieverplichtingen op aan organisaties omdat zij zich dienen te verantwoorden voor hun activiteiten aan verschillende partijen, waar onder toezichthouders, aandeelhouders, kredietverstrekkers en het maatschappelijk verkeer. De gegevens die de Belastingdienst opvraagt, zijn hier een goed voorbeeld van.

2. Het transactieperspectief zorgt voor informatieverplichtingen waaraan voldaan dient te worden om een transactie te voltooien. Het verstrekken van een factuur voor de geleverde diensten waarop het bankrekeningnummer van een organisatie staat, is een voorbeeld van de informatieverplichtingen vanuit het transactieperspectief.
3. Het beleidsmatig perspectief heeft informatieverplichtingen tot gevolg omdat organisaties deze gegevens, veelal op geaggregeerd niveau, nodig hebben om beleid te kunnen voeren. Een voorbeeld van dergelijke informatieverplichtingen zijn de verschillende statistiekrapportages die het Centraal Bureau voor de Statistiek (CBS) bij organisaties opvraagt.

Bij ieder perspectief is er sprake van een zogenaamde informatieketen waarbij informatie uitgewisseld wordt tussen minimaal twee verschillende organisaties: de aanleverende partij en de uitvragende partij. In de meeste informatieketens zullen echter meer organisaties betrokken zijn die een bepaalde functie vervullen binnen de keten, zoals intermediairs, agenten en uitvoeringsinstanties. In de onderstaande figuur is een grafische weergave opgenomen van de informatieketen (business information supply chain). Deze figuur illustreert dat in een informatieketen verschillende soorten van informatie-uitwisseling op meerdere aggregatieniveaus plaats kunnen vinden. Daarnaast geeft de figuur ook aan dat verschillende organisaties hierbij betrokken kunnen zijn.



Figuur 6.1 – Informatieketen (Hoffman & Watson, 2010)

De efficiënte uitwisseling van gegevens die horen bij de informatieverplichtingen richt zich op het uitvragen van gegevens bij organisaties tegen zo laag mogelijke operationele kosten (Nijsen, 2003). De efficiënte informatieketen is gebaat bij de digitalisering van de gegevensaanlevering door organisaties aan uitvragende partijen. Hierbij dient de vastlegging van gegevens eenmalig aan de bron plaats te vinden. Dit maakt het mogelijk dat gegevens niet meer overgetypt hoeven te worden en dat meerdere uitvragende partijen niet (gedeeltelijk) dezelfde gegevens of af te leiden gegevens hoeven op te vragen bij organisaties.

Grijpink (2010) noemt dit ook wel keteninformatisering, oftewel het tot stand brengen van een informatie-infrastructuur voor geautomatiseerde informatie-uitwisseling en -verwerking tussen organisaties binnen een informatieketen.

Organisaties kunnen om verschillende redenen kiezen om de informatieverwerking elektronisch te laten verlopen in plaats van op papier, via webformulieren of anderszins. Volgens Arendsen (2008) zijn mogelijke redenen onder meer:

- De vereiste korte reactietijd van de partners in de keten.
- Een betrouwbaar en aantoonbaar proces van uitwisseling/verwerking.
- De hoge frequentie in de uitwisseling van berichten.
- Het grote aantal berichten dat wordt uitgewisseld.

Daarnaast zijn ook andere redenen te onderkennen, zoals:

- Het besparen op de kosten van de creatie van de berichten.
- Een verlaging van transactiekosten[18] van de uitwisseling (bij gelijkblijvende eisen).
- Een verlaging van de vastlegging en handlingkosten (archief versus disks).
- Een verhoging van de productiviteit, zoals verkorting van de transactietijden en verbetering van processen.
- Het voorkomen van redundantie in de keten (het meerdere malen ingeven van dezelfde gegevens).

Bovenstaande voordelen zijn generiek en hebben met name betrekking op mogelijke kostenbesparingen op het gebied van het verwerken, opslaan, verzenden en delen van gegevens. Deze voordelen kunnen worden behaald door zowel de aanleverende als uitvragende partijen binnen een keten.

Om deze voordelen daadwerkelijk te realiseren is volgens Arendsen (2008) bij de toepassing van elektronisch berichtenverkeer integratie met de interne geautomatiseerde informatiesystemen een cruciale voorwaarde. Dit is bij de uitwisseling van zogenaamd 'digitaal papier'[19] veelal niet het geval. Wij zijn van mening dat de uitwisseling van 'digitaal papier' tussen organisaties niet kan worden gezien als elektronisch berichtenverkeer. Voor het definiëren van elektronisch berichtenverkeer wordt in dit hoofdstuk aangesloten bij de definitie van de Engelstalige term '*electronic data interchange*' van Hansen & Hill (1989). Zij definiëren deze term als "*the movement of business documents electronically between or within firms (including their agents or intermediaries) in a structured, machine-retrievable, data format that permits data to be transferred, without re-keying, from a business application in one location to a business application in another location*".

[18] Transactiekosten zijn de kosten om de verschillende schakels in de productieketen op elkaar af te stemmen (den Butter, 2010)
[19] Digitaal papier kan worden omschreven als een digitaal bestand dat geen enkele interactieve operabiliteit biedt, zoals een bestand in een formaat als Microsoft Word of Acrobat PDF.

Bovenstaande definitie benadrukt het belang van gestructureerde gegevens. De term gestructureerde gegevens verwijst naar gegevens die te identificeren zijn omdat ze georganiseerd zijn in een bepaalde structuur. De meest voorkomende vorm van gestructureerde gegevens is te vinden in databases waarin specifieke informatie wordt opgeslagen op basis van een methodologie van kolommen en rijen. Ook gegevens uitgedrukt in de vorm van eXtensible Markup Language (XML) documenten met diep hiërarchische en recursieve structuren zijn te classificeren als gestructureerde gegevens. Gestructureerde gegevens zijn doorzoekbaar op datatype, kunnen worden begrepen door computers en ook efficiënt gepresenteerd worden voor menselijke lezers. In tegenstelling tot gestructureerde gegevens, heeft ongestructureerde data geen herkenbare structuur. In de praktijk worden vaak ongestructureerde gegevens uitgewisseld op basis van 'digitaal papier'.

6.2.2 *Behoefte aan eenduidige betekenis*

Wanneer organisaties met elkaar communiceren is het belangrijk dat de betekenis van de gegevens van de ene organisatie op een juiste manier wordt overgedragen aan de andere organisatie. Deze behoefte wordt vaak gevangen onder de noemer 'semantiek' (Floridi, 2011; McComb, 2003). Semantiek is een abstract begrip en zodoende voor verschillende interpretaties vatbaar. In het kader van gegevensuitwisseling sluiten we ons aan bij de beschrijving van Ouksel & Sheth (1999), die stellen dat semantiek zich bezig houdt met het in kaart brengen van de echte wereld door deze te vertalen naar objecten in een model. Hierbij richt het zich op de bijbehorende problemen die menselijke interpretatie of de betekenis en het gebruik van gegevens of informatie met zich meebrengen. We hebben het zodoende over semantiek wanneer we praten over een (potentieel) grote set van expressies, die gezamenlijk als doel hebben om een domein van de echte wereld te vertegenwoordigen.

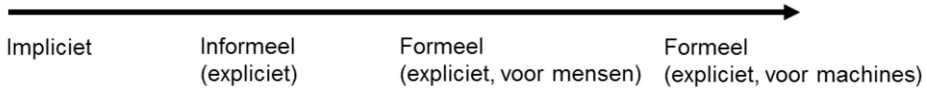
Volgens Uschold (2003) dienen drie vragen te worden beantwoord omtrent semantiek:

1. Is de semantiek expliciet of impliciet?
2. Is de semantiek formeel of informeel uitgedrukt?
3. Is de semantiek bedoeld voor menselijke of geautomatiseerde verwerking?

Met behulp van deze vragen identificeert Uschold (2003) vier soorten semantiek:

1. Impliciet
2. Expliciet en informeel
3. Expliciet en formeel voor menselijke verwerking
4. Expliciet en formeel voor geautomatiseerde verwerking

Deze vier soorten semantiek kunnen worden weergeven in een semantisch continuüm. Hierbij is de eerste extreme, dat er helemaal geen semantiek bestaat voor wat zich in de gedachten van mensen bevindt die de terminologie gebruiken. De andere extreme is de formele en expliciete semantiek die volledig geautomatiseerd is. In de figuur is een weergave van dit continuüm opgenomen. In werkelijkheid zijn de grenzen uiteraard niet zo evident en kan er sprake zijn van een tussenvorm.



Figuur 6.2 – Het semantische continuüm (Uschold, 2003)

De vier soorten semantiek worden hieronder nader uitgewerkt.

Impliciete semantiek
In eenvoudige gevallen is semantiek uitsluitend impliciet. Dit houdt in, dat de betekenis overgebracht wordt op basis van een gezamenlijk begrip dat is afgeleid van menselijke consensus. Er zal echter nergens vastgelegd of vermeld staan wat een begrip exact betekent. Het nadeel van impliciete semantiek is dat het dubbelzinnig is, waardoor mensen van mening kunnen verschillen over wat een begrip betekent. De eliminatie van deze dubbelzinnigheid is belangrijk.

Informele semantiek
Iets verder langs het continuüm is de semantiek expliciet en wordt deze uitgedrukt op een informele wijze, zoals door middel van een tekstuele beschrijving. Machines kunnen slechts in beperkte mate gebruik maken van op informele wijze uitgedrukte semantiek, als gevolg van de complexiteiten die samenhangen met het gebruik van taal. Deze vorm van semantiek is – net als de impliciete - dus meer gericht op het gebruik door mensen. Het nadeel van informele semantiek is dat twee verschillende implementaties niet noodzakelijkerwijs consistent en congruent hoeven te zijn, waardoor de implementaties op subtiele punten van elkaar afwijken. Dit kan leiden tot problemen wanneer interoperabiliteit vereist is of wanneer implementaties veranderen.

Formele semantiek voor menselijke verwerking
Nog iets verder langs het continuüm wordt semantiek expliciet gemaakt door middel van een formele taal, maar wel uitsluitend bedoeld voor menselijke verwerking. Hierbij valt te denken aan formele documenten of formele specificaties van betekenis. De formele semantiek voor verwerking door mensen helpt om dubbelzinnigheid in begrippen te elimineren. Doordat nog altijd sprake is van menselijke betrokkenheid, kunnen er fouten gemaakt worden.

Formele semantiek voor geautomatiseerde verwerking
Tenslotte is sprake van expliciete, formeel gespecificeerde semantiek die bedoeld is om begrippen geautomatiseerd te laten verwerken met behulp van computers. Wanneer nieuwe begrippen geïdentificeerd worden, kan de betekenis hiervan geautomatiseerd worden afgeleid. Daarnaast kan hierdoor ook nieuwe informatie afgeleid worden voor een verscheidenheid aan doeleinden.

In het kader van elektronisch berichtenverkeer zijn we van mening dat formele en expliciete semantiek beter is dan informele of impliciete semantiek. De uitwisseling van gegevens zorgt voor de noodzaak van eenduidige interpretatie van gegevens. Hiervoor is expliciete en formele semantiek het meest geschikt. Dit houdt in dat gegevens goed georganiseerd dienen te zijn. In de volgende paragraaf gaan we in op

verschillende benaderingswijzen voor het organiseren van gegevens die expliciete en formele semantiek mogelijk maken.

6.2.3 *Behoefte aan een gemeenschappelijke taal*

Eenduidige gegevensinterpretatie vergt niet alleen eenduidige betekenis maar ook een gemeenschappelijk taal – de syntax. Onder syntax verstaan we de verzameling van afspraken die partijen onderling zijn overeengekomen en die specificeren hoe gegevens worden gerepresenteerd middels letters, cijfers en/of andere tekens. Denk bijvoorbeeld aan de notatie van een datum. Stel dat we afspreken dat elke datum wordt genoteerd als DD-MM-CCYY, waarbij DD, MM, CC en YY twee (decimale) getallen zijn die respectievelijk de dag in een maand, een maand, een eeuw en een jaartal in die eeuw aangegeven.

Syntax richt zich dus op de vorm of structuur waarin de gegevens worden uitgedrukt. Hierbij spelen open uitwisselingsformaten zoals XML een belangrijke rol. Zij passen gestandaardiseerde formaten toe voor de uitwisseling van gegevens, waardoor de afhankelijkheid van een bepaalde partij of technologie wordt verminderd. Eisen die vaak aan een syntax gesteld worden, zijn onder meer:

- De syntax dient een open standaard te betreffen, zodat er geen afhankelijkheid gecreëerd wordt van één of enkele leveranciers.
- De syntax moet het mogelijk maken om de benodigde semantische standaardisatie te realiseren, zodat het mogelijk is om eenduidig gegevens te definiëren.
- De syntax moet de gebruiker van gegevens de vrijheid bieden om de presentatie van de gegevens naar eigen wens in te richten.
- De syntax moet de betrouwbaarheid en beheersbaarheid van gegevensstromen en verantwoordingsprocessen verbeteren.
- De syntax dient efficiëntere werkmethoden mogelijk te maken, bijvoorbeeld door het beschikbaar stellen van gegevens uit informatiesystemen voor controle, analyse en toezicht.
- De syntax moet de kosten van handmatige en geautomatiseerde interfaces tussen verschillende systemen, en daarmee de totale kosten van de informatievoorziening, reduceren.

Wat opvalt in bovenstaande eisen is dat syntax en semantiek zijn verweven. Als “31-01-2012” een datum representeert, is dit niet alleen syntactisch correct - het voldoet aan de afspraak dat een datum genoteerd wordt als DD-MM-CCYY -, maar ook semantisch correct: die datum bestaat. Een datum als “30-02-2012” is syntactisch in orde, maar semantisch niet, omdat 30 februari niet bestaat.

We kunnen de eisen aan de syntax aanscherpen, zodat een rij tekens die een datum voorstelt alleen maar syntactisch correct is als die ook een betekenisvolle datum vertegenwoordigt. De mate van precisie van syntactische regels is evenredig met het gemak dat je ervan hebt in geautomatiseerde gegevensverwerking. Als syntactische afspraken zodanig precies zijn dat elke datum alleen een bestaande is, en partijen zich aan deze afspraken houden, dan hoeft dat niet meer gecontroleerd te worden.

We hebben in het eerste deel van dit hoofdstuk gekeken naar de significatie van gegevensstandaardisatie voor elektronische berichtuitwisseling. Twee niveaus van standaardisatie – semantische en syntactische – stonden hierin centraal. In het tweede deel van dit hoofdstuk schetsen wij de relevante ontwikkelingen voor beide niveaus.

6.3 Relevante standaarden en ontwikkelingen

In het tweede deel van dit hoofdstuk spelen we in op de behoeften die in het eerste deel zijn benoemd. Hiervoor putten wij uit de literatuur over standaardisatie. Standaardisatie kan uiteraard een rol spelen op tal van toepassingsgebieden, maar we beperken ons binnen dit hoofdstuk tot de uitwerking van dit vraagstuk voor met name die standaarden die van toepassing zijn op de elektronische gegevensuitwisseling binnen ketens c.q. systemen.

Door standaardisatie van processen (bijvoorbeeld afleveren en valideren), gegevens en technologische toepassingen (waaronder platformen en applicaties), kunnen ketens de complexiteit van de werkzaamheden terugdringen (van Wessel, 2008). Dit moet leiden tot een hogere mate van efficiëntie omdat de standaardisatie van deze aspecten onder meer voorziet in besparing van tijd op de uitvoer. Bovendien wordt de ondersteuning van menselijk handelen in het proces geëlimineerd. Standaardisatie (mits gedegen uitgevoerd) kan tevens resulteren in een hogere mate van stabiliteit en betrouwbaarheid.

Standaardisatie op het gebied van gegevensuitwisseling is bedoeld om zowel de rechtstreekse digitale communicatie tussen ketenpartners onderling als ook de koppelingen tussen interne bronregisters en keteninformatiesystemen verregaand te faciliteren. De behoefte aan standaardisatie kunnen we in hoofdlijnen specificeren in de behoefte aan semantische standaardisatie en syntactische standaardisatie. Beide vormen komen in de volgende secties aan bod. We beginnen met de literatuur over de semantische standaardisatie, waarin enkele benaderingswijzen voor het organiseren van gegevens worden onderscheiden. Het verschil tussen een taxonomie en een ontologie – termen de in de praktijk nogal door elkaar worden gebruikt – wordt hier duidelijk gemaakt. Na de literatuur over semantische standaardisatie kijken we naar de literatuur over syntactische standaardisatie. De ontwikkeling van open standaarden voor elektronisch berichtenverkeer geniet hier meer aandacht. Tenslotte besteden we in dit deel aandacht aan de XBRL (eXtensible Business Reporting Language) standaard voor gegevensuitwisseling.

6.3.1 *Standaardisatie van semantiek: benaderingswijzen voor het organiseren van gegevens*

In het eerste deel hebben we gezien dat eenduidige gegevensinterpretatie vraagt om eenduidige betekenis. Volgens Uschold (2003) zijn hier twee methoden voor: (1) de eenvoudige methode en (2) de specificatiemethode. Beide methoden worden hieronder toegelicht.

De eenvoudige, en vermoedelijk meest voorkomende, methode is het negeren van dit probleem. Een organisatie zal in er in dit geval vanuit gaan dat de gehanteerde terminologie dezelfde betekenis heeft binnen andere organisaties. In de werkelijkheid kunnen organisaties er niet vanuit gaan dat andere organisaties dezelfde terminologie hanteren, of, indien ze dit wel doen, begrippen ook dezelfde betekenis hebben. Een goed voorbeeld van de laatste situatie is het begrip 'winst'. Dit begrip komt zowel voor in de aangifte vennootschapsbelasting als in de jaarrekening. De Belastingdienst hanteert echter een andere definitie van dit begrip voor de aangifte vennootschapsbelasting dan organisaties in een jaarrekening op commerciële grondslag doen. Het is duidelijk dat wanneer organisaties niet dezelfde terminologie met dezelfde betekenis hanteren er een manier gevonden moet worden waarop een organisatie kan aangeven wat ze nu precies bedoelt wanneer ze gegevens communiceert.

De tweede manier volgens Uschold (2003) is dat een organisatie dient aan te geven welke begrippen zij gebruikt en wat ze betekenen. Hiervoor kan een organisatie gebruik maken van een specificatiemethode om begrippen en de hierbij behorende relaties te organiseren. Om dit mogelijk te maken moet (een deel van) de betekenis gecodeerd worden in een formele taal, ook wel syntax genoemd. Hierbij wordt de betekenis van een begrip door relaties, resources en attributen vormgegeven.

Een organisatie kan gebruik maken van verschillende benaderingswijzen om haar begrippen en bijbehorende relaties te organiseren. Mogelijke benaderingswijzen om gegevens te organiseren zijn met behulp van gecontroleerde woordenboeken, taxonomieën, thesauri en ontologieën. De verschillende benaderingswijzen worden hieronder kort uiteengezet.

Gecontroleerd woordenboek
Een gecontroleerd woordenboek is een lijst van begrippen die expliciet worden opgesomd. Deze lijst wordt opgesteld en beheerd door een instantie die zorg draagt voor de registratie van dit gecontroleerde woordenboek (Pidcock, 2002). Een gecontroleerd woordenboek hoeft niet noodzakelijkerwijs enige betekenis te specificeren. Het kan ook alleen een set begrippen zijn die partijen overeenkomen om te gebruiken en waarvan de betekenis verondersteld wordt bekend te zijn bij alle partijen. Over het algemeen zal een term in een gecontroleerd woordenboek echter wel gedefinieerd zijn, maar zal de mate van detail van deze definities afhangen van de aard en omvang van de gegevensuitwisseling. De zorgdragende instantie dient te bewaken dat de definities van de begrippen in een gecontroleerd woordenboek ondubbelzinnig en niet-redundant zijn.

Taxonomie
Een taxonomie is een verzameling van gecontroleerde woordenboekbegrippen die georganiseerd zijn in een hiërarchische structuur (Reimer, 2001). Elke term in een taxonomie is betrokken in één of meer ouder-kind relatie(s) met andere begrippen van de taxonomie. Een taxonomie voegt additionele betekenis toe door middel van de betekenis van de hiërarchische relaties. In een traditionele taxonomie wordt vaak uitgegaan van een zogenaamde generalisatie/specialisatie relatie, waarbij een concept bezien wordt als een specialisatie of generalisatie van een ander concept. Tegen-

woordig wordt het woord 'taxonomie' ook gebruikt om te refereren naar andere soorten hiërarchieën met verschillende betekenissen van de relaties (Pidcock, 2002). Wanneer een taxonomie een variëteit aan omzichtig gedefinieerde betekenissen heeft opgesteld voor een hiërarchische relatie komt het overigens dicht in de buurt bij een ontologie.

Thesaurus
Een thesaurus is een verzameling van gecontroleerde woordenboekbegrippen, gerepresenteerd via een bepaalde netwerkstructuur. Dit betekent dat een thesaurus zowel hiërarchische, equivalente en associatieve relaties kan omvatten (Pidcock, 2002). De uitdrukkingskracht van de associatieve relaties in een thesaurus varieert sterk en hoeven niet noodzakelijkerwijs expliciete betekenis te hebben, anders dan dat twee begrippen gerelateerd zijn.

Ontologie
De term 'ontologie' wordt regelmatig gehanteerd om te refereren naar een gecontroleerd woordenboek, taxonomie, thesaurus of ontologie. Dit vloeit onder meer voort uit de definitie van een ontologie door Gruber (1993) die stelt dat een ontologie "*an explicit and formal specification of a conceptualization*" is. Op basis van deze generieke definitie is de verwarring eenvoudig te begrijpen. Indien we deze definitie in verschillende onderdelen opbreken, wordt het echter al duidelijker. In dit kader is een 'conceptualization' een abstract model van hoe mensen over bepaalde zaken in de wereld denken, waarbij deze zaken over het algemeen beperkt blijven tot een specifiek onderwerp. Een 'explicit specification' houdt in dat de concepten en relaties in het abstracte model expliciete namen en definities meekrijgen. De naam is een term en definities zijn een beschrijving van de betekenis van een concept of de relatie(s) en hoe deze zich verhouden tot anderen. Een 'formal specification' betekent dat het is uitgedrukt in een taal waarvan de formele eigenschappen goed begrepen worden. Het formaliseren is een belangrijke manier om ambiguïteit te verwijderen. Tenslotte betekent 'shared', dat een ontologie gebruikt dient te kunnen worden door verschillende applicaties en verschillende communities (Uschold, 2003).

Een ontologie kan zodoende worden gezien als een gecontroleerd woordenboek, uitgedrukt in een ontologie representatie taal. Deze taal heeft een grammatica om woordenboekbegrippen te gebruiken die iets betekenisvols uitdrukken (Pidcock, 2002). Hierbij legt de grammatica formele beperkingen op aan de wijze waarop de woordenboekbegrippen gezamenlijk gebruikt kunnen worden.

Het onderscheid tussen een gecontroleerd woordenboek, taxonomie, thesaurus of ontologie is in de praktijk niet altijd eenvoudig te maken en hangt daarnaast sterk af van de omstandigheden. Volgens Pidcock (2002) relateren taxonomieën en thesauri begrippen uit een gecontroleerd woordenboek aan elkaar door middel van hiërarchische, equivalente en associatieve relaties, maar bevatten ze geen expliciete grammatica regels hoe deze gecontroleerde woordenboek begrippen iets betekenisvols dienen uit te drukken. Een ontologie daarentegen doet dit juist wel.

De belangrijkste overeenkomsten tussen deze benaderingswijzen zijn volgens Pidcock (2002):

- Het zijn methodes die helpen om begrippen en bijbehorende relaties omtrent een bepaald onderwerp te structureren, classificeren, modelleren en representeren.
- Het zijn methodes die als doel hebben om een gemeenschap overeenstemming te laten bereiken over dezelfde terminologie en zich te committeren om deze terminologie op dezelfde wijze te hanteren.
- Er bestaat een set van begrippen die een gemeenschap besluit te gebruiken om aan deze begrippen en relaties te refereren.
- De betekenis van de terminologie is in enige mate en op enigerlei wijze gespecificeerd.

De belangrijkste verschillen tussen deze benaderingswijzen zit met name in aspecten als:

- Hoeveel betekenis kan worden gespecificeerd voor elk begrip.
- Welke notatiewijze of taal gehanteerd wordt om de betekenis te specificeren.
- Het doel waarvoor het gebruikt wordt, aangezien alle benaderingswijzen verschillende, maar overlappende gebruikswijzen kennen.

Voorbeeld van het onderscheid tussen benaderingswijzen
In een gecontroleerd woordenboek kan de term 'rosa majalis', of in het Nederlands de 'kaneelroos' voorkomen. In een taxonomie is te vinden dat de 'rosa majalis' behoort tot het geslacht 'rosa' en de familie 'rosaceae' en de uiteindelijke ouder het koninkrijk van planten is. Een thesauri vertelt dat 'rosa cinnamomea' een andere naam is voor dezelfde roos. De ontologie beschrijft in een bepaalde grammatica dat de kaneelroos van nature voorkomt in de bossen van Europa, in Nederland vooral voorkomt in de duinen, ongeveer twee meter groot kan worden, een donkerrode kleur heeft en gebruikt wordt bij de productie van rozenbottelsiroop.

In het kader van het elektronisch berichtenverkeer is het organiseren van de begrippen uit een gecontroleerd woordenboek van groot belang om een vorm van formele en expliciete semantiek te realiseren. We hanteren in dit kader de term 'taxonomie' omdat hier veelal sprake is van hiërarchische relaties en we ons willen richten op het organiseren van begrippen zonder dat hierbij een taal - of syntax - om de begrippen, in uit te drukken een rol speelt. We zijn van mening dat de beste syntax geen eisen zou moeten stellen aan de gekozen benaderingswijze voor het organiseren van de begrippen.

Het ontwikkelen van een conceptuele taxonomie is een activiteit waarbij men de informatiebehoeften van uitvragende partijen op een natuurgetrouwe wijze modelleert zonder dat men rekening houdt met de beperkingen die een syntax oplegt of die voortvloeien uit de wijze van implementatie. We kiezen hier bewust voor dit conceptueel juiste uitgangspunt, maar we realiseren ons dat dit in de praktijk niet altijd houdbaar zal zijn.

6.3.2 *Standaardisatie van syntax: de ontwikkeling van open standaarden*

In § 6.2 gaven we aan dat syntax zich richt op de vorm of structuur waarin gegevens worden uitgedrukt. De belangrijkste ontwikkelingen in dit kader hebben betrekking

op open standaarden voor de uitwisseling van gegevens. Volgens het IDABC (2004) worden standaarden als 'open' beschouwd wanneer zij:

- tot stand komen via een besluitvormingsprocedure die toegankelijk is voor alle belanghebbende partijen;
- door een organisatie zonder winstoogmerk worden beheerd;
- gepubliceerd zijn en vrijelijk opvraagbaar;
- vrij van royalty's zijn en er geen sprake is van beperkingen omtrent hergebruik.

Het gebruik van open standaarden kent veel voordelen, waaronder een ruime keuze aan ondersteunende software, een bredere afzetmarkt, en een lagere kans op 'vendor lock-in'.

De elektronische berichten zijn de containers van de uit te wisselen gegevens. Deze gegevens moeten op een gestructureerde manier worden beschreven en vastgelegd zodat ze onafhankelijk van interne gegevensformaten kunnen worden uitgewisseld. Hierbij zijn volgens Arendsen (2008) twee belangrijke standaarden te onderkennen voor het structureren van gegevens en berichten:

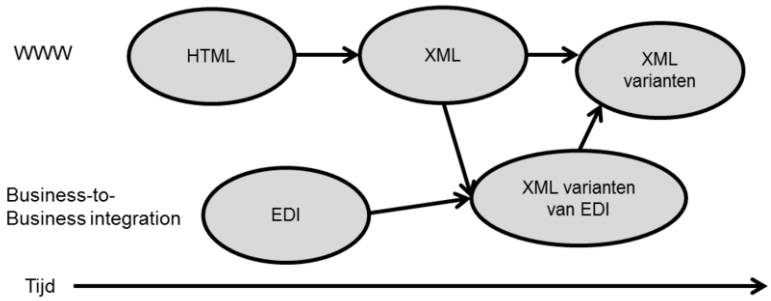
- EDIFACT, de afkorting van Electronic Data Interchange for Administration, Commerce and Transport, is een formele en voor machines leesbare taal, waarin een groot aantal elektronische berichten is gestandaardiseerd door het United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). De EDIFACT berichten zijn gebaseerd op internationale, genormaliseerde gegevenselementen en gebruiken een syntax die ontworpen is in de jaren tachtig om bestanden zo klein mogelijk te houden.
- XML, de afkorting van eXtensible Markup Language, is een standaard die eind jaren negentig ontwikkeld is door het World Wide Web Consortium (W3C) om gegevens op te slaan en te verzenden over het internet. Het is een opmaaktaal waarmee gestructureerde gegevens kunnen worden weergeven in de vorm van platte tekst. XML definieert een set van regels voor het coderen van documenten in een formaat dat zowel door mensen als machines gelezen kan worden.

Vanaf de jaren tachtig van de vorige eeuw worden geautomatiseerde informatiesystemen meer en meer ingezet ter ondersteuning van de (handels)relatie tussen organisaties. Het elektronisch berichtenverkeer werd in eerste instantie geïntroduceerd als instrument voor de optimalisatie van logistieke processen (Arendsen, 2008). Vaak werden in het kader van een klant-toeleverancier relatie de bestel- en voorraadprocessen op elektronische wijze met elkaar verbonden door middel van de EDIFACT standaard. Gelet op de relatief hoge complexiteit en kosten van de toenmalige technische infrastructuur was de introductie van deze vorm van Business-to-Business Integration (B2Bi) vooral voorbehouden aan grote organisaties (Hofman, 2003).

Het internet, en met name het World Wide Web (WWW), hebben geleid tot nieuwe standaarden ten behoeve van het onderscheiden van de presentatie en structurering van gegevens, zoals de opmaaktalen HTML en XML. Als gevolg van de opkomst van het internet rond het jaar 2000 is XML de meest gebruikte syntax geworden voor

berichtenverkeer. Dit heeft ook gevolgen gehad voor EDIFACT. De inhoudelijke, ook wel semantische, standaardisatie is nog steeds van toepassing, maar veel software applicaties hadden moeite met de syntax. Hierdoor is XML/EDIFACT tot stand gekomen, die het woordenboek en de grammatica van EDIFACT combineert met de syntax van XML.

De ontwikkeling van deze open standaarden is gevisualiseerd in de onderstaande figuur.



Figuur 6.3 – De ontwikkeling van open standaarden voor elektronisch berichtenverkeer (OSOSS, 2005)

De opkomst van XML heeft geleid tot het ontstaan van vele gecontroleerde woordenboeken en standaardberichten die hierop gebaseerd zijn. Er bestaan verschillende (inter)nationale standaarden die zich elk op een specifiek terrein richten. Zo zijn er standaarden die een specifiek proces ondersteunen, zoals Universal Business Language (UBL) dat gestandaardiseerde elektronische documenten bevat voor het inkoopproces, transportproces en verkoopproces. Andere standaarden richten zich juist op een specifieke bedrijfstak, zoals het Assurantie Data Netwerk (ADN).

De keuze voor (internationale) open standaarden is voor de hand liggend vanwege de brede ondersteuning in software, wijdverbreide kennis en vrije beschikbaarheid (geen licentiekosten). Bij de toepassing van internationale standaarden wordt er veelal een lokaal (Nederlands) profiel gemaakt dat is toegesneden op de eigen wet- en regelgeving.

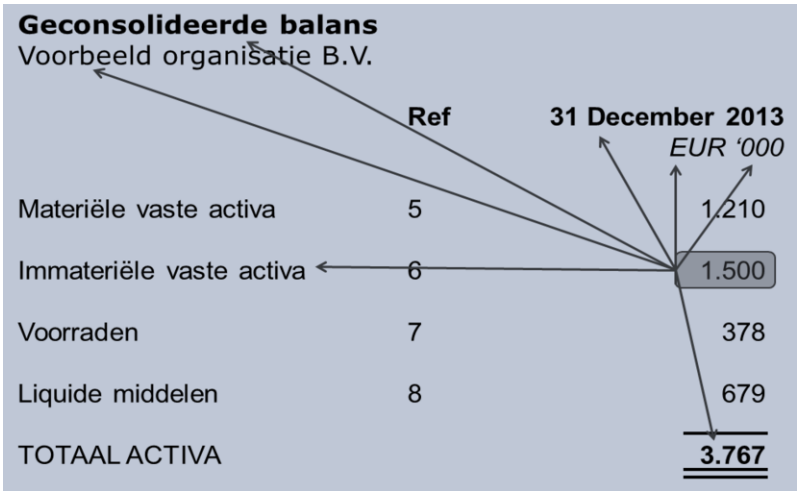
De grote hoeveelheid mogelijkheden maakt de keuze voor de juiste standaarden complex. Het terrein van de semantiek en van de gewenste (op XML gebaseerde) syntax is van groot belang bij de keuze van de standaarden. Elke standaard kent zijn eigen community en implementatiegraad, die op zijn beurt de verkrijgbaarheid van geautomatiseerde oplossingen bepaalt. Beleidsmakers dienen hun keuze voor specifieke gegevensstromen te baseren op de behoeften van de uitvragende partijen en de beschikbaarheid en ondersteuning van een geschikte (open) standaard met typerende eigenschappen die aansluiten bij hun domein.

6.3.3 *XBRL – standaardisatie van syntax én semantiek*

6.3.3.1 Achtergrond

XBRL – eXtensible Business Reporting Language – is een open standaard voor het definiëren van gestructureerde gegevens in de vorm van platte tekst. Deze standaard maakt gebruik van de XML syntax. Gegevens die zijn vastgelegd in de XML syntax zijn leesbaar voor zowel mens als machine. XML is geschikt om gegevens in op te slaan en om gegevens via het internet te verzenden. XBRL is een mix van XML technieken als XML Schema, XLink, XPointer en een aantal eigen zaken. XBRL brengt de publicatie, uitwisseling en verwerking van verantwoordingsinformatie binnen de dynamische en interactieve wereld van het internet. XBRL is ontwikkeld door XBRL International, een non-profit consortium van meer dan 400 organisaties. Het is een open standaard, wat betekent dat iedere onderneming of softwareleverancier de standaard kosteloos mag inbouwen en gebruiken. Dit gebeurt met behulp van een taxonomie, een container voor begrippen en hiërarchische relaties. Wanneer de gevraagde gegevens in gestructureerde vorm beschikbaar zijn en er een mapping met de taxonomie is, kan een organisatie de verantwoording geautomatiseerd genereren op basis van de taxonomie.

De werking van XBRL is het eenvoudigst te doorgronden aan de hand van een voorbeeld. Stel je voor dat het mogelijk is om van een pagina van een jaarrekening alle getallen af te schudden. Die losse getallen liggen op de grond en zijn dan volstrekt zonder betekenis: had die 1.500 nu betrekking op omzet of salariskosten? Bij welk boekjaar hoort het getal? Zijn het dollars of euro's? En stond er een voetnoot bij? Volgens welke waarderingsgrondslag is het getal bepaald? Het gebruik van XBRL voegt dergelijke contextuele gegevens toe aan het getal. Op papier is dit slechts impliciet aanwezig, maar XBRL maakt dit expliciet. Dit blijkt onder meer uit het onderstaande voorbeeld, waarin de geïmpliceerde informatie zichtbaar is die hoort bij het gegevensfeit '1.500'.



Figuur 6.4 –Voorbeeld van meta informatie

Het expliciteren van contextuele gegevens zorgt ervoor dat het getal betekenis krijgt, onafhankelijk van de verantwoording of de omgeving waarin het wordt gebruikt. Het toevoegen van die context zorgt ervoor dat de gegevens ook in andere systemen of door andere gebruikers op de juiste wijze kunnen worden geïnterpreteerd.

Voor de uitwisseling van gegevens uit een verantwoordingsrapportage is het van belang dat de gegevensfeiten worden getagged en middels deze tags verwijzen naar een unieke definitie. Het bestand met de gegevensfeiten heet een XBRL instance document (zie 6.3.3.3) en de set van documenten waarin de definities opgenomen zijn, is een taxonomie. Het instance document en de taxonomie zijn onlosmakelijk met elkaar verbonden, zodat de gegevens onafhankelijk van welk systeem dan ook kunnen worden ingelezen, eenduidig geïnterpreteerd en gepresenteerd (Engel et al, 2003).

6.3.3.2 Taxonomie

Taxonomieën vormen een essentieel onderdeel van de XBRL standaard. Een XBRL taxonomie is de plaats waar de begrippen worden gedefinieerd. In de taxonomie ligt vast welk soort informatie de verantwoordende partij in het instance document dient in te vullen. Bijvoorbeeld of dit een getal of een tekst dient te zijn. Een taxonomie is een elektronisch document dat een 'verklarende lijst' van begrippen bevat met hun onderlinge samenhang. Een softwareprogramma dat is voorbereid op XBRL kan op basis van de taxonomie bijvoorbeeld 'weten' wat de betekenis van 'afschrijvingen' of 'EBITDA' is, maar ook dat 'EBITDA' minus afschrijvingen en waardeverminderingen gelijk is aan 'EBIT'. Een taxonomie zorgt ervoor dat verschillende gebruikers de gegevens eenduidig interpreteren.

Een taxonomie bestaat uit één of meer schema files en linkbases. Een schema file is een .xsd bestand waarin elementen worden beschreven. Een linkbase koppelt elementen aan elkaar. Er zijn twee typen linkbases te onderkennen, namelijk voor resources en voor relaties. Een voorbeeld van een resource linkbase is de reference linkbase, waarin een resource (de referentie naar wet- en regelgeving) wordt gekoppeld aan een specifiek begrip. De linkbases die gehanteerd worden voor relaties kunnen feitelijk drie doelen dienen: het valideren van informatie, het meegeven van aanvullende semantische informatie of het presenteren van informatie. Het valideren van informatie is belangrijk om de kwaliteit van de informatie te waarborgen. Hierbij kan gedacht worden aan juiste optellingen of vermenigvuldigingen. Het meegeven van aanvullende semantische informatie kan relevant zijn om rapporteurs voldoende inzicht te geven in de aard van het begrip. Het presenteren van informatie is voor techneuten van secundair belang, maar voor veel gebruikers wel belangrijk. Hiervoor kan aan de taxonomie een opzet voor de presentatie meegegeven worden met behulp van een linkbase.

6.3.3.3 Instance document

Het instance document bevat de gegevensfeiten die gecommuniceerd worden. Deze feiten zien er in het instance document uit als een lijst van 'XBRL tags' die elk een bepaalde waarde hebben. Deze 'tags' verwijzen naar specifieke begrippen in de taxonomie. Door middel van deze tags legt het instance document de koppeling tussen het te rapporteren begrip en de hierbij behorende waarde. Hierbij dient de rappor-

teur aanvullende informatie toe te voegen, zoals de periode waarop het van toepassing is. In een XBRL instance document dient dit in de context sectie te worden vastgelegd. Hieronder een voorbeeld:

```
<nl-cd:EndDateForFinancialPeriod contextRef="FY13d">2013-12-31</nl-cd:EndDateForFinancialPeriod>
```

De waarde is de datum '31 december 2013', de XBRL tag verwijst naar het begrip 'einddatum van de financiële periode', de context verwijst naar het gehele jaar 2012 dat elders in het instance document wordt omschreven.

Een organisatie kan het instance document ook zelf op haar website zetten, zodat analisten, toezichthouders, accountants en andere partijen naar wens hun eigen verantwoordingsrapportage kunnen opdelen in de onderdelen die voor hen relevant zijn. In theorie maakt XBRL het mogelijk een digitaal rapport te creëren, waarvan de inhoud op maat in elke gewenste presentatievorm kan worden gegoten, desgewenst ook informatie van meerdere informatieverschaffers tegelijk. Het is deze flexibiliteit die XBRL zo krachtig maakt, en die onderscheidend is ten opzichte van andere standaarden voor de uitwisseling van informatie. Wanneer een organisatie het instance document op haar website zet, kunnen analisten, toezichthouders, accountants en andere partijen naar wens de gegevens gebruiken zonder vooraf een handmatige bewerking uit te voeren om de gegevens in te lezen en te vertalen naar hun eigen informatiestandaarden.

6.3.3.4 Linkbases

Een linkbase is een .xml bestand waarin links tussen elementen zijn vastgelegd. In een XBRL taxonomie is het niet voldoende om uitsluitend de begrippen vast te leggen, maar dienen deze begrippen ook nog te worden gerelateerd aan andere begrippen binnen de taxonomie en aan voorschriften en beschrijvingen die buiten de taxonomie zijn vastgelegd. Deze relaties worden links genoemd en links van eenzelfde soort zijn gegroepeerd in een zogenoemde linkbase. De achterliggende techniek van XBRL is XML en onderdeel daarvan is de XML Linking Language of XLink. Deze biedt de mogelijkheid om verbanden te definiëren; niet alleen 1-op-1 relaties maar ook complexe meervoudige relaties. De mogelijkheden van XLink worden in XBRL geheel benut, waardoor ook multi-dimensionele gegevensmodellen in een taxonomie kunnen worden vastgelegd.

In het XBRL jargon wordt het begrip linkbase vaak gebruikt. Een linkbase is niet veel meer dan een verzameling links van een bepaalde soort. Als men spreekt over het gebruik van een linkbase, bedoelt men dus het toepassen van een bepaald soort link.

De kenmerken van de verschillende linkbases, en daarmee de soorten links, zijn samengevat in de onderstaande tabel.

Tabel 6.1 – Overzicht van linkbases in XBRL

Linkbase	Doel
Label	Een label linkbase bevat labels met de tekst die in een rapportage aan de lezer getoond moet worden om een begrip voor mensen begrijpelijk en interpreteerbaar te maken.
Reference	Een reference linkbase associeert begrippen met de bron van de uitvraag, zoals wet- en regelgeving.
Definition	Een definition linkbase wordt voornamelijk gebruikt om (multi) dimensionale relaties weer te geven. Het beschrijft de relaties tussen de tabellen (hypercubes), assen (dimensies), domeinen en domeinleden. Naast het weergeven van de (multi) dimensionale relaties beschrijft de definition linkbase ook alle overige relaties die nodig zijn om een element te definiëren.
Presentation	Een presentation linkbase bepaalt de hiërarchische relatie tussen begrippen ten behoeve van de presentatie van de gegevens.
Calculation	Een calculation linkbase geeft aan welke begrippen bij elkaar opgeteld of van elkaar afgetrokken dienen te worden ter controle van de juistheid van de gegevensfeiten.
Formula	Een formula linkbase maakt het mogelijk om meer complexe berekeningen te definiëren. Het beschrijft de validatieregels die op de gegevensfeiten in het instance document worden toegepast.

6.3.3.5 Voordelen van XBRL gebruik in informatieketens

Er zijn legio boeken en artikelen te vinden waarin de voordelen van XBRL worden benoemd. We kunnen de voordelen onderverdelen in drie clusters: (1) kostenreductie, (2) transparantie en (3) kwaliteit en snelheid. We lichten deze clusters hieronder toe.

We beginnen met kostenreductie. Een groot deel van de kosten van IT zit niet in de systemen zelf, maar in de interfaces tussen verschillende systemen. Systemen en toepassingen kunnen vaak niet of onvoldoende met elkaar communiceren zonder een investering in een nieuwe module of het uitvoeren van inefficiënte extra handelingen. XBRL kan daarin verbetering brengen door het harmoniseren van informatiestromen; XBRL maakt een koppeling van verschillende systemen mogelijk zonder dat maatwerk interfaces nodig zijn (Bergeron, 2003).

Naast kostenreductie verhoogt XBRL de transparantie van rapportages. Een onderneming die bijvoorbeeld volgens de IFRS-taxonomie rapporteert, verhoogt met XBRL de transparantie en vergelijkbaarheid, want er is theoretisch geen twijfel meer mogelijk over de interpretatie van cijfers. Rapportages zijn direct, eenduidig en digitaal met elkaar te vergelijken (Bonsón, Cortijo, & Escobar, 2009). Aan de ontvangende kant van de informatie – analisten, toezichthouders, overheidsinstanties – is die uniformiteit van gegevens een belangrijk voordeel. Daardoor ontstaat immers een betere vergelijkbaarheid van informatie. Ook vervallen handmatige handelingen voor het verwerken van gegevens in eigen systemen.

Tenslotte biedt XBRL gebruikers toegang tot gegevens van hogere kwaliteit die bovendien sneller beschikbaar zijn. Dat geeft zowel intern als extern kansen om beter gebruik te maken van die informatie:

- Door het analyseren van gegevens op basis van vastgestelde business rules kan de interne beheersing van processen verbeteren. Bijvoorbeeld door bepaalde afwijkingen in grootboekmutaties direct te signaleren aan de verantwoordelijken.
- Externe partijen kunnen het monitoren van gegevens verder automatiseren. Zo kan een bank die een onderneming een lening verstrekt signalen inbouwen in de eigen systemen wanneer solvabiliteitscriteria worden overschreden. Een analist kan de ontvangen XBRL-gegevens direct toepassen in de gewenste modellen zonder inefficiënte handelingen.
- Ook op het gebied van risk management zijn er verbeteringen mogelijk. Deze belangrijke activiteit vindt bij veel ondernemingen nu nog plaats op ad-hoc basis en/of middels een arbeidsintensieve verzameling van gegevens. XBRL maakt het mogelijk dit proces te professionaliseren en kan worden gebruikt om real-time signalen over risk management te verzorgen aan het management.

De voordelen van XBRL komen pas tot uiting als er een gemeenschap van partijen ontstaat die XBRL omarmt: toezichthouders, overheidsinstanties, bedrijven, analisten enzovoort. Hoe meer partijen meedoen, hoe groter de voordelen van een naadloze informatie-uitwisseling worden. De analogie met andere communicatiemiddelen ligt hier voor de hand: zowel voor telefoon, fax als e-mail geldt, dat de werkelijke voordelen ervan pas echt duidelijk werden bij een breed publiek toen er eenmaal een grote gemeenschap gebruikers was ontstaan.

6.3.3.6 Risico's die aan het gebruik van XBRL kleven

Uit de voorgaande paragraaf kunnen we concluderen dat het gebruik van XBRL diverse voordelen met zich meebrengt. Er bestaan echter ook risico's, voor alle betrokken partijen. In algemene zin moeten zowel verzenders als ontvangers van XBRL-informatie tijdig inspelen op de kansen van XBRL, en de technologie op een beheerste manier toepassen om de voordelen te realiseren. Hieronder beschrijven we een aantal van deze risico's.

- *'Garbage in is garbage out'*: de term XBRL roept bij velen associaties op met een hogere kwaliteit van gegevens. Dit klopt ook, maar hier is alleen sprake van als de onderliggende informatiesystemen betrouwbaar zijn, als er voldoende checks and balances zijn ingebouwd, en de betrokken medewerkers met kennis van zaken handelen. In die zin hoeft XBRL dus niet altijd te betekenen dat gegevens beter zijn.
- Fouten in de taxonomie of de vulling van deze taxonomie kunnen leiden tot onjuiste interpretatie van gegevens.
- Ondeugdelijke readers kunnen leiden tot onjuiste interpretatie van gegevens; een onjuiste 'mapping' van het grootboek kan leiden tot een onjuist instance document en daarmee tot onjuiste interpretatie van gegevens.
- 'Dialecten' in het gebruik van XBRL per land, branche of organisatie kunnen leiden tot onjuiste interpretatie van gegevens. Deze 'gekleurde' taxonomieën brengen de uniformiteit in gevaar.
- Omdat het verzenden van gegevens met XBRL minder tastbaar plaatsvindt, bestaat ook de kans dat een instance document meer informatiemogelijkheden biedt dan de verzender beseft. De gebruiker van dit document heeft de

ultieme en gebruiksvriendelijke vrijheid om deze gegevens naar eigen inzicht te rubriceren en presenteren. Mogelijkerwijs ontstaan daardoor invalshoeken die de verzender van de gegevens zich niet realiseert, ook omdat bepaalde dimensies van de gegevens worden meegezonden zonder dat men zich daarvan bewust is.

Een onjuiste interpretatie van gegevens kan grote gevolgen hebben nu XBRL het mogelijk maakt om bepaalde bedrijfsmatige beslissingen te automatiseren. Zo kan een bank die de kredietverlening monitort op basis van XBRL-gegevens in de problemen komen als blijkt dat zij deze gegevens op de verkeerde wijze interpreteert. De invoering van XBRL brengt een aantal risico's met zich mee. De meeste daarvan zijn niet nieuw, maar verdienen wel extra aandacht.

6.4 Invulling in het kader van SBR

Het derde deel van dit hoofdstuk beschrijft de manier waarop het SBR Programma invulling geeft aan gegevensuitwisseling en -verwerking in ketens. Gezien de reikwijdte van het SBR Programma is dit deel omvangrijker dan de voorgaande twee delen waarin de behoeften en ontwikkelingen op hoofdlijnen zijn beschreven. We behandelen de volgende thema's:

- Een korte reflectie op het gebruik van XBRL taxonomieën binnen het SBR Programma (voor een meer volledige beschrijving van de historie van SBR verwijzen we de lezer naar de beschrijving in bijlage A).
- Specifieke eisen aan SBR taxonomieën, waaronder organisatorische eisen als het voldoen aan de Nederlandse Taxonomie Architectuur (NTA).
- Het taxonomie-ontwikkelproces dat bij de NT wordt toegepast. Dit proces wordt aan de hand van verschillende fasen ontleed. De lezer krijgt een indruk van de stappen vanaf de requirementsanalyse tot en met de publicatiefase.
- Relevante ontwikkelingen op het gebied van XBRL die – onder andere voor SBR – nieuwe kansen bieden.

6.4.1 *Achtergrond van het gebruik van XBRL taxonomieën in Nederland als onderdeel van het SBR Programma*

Aan het begin van de 21e eeuw heeft de Nederlandse overheid de voorloper van het SBR Programma opgestart, het Nederlandse Taxonomie Project, met als doel om een gedeelde XBRL-taxonomie ten behoeve van verschillende verantwoordingsdomeinen toe te passen. De basisgedachte achter het project was dat er efficiëntie-voordelen zijn te behalen door standaardisatie van gegevens (semantiek en syntax, bepaald door de keuze voor een communicatiestandaard). Hierbij dienen gegevens zoveel als mogelijk hergebruikt worden.

De doelstelling van het SBR Programma is om een generieke overheidsoplossing voor system-to-system (S2S) uitwisseling te realiseren en gedeelde verwerking van verantwoordingsinformatie in te richten. De genoemde XBRL-taxonomie, een woordenboek van geharmoniseerde gegevens dat middels een vaste syntax door alle organisaties voor verantwoording naar de overheid gebruikt kan worden, is een van de

bouwblokken van de SBR oplossing. Met de taxonomie kunnen organisaties verantwoordingen sneller en eenvoudiger samenstellen en dit beter integreren in de processen van administratie en S2S-aanlevering van verantwoordingsinformatie aan de overheid.

Het interessante aspect is, dat de opkomst van de syntax XBRL de primaire aanleiding was om het SBR Programma op te starten. XBRL maakt het mogelijk om de gewenste semantische standaardisatie te realiseren, zodat het mogelijk is om eenduidig gegevens te definiëren. Daarnaast gaat het hier om een open standaard, waardoor er geen afhankelijkheid gecreëerd wordt van slechts één of enkele leveranciers. De mogelijkheden die semantische standaardisatie met zich meebrengt werden hierdoor duidelijker voor veel partijen. Eerder in dit hoofdstuk stelden we dat het conceptueel beter is wanneer de keuze voor de syntax gemaakt wordt nadat de semantische standaardisatie heeft plaatsgevonden. Dit omdat wij van mening zijn dat de beste syntax geen eisen stelt aan de wijze waarop gegevens zijn gemodelleerd. Bij XBRL is dit door de wijze waarop de specificatie is opgesteld echter wel het geval. Het SBR Programma heeft eerst de keuze voor de syntax gemaakt, voordat de gewenste semantische standaardisatie gerealiseerd was. De keuze om dit andersom te doen ten opzichte van de conceptueel juiste methode, heeft ertoe geleid dat met name de inter-domein semantische standaardisatie en normalisatie veel vertraging heeft opgelopen.

De invoering van XBRL in Nederland illustreert ook de werking van de wet van de remmende voorsprong. Toen in 2006 de eerste versie van de Nederlandse Taxonomie werd uitgebracht, was Nederland één van de voorlopers van het gebruik van XBRL in het proces van verantwoording. XBRL als techniek was op dat moment ook sterk in ontwikkeling, wat onder meer blijkt uit publicatie van XBRL specificaties zoals Dimensions 1.0. In Nederland werd op dat moment besloten om voorlopig geen nieuwe specificaties toe te passen omdat de kennis van en ervaring met deze nieuwe technieken beperkt was. Dit leidde echter tot de situatie dat in de daarop volgende jaren geen nieuwe XBRL specificaties geadopteerd werden, ondanks het feit dat hier wel voldoende voordelen uit te behalen waren. In de tussenliggende jaren ontstonden internationaal echter meer projecten en programma's die de nieuwste specificaties van XBRL wel toepasten waardoor de Nederlandse werkwijze technologisch achterhaald begon te raken. Het duurde uiteindelijk tot versie 6.0, uitgebracht in 2011, voordat de Nederlandse Taxonomie gebruik ging maken van de nieuwere specificaties en weer op vergelijkbaar technisch niveau kwam met internationale taxonomieën als IFRS en US-GAAP. De les die hieruit kan worden getrokken is, dat het van belang is om mee te gaan met nieuwe ontwikkelingen wanneer dit functioneel gezien opportuun is.

De Nederlandse opzet van het SBR Programma wordt ook gekenmerkt door de inspraak die marktpartijen hebben in het totstandkomingsproces van de Nederlandse Taxonomie. Vanaf het begin is het SBR Programma een publiek-private samenwerking geweest, die onder meer gericht is op het bevorderen van de acceptatie en adoptie van de Nederlandse Taxonomie door marktpartijen. Andere landen in vergelijkbare situaties hebben veelal ervoor gekozen om geen publiek-private samenwerkingsverbanden op te zetten, maar het simpelweg in te voeren als een verplichting.

Dit zorgt in ieder geval voor duidelijkheid. In Nederland had het SBR Programma geen keuze omdat het verplichtstellen van een volstrekt nieuwe wijze van verantwoorden niet past in ons 'poldermodel'. De gevolgen van de vrijblijvendheid zijn de afgelopen jaren ook zichtbaar geworden door de beperkte hoeveelheid ontvangen berichten. Uiteindelijk is gebleken dat een verplichtstelling of het bieden van specifieke (financiële) incentives voor die partijen die de investering moeten doen, de enige methode is om een succesvol SBR traject te realiseren.

6.4.2 *Specifieke eisen aan SBR taxonomieën*

Een SBR taxonomie kan worden geclassificeerd als een taxonomie die voldoet aan de spelregels die het SBR Programma heeft gesteld. In principe kan elke partij door middel van het standaardiseren van semantiek en syntax een effectiever en efficiënter uitwisselingsproces van informatie realiseren. De doelstellingen achter deze standaardisatie inspanningen zullen echter per situatie verschillen en dit geldt ook voor de wijze van implementatie. Het streven van de overheid bij SBR is dat verantwoording efficiënter en effectiever verloopt. Om te verzekeren dat alle partijen die zich bij SBR willen aansluiten zich ook conformeren aan deze doelstelling, wordt het aantal vrijheidsgraden ingeperkt. Hierdoor worden wezenlijk verschillende wijzen van implementatie zoveel als mogelijk vermeden, zodat hergebruik binnen een informatieketen mogelijk wordt. Om deze beperking te realiseren is een aantal belangrijke eisen opgesteld waaraan moet zijn voldaan voordat een SBR taxonomie als zodanig geclassificeerd mag worden.

Deze spelregels zijn te verdelen in internationale regels en nationale regels. De internationale regels zijn van toepassing op projecten in het buitenland die de term Standard Business Reporting gebruiken. Een voorbeeld hiervan is Australië, alwaar SBR al is uitgerold. Internationaal bezien zijn er twee belangrijke eisen om als SBR project te worden geclassificeerd:

- Een SBR taxonomie gebruikt één of meer gecontroleerde woordenboeken met begrippen van samenwerkende (overheids)organisaties ten behoeve van de uitwisseling en verwerking van gegevens binnen een informatieketen.
- Een SBR taxonomie gebruikt binnen een informatieketen dezelfde syntax. Voor de (financiële) verantwoordingsketen is XBRL de gehanteerde syntax.

Daarnaast zouden in Nederland de volgende, meer organisatorische, eisen aan gegevensstandaardisatie projecten kunnen worden gesteld voor een classificatie als 'SBR':

- Een SBR taxonomie wordt gecreëerd onder verantwoordelijkheid van de betreffende uitvragende partij.
- Een SBR taxonomie is een onderdeel van de Nederlandse Taxonomie (NT), voor zover de uitvragende partij een overheidsorganisatie is.
- Een SBR taxonomie voldoet aan de eisen die gesteld zijn in de Nederlandse Taxonomie Architectuur (NTA).

Bovenstaande onderwerpen worden in de onderstaande paragrafen nader uiteengezet.

6.4.3 *Verantwoordelijkheid van de uitvragende partij*

Een SBR taxonomie wordt opgesteld onder verantwoordelijkheid van de uitvragende partij in de betreffende keten. Zo is in het belastingendomein logischerwijs de Belastingdienst de uitvragende partij. In theorie kan de creatie van een XBRL taxonomie op twee manieren plaatsvinden: centraal of decentraal. Bij de centrale variant is landelijk één organisatie verantwoordelijk voor de creatie van de verschillende domeinen van een taxonomie. Bij de decentrale variant is elk domein zelf verantwoordelijk voor de creatie van een (deel)taxonomie. Het lijkt dat vanuit een beheer perspectief de centrale variant eenvoudiger is, maar de vraag is wat eenvoudiger is: (1) de domeinspecialisten XBRL en NTA leren of (2) de centrale beheerder domeinkennis bijbrengen. Zodoende is binnen SBR gekozen voor de decentrale opzet. Hierbij is een uitvragende partij zelf verantwoordelijk voor de creatie van een deeltaxonomie. Daarnaast vervult het SBR Programma wel een beperkte centrale rol door het creëren van een gezamenlijke deeltaxonomie met gemeenschappelijke elementen, het samenvoegen van de verschillende deeltaxonomieën tot de Nederlandse Taxonomie en het toetsen aan de NTA.

De keuze van SBR voor dit decentrale model vindt zijn oorsprong in de opstartfase van het SBR project. Als initiatiefnemers van SBR zijn de Belastingdienst en het CBS van mening dat de deeltaxonomieën voor het belastingen- en statistiekdomein de producten zijn van de Belastingdienst respectievelijk het CBS. Zij nemen ook de volle verantwoordelijkheid voor de producten en zodoende willen zij de zeggenschap hierover volledig in eigen beheer houden. Het opstellen van de taxonomie voor het belastingendomein door een centrale organisatie is daarom onbespreekbaar.

De door SBR gekozen variant heeft als voordeel dat een uitvragende partij vaak het beste in staat is om de vereiste informatie vorm te geven door middel van een taxonomie. Het nadeel is dat door de betrokkenheid van diverse uitvragende partijen en het SBR Programma met name de inter-domein standaardisatie en normalisatie veel lastiger is geworden. In dit kader zijn er vele honderden architectuurregels om een consistente opzet van de verschillende domeinen te hebben. Deze architectuurregels moeten er in beide varianten zijn. Ook als de NT door één partij gemaakt wordt, moeten de gehanteerde regels gecodificeerd worden. Anders weet een leverancier of een ‘extender’ of een software-ontwikkelaar niet wat er zou moeten gebeuren, en is er dus geen sprake van een beheerste NT. Voor beide varianten dienen al deze partijen hun begrippen in detail omschreven te hebben om te kunnen bepalen in hoeverre zij overeenkomen in semantische zin. Daarnaast dienen zij door middel van techniek ervoor te zorgen dat ook daadwerkelijk dezelfde begrippen worden gehanteerd. Wanneer dit in één hand ligt is dit een stuk eenvoudiger te realiseren dan wanneer dit door diverse partijen op diverse locaties op diverse tijdstippen plaatsvindt.

6.4.4 *Onderdeel van de Nederlandse Taxonomie*

In Nederland heeft het SBR Programma in samenwerking met een aantal uitvragende partijen de Nederlandse Taxonomie (NT) gerealiseerd voor informatie-uitwisseling en -verwerking in de financiële verantwoordingsketen. De NT omvat op dit moment drie verschillende verantwoordingsdomeinen: belastingen, jaarverslagge-

ving en statistiek. Tussen deze domeinen bestaan niet alleen verschillen in de definities van gehanteerde begrippen, maar ook in de wijze waarop begrippen worden gedefinieerd en bekend worden gemaakt bij de verantwoordende partijen. Het doel van de NT is om op basis van de vigerende wet- en regelgeving het begrippenkader eenduidig vast te leggen. Het normaliseren van het begrippenkader is hierbij een continu proces, omdat er een jaarlijkse cyclus is waarbij aanpassingen in de begrippen plaatsvinden.

Deze aanpassingen zijn nodig omdat rapportages, stromen of domeinen worden toegevoegd, gewijzigd of verwijderd uit de NT. Rapportages moeten worden aangepast wanneer de wijzigingen in wet- en regelgeving dit noodzakelijk maken. Daarnaast kunnen ook nieuwe rapportages of stromen worden toegevoegd aan SBR als gevolg van verdere verbreding binnen bestaande domeinen. Verdere verbreding is uiteraard ook mogelijk wanneer nieuwe domeinen worden toegevoegd aan SBR.

Als gevolg van wijzigingen in wet- en regelgeving publiceert het SBR Programma elk jaar minimaal één nieuwe versie van de NT. Dit betekent overigens niet dat er ook elk jaar majoure aanpassingen noodzakelijk zijn in de administratieve processen en de onderliggende informatiesystemen. Een goede implementatie van XBRL door softwareleveranciers betekent dat alleen de mappingtabel tussen de taxonomie en de databases moet worden aangepast om de wijzigingen te faciliteren. De wijze van mappen is cruciaal om meer efficiëntie en effectiviteit bij de verantwoordende partij te realiseren.

6.4.5 *Voldoen aan de Nederlandse Taxonomie Architectuur*

De architectuur bepaalt welke onderdelen van de XBRL standaard op welke wijze in de betreffende taxonomie worden toegepast. Op hoofdlijnen heeft XBRL International een syntax gedefinieerd waarmee diverse taxonomie architecturen gemaakt kunnen worden. Een werkgroep van XBRL International heeft in 2005 een set van afspraken (best practices) gebundeld in de Financial Reporting Taxonomy Architecture (FRTA). De FRTA bevat een groot aantal min of meer vanzelfsprekende regels. Zo bevat het de richtlijn dat elk concept een standaard label moet hebben dat uniek is, dat een beschrijving begrijpelijk moet zijn en dat een element maar één keer mag voorkomen. Een concept is de term die XBRL gebruikt om een begrip aan te duiden waarvoor een waarde gerapporteerd kan worden. De meeste XBRL tools hebben de functionaliteit ingebouwd om te valideren of de taxonomie in overeenstemming is met hetgeen bepaald is in de FRTA.

Als gevolg van de doorontwikkeling van de XBRL standaard is dit document echter dermate verouderd dat grote projecten er niet langer op kunnen vertrouwen. Deze situatie, tezamen met de vele mogelijkheden die de XBRL specificatie biedt, zorgt voor de noodzaak om op lokaal niveau de architectuur van een taxonomie verder uit te werken. Binnen het SBR Programma is in overleg met de uitvragende partijen hiervoor de Nederlandse Taxonomie Architectuur (NTA) opgesteld.

De opzet van de NT is gebaseerd op de NTA. De NTA bepaald voor de gehele NT welke onderdelen van de XBRL standaard op welke wijze in de Nederlandse situatie

worden toegepast. De NTA beperkt de vrijheidsgraden van de verschillende uitvragende partijen bij het opstellen van hun deeltaxonomie waardoor deze beter op elkaar worden afgestemd.

De opzet van de NTA is gebaseerd op de gezamenlijke uitgangspunten van de uitvragende partijen bij de constructie van een SBR taxonomie. Deze bouwprincipes zijn hieronder weergegeven:

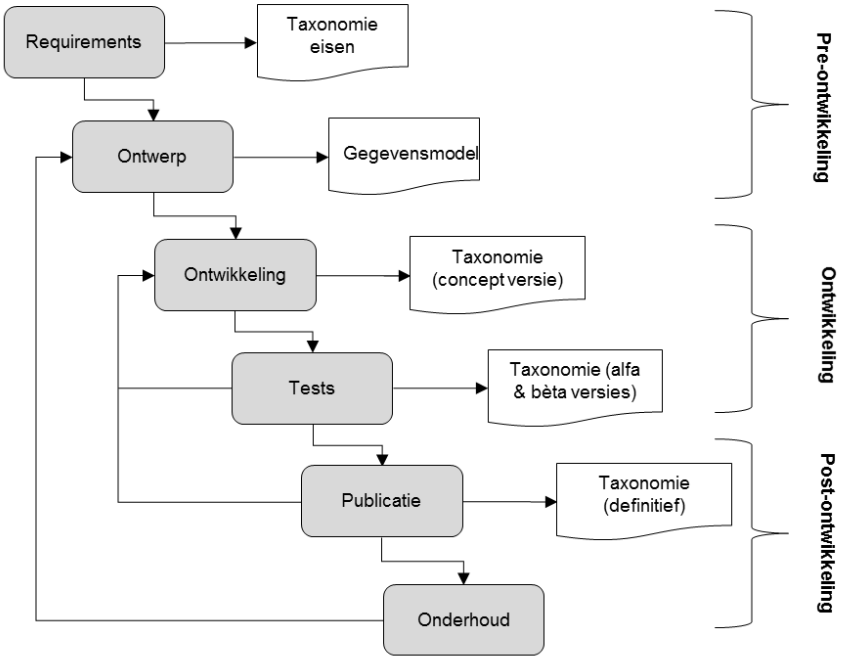
- Eenvoud van het verantwoordingsproces.
    - De architectuur moet zich richten op een zo eenvoudig mogelijke mapping en instance document creatie.
    - De architectuur ondersteunt het SBR uitgangspunt om optimaal hergebruik van gegevens te realiseren.
- Stabiliteit.
    - De architectuur ondersteunt dat wijzigingen in wet- en regelgeving een minimale impact hebben op de informatie leverende systemen (bronnen).
- Consistentie.
    - Het architectuurkader moet consistent zijn en de daarop gebaseerde taxonomie(extensies) moet vallen binnen deze opgestelde kaders (coherent en expliciet).
- Compliance met specificaties, best practices en verwante taxonomieën.
    - De architectuur moet zo min mogelijk afwijken van datgene wat in andere projecten succesvol is toegepast.
- Onderhoudbaarheid.
    - De architectuur schept een basis voor eenvoudig onderhoud door haar eigenaren.
- Prestaties.
    - De toepassing van de architectuur moet resulteren in andere technische voordelen, bijvoorbeeld zo klein mogelijke instance documenten en optimale prestaties bij de verwerking daarvan.

Bovenstaande principes zijn leidend in de stappen van het taxonomie ontwikkelproces. Deze stappen worden in de volgende paragraaf uiteen gezet.

6.4.6 *Het taxonomie-ontwikkelproces*

De activiteiten die in het kader van de ontwikkeling van een SBR taxonomie verricht worden volgen een specifiek ontwikkelproces. Dit proces kan in principe toegepast worden voor elke willekeurige XBRL taxonomie, maar wordt in dit hoofdstuk vanuit het perspectief van de ontwikkeling van een SBR taxonomie uiteengezet. Volgens Piechocki en Felden (2007) is het ontwikkelproces van een XBRL taxonomie door zijn aard niet gelijk aan de ontwikkeling van software systemen of kennissystemen. Dit brengt standaardisatie van een domein in de informatieketen in de vorm van metadata met zich mee en juist niet in de vorm van een softwareproduct. Daarnaast wordt een XBRL-taxonomie later vaak geïmplementeerd in softwareproducten als een manier om de metadata te beschrijven, op basis waarvan een rapport moet worden opgebouwd. Zij stellen dat "*XBRL taxonomy development can be regarded as a transfer of the domain knowledge from a domain expert into an implemented knowledge base which is encoded within an XBRL taxonomy*". Piechocki en Felden

(2007) hebben een taxonomie ontwikkelproces model omschreven waarin het ontwikkelproces van een taxonomie wordt geïdentificeerd. Dit model is gebaseerd op het lineaire waterval model uit het software ontwikkelingsdomein (Royce, 1970). Hierin zijn duidelijk gedefinieerde fases te onderkennen waarmee een taxonomie auteur geconfronteerd zal worden bij het ontwikkelen van een SBR taxonomie. Zij hebben dit model gebaseerd op basis van de ontwikkelingen die gaande zijn bij bestaande XBRL projecten in de wereld. In de figuur 6.5 is dit taxonomie ontwikkelproces model opgenomen.



Figuur 6.5 – Taxonomie ontwikkelproces model (gebasseerd op Piechocki & Felden, 2007)

Bij de ontwikkeling van een SBR taxonomie is sprake van dezelfde fases in het ontwikkelproces en van dezelfde op te leveren deliverables aan het einde van elke fase. Deze fases worden in de onderstaande paragrafen nader besproken.

6.4.7 *Requirementsfase*

In de eerste fase van het taxonomie ontwikkelproces worden de eisen (ook wel requirements genoemd) in ogenschouw genomen en gedefinieerd. De uitkomst van deze fase is een lijst met eisen die de opzet van de taxonomie weergeven. Bij het bepalen van deze eisen speelt de betreffende informatieketen een belangrijke rol. De eisen die aan een taxonomie gesteld kunnen worden, zijn sterk afhankelijk van een aantal eigenschappen van de informatieketen. Onderstaande tabel geeft een overzicht van die eigenschappen.

Tabel 6.2 – Eigenschappen van informatieverplichtingen in een keten

Eigenschap	Relevante aspecten	Paragraaf
1. Type	Domein, stromen, aggregatieniveau	6.4.7.1
2. Frequentie	Conditionerend, cyclisch, gebeurtenisgebonden	6.4.7.2
3. Richting	Brengplicht, haalrecht	6.4.7.3
4. Oorsprong	Dwang, belang	6.4.7.4
5. Aard	Open, gesloten verantwoording	6.4.7.5

De vijf eigenschappen in de linker kolom worden in de genoemde paragrafen in de rechterkolom nader toegelicht.

6.4.7.1 Type informatieverplichtingen

De eerste keteneigenschap die bepalend is voor de eisen betreft het type informatieverplichting in de keten. Het type keten bepaalt feitelijk het domein waarop de taxonomie van toepassing is. Een domein is een specifiek gebied, veelal met een specifieke domeineigenaar, waar binnen één of meerdere soorten gegevens worden uitgewisseld. Goede voorbeelden van domeinen zijn het belastingdomein of het jaarverslaggevingsdomein, zoals deze op dit moment in de Nederlandse Taxonomie zijn opgenomen. Binnen een domein zijn daarnaast verschillende stromen te onderkennen. Een stroom is een specifiek soort rapportage, dat binnen het betreffende domein gebruikt wordt om informatie binnen een keten uit te wisselen voor een specifiek doel. In het belastingdomein zijn bijvoorbeeld de stromen vennootschapsbelasting en omzetbelasting te onderscheiden. Deze stromen zijn sterk verschillend van aard, aangezien de ene stroom zich richt op de uitwisseling van gegevens die relevant zijn voor het (zelf berekende) af te dragen bedrag, onder andere gebaseerd op de omzetbelasting-bedragen vermeld op inkoop- en verkoopfacturen, terwijl de andere stroom zich richt op de gegevens die relevant zijn voor het bepalen van de hoogte van de vennootschapsbelasting, zoals de winst van de organisatie. Een domein kan dus meerdere stromen hebben. Veelal zijn deze stromen in aparte rapportages opgenomen in de Nederlandse Taxonomie.

Een stroom kan ook verschillende aggregatieniveaus hebben waaruit een keuze gemaakt wordt. Conceptueel gezien zijn drie verschillende aggregatieniveaus van gegevensuitwisseling te onderkennen, namelijk het rapportage niveau (sterk geaggregeerd), het administratie niveau (enigszins geaggregeerd) en het transactieniveau (niet geaggregeerd). Binnen SBR zijn alle stromen momenteel gericht op rapportageniveau, dus op het hoogste geaggregeerde niveau, omdat de informatieverplichtingen in de huidige domeinen van SBR op dit niveau worden uitgevraagd. Dit betekent echter niet dat dit de enige mogelijkheid is. In andere domeinen kunnen andere niveaus eveneens tot de mogelijkheden behoren.

6.4.7.2 Frequentie van de uitwisselingen

De tweede keteneigenschap die bepalend is voor de eisen betreft de frequentie van de uitwisselingen. Bij de informatieverplichtingen die binnen een informatieketen te onderkennen zijn, is vaak sprake van een verschil in de frequentie en het bijbehorende tijdstip van indiening. Volgens Arendsen (2008) kunnen informatieverplichtingen worden onderscheiden in conditionerende, cyclische en gebeurtenis-gebonden informatieverplichtingen.

- Conditionerende informatieverplichtingen zijn aan de orde in situaties waarin door een organisatie voor het eerst een specifieke rechtsbetrekking wordt aangegaan, zoals het aangaan van een lening. Binnen de op dat moment gevestigde rechtsbetrekking gelden de in dat kader opgelegde informatieverplichtingen.
- Cyclische informatieverplichtingen keren periodiek terug bij organisaties. Meestal hebben deze betrekking op gegevens over bepaalde periodes, zoals maand-, kwartaal- of jaaroverzichten. De aangifte BTW, die organisaties periodiek moeten indienen bij de Belastingdienst, is hier een voorbeeld van.
- Gebeurtenis-gebonden informatieverplichtingen hangen af van het optreden van bepaalde gebeurtenissen bij een organisatie. Een goed voorbeeld is bijvoorbeeld het verzoek van het Centraal Bureau voor de Statistiek om een statistiekopgave in te vullen. Dit gebeurt veelal steekproefsgewijs, waardoor dit alleen relevant is voor een organisatie wanneer zij binnen de betreffende steekproef valt.

In de Nederlandse Taxonomie zijn vooral die stromen opgenomen die aangemerkt kunnen worden als cyclische informatieverplichtingen. De keuze hiervoor valt te verklaren uit het periodieke karakter van deze stromen, waardoor hier zowel voor de uitvragende als de aanleverende partij de meeste winst in het aanleverproces valt te bereiken. Een organisatie is immers sneller bereid om te standaardiseren wanneer zij hier structureel gebruik van kan maken. Dit is bij cyclische informatieverplichtingen duidelijk het geval. De conditionerende en gebeurtenis-gebonden informatieverplichtingen hebben het in dit kader een stuk lastiger. Door het incidentele karakter van deze informatieverplichtingen is het voor veel partijen minder interessant om deze informatiestromen te standaardiseren. Dat blijkt op dit moment ook in het statistiek domein dat achterblijft met de hoeveelheid ontvangen berichten met verantwoordingsinformatie. Door het gebeurtenis-gebonden karakter van deze stromen maken aanleverende organisaties hier weinig gebruik van, ondanks het feit dat de verantwoordingen eenvoudig zijn aan te leveren voor organisaties. We kunnen twee mogelijke oplossingen voor deze situatie onderkennen. De eerste is om het gebeurtenisgebonden karakter van de informatieverplichtingen te veranderen naar een cyclisch karakter. Dit betekent echter meer verantwoordingsplichten voor organisaties, waardoor dit vaak niet als een reële optie wordt beschouwd. De tweede mogelijkheid is om SBR verplicht te stellen als aanleverkanaal en alle overige kanalen af te sluiten.

6.4.7.3 Richting van informatieverplichtingen

De derde keteneigenschap die bepalend is voor de eisen betreft de richting van de informatieverplichtingen. Hierbij zijn globaal twee richtingen te onderkennen: organisaties hebben een brengplicht van gegevens naar een uitvragende partij of de uitvragende partij heeft een haalrecht van gegevens bij organisaties. Van een brengplicht is sprake als organisaties gegevens moeten aanleveren bij een uitvragende partij. Nijsen (2003) noemt dit ook wel de actieve informatieverplichting. Van een haalrecht is sprake als een uitvragende partij gegevens bij een organisatie kan komen halen, ook wel de passieve informatieverplichting genoemd.

De verschillende stromen die momenteel zijn te onderkennen binnen SBR zijn allemaal gebaseerd op de brengplicht. Dit is niet zonder reden, aangezien de stromen

met een brengplicht vaak een cyclisch karakter hebben en de stromen met een haalrecht meestal gebeurtenis-gebonden zijn. Zoals eerder gesteld is het in de eerste situatie eenvoudiger om te standaardiseren. In theorie kan SBR echter zowel de brengplicht als het haalrecht ondersteunen. Daarnaast kan SBR ook de hieruit voortkomende communicatie ondersteunen, zoals het servicebericht aanslag van de Belastingdienst.

6.4.7.4 Oorsprong van informatieverplichtingen

De vierde keteneigenschap die bepalend is voor de eisen betreft de oorsprong van de informatieverplichtingen. De informatieverplichtingen en het daaraan gerelateerde (elektronische) berichtenverkeer vinden hun oorsprong veelal in wet- en regelgeving (Arendsen, 2008). In het geval van de plicht van organisaties om informatie aan te leveren aan de overheid, ook wel business-to-government (B2G) informatieverplichtingen genoemd, is de relevante wet- en regelgeving altijd leidend. Binnen het SBR Programma zijn de informatieverplichtingen voor de B2G informatieketens gebaseerd op de bepalingen zoals vastgelegd in de wet- en regelgeving. Dit is duidelijk waarneembaar bij de drie huidige B2G stromen, te weten het jaarverslaggevingsdomein, het belastingdomein en het statistiekdomein. Zij baseren zich alle drie op de relevante wet- en regelgeving binnen hun specifieke terrein.

In het geval van zogenaamde business-to-business (B2B) informatieketens is de situatie anders. Deze partijen kunnen immers veelal niet terugvallen op de van toepassing zijnde wet- en regelgeving waarop zij de informatieverplichtingen kunnen baseren. Binnen SBR in Nederland is op dit moment slechts één B2B informatieketen te onderkennen, namelijk het bancaire domein. In dit domein bepaalt een consortium van de drie grootbanken in Nederland gezamenlijk de informatieverplichtingen, waaraan organisaties door middel van het indienen van kredietrapportages via SBR moeten voldoen. Deze informatieverplichtingen zijn gebaseerd op de informatie die de interne systemen van deze banken nodig hebben om de relevante risico inschattingen te maken in het kader van de kredietverstrekking.

6.4.7.5 Aard van informatieverplichtingen

De vijfde keteneigenschap die bepalend is voor de eisen betreft de aard van de informatieverplichtingen. Binnen een informatieketen zijn twee verschillende soorten verantwoordingen te onderkennen – open verantwoordingen en gesloten verantwoordingen.

Bij een open verantwoording heeft de aanleverende partij (een bepaalde mate van) vrijheid welke gegevens zij aanlevert bij de uitvragende partij. Een voorbeeld van een open verantwoording is bijvoorbeeld de jaarrekening van grote organisaties. De wet- en regelgeving geeft hier een raamwerk voor de verantwoording, maar deze organisaties hebben een bepaalde mate van vrijheid in wat zij wel en niet willen toelichten en opnemen in de jaarrekening op basis van hun eigen inschatting. De meeste organisaties kiezen ervoor om een minimumpositie in te nemen en zo min mogelijk te rapporteren, maar dit neemt niet weg dat zij de optie hebben om dit anders in te steken.

In een gesloten verantwoording zijn de aan te leveren gegevens in detail voorgeschreven door de uitvragende partij en mag hier niet van worden afgeweken door de aanleverende partij. Een organisatie heeft in deze situatie geen enkele vrijheid om zelf zaken toe te voegen, maar dient alleen de zaken te rapporteren die door de uitvragende partij zijn bepaald. In een papier-centrische omgeving betekende dit dat een bepaald formulier ingevuld moest worden. Een goed voorbeeld is de aangifte BTW. Dit is een vaste set aan gegevens die organisaties kunnen aanleveren bij de Belastingdienst en van deze vaste set mag niet worden afgeweken.

De verantwoordingen die zijn opgesteld op basis van de Nederlandse Taxonomie zijn momenteel te classificeren als 'gesloten', omdat het op dit moment niet mogelijk is om in detail te bepalen welke gegevens op gestructureerde wijze ingestuurd kunnen worden naar de uitvragende partij. Dit zal op termijn vermoedelijk wel gaan spelen voor het jaarverslaggevingsdomein, aangezien dit een domein is waarbij organisaties een grote mate van vrijheid hebben om hun eigen verantwoordingen in te richten. De keuze om de taxonomie voor dit domein vooralsnog gesloten te houden is een bewuste keuze geweest van het SBR Programma vanwege de focus op kleine organisaties en de aanvullende complexiteit die dit met zich meebrengt. De inschatting was dat kleine organisaties voldoende hebben aan de huidige rapportages in de NT, zodat zij over het algemeen geen uitbreidingen nodig hebben. Voor middelgrote en grote organisaties ligt dit echter anders, waardoor in de komende jaren de mogelijkheid van open verantwoordingen in dit domein noodzakelijk zal worden. Voor het belastingen domein en het statistiek domein zal een open verantwoording nooit een reële optie zijn in Nederland, aangezien deze uitvragende partijen aan organisaties exact voorschrijven welke gegevens zij willen ontvangen. Hier heeft de rapporterende organisatie geen enkele vrijheid in.

6.4.7.6 Taxonomie raamwerk

Op basis van de voorgaande paragrafen komen de eerste contouren van de te ontwikkelen taxonomie al naar voren. De eisen waaraan de taxonomie dient te voldoen, kunnen worden afgeleid van de eigenschappen van de betreffende informatieketen. Hierbij dient in deze fase ook al een inschatting gemaakt te worden van het raamwerk van de taxonomie. Het raamwerk kan worden omschreven als een wijze waarop verschillende taxonomieën al dan niet worden gecombineerd (Piechocki & Felden, 2007). Het raamwerk geeft onder meer aan of een basistaxonomie of een extensietaxonomie ontwikkeld moet worden. Bij een basistaxonomie worden alle begrippen zelfstandig gedefinieerd, terwijl bij een extensietaxonomie gebruik gemaakt wordt van (een deel van) de begrippen uit een taxonomie die door een andere partij is opgesteld.

De NT kent zowel eigen begrippen als begrippen die geïmporteerd worden uit andere (internationale) taxonomieën. Zo is in het jaarverslaggevingsdomein een aantal rapportages beschikbaar dat een extensie vormt op de IFRS taxonomie. IFRS, de afkorting van International Financial Reporting Standards, is een verslaggevingstandaard die binnen Europa door alle beursgenoteerde ondernemingen moet worden toegepast bij het opstellen van hun geconsolideerde jaarrekening. Daarnaast hebben alle ondernemingen in Europa de optie om van deze verslaggevingsstandaard gebruik te

maken bij het opstellen van hun jaarrekening. De International Accounting Standards Board (IASB), de organisatie die de IFRS uitbrengt, brengt jaarlijks naast de zogenaamde '*bound volume*', waarin alle verslaggevingsregels in boekvorm zijn uitgeschreven, ook een IFRS taxonomie uit. De IFRS taxonomie is een representatie in XBRL formaat van de rapportagemogelijkheden uit de bound volume. In de rapportages in de Nederlandse Taxonomie waarin IFRS een rol speelt, worden begrippen en relaties uit deze taxonomie geïmporteerd en uitgebreid met specifieke Nederlandse begrippen en relaties op basis van Titel 9 van Boek 2, Burgerlijk Wetboek.

6.4.8 *Ontwerpfase*

Voor de ontwikkeling van elke taxonomie is er een mix nodig van domein experts en technische experts. Gezamenlijk brengen zij semantiek en syntax samen in de betreffende taxonomie. Volgens het taxonomie ontwikkelproces van Piechocki en Felden (2007) staat in de ontwerpfase de semantiek centraal. In deze fase draait het om het op een gestructureerde wijze inzichtelijk maken van de kennis van domein experts door middel van een semantisch gegevensmodel. We gaan hier bewust zo min mogelijk in op de syntax omdat, zoals we al eerder stelden, semantiek onafhankelijk zou moeten zijn van syntax. Als gevolg van de keuze voor XBRL als syntax gaat dit in de praktijk niet helemaal op, aangezien deze syntax wel een aantal beperkingen oplegt aan de semantiek. Desalniettemin, maken we dit onderscheid om de semantiek van het semantisch gegevensmodel zo objectief mogelijk tot stand te laten komen. In de constructie fase zullen we nader ingaan op de syntax.

In deze fase is een aantal verschillende stappen te onderkennen om tot een semantisch gegevensmodel te komen. Deze stappen zijn als volgt:

1. Identificeren van de begrippen
2. Normaliseren van de begrippen
3. Structureren van de begrippen

Deze stappen worden in de komende paragrafen nader uiteengezet.

6.4.8.1 Identificeren van de begrippen

Een domeinexpert dient op basis van de informatiebehoeften van een uitvragende partij de begrippen te identificeren. Hierbij dient de domeinexpert niet uit te gaan van de begrippen die nodig zijn in de taxonomie, maar dient hij zich de vraag te stellen welke verantwoordingsinformatie verstrekt moet worden aan de uitvragende partij. Hierbij dient hij zich volledig af te sluiten voor mogelijke technologische complicaties. In de praktijk zal een partij zich vaak baseren op de van toepassing zijnde wet- en regelgeving uit het betreffende domein of de informatiebehoeften van interne systemen van een uitvragende partij. Een analyse door de domeinexpert zal leiden tot een lijst van begrippen die door een uitvragende partij uitgevraagd kan worden. (Zie kader voor een voorbeeld bij jaarverslaggeving.)

Identificatie van begrippen op basis van wetgeving
De begrippen in het jaarverslaggevinsdomein zijn onder meer gebaseerd op de wetsartikelen in titel 9 van het Burgerlijk Wetboek, Boek 2 (BW2). Aan de hand van een willekeurig wetsartikel proberen we met behulp van een voorbeeld te illustreren hoe hieruit begrippen geïdentificeerd kunnen worden. Onderstaand is een wetsartikel uit titel 9 BW2 opgenomen, waarbij we moeten aanmerken dat dit artikel uit afdeling 3 komt dat voorschriften geeft omtrent de balans en de toelichting daarop.

Artikel 369:
Onder de tot de vlottende activa behorende voorraden worden afzonderlijk opgenomen:

a. grond- en hulpstoffen;
b. onderhanden werk;
c. gereed product en handelsgoederen;
d. vooruitbetalingen op voorraden.

Op basis van het bovenstaande wetsartikel kunnen we een zestal begrippen onderscheiden die op de balans van een jaarrekening voor kunnen komen. Deze zes begrippen zijn: 'vlottende activa', 'voorraden', 'voorraad grond- en hulpstoffen', 'voorraad onderhanden werk', 'voorraad gereed product en handelsgoederen' en 'vooruitbetalingen op voorraden'. Deze zes begrippen zal een domeinexpert dus identificeren op basis van dit wetsartikel.

6.4.8.2 Normaliseren van de begrippen

Het normaliseren van begrippen is erop gericht om ervoor te zorgen dat begrippen slechts één keer gedefinieerd zijn in een gecontroleerd woordenboek binnen een domein. Hiervoor dient een domeinexpert voldoende inzicht te hebben in de definitie van het betreffende begrip. Daarnaast wordt ook continu gekeken naar de mogelijkheden voor inter-domein normalisatie, dus over verschillende domeinen heen.

Inter-domein normalisatie kan voor complexe situaties zorgen, bijvoorbeeld wanneer gegevensdefinities uit verschillende bepalingen niet op elkaar aansluiten of niet logisch zijn gezien de context waarin ze worden toegepast. De bron is vaak de van toepassing zijnde wet- en regelgeving, maar de relevante wetten en regels zijn niet altijd even consistent. Als gevolg hiervan is verregaande normalisatie (nog) niet mogelijk. Dit behoeft eerst verdere harmonisatie, oftewel het aanpassen van de betreffende wetten en regels om de definities op een lijn te brengen met elkaar. Het eigenaarschap van deze wetten en regels ligt meestal bij verschillende ministeries of departementen, waardoor harmonisatie een langdurig traject is.

Eventuele verschillen in definities binnen wet- en regelgeving bemoeilijken gegevensstromen en het hergebruik van gegevens. Verdere standaardisatie van gegevensdefinities over specifieke wet- en regelgeving heen zal leiden tot een algemenere informatie-uitvraag, gericht op het voorkomen van nieuwe en het verminderen van de bestaande gegevens-uitvraag.

Binnen het SBR Programma spelen de bovenstaande complexiteiten op het gebied van normalisatie ook. De wet- en regelgeving, waarop de uitvragende partijen hun gegevens-uitvraag baseren, verschilt per domein, waardoor ook de definities varieren. Zij hebben regelmatig te maken met begrippen die op het eerste gezicht hetzelfde lijken te zijn als een begrip in een ander domein. Zo hanteren het belastingendomein en het jaarverslaggevingsdomein binnen SBR elk bijvoorbeeld een andere

definitie voor het begrip 'winst'. Wanneer echter in detail naar de inhoudelijke definities van deze begrippen gekeken wordt, blijkt hier (enige mate van) verschil in te zitten. Als gevolg hiervan dienen deze begrippen eerst geharmoniseerd te worden door het aanpassen van de wet- en regelgeving. Het harmoniseren is per definitie SBR overstijgend. Wanneer verdere harmonisatie niet mogelijk of gewenst is, is hier dus sprake van twee begrippen. Op basis van hun definitie zijn ze immers niet identiek. Binnen de NT wordt om verdere harmonisatie te faciliteren wel de gelijkheid tussen de twee begrippen expliciet onderkend door het toevoegen van een relatie zijn met behulp van definition links.

Wanneer nieuwe partijen aansluiten bij het SBR Programma worden zij ook verplicht om te onderzoeken in hoeverre hun gegevens uitvraag kan worden afgedekt met de reeds in de NT opgenomen begrippen. De reden om dit onderzoek verplicht te stellen ligt in het feit dat deze normalisatie het voor een organisatie eenvoudiger maakt om te verantwoorden.

6.4.8.3 Structureren van de begrippen

Inmiddels hebben we een lijst van begrippen opgesteld. Het structureren van de begrippen richt zich op het beschrijven van de relevante eigenschappen van de uit te vragen begrippen volgens vastgelegde normen. Hierbij zijn activiteiten te onderscheiden in het karakteriseren van begrippen en het beschrijven van de relaties tussen deze begrippen. De uitkomst van deze activiteiten leidt tot een semantisch gegevensmodel.

Hoewel we hier spreken van een semantisch gegevensmodel, wordt een domeinexpert vaak gedwongen om bij het structureren van begrippen rekening te houden met de te hanteren syntax. De syntax kan namelijk ook enige semantiek afdwingen. Een voorbeeld hiervan is het opnemen van een balanceType attribuut bij een concept op basis van de XBRL 2.1 specificatie. Dit attribuut wordt in eerste instantie meestal niet in een semantisch gegevensmodel opgenomen, aangezien dit niet noodzakelijk is voor de uitwisseling en verwerking van de gegevens. Het is de confrontatie met de syntax die er uiteindelijk toe leidt dat dit moet worden toegevoegd aan het semantisch gegevensmodel. Conceptueel zijn we van mening dat het beter is wanneer het semantisch gegevensmodel niet geconfronteerd wordt met verplichtingen op basis van de syntaxkeuze, maar in de praktijk is dit helaas vaak niet mogelijk.

De activiteiten inzake het beschrijven van begrippen bestaan met name uit het bepalen van de attributen, labels, definities en referenties. De activiteiten inzake het beschrijven van de relaties tussen begrippen bestaan vooral uit het bepalen van de volgorde van begrippen, van tellingen van begrippen of van andersoortige verbondenheid van begrippen. Al deze activiteiten dienen te worden verricht door een domeindeskundige met enige kennis van semantiek.

Attributen
Bij het bepalen van technische begrippen kunnen of moeten, afhankelijk van de gekozen syntax, attributen worden toegevoegd aan de geïdentificeerde begrippen. Deze attributen zijn te zien als specifieke eigenschappen van een bepaald begrip. In de XBRL 2.1. specificatie zijn er diverse soorten attributen beschikbaar. In onderstaand

kader is een aantal attributen weergegeven voor het begrip ‘voorraden’ bij het gebruik van XBRL als syntax.

Attributen
id="Inventories" (geeft de technische identificatiecode weer)
datatype="monetaryItemType" (geeft aan dat het een monetair bedrag is)
periodType="instant" (geeft aan dat het van toepassing is op een bepaalde datum)
balanceType=”debit” (geeft aan dat het een debet bedrag is)

Labels

Aan de gedeclareerde begrippen kunnen labels worden gekoppeld waarmee een leesbare weergave van een begrip kan worden gerealiseerd. Om dit te bereiken worden deze labels gekoppeld aan de technische identificatiecode van begrippen. Hierdoor kunnen ook diverse soorten labels hieraan gekoppeld worden. Dit kunnen labels in verschillende talen zijn, maar bijvoorbeeld ook zogenaamde ‘preferred labels’. Deze labels verduidelijken voor een specifiek begrip de situatie waarvoor ze in een presentatie gebruikt worden. In onderstaand kader zijn enkele labels opgenomen voor het begrip ‘voorraden’.

Labels
Voorraden (standaard label)
Voorraden aan het begin van de periode *(periodStart label)*
Voorraden aan het einde van de periode *(periodEnd label)*

Definities

Bij het normaliseren van de begrippen werd eerder al gesteld dat hierbij definities noodzakelijk zijn om de eenduidigheid van de begrippen te garanderen. Het heeft vaak toegevoegde waarde om deze definities ook aan de gebruikers van een taxonomie te kunnen tonen, zodat zij zich exact realiseren wat er met een specifiek begrip wordt bedoeld. Het is aan te bevelen deze definities ook op te nemen in de taxonomie, bijvoorbeeld door het gebruik van een documentation label. In onderstaand kader is een definitie opgenomen van voorraden.

Definities
Voorraden zijn activa die worden aangehouden:
- voor verkoop in het kader van de normale bedrijfsvoering;
- in het productieproces voor een dergelijke verkoop;
- in de vorm van grond- en hulpstoffen die worden verbruikt tijdens het productieproces;
- tijdens het verlenen van diensten.

Referenties

Het is mogelijk om referenties naar relevante wet- en/of regelgeving te koppelen aan begrippen. Het opnemen van deze referenties kan ook gezien worden als het opnemen van een soort definitie, aangezien in deze referenties uit de wet- of regelgeving iets zal worden ‘geroepen’ over het begrip.

Volgorde van begrippen

De domeinexpert zal de begrippen veelal zodanig structureren, dat deze begrippen een specifieke volgorde krijgen die getoond dient te worden aan de opsteller van de

verantwoordingen. In de praktijk sluit dit meestal aan bij een volgorde die de gebruikers gewend zijn.

Tellingen van begrippen
Naast de inhoudelijke semantische beschrijvingen kunnen ook relationele verbindingen als semantische beschrijving dienen. Het meegeven van een zogenaamde 'telling' relatie aan begrippen is voor veel partijen erg interessant. Hierbij wordt inzichtelijk gemaakt dat de waarde van begrip A plus de waarde van begrip B optelt tot begrip C. Hierbij dient wel te worden vermeld dat het tonen van deze 'telling' relaties iets anders is dan het valideren van deze relaties. Het tonen van deze relatie kan op basis van de taxonomie plaatsvinden, maar voor het valideren of de waarden ook daadwerkelijk optellen is per definitie een instance document met waarden vereist.

Verbondenheid van begrippen
Er zijn diverse nadere relationele verbindingen te onderkennen naast de 'telling' relatie. De relatie die een bepaalde mate van verbondenheid tussen begrippen laat zien is bijvoorbeeld de relatie dat begrip A een verbijzondering is van begrip B. Het kan waarde hebben voor gebruikers om te weten of en hoe bepaalde begrippen aan elkaar verbonden zijn. In de taxonomie worden de semantische beschrijvingen van de relationele verbindingen en inhoudelijke aspecten als metadata uitgedrukt. Hoe meer relationele verbindingen en inhoudelijke aspecten een uitvragende partij kan definiëren hoe meer metadata meegeleverd kan worden aan de rapporteurs. Een grote hoeveelheid metadata die de rapportage begrippen omgeeft zou deze begrippen eenduidiger moeten maken. Hierdoor is het eenvoudiger voor rapporteurs om te begrijpen wat de uitvragende partij precies bedoelt en welke informatie zij wenst te verkrijgen.

In de SBR context wordt geprobeerd om zoveel mogelijk bruikbare relationele verbindingen en inhoudelijke aspecten van de begrippen in de vorm van metadata aan de rapporteurs te leveren. De beslissing welke metadata meegeleverd wordt met een taxonomie is vaak het resultaat van een belangenafweging. Hier moeten regelmatig trade-offs worden gemaakt tussen enerzijds de toegevoegde waarde voor de rapporteurs en anderzijds de inspanning om de metadata te realiseren. Hieruit kan het resultaat voortvloeien dat een bepaald soort metadata (voorlopig) niet wordt meegeleverd. Een goed voorbeeld van een dergelijke situatie zijn de tellingen van begrippen. SBR heeft ervoor gekozen om in de afgelopen jaren geen tellingen mee te leveren bij de taxonomie. De reden hiervoor was dat de functionaliteit, met nog niet ver genoeg ontwikkelde techniek onvoldoende was. Inmiddels heeft deze ontwikkeling plaatsgevonden, waardoor het meeleveren van tellingen in de toekomst naar verwachting weer zal gaan plaatsvinden.

Ondanks de trade-offs die soms gemaakt dienen te worden in het meeleveren van metadata is dit een essentieel onderdeel van de semantische beschrijvingen. Het heeft als doel om te komen tot een eenduidige definitie van de betekenis van de uitgewisselde gegevens.

6.4.9 *Ontwikkelingsfase*

De ontwikkelingsfase kenmerkt zich door de vertaling van het semantische gegevensmodel naar een syntactische representatie hiervan, oftewel een concept versie

van de taxonomie. Een van de grote uitdagingen van het ontwikkelen van een taxonomie is het omzetten van de kennis en wensen uit een expertisedomein naar de syntax die door een geautomatiseerd systeem kan worden geïnterpreteerd (Claassens, 2007). De technische kennis die nodig is om een semantisch gegevensmodel te modelleren naar een syntax, is dusdanig specifiek dat hiervoor technische expertise essentieel is.

6.4.9.1 Modelleren van begrippen naar een gegevensmodel

Het modelleren van begrippen naar een gegevensmodel leidt uiteindelijk tot de realisatie van een concept versie van een taxonomie. Deze activiteiten worden voornamelijk uitgevoerd door een technisch expert of data modelleur. Hierbij is het van groot belang dat de mogelijkheden die een open standaard als XBRL biedt zoveel als mogelijk zijn ingeperkt, omdat verschillende experts of data modelleurs met dezelfde grondstoffen tot volstrekt andere taxonomieën kunnen komen. Hiertoe is het wenselijk om een specifieke architectuur te hanteren die dit verder inperkt. De syntax architectuur is expliciet bedoeld om in een dergelijke situatie een eenduidige taxonomie te realiseren.

Een ander aspect dat hierbij helpt is het gebruik van ontwerppatronen. Er is een aantal verschillende semantische scenario's te onderkennen in een rapportage, waarvoor de technisch expert of data modelleur een patroon zal identificeren in de syntax. Door deze patronen een specifieke wijze van verwerken mee te geven op basis van de bestaande syntax mogelijkheden, en dit op te nemen in de architectuur, worden de taxonomieën eenduidiger. Een voorbeeld van een patroon is de wijze waarop verloopoverzichten (beginstand + mutatie = eindstand) dienen te worden gemodelleerd. Het staat de technisch expert of data modelleur uiteraard vrij om zelf te bepalen of deze patronen gehanteerd worden, maar veelal zijn dergelijke patronen verplicht gesteld in situaties waarbij het achterliggende probleem opgelost dient te worden.

Er zijn verschillende perspectieven te onderkennen wanneer we praten over het modelleren van begrippen naar een gegevensmodel (Simsion & Witt, 2005). Deze perspectieven zijn:

- Het communicatieperspectief
- Het presentatieperspectief
- Het opslagperspectief

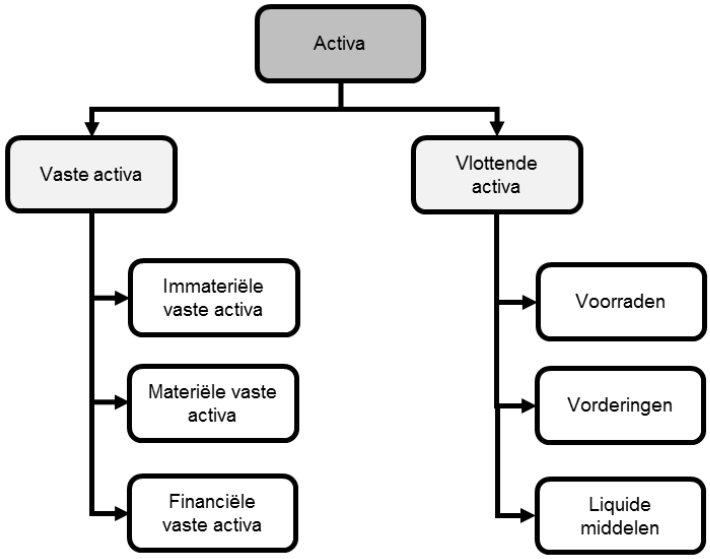
Uit onze praktijkervaring blijkt dat gebruikers vaak geen onderscheid maken in deze perspectieven, waardoor bij het modelleren vaak onnodige of ongewenste eisen worden gesteld. Deze perspectieven worden hieronder nader besproken.

6.4.9.2 Communicatieperspectief

Het communicatie perspectief is het belangrijkste perspectief op een gegevensmodel voor het elektronisch berichtenverkeer. Communiceren is immers de primaire taak van een elektronisch bericht. Om de uitwisseling van het bericht zo goed mogelijk in te vullen zijn – afhankelijk van de gekozen syntax – verschillende modelleertechnieken beschikbaar.

Modelleertechnieken
De genormaliseerde lijst van begrippen dient nog verder te worden gemodelleerd in een taxonomie. Het gebruik van XBRL als syntax geeft de datamodelleur de mogelijkheid de gegevens op twee manieren te modelleren. Via een hiërarchische modelleerwijze of via een (multi-)dimensionele modelleerwijze.

Bij hiërarchisch modelleren worden gegevens georganiseerd in een zogenaamde boomstructuur. Deze structuur vertegenwoordigt gegevens door middel van ouder-kind relaties. Elke ouder kan meerdere kinderen hebben, maar elk kind heeft maar één ouder (1 op n relatie). In deze structuur worden delen van de conceptnaam als ouder gebruikt en vormen op deze wijze een 'pad', zoals Activa-Vaste Activa-Materiële Vaste Activa. De hiërarchische modelleerwijze is een goede methode wanneer de begrippen genormaliseerd zijn en de syntax alleen een hiërarchisch model toestaat. Een grafische weergave van hiërarchische modellering is opgenomen in de onderstaande figuur.



Figuur 6.6 – Grafische weergave van een hiërarchische structuur

De tweede modelleringstechniek werkt met een (multi-)dimensioneel model. Bij (multi-) dimensionele modellering kunnen begrippen hergebruikt worden door het verplaatsen van delen van de semantiek naar dimensies. Op deze wijze hoeft niet elk begrip van deze semantiek te worden voorzien en minimaliseert dit het aantal begrippen in een taxonomie.

De (multi-)dimensionele modelleerwijze is met name interessant in complexere verantwoordingen, waarbij bijvoorbeeld grote tabellen verstuurd dienen te worden. Een voorbeeld van een complexere rapportage is wanneer soortgelijke begrippen voor verschillende categorieën uitgevraagd worden. In de tabel is een illustratie opgenomen van een (multi-)dimensionele modellering van de omzet naar producten en landen met behulp van assen. De rapporteerbare begrippen kunnen worden opgenomen

voor verschillende aspecten, zoals uitgedrukt in de as waarin de verschillende componenten van het eigen vermogen worden weergegeven.

Tabel 6.3 – Dimensionele structuur van de uitsplitsing van omzet naar regio en product

Omzet	Benelux			Frankrijk	Spanje	Totaal
	Nederland	België	Subtotaal			
Omzet product X	10	2	12	-	-	12
Omzet product Y	1	-	1	6	8	15
Omzet product Z	5	3	8	1	2	11
Totaal	16	5	21	7	10	38

In de NT wordt zowel de hiërarchische als de (multi-)dimensionele modelleerwijze toegepast. De complexiteit van de dimensionele modellering in de NT is echter vooralsnog beperkt. In diverse Europese projecten wordt momenteel gewerkt aan meerdere complexe XBRL taxonomieën die van een zeer groot aantal dimensies gebruikmaken, waarbij het gelijktijdige gebruik van tientallen dimensies geen uitzondering is. Deze methodiek van multi-dimensioneel modelleren staat bekend als 'data point model' (DPM).

Granulariteit
Een aspect dat relevant is vanuit het communicatie perspectief betreft het bepalen van het niveau van granulariteit van gegevens. Onder granulariteit wordt verstaan de mate van fijnmazigheid (of het aggregatieniveau, de mate van detaillering) waarop de informatiebehoeften worden gedefinieerd. Een goed voorbeeld van een discussie omtrent granulariteit is te zien in de definitie van huisvestingskosten. Als je wilt dat huursubsidie geen onderdeel is van de huisvestingskosten (de definitie is dan: huisvestingskosten, dus huren, energiekosten, schoonmaakkosten exclusief huursubsidies…), maak die 'grains' dan ook expliciet. Dit is een vrij subjectieve keuze van de data modelleur. Bij SBR wordt hierbij het uitgangspunt gehanteerd dat de wet- en regelgeving leidend is voor het bepalen van de mate van granulariteit. Indien deze wet- en regelgeving bepaalde onderwerpen expliciet benoemt, zal de mogelijkheid geboden worden om dit ook in een apart begrip uit te vragen.

Valideren
Ook de validatie van gegevens is relevant vanuit het communicatie perspectief. Het valideren van gegevens is van belang, doordat het ervoor zorgt dat de gegevens die uitgewisseld worden voldoen aan de daaraan te stellen kwaliteitseisen. De validatie van de gegevens kan deels worden bepaald door de gehanteerde syntax, bijvoorbeeld door het toekennen van bepaalde datatypes aan begrippen. Het is ook mogelijk om op basis van de gehanteerde wijze van modelleren af te dwingen wanneer welke zaken wel en niet gerapporteerd mogen worden. Een derde manier om gegevens te valideren is door het gebruik van specifieke business rules die onderdeel uit kunnen maken van een gegevensmodel. Binnen SBR worden alle drie methodes toegepast.

6.4.9.3 Presentatieperspectief

Het presentatie perspectief is vanuit het gegevensmodel bezien een minder interessant perspectief. Het richt zich immers op de weergave (rendering) van de gegevens uit het gegevensmodel. Dit kan zowel op papier, in een digitaal document, dan wel in de programmatuur die XBRL berichten aan een mens op een scherm aanbiedt. De

essentie die hierbij van belang is, is dat deze weergave van de gegevens niets te maken hoeft te hebben met de wijze waarop de gegevens in een gegevensmodel zijn opgenomen. Het is immers slechts een manier om deze gegevens weer te geven.

Voor zakelijke gebruikers is deze essentie vaak lastig te bevatten, aangezien zij vrijwel uitsluitend gericht zijn op het presentatie perspectief. Dit type gebruikers is veelal gewend om formulieren of template verantwoordingen te maken of in te vullen waarin de weergave min of meer stabiel blijft. Deze weergave is in de loop der jaren vaak geoptimaliseerd om door menselijke ogen geconsumeerd te worden. Het geeft ook vaak impliciete relaties weer. Voor geautomatiseerde verwerking is het presentatie perspectief veelal ongeschikt. De impliciete verbanden in een weergave zijn onbegrijpelijk voor de computer. Mensen zijn gewend om dit perspectief te gebruiken, maar moeten niet vergeten dat er binnen en buiten dit perspectief nog vele mogelijke manieren zijn om gegevens consistent te groeperen met behulp van metadata.

Er zijn verschillende soorten relaties te onderkennen die gelegd kunnen worden tussen begrippen in het kader van presentatie. Denk hierbij onder meer aan de volgorde waarin begrippen gepresenteerd worden, het (hiërarchisch) niveau waarop begrippen worden weergegeven, een tabelvorm waarin begrippen worden weergegeven, etc. Deze voorbeelden zijn allemaal inhoudelijke kenmerken van een weergave, maar het is ook mogelijk om begrippen met typografische kenmerken weer te geven. Denk hierbij aan het weergeven van begrippen in een bepaalde kleur om een zekere classificatie hieraan mee te geven. Deze relaties moeten wel worden opgenomen in een taxonomie om gehanteerd te kunnen worden. Dit gebeurt vaak door middel van diverse ouder-kind relaties. In de onderstaande figuur is een voorbeeld opgenomen van de activa zijde van de balans, waarin de presentatie volgorde door middel van ouder-kind relaties is gemaakt.

Balans [titel]			
Activa [titel]			
Vaste activa [titel]			
Immateriële vaste activa	X		
Materiële vaste activa	X		
Financiële vaste activa	X		
Vaste activa		X	
Vlottende activa [titel]			
Voorraden	X		
Vorderingen	X		
Liquide middelen	X		
Vlottende activa		X	
Totale activa			X

Figuur 6.7 – Een weergave van de presentatiestructuur van een (verkorte) balans

Het presenteren van begrippen in XBRL taxonomieën is altijd een probleem geweest. Feitelijk kon in de afgelopen jaren alleen de presentatievolgorde meegegeven worden

van rapporteerbare begrippen en geen nadere presentatie-informatie zoals context-informatie (periode, eenheid, etc.). Met name door de mogelijkheden die (multi-) dimensioneel modelleren biedt, worden de beperkingen van deze aanpak duidelijk. Hierdoor moesten uitvragende partijen die een gerenderde versie van de gegevens beschikbaar wilden stellen veelal specifieke softwareoplossingen invoeren om dit mogelijk te maken.

6.4.9.4 Opslagperspectief

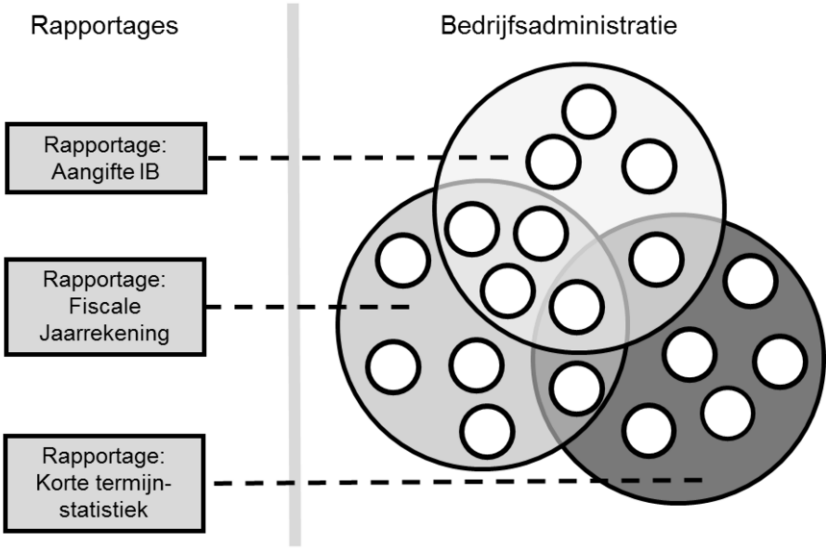
Het opslagperspectief richt zich op het gebruik van een taxonomie als opslagmiddel. Een XML bestand kan in theorie ook gebruikt worden als opslagdocument voor data. In sommige situaties kan dit handig zijn, maar we zien zelf vooral een groot nadeel in deze methodiek: de performance. Het opvragen van gegevens is nog altijd veel sneller in een genormaliseerde database dan in verschillende XML bestanden of een native XML database, waardoor we in dit document niet verder ingaan op XML als opslagformaat.

We richten ons vanuit dit perspectief op de wijze hoe de taxonomie gekoppeld kan worden aan de databases van zowel de aanleverende als de uitvragende partij. De 'mapping' is essentieel om aanleverende partijen geautomatiseerd een verantwoording te laten genereren op basis van de meest recente taxonomie. Deze mapping kunnen aanleverende partijen veelal in hun eigen administratie software realiseren. De administratie software laadt de taxonomie in en stelt de aanleverende partij in staat om een mapping te realiseren tussen de begrippen van de uitvragende partij en de begrippen zoals zij die zelf in hun administratie voeren. Sommige administratie-software regelt dit zelfs voor haar klanten. Een uitvragende partij heeft vaak een soortgelijke mapping beschikbaar, waarmee zij de begrippen uit de taxonomie koppelt aan de begrippen in hun interne systemen, zodat deze automatisch doorgezet kunnen worden.

6.4.9.5 Realisatie van SBR taxonomieën en de rol van de NT

De realisatie van een SBR taxonomie kent een aantal bijzondere aspecten dat niet altijd bij andere taxonomieën te vinden is. Zoals eerder gesteld, worden SBR taxonomieën altijd gemaakt onder verantwoordelijkheid van de betreffende uitvragende partij. Dit betekent overigens niet, dat zij van alle begrippen die zij gebruiken ook de daadwerkelijke eigenaar hoeven te zijn. De uitvragende partij heeft de vrijheid om de taxonomie in-house te ontwikkelen of het te outsourcen naar een service provider.

De SBR taxonomie is een zogenaamde deeltaxonomie, oftewel de taxonomie voor een specifiek domein die is opgenomen in de NT. Het belastingendomein, het jaarverslaggevingsdomein en het statistiekdomein zijn de drie deeltaxonomieën die op dit moment onderdeel uit maken van de NT. De kenmerken van een deeltaxonomie zijn dus, dat het zich richt op een specifiek domein en dat het is opgenomen in de NT. Rapportages die onderdeel uitmaken van een domein in de NT halen hun begrippen zoveel als mogelijk uit een gezamenlijke set van begrippen uit de bedrijfsadministratie. Daarnaast zijn er altijd begrippen die alleen voor een specifiek domein van toepassing zijn. In de onderstaande figuur is een grafische weergave van dit principe opgenomen.



Figuur 6.8 – Grafische weergave van de opbouw van de Nederlandse Taxonomie

Een deeltaxonomie is dus niet hetzelfde als een extensietaxonomie. Bij een extensie taxonomie wordt in het verantwoordingsproces in de basis gebruik gemaakt van de begrippen in de NT, maar heeft de uitvragende partij voor specifieke (verantwoordings) doeleinden een (beperkt) aantal andere definities nodig om tot de juiste rapportages te komen. Een goed voorbeeld van een extensietaxonomie is de bankentaxonomie. De bankentaxonomie wordt door het consortium van de drie grootbanken in Nederland gebruikt om gegevens uit te wisselen tussen ondernemer en een bank in het kader van de kredietverstrekking. De bankentaxonomie is een extensie op de NT, aangezien het voor een groot deel aansluit bij de jaarrekening en belastingaangiften uit de NT. Daarnaast heeft de bankentaxonomie aanvullende begrippen gedefinieerd, die specifiek nodig zijn voor kredietrapportages. De bankentaxonomie wordt als separate taxonomie uitgebracht en maakt geen onderdeel uit van de NT, maar voldoet wel aan de in de NTA opgenomen architectuurafspraken.

6.4.10 *Testfase*

Na de oplevering van de concept versie van de taxonomie zal deze een uitgebreide testfase ondergaan. We hebben hierbij een aantal meeteenheden nodig voor het bepalen van de kwaliteit. De vraag die we ons hier dienen te stellen is in hoeverre het gegevensmodel de eisen aan informatie ondersteunt (Simsion & Witt, 2005). Dit betekent dat we bij het testen vaststellen of rekening is gehouden met de verschillende kwaliteitseisen. Daarbij helpen specifiek voor gegevens gedefinieerde kwaliteitskenmerken. Kwaliteit betekent in dit hoofdstuk ‘geschikt voor het doel’ (Juran, 1992). Tijdens de testfase worden testwerkzaamheden uitgevoerd om te bepalen of de semantische en syntactische kwaliteitseisen worden gewaarborgd.

6.4.10.1 Semantische kwaliteitseisen

De semantische kwaliteitseisen richten zich op de inhoudelijke kwaliteit van het gegevensmodel. Deze eisen worden meegenomen tijdens het modelleren van het gegevensmodel. Het gegevensmodel en de hierin opgenomen gegevens worden beoordeeld op basis van de in onderstaande tabel opgenomen kwaliteitseisen.

Tabel 6.4 – Eisen aan gegevenskwaliteit (Lee, Strong, Kahn, & Wang, 2002)

Kwaliteitseisen	Uitwerking
Consistentie	De mate waarin het gegevensmodel vrij is van innerlijke tegenspraak in inhoud en verschijning.
Geschiktheid	De mate waarin het gegevensmodel voor een specifiek doel gebruikt kan worden.
Bruikbaarheid	De mate waarin het gegevensmodel aan de gebruikersbehoeften voldoet.
Herbruikbaarheid	De mate waarin de gegevens ook voor nieuwe situaties gehanteerd kunnen worden.
Uitbreidbaarheid	De mate waarin constructies kunnen worden toegevoegd aan het gegevensmodel.
Redundantie	De mate waarin redundante gegevens afwezig zijn in het gegevensmodel.
Compliance met best practices	De mate waarin het gegevensmodel overeenkomt met de normen en regels die goede praktijken stellen.
Volledigheid	De mate waarin er geen gegevens ontbreken in het gegevensmodel.
Relevantie	De mate waarin gegevens voor een specifieke situatie van toepassing zijn.
Interpreteerbaarheid	De mate waarin de symbolen, eenheden en definities, waarin de gegevens zijn uitgedrukt, duidelijk zijn.
Valideerbaarheid	De mate waarin de kwaliteit van gegevens aantoonbaar gemaakt kan worden.
Beknoptheid	De mate waarin de gegevens in het gegevensmodel in een compacte vorm zijn vertegenwoordigd.
Begrijpbaarheid	De mate waarin de gegevens en het gegevensmodel eenvoudig zijn te begrijpen.
Toegankelijkheid	De mate waarin gegevens snel en eenvoudig zijn te verkrijgen.
Afdwingbaarheid van business rules	De mate waarin het gegevensmodel de regels weergeeft en afdwingt die van toepassing zijn op de gegevens.
Flexibiliteit	De mate waarin de gegevens en het gegevensmodel kunnen omgaan met wijzigingen in de informatie-eisen
Stabiliteit	De mate waarin het gegevensmodel gedurende een langere periode dezelfde uitgangspunten voor modellering hanteert.
Elegantie	De mate waarin het gegevensmodel een nette en eenvoudige classificatie hanteert van de gegevens.
Communiceerbaarheid	De mate waarin de gegevens effectief en efficiënt binnen een keten gecommuniceerd kunnen worden.
Integreerbaarheid	De mate waarin het gegevensmodel geïntegreerd kan worden met andere gegevensmodellen, zoals IFRS.
Compromis	De mate waarin het gegevensmodel rekening houdt met de afwijkende belangen van verschillende betrokken partijen.
Normalisatie	De mate waarin de gegevens in het gegevensmodel genormaliseerd zijn.
Representeerbaarheid	De mate waarin de gegevens een representatie zijn van de van toepassing zijnde wet- en regelgeving.

De eisen in tabel 6.4 zijn enerzijds bedoeld als een checklist bij het modelleren van gegevens en anderzijds als criteria waaraan het gegevensmodel dient te worden getoetst. Hoewel het raamwerk zelf geen normen biedt, kunnen de opgenoemde kwaliteitsdimensies worden gebruikt voor het formuleren van kwaliteitseisen.

De semantische kwaliteitseisen worden veelal beoordeeld door domeinexperts. Deze experts hebben de vereiste kennis en ervaring om de taxonomie voor een specifiek domein van inhoudelijke opmerkingen te voorzien. In veel gevallen gebeurt dit op basis van een eerste concept versie van de taxonomie (Piechocki en Felden, 2007).

6.4.10.2 Syntactische kwaliteitseisen

De syntactische kwaliteitseisen richten zich op de juiste (technische) toepassing van de gehanteerde syntax. Hiertoe worden diverse testwerkzaamheden uitgevoerd om vast te stellen of er geen technische onjuistheden bestaan. In het geval van SBR, waarbij XBRL als syntax is gekozen, zijn er verschillende niveaus van technische testactiviteiten te onderkennen. De eerste laag betreft de controle of de taxonomie zowel 'XML well-formed' is en voldoet aan de eisen van XML Schema. De daarop volgende laag vereist dat de taxonomie voldoet aan de eisen van de XBRL 2.1 specificatie en eventuele aanvullende XBRL specificaties.

Wanneer een taxonomie zowel XML als XBRL valide is wordt de verdieping gemaakt naar de compliance met de architectuurregels. Zoals in § 6.4.5 besproken zijn er binnen SBR voor wat betreft de architectuur eveneens twee niveaus te onderkennen: de compliance met de FRTA regels en de compliance met de NTA regels. In het kader van SBR worden de NTA regels actueler en relevanter geacht dan de FRTA regels. De compliance van de taxonomie met zowel de FRTA als de NTA wordt (grotendeels) geautomatiseerd gecontroleerd. Alle XBRL tooling heeft in principe de FRTA eisen ingebouwd, waardoor dit eenvoudig gecontroleerd kan worden. Het SBR Programma heeft custom tooling laten ontwikkelen waarmee de meeste van de honderden regels die opgenomen zijn in de NTA geautomatiseerd gecontroleerd kunnen worden. Elke versie van een deeltaxonomie zal in de testfase door deze tooling worden gehaald om de compliance met de architectuurregels te beoordelen. Door de grote hoeveelheid regels, noodzakelijk om de vrijheidsgraden in te perken, is dit simpelweg niet handmatig te realiseren. De uitkomsten van deze testen worden geëvalueerd en onjuistheden in de syntactische verwerking van de taxonomie waar nodig verholpen.

6.4.10.3 Externe testactiviteiten

Het consulteren van belanghebbende marktpartijen is een internationaal veelgebruikte methode om de kwaliteit van de taxonomie te testen. Dit heeft in de begindagen veel bijgedragen aan de kwaliteit van taxonomieën, zowel op semantisch als syntactisch gebied. De afgelopen jaren is echter duidelijk geworden dat (onbezoldigde) marktconsultatie alleen onvoldoende is om een hoge kwaliteit van een taxonomie te garanderen. De hoeveelheid reacties blijft vaak beperkt tot die van een aantal voorlopers. En wanneer marktpartijen reageren richten ze zich logischerwijs op onderdelen die voor hen van toepassing zijn. Hierdoor zal vrijwel nooit de volledige taxonomie in detail gecontroleerd worden door deze marktpartijen. Het actief bena-

deren van specifieke koepelorganisaties om mee te werken aan een dergelijke controle zorgt op zich voor een hogere mate van kwaliteit van de taxonomie, maar dit is primair gericht op de semantiek.

De controle op een juiste toepassing van de syntax is de afgelopen jaren lastiger geworden. De gehanteerde technieken zijn complexer geworden en de personen met voldoende XBRL kennis om dit te beoordelen zijn beperkt. Bovendien zijn er de afgelopen jaren internationaal veel meer XBRL taxonomieën bijgekomen, waardoor de input vanuit deze experts op het openbare (onbezoldigde) verzoek tot commentaar vrijwel nihil is. Het is daarom van groot belang om de juiste technische experts beschikbaar te hebben bij de constructie van een taxonomie.

6.4.10.4 Testen van de Nederlandse Taxonomie

De testfase bij SBR is vergelijkbaar met hetgeen in de voorgaande paragrafen is beschreven. Indien de conceptversie van de NT door de interne validatiewerkzaamheden heen komt, wordt deze versie per domein, samen met de eerder genoemde gezamenlijke begrippen, als alfa-versie uitgebracht. Er worden dus meerdere alfa-versies uitgebracht, minimaal één voor elk van de domeinen. De alfa-versie wordt gepubliceerd op de SBR website ter consultatie door marktpartijen.

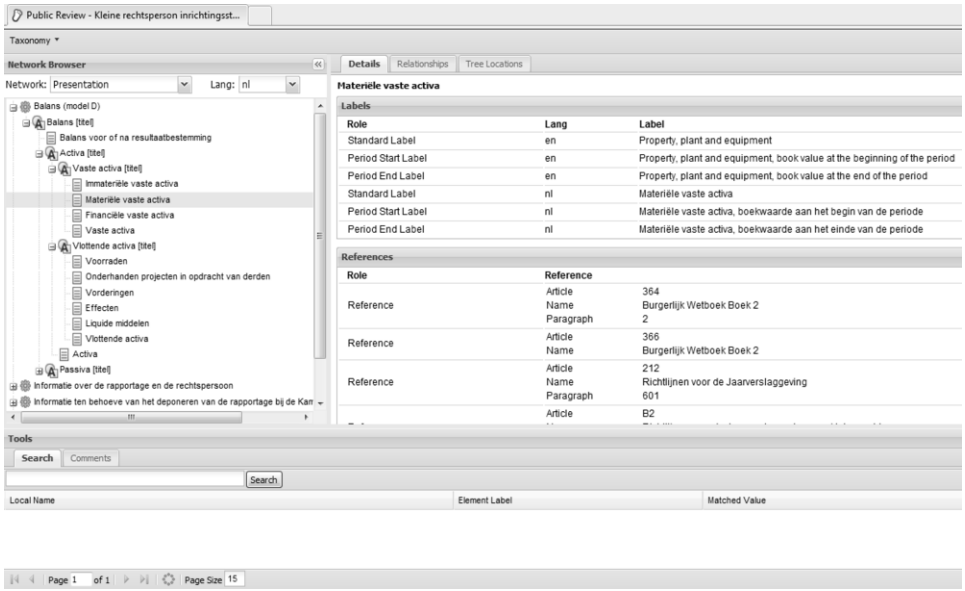
Op basis van commentaar van marktpartijen stellen de verschillende uitvragende partijen een bèta-versie van hun deeltaxonomie beschikbaar aan het SBR Programma. Deze verschillende deeltaxonomieën worden nu samengevoegd tot één geheel: de Nederlandse Taxonomie. Deze versie staat bekend als de bèta-versie en wordt eveneens gepubliceerd op de SBR website ten behoeve van marktconsultatie.

Eventuele reacties en commentaren op de bèta-versie van de NT worden door de uitvragende partijen meegenomen in de definitieve versie, die jaarlijks verschijnt. Het proces van de totstandkoming van een definitieve versie van de NT is vergelijkbaar met die van een bèta versie.

6.4.11 *Publicatiefase*

In de publicatie fase worden de informatiebehoeften van een uitvragende partij, zoals in gestructureerde vorm opgenomen in een taxonomie, gecommuniceerd aan marktpartijen. De taxonomie zelf is een technische verzameling van bestanden, die op verschillende manieren beschikbaar gemaakt kunnen worden aan de relevante (markt)partijen. In het geval van SBR wordt op de publicatiedatum de NT op drie manieren beschikbaar gesteld, namelijk als een .zip bestand op de SBR website, als direct benaderbare taxonomie op nltaxonomie.nl en via een taxonomie viewing tool (zie kader). De meest praktische manier om de structuur en opzet van de taxonomie te begrijpen, is om door de taxonomie te navigeren met behulp van een tool die XBRL begrijpt en een raadpleeg-functionaliteit bezit. Voor het gebruik van de taxonomie door rapporteurs is meestal geen speciale XBRL software noodzakelijk. Zij worden geholpen door hun eigen administratiesoftware, die op de achtergrond de taxonomie laadt en hen in staat stelt de mapping aan te brengen tussen de begrippen van de uitvragende partij en de begrippen zoals zij die zelf in hun administratie voeren.

Taxonomie viewing tool
Voor het bekijken van de NT heeft het SBR Programma een taxonomie viewing tool beschikbaar gesteld. Yeti is een taxonomie viewing tool die de mogelijkheid biedt om taxonomieën te bekijken. De taxonomie viewing tool biedt de functionaliteit om per rapportage van de aanwezige informatiebehoeften de datatypes, labels, referenties en overige eigenschappen te bekijken.



Figuur 6.9 – Screenshot van de taxonomie viewing tool

Bij elke publicatie van een taxonomie wordt aanvullende informatie aangeleverd. De partijen die een taxonomie uitbrengen, hebben veel vrijheid in de mate waarin zij deze aanvullende documentatie beschikbaar stellen. Het SBR Programma is van mening dat elke release van een taxonomie vergezeld dient te gaan van release notes, FRIS documentatie, versioning informatie, voorbeeld instance documenten en een handleiding voor het opstellen van een instance document. Het SBR Programma ziet het uitbrengen van deze aanvullende documenten als een best practice bepaling, omdat dit een wijze is waarop verschillende gebruikers bekend gemaakt kunnen worden met de opzet en structuur van de taxonomie, evenals met mogelijke wijzigingen hierin. De partijen die belang hebben bij de rapportages in de NT variëren enorm. Het gaat onder meer om de rapporterende organisaties, accountants, fiscalisten en softwareleveranciers. Het is dus van belang dat de taxonomie voor al deze partijen duidelijk is, waardoor veel aanvullende documenten noodzakelijk zijn. De te onderscheiden aanvullende documenten worden hieronder kort besproken.

Release notes
De release notes bevatten de belangrijkste architectuur en inhoudelijke verschillen tussen de voorgaande versie van de taxonomie en de huidige versie. In het geval van

de NT wordt altijd een vergelijking getrokken tussen de nieuwe en de laatste definitieve versie van de taxonomie. In de release notes wordt tekstueel een korte opsomming gegeven van welke wijzigingen de taxonomie heeft ondergaan, zodat de gebruikers zich hier een beeld van kunnen vormen.

FRIS documenten
Een FRIS (Financial Reporting Instance Standards) document beschrijft de eisen waaraan de XBRL instance documenten moeten voldoen. Dit zijn dus niet-technische regels die bepalen of een instance document valide is. Een voorbeeld kan zijn dat er minimaal drie contexten opgenomen dienen te zijn in een instance document. Eisen aan een instance document kunnen niet altijd geïntegreerd worden in de taxonomie. Zodoende worden deze eisen als aanvullende documenten in PDF formaat gepubliceerd bij de taxonomie. De documenten zijn zodanig opgezet dat de paragrafen overeenkomen met de paragrafen uit de Financial Reporting Instance Standards 1.0 van XBRL International.

In het geval van de NT zijn er meerdere FRIS documenten te vinden. Zo is er een overkoepelend FRIS document, dat de eisen aan de instance documenten bevat die voor alle domeinen van toepassing zijn. Daarnaast heeft elk domein ook een eigen FRIS document om invulling te geven aan een aantal specifieke situaties dat uitsluitend voor het betreffende domein van toepassing is. Het SBR Programma heeft de intentie om de FRIS regels zo beperkt als mogelijk te houden, aangezien het handmatige activiteiten vereist van de partijen die deze regels willen inbouwen. In 2012 wordt geëxperimenteerd met de FRIS regels, om ze, voor zover als mogelijk, beschikbaar te maken als XBRL formules. Deze formules zijn executeerbaar en kunnen meegeleverd worden met de NT, zodat software ontwikkelaars de controles kunnen aanroepen en niet zelf hoeven te programmeren. Het FRIS document zelf zal de beschrijving van deze regels blijven vastleggen.

Versioning informatie
Versioning informatie is de vastlegging van de inhoudelijke verschillen tussen twee versies van een rapportage in de taxonomie. Deze informatie kan op twee manieren verstrekt worden. Ten eerste op een gestructureerde en door computers leesbare manier conform een specificatie van XBRL International en ten tweede in een voor de mens leesbare versie.

Voorbeeld instance documenten
Het beschikbaar stellen van voorbeeld instance documenten geeft de gebruikers een beeld van hoe een instance document eruit moet zien om te voldoen aan de eisen die in de taxonomie gesteld worden. Hierbij dient benadrukt te worden dat voorbeeld instance documenten alleen voorbeelden zijn en dus geen generieke templates, die 'hardcoded' door softwareleveranciers dienen te worden ingebouwd. Bij de NT worden voor elke rapportage voorbeeld instance documenten beschikbaar gesteld. Deze voorbeelden worden als aanvullende documentatie opgenomen op de SBR website. Voorbeeld instance documenten zijn functioneel en technisch valide instance documenten. Dit in tegenstelling tot test instance documenten die (bewust) foutieve situaties kunnen bevatten om foutmeldingen te genereren. Er worden geen test instance documenten aan de markt ter beschikking gesteld.

Handleiding voor de creatie van instance documenten
Voor gebruikers die een beperkte mate van ervaring hebben met XBRL wordt een domein specifieke handleiding beschikbaar gesteld die ingaat op de wijze waarop instance documenten voor het betreffende domein gecreëerd dienen te worden. Vanaf het jaar 2011 is bij het SBR Programma een handleiding beschikbaar gesteld, voor de creatie van rapportages in het jaarverslaggevingsdomein. In deze handleiding wordt een diversiteit aan onderwerpen uiteengezet waarmee een gebruiker te maken kan krijgen bij het opstellen van een rapportage. Het SBR Programma streeft ernaar om voor elke domein zo duidelijk mogelijk toe te lichten hoe een instance document gecreëerd dient te worden.

Gegevensadministratie
Vanuit het oogpunt van zowel uniformiteit als kwaliteit is het beter om taxonomieën te genereren vanuit een gegevensadministratie dan om dit handmatig met toepassing van specifieke software of tekst editors te realiseren. In de gegevensadministratie is een semantische gegevensverzameling opgenomen, waarbij de rapportagebegrippen, voorzien van definities, referenties en andere relevante bronnen evenals hun onderlinge relaties, zijn opgenomen. De gegevensadministratie dient, naast het ondersteunen van een semantische gegevensverzameling en de gewenste syntax, ook een nauwgezette en transparante werkwijze te hebben voor het aanbrengen van mutaties. Deze werkwijze zal ondersteund moeten worden door een workflow component, waarbij alleen geautoriseerde gebruikers wijzigingen kunnen aanbrengen en alle wijzigingen in detail gelogd worden. Dit is ook van belang om het proces van de totstandkoming van een taxonomie te kunnen auditen.

De eenmalige creatie van een taxonomie en de bijbehorende validatieregels vormen slechts een eerste stap in een groter proces. Daarna komen de taxonomie en de validatieregels terecht in een beheerproces. Hierbij zal een taxonomie periodiek, veelal jaarlijks, aangepast moeten worden om de laatste wijzigingen in wet- en regelgeving te reflecteren of door de introductie van nieuwe XBRL technieken in de taxonomie. Om dit mogelijk te maken is het van belang dat een goede gegevensadministratie bijgehouden wordt, waarin zowel de semantische als syntactische aspecten van de taxonomie worden onderhouden.

6.4.12 *Onderhoudsfase*

Het onderhouden van een taxonomie betreft de activiteiten die plaatsvinden na de publicatie van de betreffende versie van een taxonomie. Deze activiteiten staan ook wel bekend als 'toepassingsondersteuning', oftewel het beantwoorden van vragen en het beoordelen van meldingen omtrent potentiële onjuistheden die naar aanleiding van deze taxonomie ontvangen worden.

Vragen en opmerkingen dienen geregistreerd te worden en van een formele reactie te worden voorzien. De meldingen omtrent potentiële onjuistheden dienen te worden geëvalueerd door de 1e, 2e of 3e lijns ondersteuning. Hierbij zullen de domeinexpert en de technisch expert vaak als 3e lijns ondersteuning functioneren. Over het algemeen kunnen meldingen omtrent potentiële onjuistheden leiden tot vier scenario's:

1. Onterechte melding, geen verdere acties.

2. Terechte melding, verwerken in eerstvolgende versie van de taxonomie.
3. Terechte melding, zo snel mogelijk verhelpen met een quick-fix.
4. Terechte melding, zo snel mogelijk verhelpen met een nieuwe versie.

Hierbij definiëren we de quick-fix als een praktische oplossing wanneer er slechts een enkel bestand in de taxonomie een belangrijke onjuistheid bevat. Omdat het slechts een enkel bestand betreft wordt uitsluitend het betreffende bestand vervangen in de taxonomie. Wanneer meerdere bestanden belangrijke onjuistheden bevatten dient echter een nieuwe versie van de taxonomie te worden gepubliceerd.

De output van de activiteiten in de onderhoudsfase is een registratie met (afgewikkelde) vragen en/of meldingen, een groslijst met aanpassingen voor de eerstvolgende versie van de taxonomie en eventueel de uitgebrachte quick fixes of nieuwe versies van een taxonomie. Het einde van de onderhoudsfase wordt bereikt wanneer alle rapportages in een taxonomie niet langer in productie draaien voor de uitwisseling van gegevens.

6.4.13 *Relevante ontwikkelingen rond gegevens*

Op het gebied van gegevens spelen er twee relevante ontwikkelingen die gericht zijn op het valideren van ontvangen verantwoordingen en het kunnen renderen of weergeven van de gegevensfeiten in instance documenten. Beide ontwikkelingen worden hieronder nader uiteengezet.

6.4.13.1 Valideren van ontvangen verantwoordingen

De rapporterende organisaties sturen hun verantwoordingen in naar uitvragende partijen op basis van de informatiebehoeften zoals opgenomen in de taxonomie. De gedachte achter SBR is dat de informatie system-to-system uitgewisseld en verwerkt kan worden, zonder handmatige tussenkomst. Concreet wordt hiermee bedoeld dat de door de aanleverende partij geautomatiseerd opgestelde rapportage op een veilige wijze verstuurd wordt naar de uitvragende partij, alwaar de verwerking in de achterliggende systemen ook geautomatiseerd plaatsvindt. Het is hierbij uiteraard van cruciaal belang dat de uitvragende partij de gegevens uit de verantwoording valideert ten opzichte van de verschillende eisen die aan de gegevens gesteld kunnen worden, alvorens de gegevens verwerken wordt door de achterliggende informatiesystemen. Het uitvoeren van validatieregels verhoogt de waarde van informatie en leidt dus tot informatie die geschikter is voor het beoogde doel, een betere kwaliteit.

Het is voor de rapporterende organisatie van belang dat fouten in een zo vroeg mogelijk stadium ontdekt worden. Er zijn drie niveaus beschikbaar om validatieroutines uit te voeren: bij de verzender (en/of de rapporteur indien dit niet dezelfde organisatie is), in de gedeelde procesinfrastructuur (Digipoort) (zie de beschrijving van de validatieservice in hoofdstuk 7) en bij de betreffende uitvragende partij. Tevens spelen, bij zowel zender als ontvanger, nog mogelijkheden van het aanbrengen van meerdere niveaus van validatie. Denk hierbij aan een validatie direct bij het zenden of ontvangen, of op een ander moment, indien er een combinatie met gegevens uit de back office plaatsvindt.

Het uitvoeren van een validatieslag is noodzakelijk, omdat een uitvragende partij zich ervan wil verzekeren dat de aanleverende partij zich inderdaad aan de eisen heeft gehouden die de uitvragende partij gesteld heeft. Bovendien wil de aanleverende partij de bevestiging dat zijn inzending geaccepteerd is, zodat hij aan zijn (wettelijke) verplichtingen heeft voldaan. Hierbij speelt validatie een belangrijke rol. De verschillende validatieslagen die te onderkennen zijn binnen het SBR Programma, zijn als volgt:

1. Validatie of de verantwoording XML well-formed is.
2. Validatie of de verantwoording voldoet aan de XML schema specificatie.
3. Validatie of de verantwoording voldoet aan de XBRL 2.1 specificatie.
4. Validatie of de verantwoording voldoet aan de XBRL Dimensions 1.0 specificatie.
5. Validatie of de verantwoording voldoet aan de internationale FRIS regels.
6. Validatie of de verantwoording voldoet aan de NL-FRIS regels.
7. Validatie of de verantwoording voldoet aan de domein-FRIS regels.
8. Validatie of de verantwoording voldoet aan de rapportage specifieke domein-FRIS regels.
9. Validatie of de verantwoording voldoet aan de consistentie regels (business rules).

Bovenstaande lijst bevat de verschillende lagen waarop validatie routines plaatsvinden in SBR verband. De eerste lagen richten zich op de technische compliance met de relevante standaard en hebben als doel om vast te stellen of een taxonomie 'XML well-formed' is en voldoet aan de technische eisen van XML schema. De volgende lagen gaan nader in op de technische eisen die XBRL stelt. Zo dient de taxonomie te voldoen aan de technische eisen van de XBRL 2.1 specificatie. Wanneer dimensionele structuren in de taxonomie verwerkt zijn dient de taxonomie ook compliant te zijn met de XBRL Dimensional Taxonomies 1.0 (XDT) specificatie. Dit is feitelijk een technische validatieslag om te voldoen aan de syntactische kwaliteitseisen van § 6.4.10.2. De volgende lagen hebben betrekking op de juiste toepassing van FRIS regels op verschillende niveaus, namelijk op NT niveau, op domein niveau of op entrypoint (rapportage) niveau. Tenslotte zijn ook nog consistentie controles te identificeren. Dit zijn veelal validatieslagen die voortvloeien uit semantische eisen en richten zich op de juistheid, volledigheid en nauwkeurigheid van de documentinhoud.

Validatieregels kunnen in verschillende formaten geprogrammeerd worden, maar het is aan te bevelen om ook dit op basis van een open standaard te ontwikkelen. XBRL kent sinds 2009 ook een specificatie voor het inrichten van validatieroutines, namelijk XBRL Formulas. Deze open standaard voor het creëren van validatieregels richt zich volledig op het werken met taxonomieën en instance documenten. Het biedt de mogelijkheid om de inhoud van instance documenten te controleren op bepaalde aspecten die te achterhalen zijn uit zowel de instance als uit de betreffende taxonomie. Het is derhalve de beste keuze om validatieregels te creëren die van toepassing zijn bij het valideren van een instance document op basis van een bestaande taxonomie.

6.4.13.2 Rendering van instance documenten

Het renderen van instance documenten op een wijze die overeenkomt met het papieren equivalent, is de afgelopen jaren vrij lastig geweest. Deze situatie is opmerkelijk, omdat hier wel degelijk behoefte aan is bij marktpartijen. In de beginjaren van XBRL, waarin alleen de XBRL 2.1 specificatie beschikbaar was, konden met behulp van de presentation linkbase de presentatierelaties in ouder-kind relaties weergegeven worden. Hiermee konden de begrippen in verantwoordingen in een gewenste volgorde worden geplaatst, die vervolgens gebruikt werd voor de weergave van de rapportage. Voor eenvoudige verantwoordingen is er geen probleem, maar voor complexere verantwoordingen wel.

De invoering van XBRL Dimensions 1.0 heeft het gebruik van (multi-) dimensionele structuren in de taxonomie mogelijk gemaakt. Hierdoor kunnen ook tabellen worden opgenomen in een taxonomie. Het weergeven van deze tabellen bleek echter een probleem, omdat de presentation linkbase het weergeven van dimensionele structuren niet ondersteunt. Hiervoor werd bij sommige projecten de keuze gemaakt om met maatwerk oplossingen de rendering van instance documenten en taxonomieën te realiseren.

Voor het renderen van een instance document kwam in 2011 ook de Inline XBRL specificatie beschikbaar. Inline XBRL combineert de presentatiemogelijkheden van HTML met de communicatiekracht van XBRL. Deze specificatie biedt echter ook de mogelijkheid om gegevens weer te geven die niet in XBRL formaat beschikbaar zijn. Hierdoor ontstaat de mogelijkheid dat gegevens die niet geautomatiseerd verwerkt kunnen worden, aan mensen worden getoond. Dit is dan ook een reden waardoor Inline XBRL voor veel uitvragende partijen geen aantrekkelijke optie is.

Naar verwachting zal in 2014 de table linkbase specificatie worden gepubliceerd. Dit is de belangrijkste ontwikkeling op dit gebied. De table linkbase maakt het mogelijk om op een gestandaardiseerde wijze weergaven te genereren van de begrippen die opgenomen zijn in een XBRL taxonomie. Hierbij worden nadrukkelijk (multi-)dimensionele structuren gefaciliteerd, zodat tabellen daadwerkelijk kunnen worden gepresenteerd.

6.5 Afsluiting

Het doel van dit hoofdstuk is om, conform enkele uitgangspunten, het bouwblok van de SBR-oplossing, berichtspecificaties, en de bijbehorende afspraken en standaarden, grondig te beschrijven. De structuur van dit hoofdstuk volgt dit doel. In de uitwerking hebben we rekening gehouden met de interesses van zowel 'beginners' als deskundigen (gegevensexperts), waardoor dit hoofdstuk veel pagina's in beslag neemt. Dit blijkt ook nodig om een integrale beschouwing (van behoefte en invulling tot en met ontwikkelingen) te bieden op het thema gegevens in informatieketens. Hierbij zijn onder andere communicatiebehoeften, standaardisatie van syntax en semantiek, eisen uit de wetgeving, perspectieven (bijvoorbeeld communicatie en presentatie) en fasen in taxonomie ontwikkeling aan bod gekomen. In het geheel heeft XBRL als standaard veel aandacht gekregen. XBRL maakt het mogelijk om de gewenste semantische standaardisatie te realiseren, zodat het mogelijk is om eenduidig

gegevens te definiëren. We zien steeds meer literatuur over XBRL opduiken. Het accent ligt meestal echter op de mogelijkheden die XBRL schept voor de standaardisatie van syntax en semantiek. De bijdrage van dit hoofdstuk ligt in een concrete beschrijving van de daadwerkelijke toepassing van XBRL in informatieketens. Dit schept een ander licht op de mogelijkheden, maar ook op de inspanningen die nodig zijn om de voordelen van XBRL te kunnen plukken. Duidelijk is dat XBRL een belangrijke rol speelt in system-to-system uitwisseling en verwerking van verantwoordingsinformatie.

Het belang van deze rol zal de komende jaren toenemen. Pinsker (2003) noemt XBRL zelfs een 'sleeping giant', die de komende jaren de verantwoordingswereld en informatieketens verregaand zal transformeren. SBR is slechts één voorbeeld van een dergelijke transformatie. Wat we vanuit een onderzoeksperspectief willen meegeven is dat, gezien de recente, relatief grootschalige toepassing van XBRL in keteninformatiesystemen, de literatuur nog blinde vlekken kent die nader onderzoek vereisen. Voorbeelden zijn de condities voor de effectieve toepassing van specificaties als Inline XBRL en dimensions, en succesfactoren voor de multi-domein toepassing van XBRL (bijvoorbeeld in zorg- en onderwijsketens). SBR biedt een empirische omgeving, waarin dergelijke vragen kunnen worden onderzocht.

7 Technische inrichting SBR

7.1 Inleiding

Dit hoofdstuk bevat een verdieping op de techniek achter de generieke procesinfrastructuur die bij SBR wordt gebruikt.

Als we in de context van informatieketens spreken over techniek, hebben we het feitelijk over 'Informatie Technologie' (IT). Nu beslaat IT een zeer breed domein en zelfs wanneer er een specifiek perspectief gekozen wordt – bijvoorbeeld SBR – is het onmogelijk in één boek – laat staan in één hoofdstuk – alle relevante IT uit te diepen. Dat is mede dankzij technische standaarden en gestandaardiseerde berichtspecificaties, waardoor partijen niet aangewezen zijn op een exclusief ontwikkelplatform. Dit maakt het aantal voorkomende technische implementaties in de SBR-keten groot. Maar zelfs als de ontwikkelaars in de SBR-keten zeer uniform te werk zouden gaan, zouden wij bij het nastreven van volledigheid verdrinken in een stroom van toelichtingen en specificaties. Alleen al over de implementatie van SSL/TLS (cryptografie protocol voor beveiligde communicatie over het internet) zijn legio titels verschenen. We moeten daarom keuzes maken in wat we behandelen. Als leidraad hebben wij hiervoor onszelf het volgende uitgangspunt opgelegd:

- Het hoofdstuk moet dieper inzicht geven in juist die technologische ontwikkelingen die de achtergrond vormen voor de keuzes ten aanzien van technologie, zoals die bij SBR zijn gemaakt.
- Het hoofdstuk moet inzicht geven in de invulling van deze keuzes door middel van de generieke procesinfrastructuur (Digipoort).

Zelfs met deze scope zullen we nog een beetje vals moeten spelen om de hoeveelheid inhoud enigszins beperkt te houden. We richten ons op het gebruik van een generieke procesinfrastructuur voor S2S-integratie in verantwoordingsketens. De term procesinfrastructuur verwijst naar het geheel van middelen zoals hardware, software en netwerkapparatuur, inclusief beveiliging, dat nodig is voor de geautomatiseerde afhandeling van i-processen in kader van het elektronisch berichtenverkeer tussen aanleverende en uitvragende partijen. De toevoeging 'generiek' betekent hier: voor meerdere toepassingen te gebruiken. De toevoeging ‘gedeelde’ betekend hier: door meerdere partijen te gebruiken.

We beginnen met verschillende scenario’s voor S2S-integratie in informatieketens om wat meer inzicht te geven in welke alternatieve wegen níet zijn gekozen bij SBR (§ 7.2). Vervolgens gaan we dieper in op de relevante technologie die nodig is voor een generieke procesinfrastructuur (§ 7.3). Tenslotte leggen we uit hoe daar in de vorm van Digipoort, de gerealiseerde generieke procesinfrastructuur bij SBR, invulling aan is gegeven (§ 7.4). We beschrijven de karakteristieken van Digipoort en de twee bouwblokken van de SBR-oplossing die het omvat: de koppelvlakservices en verwerkingsservices. Een en ander is vastgelegd in en conform de technische standaarden voor SBR (onderdeel van het afsprakenstelsel).

Gezien de samenhang en afhankelijkheid tussen de bouwblokken van de SBR oplossing is het onvermijdelijk, dat we de lezer in sommige gevallen zullen doorverwijzen naar datgene wat in de voorgaande hoofdstukken is behandeld.

Als ‘verdieping in de techniek achter SBR’ is het onvermijdelijk dat in dit hoofdstuk een relatief groot aantal begrippen wordt gehanteerd. Deze worden weliswaar toegelicht, maar voor een bredere uiteenzetting moet toch worden verwezen naar de daarvoor geëigende, specifieke boekwerken. Deze zijn aan het eind van dit hoofdstuk opgesomd.

7.2 Welke technische inrichting past bij SBR?

7.2.1 *Scenario’s voor inrichting van de techniek*

Het eerste deel van dit hoofdstuk behandelt de theoretische mogelijkheden ten aanzien van de technologie die voor het SBR Programma ingezet hadden kunnen worden. Het doel van het SBR Programma en de projecten waar dit programma uit voortkwam, was een generieke overheidsoplossing voor system-to-system (S2S) uitwisseling en gedeelde verwerking van verantwoordingsinformatie te realiseren. De vraag was hoe daar te komen vanuit een situatie waarin de partijen allemaal hun eigen applicaties, datamodellen en bedrijfsprocessen hanteren. We hebben in de voorgaande hoofdstukken gezien hoe gestandaardiseerde i-processen (hoofdstuk 5) en de gekozen gegevensstandaard en berichtspecificaties (hoofdstuk 6) bijdragen aan dit doel. Deze paragraaf behandelt de vorm van technologie, ofwel de infrastructuur die, gelet op dit specifieke doel, onderdeel van de SBR oplossing kan zijn.

Redenerend vanuit de uitvragende partijen zijn er vier scenario’s voor gestructureerde elektronisch berichtenuitwisseling denkbaar, namelijk:

- Scenario A: Traditioneel/heterogene procesinfrastructuren: eigen koppelvlakken, eigen procesinfrastructuur (voor uitvragende partijen).
- Scenario B: Eigen procesinfrastructuur: gestandaardiseerde koppelvlakken, eigen procesinfrastructuur.
- Scenario C: Concern-procesinfrastructuur: gestandaardiseerde koppelvlakken, gestandaardiseerde procesinfrastructuur.
- Scenario D: Gedeelde dienstverlener: gestandaardiseerde koppelvlakken, generieke procesinfrastructuur.

Deze scenario's zijn opgesteld langs twee dimensies: de vorm van de koppelvlakken en de vorm van de procesinfrastructuur. Een koppelvlak (interface) is de daadwerkelijke invulling van een set van afspraken en standaarden die de uitwisseling van gegevens tussen informatiesystemen verzorgt. De procesinfrastructuur analogie wordt gebruikt om een stelsel van functionaliteiten aan te duiden, dat nodig is voor het geautomatiseerd afhandelen (sorteren, initiële controles, verspreiden) van berichten. Om de aandacht bij de scenario's te houden, worden beide concepten hier nog als 'black box' behandeld. In § 7.3 worden ze verder ontleed. Hieronder worden de vier scenario's verder uitgewerkt. We geven eerst een overzicht van de scenario's en staan daarna pas stil bij de voor- en nadelen per scenario. We sluiten af met een tabel waarin de overeenkomsten en verschillen worden samengevat.

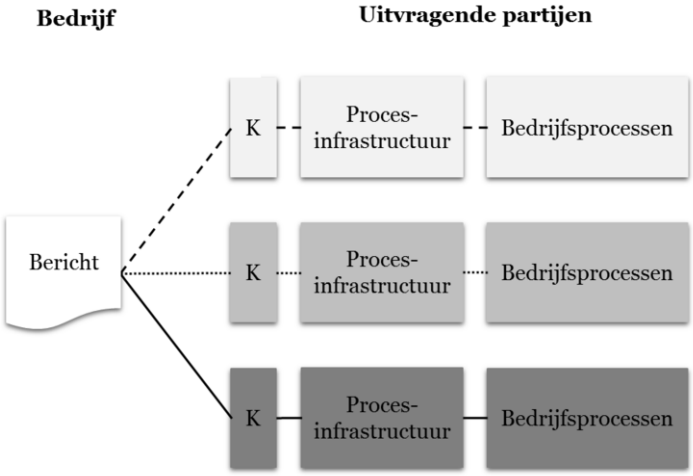
Scenario A: Traditioneel/heterogene procesinfrastructuren (niet gestandaardiseerde koppelvlakken en eigen procesinfrastructuur)

In dit scenario heeft iedere uitvragende partij zijn eigen 'modaliteit'. Dit betekent dat partijen zoals de Belastingdienst, het CBS en de KvK op hun eigen manier definiëren hoe een bedrijf een verbinding kan leggen, ook wel koppelvlak genoemd. Daarnaast hebben deze partijen elk een eigen digitale proces-infrastructuur waarin het aangeleverde bericht wordt 'verwerkt'. Voor het gemak verstaan we hier onder verwerking dat de identiteit van de afzender wordt gecontroleerd (authenticatie), dat het bericht wordt gevalideerd (klopt de syntax?) en wordt doorgestuurd als input voor een business proces. Pas daarna wordt naar de inhoud gekeken. Dit scenario

Het traditionele scenario

Het traditionele scenario gaat uit van de volgende beginsituatie: partijen zoals de KvK, het CBS en de Belastingdienst vragen ieder op hun eigen wijze informatie uit bij bedrijven, waarbij de wettelijke taak en eigen processen leidend zijn. De uitwisseling tussen bedrijven en uitvragende partijen verschilt m.b.t. inhoud (eisen aan gegevens), processen (procedures voor samenstelling en verwerking van de inhoud) en vorm (technisch aanleveren van gegevens). Voldoen aan de verantwoordingsverplichting vergt van elke verantwoordende partij bepaalde IT en organisatie, die bij een verandering in de verantwoordingsplicht moeten worden aangepast. Een bedrijf dat aan de verantwoordingsverplichting wil voldoen, moet o.a. het juiste formulier/formaat voor uitvraag selecteren, de relevante data uit verschillende administratieve databronnen met de vraag matchen, de juiste data aanleveren in een specifiek formaat en via de daarvoor aangewezen 'technische modaliteit'. Ook de wijze waarop de aanleverende partij feedback krijgt op het proces, verschilt per uitvragende partij. Dit is een *point-to-point* manier van informatie-uitwisseling.

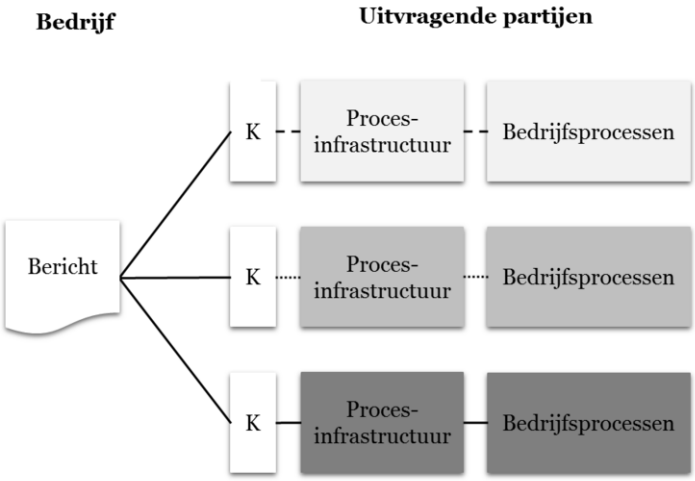
wordt vereenvoudigd afgebeeld in figuur 7.1. We zeggen bewust vereenvoudigd, omdat de interacties rondom het standaardiseren van gegevens (XBRL en NT) niet worden afgebeeld.



Figuur 7.1 – Huidige situatie: eigen koppelvlakken (K), eigen digitale procesinfrastructuur (Scenario A)

Bovenstaande figuur laat een heterogeniteit in koppelvlakken, digitale procesinfrastructuren en bedrijfsprocessen zien. Om vanuit één bronadministratie meerdere partijen te kunnen bedienen, moeten er meerdere technische uitwisselingsstandaarden en verschillende vormen van authenticatie en machtiging geïmplementeerd worden. Toegesneden op de verantwoordingsketens zou je het volgende beeld zien: in de softwaremarkt bestaan niches en modules die de verkokering in de wetgeving volgen. Zo zijn er administratiepakketten die een koppeling onderhouden voor de OB aangifte. Je hebt rapportagesoftware die gebruikt kan worden om de VPB aangifte op te stellen of de jaarrekening te genereren. Voor de Belastingdienststromen is het BAPI-kanaal beschikbaar, waarmee geautomatiseerde consistentiecontroles uitgevoerd kunnen worden. Jaarrekeningen worden meestal per post of in PDF verzonden. Er zijn meerdere koppelvlakken die door ondernemers of door intermediairs moeten worden geïmplementeerd. Dit resulteert in een enorme beheerinspanning.

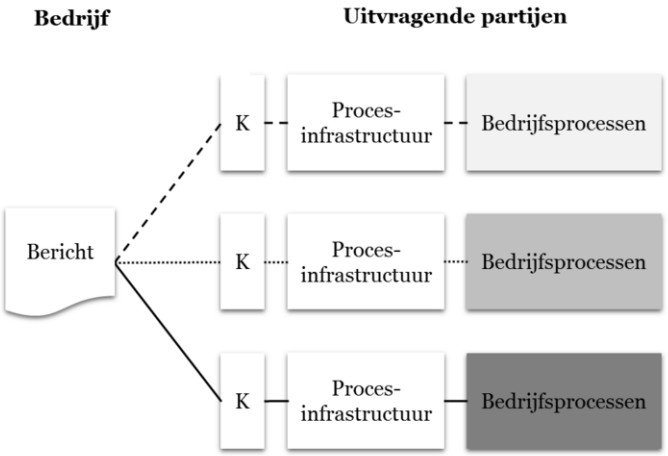
Scenario B: Eigen procesinfrastructuur (gestandaardiseerde koppelvlakken, eigen digitale procesinfrastructuur)
Het tweede scenario omvat het aanbieden van koppelvlakken voor informatie-uitwisseling met overheidsinstanties, zoals afgebeeld in figuur 7.2.



Figuur 7.2 – Gestandaardiseerde koppelvlakken (K), eigen digitale procesinfrastructuur (Scenario B)

Dit scenario voor informatie-uitwisseling hanteert als principe, dat alleen die koppelvlakken worden aangeboden die nodig zijn om informatie uit te kunnen wisselen. Het is feitelijk een automatisering van de oude situatie, zonder de voordelen van nieuwe technologieën te benutten. Dat komt neer op het 'aan elkaar knopen' van de voorzieningen van de organisaties door het beschikbaar maken van standaard koppelvlakken. Zo kun je als overheid overwegen om alle noodzakelijke (technische) afspraken netjes te beschrijven en ervoor pleiten dat alle bedrijven en uitvragende partijen deze implementeren. Door gebruik te maken van koppelvlakstandaarden is er geen maatwerk nodig voor implementatie.

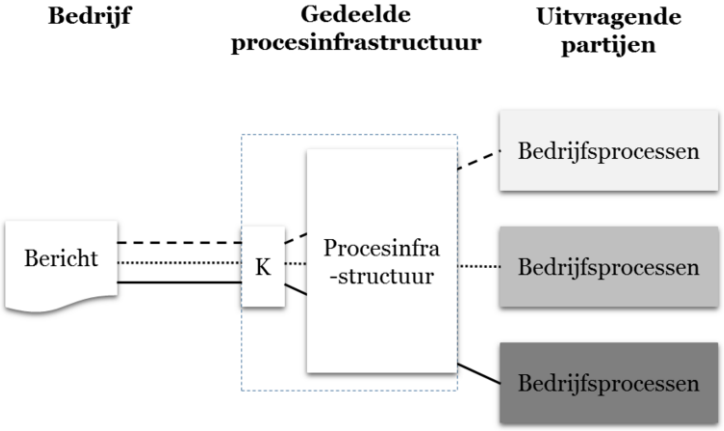
Scenario C: Concern-procesinfrastructuur (gestandaardiseerde koppelvlakken, gestandaardiseerde procesinfrastructuur)
Het derde scenario voor informatie-uitwisseling gaat ervan uit dat zowel de koppelvlakken als de procesinfrastructuur functionaliteiten zijn gestandaardiseerd, zoals afgebeeld in figuur 7.3.



Figuur 7.3 – Gestandaardiseerde koppelvlakken (K) en gestandaardiseerde procesinfrastructuur (Scenario C)

Dit scenario voor informatie-uitwisseling impliceert het uniform maken van het IT landschap. Daarmee wordt bedoeld: de keuze voor identieke hardware, systeemsoftware en toepassingssoftware ('overal dezelfde kastjes') bij alle uitvragende organisaties. Het past bij het zogenaamde 'concerndenken', waarbij partijen bereid zijn (of moeten zijn) om de voor hen gemaakte keuzes te implementeren (Berkelaar, 2007).

Scenario D: Gedeelde dienstverlener (gestandaardiseerde koppelvlakken en gedeelde procesinfrastructuur)
Het vierde scenario voor informatie-uitwisseling impliceert een gedeelde dienstverlener die de koppelvlakken en services beheert.



Figuur 7.4 – Gedeelde dienstverlener: gestandaardiseerd koppelvlak (K) en generieke procesinfrastructuur (Scenario D)

De generieke procesinfrastructuur is het geheel van middelen zoals hardware, software en netwerkapparatuur, inclusief beveiliging, dat nodig is voor de S2S-uitwisseling en gedeelde verwerking van informatie voor meerdere toepassingen.

Er kan bij dit scenario een vergelijking worden gemaakt met een multi-sided platform (MSP). MSP is een concept uit de institutionele economie en wordt gedefinieerd als "*products, services or technologies that connect different types of customers to each other*" (Hagiu & Yoffie, 2009, p. 75). De toevoeging 'multi-sided' wijst op het feit dat er meerdere typen consumenten te onderscheiden zijn die van het platform gebruik maken. In dit geval kan het gaan om informatie aanleveraars (bedrijven en intermediairs) en afnemers (uitvragende partijen). Het concept 'platform' verwijst naar een aantal samenhangende voorzieningen.

Het MSP reguleert de toegang en uitwisseling via een centrale infrastructuur door een combinatie van voorwaarden die technisch, juridisch, procedureel of financieel van aard kunnen zijn (Boudreau & Hagiu, 2010). Neem hier het voorbeeld van de App Store van Apple, die strikte eisen stelt aan derde partijen die apps ontwikkelen en willen distribueren via het MSP. MSP's zijn niet nieuw. Eén of meer van onderstaande voorbeelden zullen vast bekend zijn:

- Google's zoekmachine die adverteerders en gebruikers van hun diensten verbindt.
- Microsoft Windows Development Platform dat applicatie ontwikkelaars, gebruikers en OEMs/hardware fabrikanten aan elkaar verbindt.
- De Blu-ray standaard voor high-definition films die contentleveranciers, producenten van Blu-ray spelers en consumenten aan elkaar verbindt.
- Fabrikanten van videogame hardware consoles, waaronder Sony Playstation en Nintendo Wii, die zo veel mogelijk spelers moeten binden om game-ontwikkelaars aan te trekken, terwijl spelers alleen de hardware kopen als ze er veel interessante games op hierop kunnen draaien (Osterwalder & Pigneur, 2010).

Wat opvalt uit bovenstaande voorbeelden is dat een MSP zowel de rol van platform als die van een regisserende partij moet vervullen. Daarnaast acteren MSP's tussen de verschillende typen klanten zonder dat ze eigenaar worden van de uitgewisselde gegevens. MSP's ondersteunen op deze manier spelers die onderling afhankelijk zijn. We zien deze kenmerken terug bij de gedeelde dienstverlener bij SBR (Logius). We gaan hier in hoofdstuk 9 (Governance en beheer) verder op in.

Vergelijking van scenario's

Genoemde scenario's hebben uiteraard elk hun voor- en nadelen ten opzichte van de traditionele/heterogene situatie (scenario A). Scenario B (eigen procesinfrastructuur) is aantrekkelijk, omdat het weinig verandering met zich meebrengt. Dat kan zich ook uiten in lagere investeringskosten. Daarnaast wordt de autonomie van partijen niet aangetast en voorkomt men bij deze strategie discussie over wie eigenaar is van voorzieningen. Een gevaar hierbij is wel, dat door het ontbreken van een exclusief ontwikkelplatform de implementaties uit elkaar gaan lopen en het praktisch bijna onmogelijk wordt om de samenhang te bewaken. Tevens levert het koppelen van oude aan nieuwe systemen vaak technische problemen op, die alleen kunnen

worden opgelost met een flinke dosis technische kennis. Deze kennis is schaars en kostbaar. Tenslotte betekent het dat soortgelijke activiteiten meerdere keren (bij elke partij) worden ontwikkeld en beheerd. Dat leidt tot dubbelingen in ontwikkelingskosten en het verspillen van schaarse middelen.

Scenario C (concern-procesinfrastructuur) werd vaak in grote bedrijven met een centrale ICT-afdeling en meerdere geografische locaties toegepast. In theorie kan dit scenario alle interoperabiliteitsproblemen oplossen en kunnen schaalvoordelen op diverse fronten (licentiekosten, training etc.) behaald worden. Toch hebben veel grote bedrijven het concerndenken verlaten en thans is dit het minst voor de hand liggende scenario. En wel vanwege de volgende redenen:

- Er is strakke regie nodig om te slagen en niet terug te vallen naar scenario B.
- Voor een aantal partijen in een samenwerkingsverband zal het betekenen dat er gedesinvesteerd moet worden in de bestaande, 'eigen', procesinfrastructuur.
- Het homogeniseren brengt voor de overheid forse investeringen met zich mee. Dezelfde nieuwe digitale procesinfrastructuur moet meerdere keren uitgerold worden. Dit past niet in het streven naar een compacte overheid.
- De doorlooptijd van dergelijke operaties is relatief lang. Het zijn complexe operaties die makkelijk onderschat kunnen worden (Berkelaar, 2007).
- Deze strategie veronderstelt dat partijen hun autonomie in het bepalen van de inrichting van hun procesinfrastructuur willen opgeven. Het betekent dat hierover consensus bereikt moet worden of dat een partij voldoende macht moet hebben om dit af te kunnen dwingen.
- Het veronderstelt dat partijen in een 'one size fits all' gedrukt worden, waarbij er geen ruimte is om specifieke eisen in te willigen.

Gezien bovenstaande overwegingen is in het kader van SBR gekozen voor scenario D, de gedeelde dienstverlener. Wat opvalt ten opzichte van scenario A is de reductie van de interfaces (in zowel type als aantal) tussen bedrijven en de uitvragende partijen. Bedrijven kunnen voor al hun communicatie met de overheid gebruik maken van één koppelvlak (en hebben dus niet te maken met specifieke koppelvlakken voor Belastingdienst, CBS, KvK, etc.). Deze technische inrichting verlaagt op die manier de transactiekosten en vergroot tegelijkertijd het klantbereik van de uitvragende partijen. Dit wordt in de literatuur het "*electronic brokerage effect*" genoemd (Malone, Yates, & Benjamin, 1987). Daarnaast worden de eerder benoemde nadelen die horen bij scenario A (traditionele/heterogene infrastructuren), scenario B (eigen procesinfrastructuur) en scenario C (concern-procesinfrastructuur) vermeden. Het werken met een gedeelde dienstverlener brengt ook indirecte netwerkeffecten mee, zowel aan de vraag- als aan de leverkant. Voorbeelden van indirecte netwerkeffecten zijn schaalbaarheid (er kunnen mogelijk veel meer transacties plaatsvinden) en positieve feedback: meer gebruikers→ meer transacties→ meer inkomsten → investeringen in hogere kwaliteit tegen een lagere prijs → meer gebruikers (Cusumano, 2005).
De volgende tabel helpt met een vergelijking de keuze voor Scenario D te beargumenteren.

Tabel 7.1 – Samenvatting van scenario's

Scenario	A. Traditionele/ heterogene procesinfra-structuren	B. Eigen proces-infrastructuur	C. Concern procesinfra-structuur	D. Gedeelde dienstverlener
Koppelvlakken	Verschillend	Standaard	Standaard	Standaard
Ontwikkelen en beheren van functionaliteiten	Individueel	Individueel	Gezamenlijk	Gedelegeerd aan een gespecialiseerde en gemandateerde organisatie
Implementatie van procesinfrastructuur	Eigen manier, divergent	Eigen manier, divergent	Opgelegde manier, homogeen	Overeengekomen manier, centraal
Benodigde kennis per organisatie	Hoog	Hoog	Hoog	Kennispool/ samen ontwikkelde kennis
Keten-bestuur (afstemming tussen partijen)	Geen	Laag/ decentraal	Hoog/ decentraal	Publiek-private samenwerking
Transactiekosten voor bedrijf	Hoog, conformeren aan meerdere standaarden	Gemiddeld	Gemiddeld	Laag
Transactiekosten voor overheid	Hoog	Hoog	Gemiddeld	Laag (schaalvoordelen)

Zoals we in eerdere hoofdstukken al hebben gezien, hangt dit scenario samen met de gedeelde berichtspecificaties (Nederlandse Taxonomie) en i-processpecificaties (generieke procesplaten). De procesinfrastructuur omvat de webservices die kunnen worden aangeroepen voor de uitvoering van i-processen, met de nodige beveiligingsmiddelen (zie hoofdstuk 8 voor de invulling van de beveiliging).

Wat opvalt in bovenstaande tabel is dat een gedeelde dienstverlening (ontwikkeld en beheerd door een gedeelde dienstverlener) voordelen biedt en om minder investeringen (geld en kennis) vraagt in vergelijking met de voordelen van outsourcing, zoals genoemd in de inleiding van het boek. Wel is het de vraag wie de investeringen doet. Betrokken partijen hebben in het kader van SBR op dit scenario ingezet, met Digipoort als gedeelde procesinfrastructuur. Maar met 'één procesinfrastructuur' en een gedeelde dienstverlener zijn we er nog niet. Er zijn nog twee gerelateerde, essentiële eisen aan de SBR-oplossing die geadresseerd moeten worden, namelijk:

- Hoe om te gaan met verschillen in de inhoud van berichten/verantwoordingsinformatie (de zogenaamde *payload*). De payload is de berichtinhoud, de boodschap die voor een bepaald doel van A naar B wordt verstuurd. Dit is belangrijk, aangezien de eisen aan wat er gerapporteerd moet worden per uitvragende partij ieder jaar verandert. Daarnaast kan de specificatie van de payload per berichtsoort verschillen. Bovendien kan een stroom meerdere

soorten berichten bevatten, zoals verantwoording, mededeling, status, machtiging.
- Hoe om te gaan met verschillende i-processen? Dit is belangrijk, omdat de i-processen voor diverse uitvragende partijen verschillend kunnen zijn.

7.2.2 *Programma van Eisen van de Generieke Procesinfrastructuur*

Het eerder genoemde PvE GEIN (2006) beschrijft een architectuur die tegemoet komt aan de twee bovengenoemde eisen: om kunnen gaan met verschillende payloads en verschillende i-processen. Het PvE GEIN laat ook zien dat in 2006 scenario D - een gedeelde dienstverlener – al duidelijk de geschikte technische inrichting was voor SBR. De volgende principes uit het PvE GEIN zijn relevant:

- Gebruik van open standaarden: oplossingen moeten herbruikbaar zijn.
- Platform onafhankelijkheid: informatie-uitwisseling ongeacht de specifieke eigenschappen van de technische omgeving.
- Ontkoppeling ('loose coupling'): bestendig tegen dynamiek (belangen, weten regelgeving, dienstenaanbod in de markt, etc.), doordat delen onafhankelijk van elkaar zijn.
- Flexibel procesverloop: verschillende berichten moeten grotendeels op dezelfde, maar deels op een andere manier worden afgehandeld.

Bovenstaande principes zijn in PvE GEIN sterk gevoed door technologische ontwikkelingen op het gebied van Service Oriented Architecture (SOA) en webservices. We lichten deze technologieën hieronder kort toe in het kader van bovenstaande beginselen en de manier waarop ze bijdragen aan het invullen van eerder genoemde eisen. In § 7.3 gaan we nader in op de technologieën.

Hoewel SOA en webservices-technologie vaak door elkaar worden gebruikt, representeren deze concepten twee verschillende abstractieniveaus. SOA is een manier van ontwerpen (architectuurstijl) die streeft naar een platformonafhankelijke, losgekoppelde en gedistribueerde informatie-uitwisseling, waarbij software elementen (verspreid in het netwerk) te beschouwen zijn als services (Fremantle, Weerawarana, & Khalaf, 2002). In een informatievoorziening die volgens SOA is opgezet, worden de functionaliteit en gegevens van applicaties via services ter beschikking gesteld. Dit kan worden gerealiseerd middels webservices technologie. Webservices technologie representeert een palet aan open standaarden (lees: protocollen), dat het mogelijk maakt functionaliteit, zowel op applicatie- als op bedrijfsniveau, aan te bieden via gestandaardiseerde interfaces (Janssen & Gortmaker, 2005). Een SOA kan geïmplementeerd worden zonder Webservices technologie, en Webservices kunnen gebruikt worden voor architectuur anders dan SOA (zoals een remote procedure call). Toch worden in de praktijk webservices het meest gebruikt voor SOA. Er zijn vier redenen hiervoor waarin de eerder genoemde beginselen weerklinken.

Allereerst biedt webservices technologie de noodzakelijke open standaarden voor de implementatie van SOA op technisch niveau (Erl, 2008). Standaarden kunnen zowel gesloten als open zijn (West, 2007). Een gesloten standaard is een standaard die is vastgesteld en wordt onderhouden door een natuurlijke persoon of een rechtspersoon (meestal een bedrijf of een groep bedrijven). Veel gesloten standaarden bevatten onderdelen die octrooirechtelijk beschermd zijn en waarvoor de gebruiker moet

betalen (Folmer & Punter, 2010). Open standaarden daarentegen zijn vrij te gebruiken, maar dat wil niet automatisch zeggen dat ze ook daadwerkelijk gebruikt worden. Voorbeelden van open standaarden zijn XML, SOAP en BPEL4WS, die door de meeste softwareleveranciers ondersteund worden (Curbera et al., 2002). Deze standaarden worden later in dit hoofdstuk toegelicht.

Een tweede reden voor het gebruik van webservices is het feit dat ze platform onafhankelijk zijn. Dat wil zeggen dat de legacy (bestaande/verouderde systemen), in termen van de hardware, besturingssystemen en de programmeeromgevingen van de aan te sluiten organisaties, geen barrière moet vormen voor informatie-uitwisseling. Hierdoor kan een bedrijf dat gebruikt maakt van .NET gebaseerde software toch berichten versturen naar een uitvragende partij die Java of software uit een andere programmeeromgeving gebruikt.

Een derde reden om webservices te gebruiken is de hoge mate van ontkoppeling ('loose coupling') waardoor substitutie en hergebruik van services mogelijk wordt (Fremantle et al., 2002). Loose coupling duidt op zowel technische als organisatorische onafhankelijkheid van een deel met andere delen. We leggen beide vormen hier kort uit. Technische loose coupling duidt op de mogelijkheid om 'on demand' services te combineren als een 'service compositie' (software bouwsteen met een samengestelde functionaliteit) en ze na gebruik net zo makkelijk weer te ontbinden (Carter, 2007). Dit is mogelijk door de ontkoppeling van de service-interfaces van de implementaties, waardoor er sprake is aan een minimale set van eisen aan het bericht zelf (Weerawarana, Curbera, Leyman, Storey, & Ferguson, 2005). Het tegengestelde hiervan is de voorheen vaak toegepaste 'tight coupling' tussen applicaties, waarbij een semipermanente verbinding werd gelegd in de code van applicaties (hard coded connectie) (Arsanjani, 2002). Organisatorische loose coupling duidt op de mogelijkheid om uit verschillende aanbieders (service providers) van webservices te kiezen voor het leveren van een specifieke functionaliteit. Neem het voorbeeld van het valideren van een bericht dat van A naar B moet. B heeft namelijk specifieke eisen aan dit bericht, zoals het formaat ervan (XBRL), de grootte (bijvoorbeeld niet groter dan 20 MB), de adressering, etc. Om dit bericht te valideren kan een validatieservice worden aangeroepen, die controleert of het bericht voldoet aan de gemaakte afspraken. Door de ontkoppeling van code en implementatie kunnen verschillende aanbieders een dergelijke validatieservice bieden. Hierdoor is het mogelijk om bij uitval of contractvernieuwing andere service aanbieders te seleceren voor het aanbieden van een servicefunctionaliteit.

De vierde reden om webservices te gebruiken is de mogelijkheid voor 'flexibele procesuitvoering'. Dankzij de loose coupling kunnen webservices worden aangeroepen volgens een gewenst procesverloop. In tegenstelling tot één totaalproces, worden diensten aangeboden door het 'on demand' samensmelten van losse functionaliteiten (bouwstenen) tot één i-proces. Dit wordt ook wel technische orkestratie genoemd, welke door de technische open standaard BPEL4WS ondersteund wordt. Met orkestratie kunnen we verschillende bouwstenen in de juiste volgorde aan elkaar rijgen, waardoor een i-proces gecreëerd wordt (zie hoofdstuk 5 - I-Processen). De logica voor 'het aan elkaar rijgen' is flexibel en kan worden aangepast aan eventuele nieuwe eisen in de wet- en regelgeving.

Concluderend kunnen we stellen dat met het oog op het doel van SBR - S2S-uitwisseling en gedeelde verwerking van verantwoordingsinformatie – het scenario van de gedeelde infrastructuur het meest geschikt is. Het PvE GEIN wijst ook in die richting en biedt handvatten voor de manier waarop er invulling kan worden gegeven aan dit scenario: aan de hand van SOA en webservices.

In de volgende paragraaf diepen we de technologie uit die nodig is om invulling te geven aan de gedeelde (proces)infrastructuur. Daarna (in § 7.4) beschrijven we de wijze waarop deze technologie bij SBR wordt gebruikt: Digipoort en de keuzes die daarbij zijn gemaakt.

7.3 Relevante technologie

7.3.1 *Interoperabiliteit*

Het tweede deel van dit hoofdstuk behandelt technologische ontwikkelingen die in het kader van het opzetten van een gedeelde procesinfrastructuur relevant zijn. Het startpunt voor deze technologische ontwikkelingen is het streven naar S2S-integratie (zie hoofdstuk 1). We merken een aantal zaken op ten aanzien van eerder in dit boek behandelde thema's, die de lezer in het achterhoofd kan houden bij het lezen van deze paragraaf.

- Interoperabiliteit is een randvoorwaarde voor S2S-integratie. Standaarden spelen bij elk bouwblok van de SBR-oplossing (waaronder i-processpecificaties, koppelvlakservices en verwerkingsservices) een belangrijke rol in het creëren van interoperabiliteit.
- De i-processpecificaties en berichtspecificaties zijn vooral definiërend van aard, het 'echte' werk gebeurt met het aanroepen en orkestreren van de services.
- De essentie van de taxonomie voor bedrijven is dat zij éénmalig inrichten, namelijk door de concepten in de taxonomie te 'mappen' op hun eigen gegevensadministratie, zodat zij daarna eenvoudig verschillende verantwoordingen kunnen genereren: het 'Store once, report many' concept. Niet te verwarren met het 'éénmalig aanleveren' van gegevens.
- De koppelvlakken zijn essentieel voor het daadwerkelijk uitwisselen van gegevens.
- De fysieke laag is een commodity geworden. In de huidige IT-wereld bestaat er nauwelijks nog discussie over de standaarden voor fysieke componenten. Als je morgen een netwerk nodig hebt, dan vraag je om een TCP/IP-netwerk. De tijd dat je moest discussiëren of het nu een X25, een token-ring of een TCP/IP netwerk moest zijn, is voorbij. In feite is er vrij grote instemming over dit soort basisstandaarden.
- De keuze van SBR voor webservices brengt een keuze voor de individuele standaarden voor koppelvlakken met zich mee.
- Enterprise service bus, ESB, maakt het mogelijk dat de services onderling communiceren en op die manier een vast gedefinieerd i-proces uitvoeren.
- Een process-engine is noodzakelijk voor het automatisch kunnen aanroepen van webservices conform een vooraf bepaalde procesplaat (BPMN).

Bovenstaande opsomming benoemt concepten als koppelvlakken, webservices, enterprise service bus en process-engine, die we al eerder hebben zien langskomen. Gezien de vervlechting tussen deze concepten is het een uitdaging om ze in de juiste volgorde te behandelen. Als we hiervoor de beschreven berichtenstroom als leidraad nemen, komen we op de volgende indeling:

1. Koppelvlakken (§ 7.3.2)
2. Webservices (§ 7.3.3)
3. SOA voor de ondersteuning van flexibele i-processen (§ 7.3.4)

7.3.2 *Koppelvlakken*

Een koppelvlak is een system-to-system verbinding tussen informatiesystemen die de uitwisseling van informatie faciliteert. Dit hanteren we voorlopig als definitie. We zullen straks zien dat deze definitie in de praktijk niet helemaal dekkend is. We beperken ons hier tot de functie van koppelvlakken en de standaarden die hiervoor beschikbaar zijn.

Een simpele vergelijking van een koppelvlak met een voorbeeld uit de praktijk is het elektriciteitsnetwerk. Vergelijk een koppelvlak met een stopcontact dat op een standaard manier (middels een stekker) via een gestandaardiseerd netwerk een dienst (elektriciteit) levert. Om van een dergelijke dienst gebruik te maken heb je dus alleen een stekker nodig. Je hoeft geen eigen elektriciteitscentrale te bezitten en je hebt geen kennis van de werking van een elektriciteitscentrale nodig. Pas wanneer de koppelvlakken goed ingevuld zijn door de verschillende partijen kunnen berichten verstuurd en ontvangen worden. Vaak kunnen deze allerhande bijlagen bevatten. Ook wordt het mogelijk verschillende soorten berichten te versturen met een hoge mate van interoperabiliteit.

Koppelvlakken zijn dus belangrijk, maar hoe kies je er een? Bij het kiezen voor de te gebruiken koppelvlakken spelen meerdere variabelen een rol. Ten eerste moet het koppelvlak een (open) standaard zijn die in voldoende mate ondersteund wordt, zodat er reeds oplossingen en expertise in de markt aanwezig zijn. Daarnaast moeten de koppelvlakken aan de eisen voldoen die uit de i-processen volgen. Het doel van de informatieoverdracht bepaalt de benodigde eigenschappen, zoals een mate van betrouwbaarheid, beveiliging of capaciteit. Gezien de verschillende eigenschappen van de beschikbare protocollen kunnen er meerdere naast elkaar worden gebruikt om zo te voldoen aan de eisen van meerdere i-processen. Vanuit praktisch en economisch oogpunt kunnen niet *alle* mogelijkheden aangeboden worden.

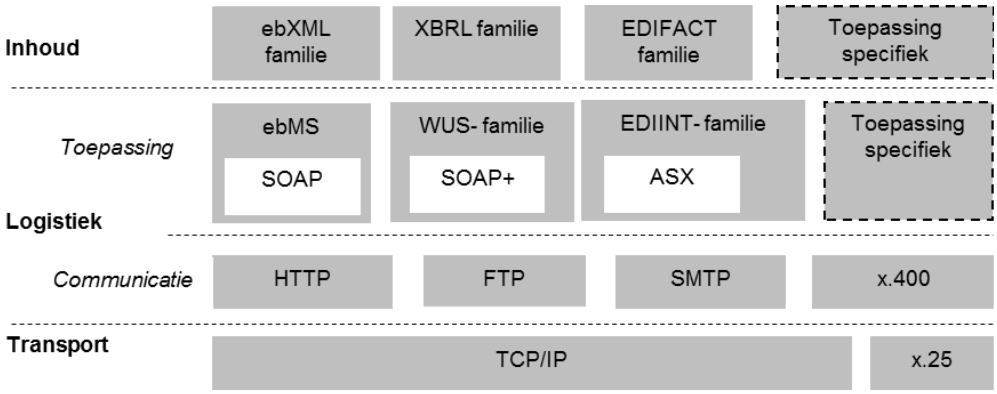
In de praktijk zijn er nogal wat verschillende standaarden beschikbaar om koppelvlakken op te stellen, soms aanvullend, soms concurrerend. De uitwisseling tussen service-aanbieders en gebruikers kan in drie lagen worden opgedeeld:

1. Inhoud: deze laag omvat de afspraken die organisaties maken over de inhoud van het uit te wisselen bericht, zoals de structuur, semantiek, bereik van waarden etc.
2. Sessie (logistiek): deze tussenlaag is op te delen in twee sublagen:
    - Communicatie: refererend aan de transportprotocollen (HTTP, SMTP etc.)

- Toepassing: refererend aan standaarden omtrent messaging (zoals de op SOAP gebaseerde ebMS en WUS), beveiliging (authenticatie en encryptie) en betrouwbaarheid

3. Transport: deze laag verzorgt de uiteindelijke overdracht van berichten.

Figuur 7.5 geeft een overzicht van koppelvlakstandaarden in een lagenmodel. De samenhang tussen de lagen en de afgebeelde standaarden wordt hieronder toegelicht. Het blokje 'toepassing specifiek' geeft aan, dat er ook vele specifieke communicatieoplossingen voor een bepaalde toepassing bestaan die niet zijn vastgelegd in formele standaarden.



Figuur 7.5 – Typische standaarden voor de realisatie van koppelvlakken

Wat in bovenstaande figuur opvalt, is dat de inhoud strikt gescheiden is van logistiek en transport. Immers, de inhoud betreft de informatie die overgedragen moet worden, ongeacht de keuze voor het transportmiddel. De algemeen gehanteerde techniek is om de inhoud dan te verpakken in een gestandaardiseerde envelop. De transportlaag en sessielaag worden hieronder nader toegelicht. Daarna zoomen we in op SOAP, omdat dit het belangrijkste protocol voor de realisatie van koppelvlakstandaarden is in het SBR-stelsel. De inhoudlaag komt in hoofdstuk 6 (Gegevens) aan bod.

Op de transportlaag komen we TCP/IP tegen. Door de komst van het Internet is dit een algemeen geaccepteerde standaard voor netwerkcommunicatie ten behoeve van berichtuitwisseling (Stallings, 2009). Ook in besloten netwerken wordt het TCP/IP-model algemeen toegepast. Daarmee is het protocol algemeen bruikbaar als fundament voor alle koppelvlakken. In dit hoofdstuk wordt TCP/IP als een gegeven gezien en gaan we niet verder in op de werking.

De hogere lagen zijn strikt genomen allemaal aan te duiden als 'de applicatielaag'. In de praktijk blijkt dat hier ook een verdere gelaagdheid in aan valt te brengen. In ieder geval is er duidelijk onderscheid te maken tussen een laag die zich bezig houdt met de logistiek van berichten (ongeacht de inhoud) en een laag die zich bezig houdt met de inhoud (ongeacht de logistiek). Hierdoor kunnen we de 'logistiek laag' in twee

sublagen splitsen: de communicatie-sublaag en de toepassing-sublaag. Deze lagen worden hieronder nader uitgelegd.

- De communicatie-sublaag is de laag waarin communicatieprotocollen zoals HTTP, FTP en SMTP zijn te vinden. FTP is gericht op het ophalen en plaatsen van *bestanden* op een server, SMTP is gericht op het aanbieden en ontvangen van berichten van een server (bijvoorbeeld e-mail), en HTTP is oorspronkelijk gericht op het ophalen en aanbieden van (tekst)documenten op een server. In de communicatie-sublaag bevindt zich ook nog X.400, een ouder protocol dat steeds minder wordt ingezet. Ondanks de verschillende oorsprong van deze protocollen zijn ze allemaal bruikbaar om inhoudelijke 'berichten' te transporteren. Er zijn wel grote verschillen in de manier waarop dit wordt gedaan. Met name de mate waarin informatie aanwezig is over zender en ontvanger en de routeringsmogelijkheden verschillen per protocol. De protocollen voorzien standaard bovendien niet in beveiliging (anders dan die van de verbinding) en kennen een beperkte mate van betrouwbaarheid. Met name voor SMTP en HTTP zijn veel uitbreidingen bedacht die stuk voor stuk zijn vastgelegd in aanvullende standaarden. Niet al die uitbreidingen zijn afgestemd op elkaar, en verschillende softwareleveranciers maken andere keuzes in welke extensies ze ondersteunen.

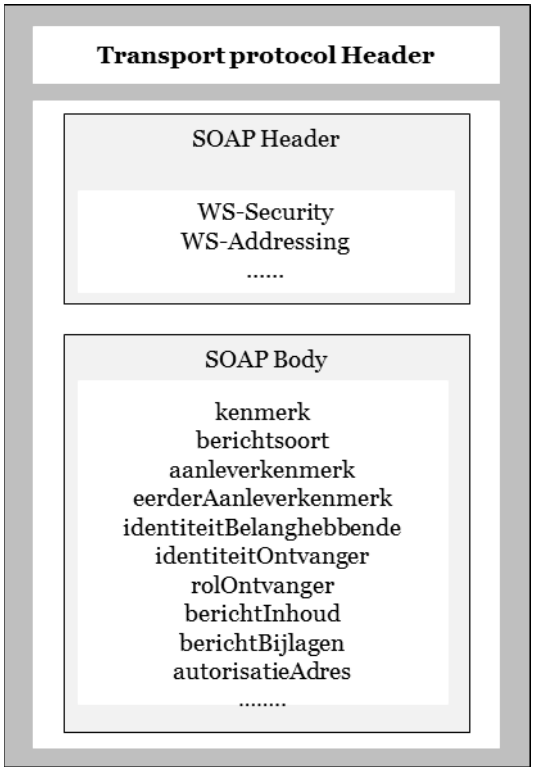
- De toepassing-sublaag is feitelijk ontstaan doordat niet alle protocollen uit de communicatie-sublaag op dezelfde manier werken. Voor applicaties die in een heterogene omgeving werken is dat niet wenselijk, omdat ze dan voor het ene protocol andere functionaliteit moeten implementeren dan voor een ander. Het wijdverspreide gebruik van EDI (electronic data interchange) voordat webservices hun intrede deden, heeft geleid tot 'EDI over the internet' (ofwel EDIINT), ook wel bekend als de ASx-familie. Deze protocollen standaardiseren de wijze waarop EDI-toepassingen omgaan met beveiliging en betrouwbaarheid voor verschillende communicatieprotocollen: SMTP (AS1), HTTP (AS2), FTP (AS3) en – in ontwikkeling – Webservices (AS4, op basis van ebMS).

Functioneel voorzien alle genoemde toepassingsgerichte protocollen in de behoefte van betrouwbaar en veilig transport van inhoudelijke berichten. De manier waarop is wederom per protocol heel verschillend. Aangezien voorkeuren voor technologie heel verschillend kunnen zijn tussen verschillende organisaties en sectoren is het niet haalbaar om op één standaard voor te sorteren. Een deel van het bestaansrecht van een generieke procesinfrastructuur ligt dan ook in het kunnen vertalen van het ene protocol naar het andere. Daarmee kan het gebruik van verschillende protocollen en standaarden tussen organisaties en sectoren worden overbrugd.

Inzoomen op SOAP
We lopen even vooruit op de toepassing bij Digipoort: alle drie de koppelvlakken die in het kader van S2S-integratie via Digipoort zijn gerealiseerd, maken gebruik van het SOAP protocol (zie: http://www.w3.org/TR/soap/). De drie koppelvlakken – SOAP2008, WUS en ebMS Digikoppeling – worden in hierna beschreven.

SOAP stond in de oorspronkelijke uitgave (April 2000) als acroniem voor de Simple Object Access Protocol. Gezien de bredere toepassing van SOAP als onderdeel van zowel de XML stack en Web Services stack werd het onduidelijk waar het acroniem precies voor stond. Sinds de voltooiing van de SOAP 1.2-specificatie heeft het World Wide Web Consortium (W3C) het protocol gebruikt zonder het acroniem voluit te schrijven.

De behoefte aan SOAP kwam voort uit de beperkingen van andere protocollen. HTTP en het internet mail-protocol (SMTP) voorzagen maar in zeer beperkte mogelijkheden voor de overdracht van gegevens: een enkel blok 7-bits ASCII-tekst. Al snel was er behoefte om meer en andersoortige gegevens via internet mail te transporteren, bijvoorbeeld binaire bestanden of meerdere bestanden (Stallings, 2007). SOAP gaf invulling aan deze behoefte. SOAP kent een andere benadering en werkt als een envelop (Weerawarana et al., 2005).
SOAP levert de envelop om elektronische berichten die door webservices worden uitgewisseld, over het internet te versturen. De figuur geeft een versimpelde weergave van de onderdelen van een SOAP bericht, inclusief een SOAP-envelop.



Figuur 7.6 – De structuur van een SOAP bericht

Zoals afgebeeld bestaat en SOAP-bericht uit:

- de transportprotocol-header;

- de SOAP-envelop met daarbinnen:
    - de SOAP-header;
    - de SOAP-body.

Voor het feitelijke transport van de berichten maakt SOAP gewoonlijk gebruik van HTTP, maar andere protocollen, zoals Simple Mail Transfer Protocol (SMTP), mogen ook worden gebruikt. In de SOAP-envelop zijn de header en de body opgenomen. Dit onderscheid is –zoals we in het beveiligingshoofdstuk zullen zien – in meerdere opzichten relevant. Bij Digipoort dient een bedrijf[20] met oog op beveiliging de body- en de header-elementen van een aanleververzoek digitaal te ondertekenen. Dit ondertekenen dient te geschieden met behulp van een elektronische handtekening en aan de hand van een door een Certificate Service Provider (CSP) uitgegeven PKIoverheid certificaat. Een certificaat is een digitaal document dat gegevens bevat voor het waarborgen van de integriteit en authenticiteit van bestanden en/of voor het opzetten van een beveiligde verbinding. Hierover meer in hoofdstuk 8; we gaan hier terug naar het onderscheid tussen SOAP-header en -body.

SOAP-headers leveren informatie over codering van gegevens, authenticatie of hoe de ontvanger het SOAP-bericht moet verwerken. Een SOAP-header kan tevens worden gebruikt om aansturings- en controle-informatie door te geven tussen de servicegebruiker en de service provider, voor zaken zoals asynchrone communicatie, transacties, routing en security, en om andere quality-of-service-attributen te implementeren. Om de eigenlijke berichtinhoud betrouwbaar, integer en veilig te kunnen transporteren is een groot aantal aanvullende afspraken nodig, waaronder WS-adressing en WS-security. Deze worden later toegelicht.

De SOAP-body bevat het bericht – een invulling van een verzameling elementen zoals afgebeeld in figuur 7.6. Het element kenmerk bijvoorbeeld beschrijft het unieke kenmerk van een instance van het i-proces. Het kenmerk kan worden gebruikt bij het opvragen van statussen. Het element 'berichtsoort' beschrijft het soort i-proces dat met een bericht aanleververzoek wordt geïnitieerd. De elementen kunnen worden gedefinieerd door de WSDL-specificatie te gebruiken.

Op basis van SOAP zijn twee belangrijke protocolfamilies ontstaan: webservices (in de zin van SOAP via HTTP) en ebMS (e-business XML Message Service). Omdat deze ook voor Digipoort worden gebruikt, worden ze hieronder kort toegelicht.

7.3.3 *Webservices*

Het is in dit kader belangrijk om een onderscheid te maken tussen webservices (meervoud) en webservice (enkelvoud). De term 'webservices' refereert aan een set van standaarden (protocol stack) voor informatie-uitwisseling (zie figuur 7.8). De term 'webservice' refereert aan een afgebakende functionaliteit voor de transformatie van input informatie naar output informatie, die aangeroepen kan worden via de

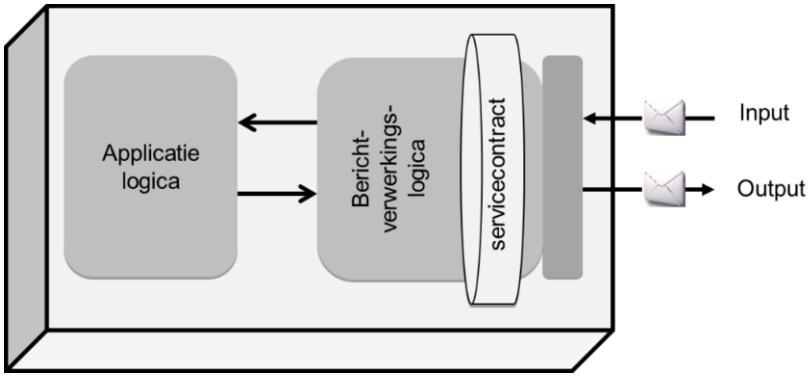
[20] Dit hoeft niet door de berichteigenaar (belanghebbende) te gebeuren; ondertekening wordt in de regel gedaan door de partij die voor de technische implementatie zorgt. Dit kan dus ook een intermediair zijn.

standaarden. Om verwarring te voorkomen hanteren we in het vervolg bij aanduiding van meerdere webservices de term services. Met het gebruik van de standaarden kan een SOA worden gerealiseerd voor het ondersteunen van berichtuitwisseling (messaging) tussen verschillende systemen. Zie bijvoorbeeld onderstaande definitie van het World Wide Web Consortium (W3C):

"A Webservice is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web-service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards" (W3C, 2004).

Een webservice kan niet enkel informatie overbrengen van systeem naar systeem, maar ook direct een applicatie aanspreken en het resultaat daarvan weer als retourbericht ontvangen. In dit hoofdstuk wordt daarom onderscheid gemaakt tussen het overbrengen van informatie en het direct aanspreken van een (stukje) applicatie.

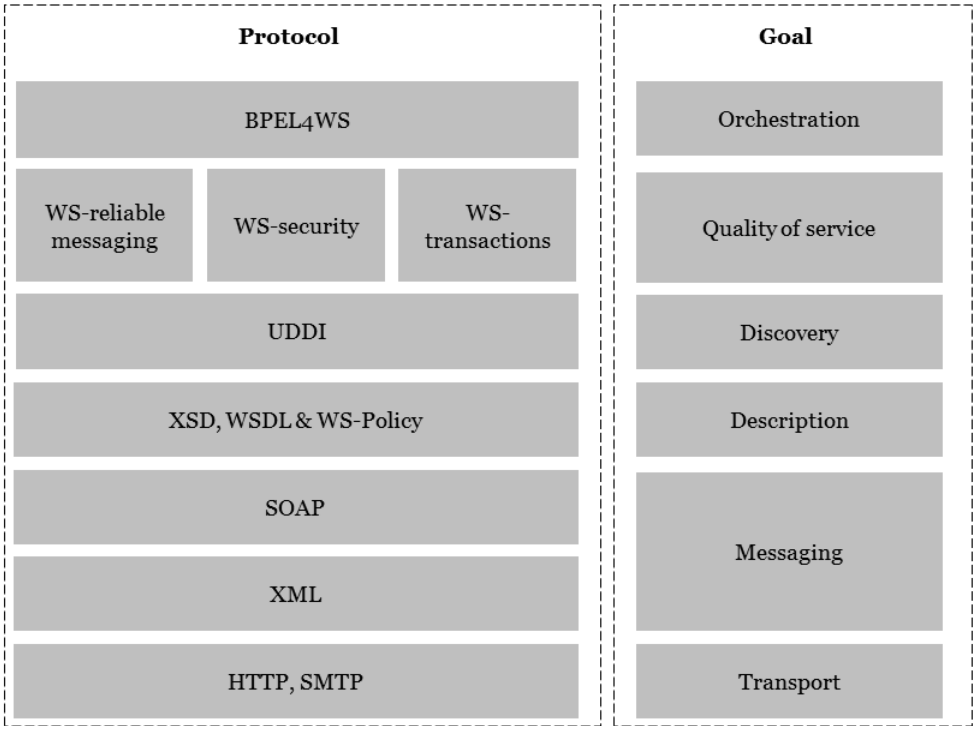
Een webservice bestaat uit de volgende elementen (Erl, 2008): de applicatielogica, de berichtverwerkingslogica en het servicecontract. Deze elementen zijn in de onderstaande figuur afgebeeld.



Figuur 7.7 – Elementen van een webservice (gebaseerd op Erl, 2008)

Zoals afgebeeld bestaat een webservice uit drie elementen, die we hier kort beschrijven. We beginnen bij de applicatielogica, een blokje functionaliteit dat input (gegevens) verwerkt tot output. Om dit te kunnen doen, moet de input op een gepaste manier worden aangeboden aan de applicatielogica. Het gepast aanbieden is de taak van de berichtverwerkingslogica. En dan hebben we nog het servicecontract, waarin staat wat de service doet (de zogenaamde operaties). Het servicecontract staat los van de andere elementen en bestaat uit een WSDL definitie en een XML-schema definitie. Hierdoor is het vergelijkbaar met een traditionele application programming interface (API). Technisch gezien is het service contract de basis voor een koppelvlak, al dan niet aangevuld met andere specificaties.

Uit bovenstaande kunnen we concluderen dat een webservice meer bevat dan alleen een stukje functionaliteit. Het gebruik van services voor informatie-uitwisseling vereist daardoor meer standaarden dan alleen SOAP en XML. Onderstaande protocol stack laat zien welke standaarden worden gebruikt voor informatie-uitwisseling met services.



Figuur 7.8 – Webservices protocol stack (Juric, Mathew, & Sarang, 2006)

We hebben eerder al aangehaald, dat het gebruik van services om meer vraagt dan SOAP en XML. Bovenstaande afbeelding laat dit goed zien. Het is niet de bedoeling dat we hieronder de hele stack uitgebreid gaan beschrijven, hiervoor zijn er al tal van artikelen en boeken te vinden (zie bijvoorbeeld Curbera et al., 2002; Erl, 2008; Newcomer & Lomow, 2005; Weerawarana et al., 2005). In het kader van de generieke procesinfrastructuur die we later gaan beschrijven, is het nodig om de functie van de belangrijkste open standaarden hieronder kort toe te lichten. We beginnen onderaan:

- HTTP is voor adressering en communicatie tussen een webclient (meestal een webbrowser) en een webserver.
- XML is voor het coderen/opmaken van berichtinhoud.
- SOAP is voor het schrijven van berichten.
- WSDL is voor het beschrijven van interfaces van services.
- UDDI is een bibliotheek (telefoonboek) voor het vinden van services.

- WS- staat voor de vele deelaspecten die om wat meer uitleg vragen. Zo zijn er standaarden voor adressering (WS-addressing), beveiliging (WS-security), betrouwbaarheid (WS-reliable messaging), etc. Het wordt aan de gebruikers van de standaarden overgelaten welke aspecten voor hun services van belang zijn. Dat heeft voordelen (meer flexibiliteit, snellere implementatie), maar ook nadelen (complexe structuur van berichten en minder interoperabiliteit). Een voorbeeld is de keuze voor een beveiligingsarchitectuur. In point-to-point situaties wordt de vertrouwelijkheid en de integriteit van de gegevens meestal afgedwongen door het gebruik van de Secure Socket Layer (SSL), of diens opvolger Transport Layer Security (TLS), bijvoorbeeld door het verzenden van berichten via HTTPS. TLS werkt op transport niveau en WS-Security werkt op berichtniveau. WS-Security lost het bredere probleem op van de handhaving van de integriteit en de vertrouwelijkheid van de berichten, onafhankelijk van het transportprotocol. Dus ook als het bericht via verschillende transportprotocollen en tussenstations wordt getransporteerd (end-to-end security). Deze vorm van services is eenvoudig te implementeren, maar kent een relatief grote overhead. Toepassing van TLS reduceert de overhead in SOAP berichten, omdat het niet nodig is de sleutels en handtekeningen voor het verzenden te coderen in XML. TLS is geen signing protocol, XML-Signature wel. Tevens geldt dat encryptie op transport niveau om andere maatregelen vraagt dan encryptie op berichtniveau. We besteden in hoofdstuk 8 meer aandacht aan de gemaakte keuzes rond het beveiligingsvraagstuk.
- BPEL4WS is een taal voor het beschrijven in welke volgorde en onder welke voorwaarden individuele of gebundelde services worden aangeroepen. Bij gebundelde services, ook wel een service compositie genoemd, wordt via een service een set services aangeroepen. Met BPEL4WS kunnen in de procesinfrastructuur applicaties en i-processen met behulp van diensten van heterogene omgevingen worden gebundeld, zonder rekening te houden met de details en verschillen van die omgevingen. We komen later terug op het belang van deze standaard voor het flexibel aanroepen en orkestreren van services.

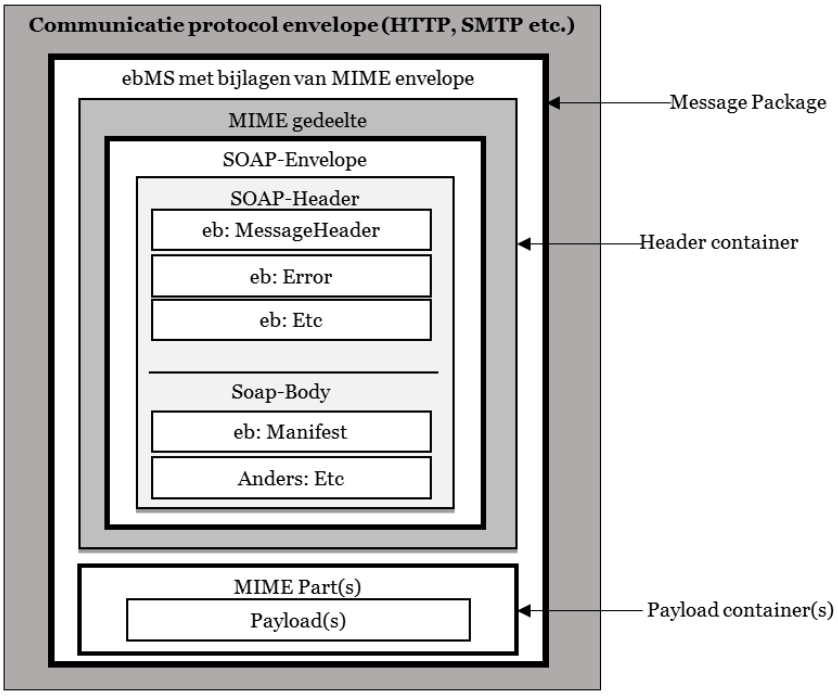
Zoals afgebeeld vormt het XML-document het fundament van de webservice, omdat het al de toepassingsspecifieke gegevens bevat die een service gebruiker ter verwerking aan de service aanbieder zendt. De documenten die een webservice kan verwerken zijn beschreven in een XML-schema; twee i-processen die deelnemen in een webserviceconversatie moeten toegang hebben tot dezelfde beschrijving om te verzekeren dat ze de documenten die ze uitwisselen kunnen valideren en interpreteren. Deze informatie wordt meestal met WSDL beschreven. Het gebruik van de bovengenoemde standaarden maakt services onafhankelijk van leverancier, programmeertaal of besturingssysteem.

EbMS

We hebben gezegd dat op basis van SOAP twee belangrijke protocolfamilies zijn ontstaan, namelijk Webservices en ebMS (e-business XML Message Service). We staan hier kort stil bij ebMS, aangezien deze familie relevant is voor het Digikoppeling koppelvlak dat we later zullen beschrijven. Net als webservices is EbMS gebaseerd op open standaarden, waarbij dezelfde duidelijke combinatie aanwezig is van XML en

internet gerelateerde standaarden, waaronder SOAP (Turner, 2003). Deze protocolfamilie kent een beperkter toepassingsgebied dan webservices, en is gericht op situaties waarin beveiliging en betrouwbaarheid van oudsher een grote rol spelen. De standaard regelt die aspecten al door middel van een Collaboration Protocol Agreement (CPA), een contract waarin de configuratie van de verbinding is opgenomen.

Bij ebMS is er sprake van twee endpoints, beide systemen 'kennen' de locatie van de ander. Aspecten als beveiliging, betrouwbaarheid en adressering liggen al vast in de CPA. Daarmee ontstaat de situatie dat de implementatie van ebMS ingewikkelder is, maar dat eenmaal geïmplementeerd de communicatie zelf veel simpeler is en minder overhead kent. Door de simpelere en kleinere berichten kent ebMS vooral een toename in efficiëntie bij grote hoeveelheden gegevens en hoogfrequente informatieuitwisseling. Onderstaande figuur geeft een versimpelde weergave van de onderdelen van een ebMS bericht, inclusief een SOAP envelop.



Figuur 7.9 – De structuur van ebMS berichten

SOAP versie 1.1 kan niet dienen als envelop voor meerdere soorten berichtinhoud. Soms is het echter wenselijk om meerdere soorten payload in één SOAP-envelop te stoppen, bijvoorbeeld omdat deze bij elkaar horen. Denk aan een bericht en een bij-

behorende digitale handtekening als ondertekening van dat bericht. Om dit wel mogelijk te maken worden binnen ebMS verschillende MIME-onderdelen hiërarchisch in de body van het SOAP-bericht opgenomen.

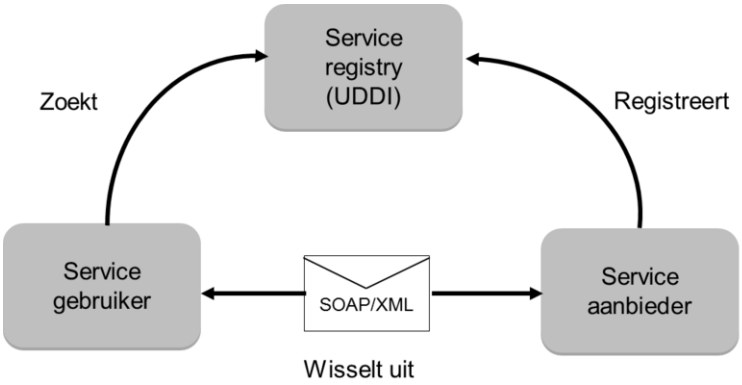
MIME (Multipurpose Internet Mail Extensions) definieert onder andere mogelijkheden om in het bericht aan te geven welke soort gegevens het bevat ('mimetype') en om het bericht op te delen in meerdere delen ('multipart'). Elk deel ('part') kan weer een eigen mimetype hebben, waaronder opnieuw het type multipart. Het bijzondere is dat hiermee hiërarchische structuren kunnen worden gedefinieerd, en dat daarmee in principe alle soorten gemengde inhoud in één enkel bericht kan worden opgenomen (uiteraard zitten daaraan wel technische limieten). Dat maakt het mogelijk om bijvoorbeeld het eigenlijke bericht in tekstformaat te combineren met stuurinformatie, een binaire bijlage en een digitale handtekening. Elk in hun eigen mimepart gescheiden door boundaries.

7.3.4 *SOA voor de ondersteuning van flexibele i-processen*

Service oriented architecture (SOA) gaat verder dan de eerder beschreven SOAP, webservices, BPEL en andere technologische mogelijkheden. Koppelvlakken en webservices op zich zijn onvoldoende voor de realisatie van eenduidige informatie-uitwisseling. Er is ook behoefte aan een overkoepelende visie over de interacties, koppelingen en het procesverloop (wanneer is welke service nodig en waar staat die service?). SOA is een strategische richting binnen de evolutie van IT in het algemeen.

Op zichzelf is SOA geen revolutionair concept - het basisidee bestond al halverwege de jaren tachtig. Toename van elektronisch berichtenverkeer in ketens en de behoefte aan flexibiliteit en hergebruik hebben dit concept de afgelopen jaren opnieuw en prominenter op de business en IT agenda gezet. Dit omdat SOA de nadruk legt op samenwerking van services, onafhankelijk van implementatie en ook van platform. Daarnaast speelt SOA een rol bij de behoefte om applicaties te laten samenwerken (enterprise application integration) en bij de behoefte om de interacties tussen organisaties onderling te automatiseren (Linthicum, 2003). Het meest onderscheidende van dit concept is dat het organisaties dwingt om na te denken over hergebruik van functionaliteiten, de interfaces van services, de granulariteit van services en contractueel vastgelegde kwaliteit van services. De assumptie is dat services zullen worden gebruikt in meer dan één i-proces. Hierdoor wordt een grote nadruk gelegd op het ontwerp van elektronisch berichtenverkeer en tegelijkertijd op ontwerp en implementatie van de procesinfrastructuur waarop deze services draaien. Dit dwingt partijen verder ook tot gebruik van standaarden binnen een keten.

De basis van de SOA-architectuurstijl is de driedeling tussen service gebruikers, aanbieders en een service directory, zoals afgebeeld in figuur 7.10. In dit SOA-patroon is het idee, dat iedere keer dat een gebruiker iets wil, eerst in de 'gouden gids' gekeken wordt (Service directory, UDDI). Waarna vervolgens de meest geschikte aanbieder of combinatie van aanbieders geselecteerd wordt. Hierna wordt een proces gestart om de aanbieders ook daadwerkelijk aan te roepen (via webservices-technologie: SOAP/XML).



Figuur 7.10 - Oorspronkelijke gedachte achter de service gerichte architectuur (Curbera et al., 2002)

Het onderschrift van bovenstaande figuur verwijst bewust naar de oorspronkelijke gedachte achter een SOA. Er zijn drie redenen waarom we dit als oorspronkelijk betitelen:

1. In de praktijk wordt er nauwelijks meer 'naar buiten gebeld' voor het aanroepen van services uit een UDDI. Dit vanwege beveiligingsoverwegingen (zie § 7.4).
2. Er zijn veel alternatieve patronen binnen SOA, onder andere met een service bus voor het koppelen van services. We beschrijven later in dit hoofdstuk dit alternatieve patroon.
3. In SOA is er de partij die de service 'host' en een partij die de service aanroept. Maar dat zegt niet altijd iets over welke kant de informatie opgaat. Tegenwoordig is het gebruikelijk dat zowel een basisregistratie als een afnemer services hosten. De afnemer kan ad hoc een basisregistratie (service) raadplegen, maar kan ook gebeurtenis gedreven informatie ontvangen (op zijn eigen service) van de basisregistratie.

Ondanks bovenstaande is het voor dit hoofdstuk relevant om de basis achter SOA volgens het oorspronkelijke model uit te leggen. Hierin worden drie rollen onderscheiden, namelijk die van de service gebruiker, service aanbieder en service registry. Deze rollen worden hieronder uitgewerkt.

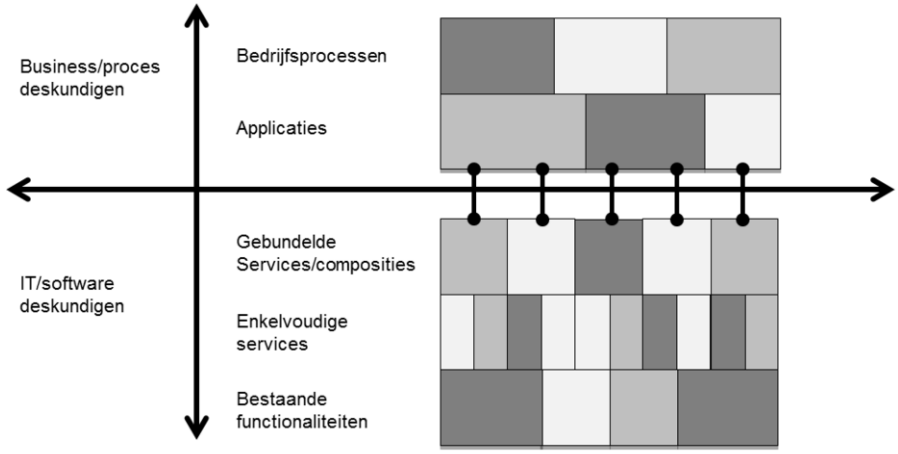
De service aanbieder biedt een service aan om een stukje geautomatiseerde procesafhandeling te realiseren. Middels de service is de service aanbieder in staat om te reageren op externe verzoeken in de vorm van berichten. De partij die deze berichten verstuurt, de service gebruiker, verlangt een zekere prestatie van de ontvangende partij; diens service representeert deze prestatie. De aanbieder van een service registreert deze in een service register. Dit register (in het jargon ook wel UDDI – Universal Description, Discovery and Integration genaamd) is te vergelijken met een telefoongids (Curbera et al., 2002). Aanbieders kunnen zichzelf en hun services via het register kenbaar maken en gebruikers kunnen deze op afstand aanroepen ('naar buiten bellen'). De wijze waarop van services van een aanbieder gebruik kan worden

gemaakt, is in een zogenaamd servicecontract (zie figuur 7.7) beschreven. Deze beschrijving wordt via een service register aan de omgeving beschikbaar gesteld. Een service beschrijft dus zowel de gegevens die worden geleverd/verwerkt als de condities waaronder deze gegevens worden geleverd/verwerkt. Het daadwerkelijk uitwisselen van gegevens vindt plaats middels een technische implementatie van zo'n service. Vaak wordt daarbij gebruik gemaakt van de eerder besproken webservices technologie, die gebruik maakt van een onderliggend webserviceprotocol stack (figuur 7.8) voor elektronisch berichtenverkeer. Service gebruikers kunnen vervolgens deze services aanroepen, die ze vinden in een service directory. Software systemen worden als service aanbieders gezien voor andere software systemen, de service aanvragers.

Tenslotte is het hier belangrijk om stil te staan bij de typen services. Volgens McGovern c.s. (2006) kunnen services op verschillende manieren worden getypeerd. Een bekende indeling in typen functionaliteit is: presentatieservices, processervices, business-services, applicatieservices en dataservices. Voor elk type service gelden verschillende methoden voor het identificeren. In dit hoofdstuk gaan we vooral in op de business- en applicatieservices. Ook deze twee typen services kunnen echter nog verder worden getypeerd, bijvoorbeeld raadplegen, selecteren, registreren, muteren, verwijderen, beëindigen, transformeren, genereren of waarden valideren en berekenen.

Granulariteit

We maken hier een zijsprong in de verhaallijn om aandacht te besteden aan een complex vraagstuk in SOA, namelijk wat de granulariteit of fijnkorreligheid van de services moet zijn om de doelstelling rond informatie-uitwisseling te realiseren. Met de granulariteit van een service wordt de reikwijdte van de geboden functionaliteit weergegeven (Van der Laan, 2006). Sinds SOA en webservices populair zijn geworden, wordt er gediscussieerd over de vraag hoe services het beste kunnen worden geïdentificeerd. Wanneer is een service 'te groot' of 'te klein', wanneer is deze 'te specifiek' of juist precies 'goed'? We beschouwen hier enkele inzichten uit de literatuur op dit gebied (Feenstra, 2011). Vaak wordt in dit kader een onderscheid gemaakt tussen 'fine-grained' (enkelvoudige functionaliteit) en 'coarse-grained' (gebundelde functionaliteit) services (Arsanjani, 2002). Fine-grained services leveren een beperkt stukje bruikbare business-proces functionaliteit, zoals basic data toegang. Coarse-grained services worden samengesteld uit fine-grained services, die intelligent samengevoegd worden om aan specifieke bedrijfsbehoeften te voldoen. We komen hier weer op het punt van gebundelde services (zogenaamde composities). Onderstaande afbeelding helpt om dit onderscheid helder te maken.



Figuur 7.11 – Granulariteitsvraagstuk

Volgens Carter (2007) slagen veel SOA projecten niet, omdat de granulariteit verkeerd bepaald is. Dit komt omdat business/proces deskundigen vaak in gebundelde functionaliteiten denken, terwijl IT-deskundigen in enkelvoudige functionaliteiten denken. Om deze twee werelden te overbruggen beveelt hij aan de granulariteit van een service zo grof mogelijk te houden; liefst op het niveau van de applicatie(module). Hoe grover de granulariteit, hoe groter de onafhankelijkheid en de zelfvoorziening van de service kan zijn (Papazoglou & Georgakopoulos, 2003). Dat wil zeggen, de service kan een complete interne transactie aan (zoals een nieuwe order) zonder daarbij afhankelijk te zijn van andere services. Dit is natuurlijk een algemene uitspraak. De praktijk is ingewikkelder: een te grof niveau van granulariteit kan hergebruik ook weer in de weg staan, omdat maar bepaalde elementen hergebruikt kunnen worden en niet gehele applicaties. Bovendien moeten services voor hergebruik ontworpen worden, bijvoorbeeld door configuratie opties toe te voegen (Feenstra, 2011). Het vaststellen van het juiste niveau van granulariteit in specifieke situaties is bij uitstek het werk van de architect. Tot slot: wat een goed afgebakende service is, hangt uiteraard ook af van de invalshoek. Zo stelt een beheerder andere eisen dan een procesontwerper of een tester.

7.3.4.1 Enterprise Service Bus

Een belangrijk SOA-patroon is dat van de zogenaamde Service Bus. In ICT-jargon ook wel een Enterprise Service Bus (ESB) genoemd. Dit is een bepaalde invulling voor een SOA, zoals we die eerder hebben afgebeeld in figuur 7.10. Als integratietechnologie zorgt een ESB ervoor dat de services overal kunnen worden aangeroepen, ongeacht platform en programmeertaal. Het is hier belangrijk om te realiseren dat een ESB in de generieke zin geen softwareproduct is, maar een bepaalde architectuurstijl of patroon. Hierdoor zijn er veel soorten ESB's en ze verschillen in de mogelijkheden die geboden worden (Chappell, 2004). Wel bieden ze elk een 'abstractie laag' die verantwoordelijk is voor het beheer van het berichtenverkeer, waardoor de software componenten consistent en efficiënt kunnen aansluiten en berichten

naar elkaar kunnen sturen. Een ESB maakt het mogelijk dat de services onderling communiceren en op die manier een vast gedefinieerd i-proces uitvoeren.

Volgens Carter (2007) zijn de belangrijkste functies van een ESB:

- Routeren van berichten tussen services
- Converteren van transport protocollen tussen aanroep en service (koppelvlakfunctie)
- Transformeren van berichtformaat tussen aanroep en service
- Bewaken van de afgesproken quality of service (security, reliability, en transacted interactions)

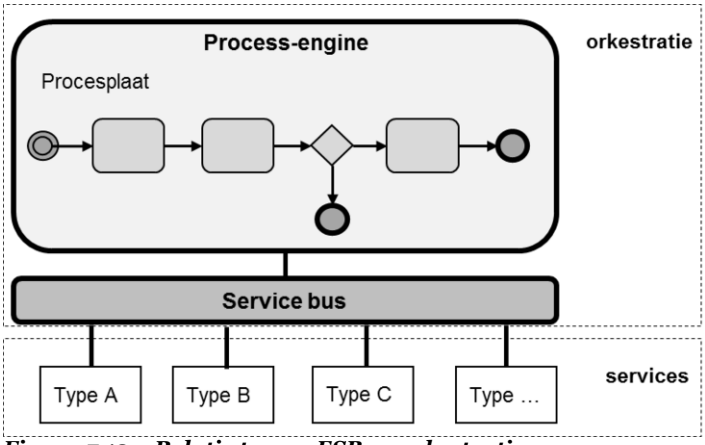
Naast bovenstaande functies leidt het gebruik van een ESB tot complexiteitsreductie, aangezien een grote hoeveelheid bilaterale relaties wordt vervangen door een kleiner aantal multilaterale relaties. Deze zijn gemakkelijker te onderhouden. Vanuit het oogpunt van een procesinfrastructuur bevordert dit de mogelijkheid tot het (her)gebruiken van de gewenste services, zowel intern als buiten de organisatie. Gewenste services kunnen uit een grotere pool geselecteerd worden wanneer bijvoorbeeld geen specifieke programmeertaal vereist is. Nieuwe services worden door hergebruik of minder eisen aan compatibiliteit sneller in de generieke procesinfrastructuur opgenomen. Gevolg is dat gemakkelijker aan de eisen van de gebruikers tegemoet gekomen kan worden.

De meerwaarde van de ESB zit in het verbinden van ontkoppelde services. Een ESB kan in meerdere (typen) omgevingen toegepast worden, van specifiek tot zeer generiek. Er is sprake van een specifieke situatie wanneer de services gezamenlijk een applicatie met één functionaliteit bieden (één compositie). De voordelen van ontkoppelde services, qua onderhoud en reductie van complexiteit, worden hier gecombineerd met een rigide procesuitvoering. De geschetste situatie heeft alleen voordeel bij omvangrijke en complexe systemen die één specifieke taak hebben. Een ESB kan gebruikt worden in combinatie met een process-engine die de volgorde van de aan te roepen services bepaalt (meerdere composities). De process-engine kan op deze wijze verschillende i-processen uitvoeren, die al dan niet dezelfde services gebruiken. De volgende paragraaf gaat hier nader op in.

7.3.4.2 Orkestratie door de process-engine (BPEL4WS)

Hoewel de ESB als koppelvlak tussen services een essentiële functie vervult, moet er nog meer gebeuren willen we geautomatiseerd verschillende functionaliteiten aanroepen voor het verwerken van een bericht. Hiervoor is het concept process-engine ontwikkeld, dat webservice functionaliteiten volgens een bepaalde volgorde aanroept. De uitkomst daarvan wordt procesorkestratie genoemd. Dit is wat anders dan het ketenorkestratie concept, dat in de volgende hoofdstukken terugkomt. De term orkestratie wordt hier gebruikt om aan te geven dat process-engine zich verhoudt tot individuele webservices als een dirigent tot alle orkestleden (Janssen & Gortmaker, 2005). Tijdens het concert geeft de dirigent (process-engine) aan wanneer welk orkestlid (webservice) wat moet doen. De process-engine heeft een sturende rol, omdat deze de procesflow bepaalt. De ESB maakt het mogelijk dat één generieke process-engine een verscheidenheid aan services aan kan spreken. Deze services kunnen in verschillende programmeertalen opgezet zijn en zich binnen en buiten de organisatie

bevinden. Op deze wijze maakt een ESB orkestratie veel eenvoudiger. Onderstaande figuur geeft een overzicht hiervan.



Figuur 7.12 – Relatie tussen ESB en orkestratie

Wat opvalt in de getoonde opzet is de procesplaat die sturing geeft aan de procesflow. In de process-engine worden de geautomatiseerde informatieverwerkingsprocessen direct afgeleid van de bedrijfsprocessen – bijvoorbeeld gedefinieerd in BPMN (zie hoofdstuk 5 – I-Processen over deze standaard voor procesmodellering) – en als uitvoerbaar i-proces geïmplementeerd. Wanneer informatie met bijbehorend informatieverwerkingsverzoek wordt aangeleverd bij de ESB (via een koppelvlak moet worden afgehandeld, portaal of een onafhankelijke applicatie), stelt de process-engine vast welk i-proces dient te worden afgehandeld. Vervolgens worden stap voor stap automatisch alle services uitgevoerd die onderdeel uitmaken van het i-proces dat bij de aangevraagde informatieverwerking hoort. Figuur 7.12 zegt ook iets over de rol van een ESB. Een ESB kan meerdere typen services ondersteunen met de bijbehorende protocollen. Wanneer bijvoorbeeld webservices ondersteund worden, dan betekent dit dat er invulling gegeven wordt aan SOAP en WSDL. De meeste ESB's leveren een brede ondersteuning van communicatiestijlen, waaronder publish-subscribe en gegarandeerde aflevering (Van der Laan, 2006). Zoals we in § 7.4 beschrijven is dit een belangrijke voorwaarde bij het uitwisselen van verschillende typen berichten.

BPEL4WS

Nu de relatie tussen de ESB en de process-engine is beschreven, kunnen we kijken naar de standaarden voor orkestratie. De de-facto standaard voor orkestratie is BPEL4WS. Dat staat voor Business Process Execution Language (BPEL) for Web-Services (https://www.oasis-open.org/committees/wsbpel/). Bij deze taal wordt er van uitgegaan dat er een centrale component bestaat, een zogenaamde process-engine, die alle webservices aanstuurt en aanroept (Khalaf, Keller, & Leymann, 2006). Hierdoor ontstaat een hub-en-spoke model met de process-engine in het midden. Dit is anders dan bij choreografie, dat meer een peer-to-peer karakter heeft (Kloppmann, Koenig, Leymann, Pfau, & Roller, 2004). BPEL is ontwikkeld om invocaties van webservices in een bepaalde volgorde te orkestreren. Hierbij worden met behulp van BPEL uitvoerbare processen (executables) gedefinieerd. Een uitvoerbaar

proces beschrijft een white-boxmodel van een proces en kan door een BPEL-server daadwerkelijk worden uitgevoerd. Een executable is ontworpen om webservices aan te roepen en daarnaast is het ook mogelijk het uitvoerbare proces zelf als een webservice aan te bieden. Versie 2.0 van BPEL4WS zal ook proceslogica gaan bevatten, die traditioneel alleen in workflowtalen aanwezig was. Zo biedt het de mogelijkheid taken door mensen te laten uitvoeren. Door individuele services in de gewenste volgorde te orkestreren kunnen i-processen optimaal worden ondersteund met functionaliteit en gegevens uit alle interne systemen én uit systemen van partners (Janssen, Gortmaker, & Wagenaar, 2006). Per uitgewisseld bericht kunnen de beschikbare services in de gewenste volgorde met de gewenste parameters worden aangeroepen. De gedachte achter SOA wat betreft hergebruik van services kan op deze manier worden gerealiseerd. Op deze wijze draagt orkestratie bij aan het generieke karakter van een procesinfrastructuur.

Bij de invulling die aan de orkestratie wordt gegeven, moet een aantal keuzes gemaakt worden die bepalend zijn voor de eigenschappen van de procesinfrastructuur. De processtappen (volgorde van aan te roepen services) kunnen volledig van tevoren worden gedefinieerd. Een andere mogelijkheid is om op basis van de laatst bekende proceseigenschappen de volgende service te bepalen. In beide gevallen kunnen individuele services die worden aangeroepen, lokaal (binnen het eigen systeem) aanwezig zijn of buiten de grenzen van de organisatie in het beheer van derden. Bij services van derden kan ervoor worden gekozen alleen bekende, gescreende services te gebruiken of een openbare servicecatalogus aan te roepen waar derden zelf de services aanbieden.

Het gebruik van BPEL kent twee voordelen (Gortmaker, Janssen, & Wagenaar, 2004). Ten eerste is orkestratie nodig voor een volledige procesbeschrijving en zorgvuldige afhandeling van de i-processen. Een process-engine wordt gebruikt om i-processen te automatiseren die onderdeel uitmaken van een workflow waarvoor andere applicaties en services nodig zijn. Om dit mogelijk te maken gebruikt de procesengine de integratie- en mediationfunctionaliteit van de ESB. Ten tweede kan het uitvoeren van het i-proces worden ontkoppeld van de machine waar de deelprocessen uiteindelijk wordt uitgevoerd. Daarmee worden deze processen beter beheersbaar en ook wordt hergebruik op deze manier makkelijker gemaakt. Webservices kunnen immers vervangen worden door andere webservices. In hoofdstuk 5 (I-Processen) is hiervan een voorbeeld opgenomen. Tot slot moet orkestratie gezien worden als meer dan alleen een technische laag. Net zoals webservices op herbruikbaarheid ontworpen moeten worden, dienen processen ook herbruikbaar te zijn en moet duidelijk zijn wie verantwoordelijk is voor de uitvoering. Hoofdstuk 9 gaat dieper in op de verantwoordelijkheidsverdeling.

7.4 Digipoort

In dit derde deel van het hoofdstuk behandelen we hoe bij SBR invulling is gegeven aan de hiervoor beschreven technologie: Digipoort. Digipoort kan worden beschouwd als het resultaat van de wisselwerking tussen de behoefte aan een generieke infrastructuur en de technologische mogelijkheden daarvoor, die in voorgaande paragrafen behandeld zijn.

In hoofdstuk 1 zijn de bouwblokken van SBR kort beschreven. Digipoort omvat de twee bouwblokken Koppelvlakservices en de Verwerkingsservices, die werken conform de technische standaarden.

We hebben in de voorgaande delen Digipoort aangeduid als een procesinfrastructuur voor de S2S uitwisseling en gedeelde verwerking van verantwoordingsinformatie. Er komt echter veel meer bij kijken als we deze black box willen ontsluieren. Zelfs de naam behoeft meer uitleg. Enerzijds is er Digipoort PI (Procesinfrastructuur), anderzijds is er Digipoort OTP (Overheidstransactie-poort). Deze tweedeling kan enige verwarring opleveren. Het is daarom van belang om helder weer te geven wat we in dit hoofdstuk onder de naam 'Digipoort' verstaan. Beide procesinfrastructuren zijn technisch gescheiden E-infrastructuren die door Logius worden onderhouden, maar hebben - behalve de benaming 'Digipoort' - qua opzet weinig overeenkomsten. Digipoort OTP komt voort uit het OTP-programma en de voorlopers daarvan. De OTP wordt onder andere voor communicatie met de Douane gebruikt via het verouderde X.400 protocol, maar gebruikt ook SMTP (MSA/MTA), POP3 en FTP. Digipoort PI is voortgekomen uit het PvE GEIN, zoals genoemd in § 7.2.2. De informatieverwerkingsprocessen voor verantwoordingsinformatie (i-processen) binnen het SBR Programma lopen alleen over Digipoort PI. Andere informatiestromen dan verantwoordingsprocessen kunnen ook aansluiten op de PI. Wanneer in deze paragraaf over Digipoort wordt gesproken, wordt alleen gerefereerd aan het gedeelte van Digipoort PI waar de verantwoordingsprocessen over lopen. Digipoort OTP blijft volledig buiten beschouwing.

Ondanks deze afbakening is het te pretentieus om te stellen dat we in één hoofdstuk alle relevante aspecten kunnen uitdiepen. Met alle documentatie die de afgelopen jaren omtrent Digipoort is opgeleverd, kan een boekenkast worden gevuld. Dat is overigens geheel in lijn met projecten van deze omvang in de publieke sector. We moeten daarom keuzes maken in wat we hier behandelen. Opnieuw is het principe dat we relevante technische inzichten willen bieden voor gebruikers, leidend. Het voordeel is nu, dat zowel de behoefte als de onderliggende technologie (webservices, SOAP, BPEL4WS) al in de vorige paragrafen zijn beschreven. Voor niet technische zaken, zoals regie, organisatie en beheervraagstukken verwijzen wij naar de hoofdstukken 2 tot en met 4 en hoofdstuk 9. Hierdoor kunnen we ons concentreren op de volgende aspecten van Digipoort:

- Welke afspraken zijn er rond koppelvlakken gemaakt?
- Wat doet Digipoort?
- Hoe is de gewenste flexibiliteit in i-processen gerealiseerd?
- Welke i-processen worden georkestreerd?
- Welke services worden uiteindelijk aan de uitvragende partijen geboden?
- Wat zijn de implicaties voor de gebruikers?

Bovenstaande vragen vormen de inhoudsopgave voor de rest van deze paragraaf.

7.4.1 *Welke afspraken zijn er rond koppelvlakken gemaakt?*

De gewenste loose coupling binnen de keten, toegankelijkheid van Digipoort en ontkoppeling met de gegevenslaag worden gerealiseerd met generieke koppelvlakken.

Hierbij gaat het om koppelvlakken ten behoeve van gebruikers (bedrijven) en koppelvlakken ten behoeve van de afnemers (overheid). Dit onderscheid resulteert in drie typen geïmplementeerde koppelvlakken:

1. SOAP2008
2. WUS (acroniem voor WSDL, UDDI en SOAP) voor Bedrijven
3. ebMS Digikoppeling

Eerder hebben we een vrij eenvoudige definitie voor een koppelvlak gegeven, een system-to-system verbinding tussen informatiesystemen die de uitwisseling van informatie faciliteert. Deze definitie is technisch georiënteerd, maar er komt meer bij kijken dan standaarden alleen. Dit wordt ook al gesuggereerd door het gegeven dat interoperabiliteit zich vooral op organisatorisch niveau bevindt. De koppelvlakspecificaties zijn een afsprakenset voor gegevensuitwisseling met Digipoort. Binnen deze afsprakenset komt een aantal aspecten aan bod:

- De technische standaarden. De specificatie van de verschillende (open) standaarden die gebruikt worden voor verbinding, gegevensuitwisseling en beveiliging. De technische standaarden beslaan de fysieke laag, communicatie-sublaag en applicatie-sublaag. Deze lagen zijn eerder toegelicht in § 7.3. Verbinding vindt plaats op de fysieke laag. Hier vinden we de gangbare internetstandaarden zoals TCP/IP en HTTP. De gegevensuitwisseling beslaat de daadwerkelijk uitgewisselde berichten op de communicatie-sublaag. De standaard SOAP is al aan bod gekomen. De beveiliging speelt een rol op verschillende lagen. Deze variëren van de verbinding via de fysieke laag (SSL/TLS) tot de communicatie-sublaag (encryptie van uitgewisselde berichten), tot en met de berichtinhoud (digitaal ondertekenen). We komen terug op de beveiligingsaspecten in hoofdstuk 8.
- De toepassing /configuratie. Een koppelvlakspecificatie is meer dan alleen een specificatie van de gebruikte technische standaard(en). De specificaties omvatten ook afspraken over hoe precies met de technische standaarden wordt omgegaan. Er gelden afspraken over de invulling van verplichte en verboden velden in het SOAP-bericht, er zijn eisen aan de gebruikte certificaten en er is een maximum berichtgrootte opgelegd. Deze afspraken maken dat het gebruik van de gekozen technische standaarden daadwerkelijk aansluit bij de specifieke eisen van de i-processen qua beveiliging, authenticatie, onweerlegbaarheid en verwerkingscapaciteit.
- De endpoints. Een eenvoudig, maar essentieel onderdeel van een koppelvlak is het adres waarop Digipoort via het desbetreffende koppelvlak te bereiken is. Dit wordt een endpoint genoemd. Het endpoint is een URL zoals wij deze kennen van websites. Er wordt alleen geen server aangesproken die ons een website in onze browser laat zien; met de URL wordt de aanleverservice van Digipoort aangesproken.
- De payload (inhoud van een bericht). Het gebruik van generieke koppelvlakken maakt dat de uitgewisselde informatie los staat van de modaliteit. Een SOAP-bericht geldt als een envelop voor de verantwoordingsinformatie, statusmelding of mededeling die via de koppelvlakken wordt uitgewisseld. De SOAP-standaard kan een MIME-object als payload hebben. MIME is geen bekende term, maar toch kent iedereen het van de bijlagen (attachment) in een e-mail. We kunnen verschillende bestanden meesturen, bijvoorbeeld

een PDF-bestand, vakantiefoto's, een XML-bericht, (malafide) programmacode, een XBRL-instance etc. In het geval van Digipoort wordt alleen een XBRL-instance als payload geaccepteerd.

Keuze voor open standaarden
De drie typen koppelvlakken van Digipoort zijn zo generiek mogelijk van opzet door aan te sluiten bij gangbare open standaarden. De volgende beweegredenen lagen ten grondslag aan deze keuze binnen het SBR Programma:

- Open standaarden worden veelal door een groot aantal partijen omarmd en hoe meer deze gebruikt worden, hoe groter de interoperabiliteit wordt.
- Over een groot aantal open standaarden is reeds kennis in de markt aanwezig. Dit maakt acceptatie eenvoudiger en resulteert in minder kosten bij marktpartijen en overheden. Ook is er geen afhankelijkheid van een beperkte capaciteit aan expertise bij Logius of een niche in de markt. De gekozen open standaarden zijn vaak al (deels) ingericht voor andere doeleinden.
- De meer gangbare open standaarden zijn over het algemeen relatief eenvoudig te implementeren. Er bestaan modules voor vele nieuwe en legacy (oude) systemen, softwarepakketten en programmeertalen. Het aansluiten van een heterogeen publiek is daarmee eenvoudiger.
- De overheid kan bedrijven moeilijk verplichten producten bij één private partij af te nemen. Dit is vanuit maatschappelijk oogpunt onwenselijk. Met de keuze voor een gesloten (proprietary) standaard zou er kunstmatig een monopolypositie worden gecreëerd. Mogelijke gevolgen zijn vendor lock-in, concurrentievoordeel en prijsstijgingen. De kans hierop wordt groter wanneer er door verplichtstelling geen alternatieve kanalen beschikbaar zijn.
- Open standaarden worden in overleg tussen vele partijen veranderd. Over het algemeen wordt er goed nagedacht over de gevolgen van veranderingen, waardoor men niet aan de willekeur van een bepaalde partij wordt overgeleverd.

De drie typen koppelvlakken zijn goed gedocumenteerd en informatie is vrij beschikbaar. We gaan hieronder verder met een korte beschrijving van de koppelvlakken.

Drie typen geïmplementeerde koppelvlakken
Zoals beschreven zijn er drie typen koppelvlakken die Digipoort kent: SOAP2008, WUS voor Bedrijven en ebMS Digikoppeling. Dit zijn koppelvlakken die door Logius zijn ontworpen op basis van open standaarden. Deze worden ook buiten het SBR-domein toegepast. Binnen het SBR-domein wordt nog een aantal aanvullende eisen gesteld. Die eisen komen voort uit de specifieke context van de verantwoordingen. De aanvullende eisen vallen onder de eerder genoemde configuratie binnen de koppelvlakspecificaties. We beschouwen hieronder de overeenkomsten en verschillen tussen de drie typen.

Elk van de drie beschikbare koppelvlakspecificaties is gebaseerd op het SOAP-protocol. De aanvullende eisen en specificaties die het kader vormen waarbinnen het SOAP-protocol gebruikt wordt, maken dat de eigenschappen van de koppelvlakken sterk uiteen lopen. Van de drie typen koppelvlakken zijn inmiddels nieuwe versies

verschenen. Op hoofdlijnen verandert een koppelvlakspecificatie niet. Details wijzigen om aan de laatste eisen en wensen van de i-processen voor verantwoording te voldoen, bijvoorbeeld door een nieuwe functionaliteit of andere vorm van beveiliging te ondersteunen. De verschillende versies blijven maanden naast elkaar beschikbaar, zodat alle gebruikers ruim voldoende tijd hebben om over te gaan naar de nieuwe versies.

De koppelvlakken SOAP2008 en WUS voor Bedrijven zijn afgeleid van de standaard Webservice specificaties. Beide gebruiken het SOAP-protocol als basis en vereisen een aantal aanvullende WS-specificaties, waaronder WS-security. SOAP2008 geeft bij aanlevering direct terugkoppeling over het hele proces, terwijl aanleveren via WUS voor Bedrijven alleen directe terugkoppeling geeft over de eerste stap (aanlevering bij Digipoort). Hiertegenover staat dat WUS vooral bij piekbelasting betrouwbaarder is.

SOAP2008 en WUS voor Bedrijven zijn gericht op de 'voorkant' van Digipoort: de aanleverende partijen. De overhead van deze koppelvlakken is door de vele WS-extensieprotocollen groter dan bij ebMS Digikoppeling, maar de implementatie en het gebruik zijn vele malen eenvoudiger. Ook kennen deze protocollen één endpoint, dat van Digipoort. Het geheel van deze eigenschappen maakt SOAP2008 en WUS voor Bedrijven bij uitstek geschikt om een grote groep heterogene gebruikers aan te sluiten. Ze kunnen gezien worden als het stelsel van kleine wegen dat een woonwijk ontsluit: veel aansluiting met weinig verkeer.

Het koppelvlak ebMS Digikoppeling is afgeleid van de ebMS-standaard. In vergelijking met SOAP2008 en WUS voor Bedrijven is het een veel gecompliceerder koppelvlak. Implementatie en dagelijks gebruik vergen meer expertise en inzet. Daar staat een aantal voordelen tegenover, dat vooral bij grote hoeveelheden berichten naar voren komt. De overhead per bericht is veel kleiner én 'reliable messaging' – een aantal beveiligingsaspecten voor wederzijds berichtenverkeer – is al ingebakken. In analogie met het wegennet kan ebMS Digikoppeling gezien worden als een snelweg: lastiger aan te leggen dan een klein weggetje, maar het kent een veel hogere capaciteit en grotere mate van efficiëntie. Vandaar dat gebruik van ebMS Digikoppeling met name zinvol is aan de 'achterkant' van Digipoort, als verbinding met de uitvragende partijen.

Het ebMS-protocol gebruikt twee endpoints: één aan elke kant van de verbinding. De andere partij, naast Digipoort, moet vooraf bekend zijn. Dit zou onhandig zijn aan de 'voorkant'. Authenticatie op basis van een PKIoverheidscertificaat is aan de voorkant beter op zijn plaats. De beschikking over twee endpoints maakt het wel mogelijk dat elke partij berichtenverkeer kan initiëren. Op elk gewenst moment kan Digipoort gevalideerde berichten en statusinformatie afleveren bij de uitvragende partij. Statusupdates en mededelingen kunnen van en naar Digipoort worden gestuurd.

Hoewel we hebben beschreven langs welke koppelvlakken we de procesinfrastructuur kunnen bereiken, is nog niet uitgelegd wat Digipoort – de procesinfrastructuur – nu precies doet. De volgende paragraaf gaat in op de werking van de procesinfrastructuur.

7.4.2 *Wat doet Digipoort?*

We hebben hiervoor Digipoort steeds als een black box beschouwd. Hier gaan we de black box openen, zodat duidelijk wordt welke functionaliteiten vervuld moeten worden, oftewel: welke services moet Digipoort bieden? Het antwoord op deze vraag hangt af van de keten die aangesloten wordt. De eigenschappen van het uit te wisselen bericht en die van de te ondersteunen bedrijfsprocessen bepalen de eisen van de generieke procesinfrastructuur. Er zijn behoorlijk wat aspecten die hierbij aan bod komen, zoals het noodzakelijke beveiligingsniveau en de noodzaak voor archiveren. We starten met een simpel voorbeeld, gevolgd door een uitgebreide analyse.

Simpel uitgedrukt werkt Digipoort in drie stappen:

1. Een bedrijf stuurt een envelop met adresgegevens (elektronisch bericht), waar documenten aan kunnen worden toegevoegd, naar Digipoort.
2. Digipoort sorteert de documenten uit het bericht, voert eventuele validaties uit en kijkt voor welke overheidsinstelling ze bestemd zijn.
3. Digipoort levert het bericht met de juiste documenten af bij de juiste ontvanger(s).

Van iedere verstuurde envelop wordt bekeken of de afzender wel bekend en geautoriseerd is voor het versturen van gegevens naar de ontvanger. Authenticatie en beveiliging zijn daarom belangrijke aspecten van Digipoort. Hieronder volgt een uitgebreidere analyse van de eisen die voortkomen uit de verantwoordingsketen.

Tabel 7.2 – Typische eisen en functionaliteiten die noodzakelijk zijn voor informatie-uitwisseling

Eisen aan informatie-uitwisseling	**Communicatie-sublaag**	**Applicatie- en gegevenslaag**	**Proces- en gebruikerslaag**
Onweerlegbaarheid	Transportbevestiging, Reliable messaging	Ontvangstbevestiging, logging	Audit trail
Vertrouwelijkheid	Versleuteling kanaal	Versleuteling bericht	Autorisatie, machtiging
Integriteit	Grensvlak-bescherming	Ondertekening bericht	Elektronische handtekening
Betrouwbaarheid	Bufferen	Zeker stellen/ herinjecteren	Archiveren
Juistheid	Conformiteitscontrole koppelvlak	Schemavalidatie, inhoudelijke validatie	Bedrijfsregelvalidatie
Identificatie	Resource-identificatie	Berichtidentificatie	Partneridentificatie
Logistiek	Netwerkadressering en routering	Logische adressering en routering	Orkestratie
Informatieverwerking	Stapelen, ontstapelen	Samenvoegen, splitsen	Extractie, verrijking
Vertaling	Kanaalconversie	Berichtconversie	Transformatie

Bovenstaande tabel geeft een breed spectrum aan functionaliteiten. Niet alle functionaliteiten zijn nodig voor ieder i-proces. Het is denkbaar dat bepaalde berichten geen verrijking of splitsing behoeven.

7.4.3 *Hoe is de gewenste flexibiliteit in i-processen gerealiseerd?*

De gewenste flexibiliteit in de procesgang is binnen Digipoort door middel van een SOA gerealiseerd. We hebben in § 7.3 gezegd dat drie aspecten van SOA hiervoor cruciaal zijn: de services, de service bus en de process-engine. De hoofdelementen uit de SOA-architectuurstijl zijn terug te vinden in het ontwerp van Digipoort. Het applicatielandschap bestaat uit webservices. Er is een service bus als verbindend element tussen de services en een process-engine verzorgt orkestratie van de verschillende i-processen. De BPMN-i-processen en Nederlandse Taxonomie gelden als basis voor de orkestratie van services. Bij orkestratie gaat het om op basis van ontvangen informatie beslissingen te nemen over het te volgen i-proces en generieke delen van dat i-proces centraal uit te voeren. De centrale component – de process-engine – wordt ondersteund door verschillende hulpdiensten (services) voor bijvoorbeeld validatie, autorisatie en statusupdates (dit noemen we verwerkingsservices, deze zien toe op de technische verwerking van de aangeleverde informatie).

Zoals gezegd kent Digipoort verschillende koppelvlakken om te communiceren met zowel aanleverende als uitvragende partijen. Koppelvlakservices zorgen voor het aanleveren en afleveren van de berichten. De processen die binnen een bedrijf (bijvoorbeeld verantwoording opstellen) en uitvragende partij (verwerken van verantwoordingsinformatie) spelen, worden buiten beschouwing gelaten. We leggen hieronder de i-processen binnen Digipoort uit. Daarna worden de koppelvlakservices en verwerkingsservices beschreven die bij de procesuitvoering worden aangeroepen.

7.4.4 *Welke i-processen worden uitgevoerd?*

We hebben het eerder al over procesorkestratie gehad. Procesorkestratie is de vakterm voor de geautomatiseerde aanroep van services die volgens een specifieke volgorde i-processen uitvoeren. De i-processen, die zijn vastgelegd met behulp van een processtandaard, moeten gecontroleerd worden uitgevoerd met behulp van een process-engine. De process-engine en de koppelvlakservices waarborgen dat de i-processen steeds adequaat worden uitgevoerd en dat de betrokken partijen op de hoogte worden gehouden van de status van de lopende i-processen. Het uitvoeren van de i-processen bestaat uit het beheerst afwikkelen van afgebakende processtappen volgens een vastgestelde volgorde. De volgorde en condities worden direct afgeleid van de BPMN procesplaten en als executeerbaar i-proces geïmplementeerd. Wanneer informatie met bijbehorend informatieverwerkingsverzoek door een koppelvlakservice aangeleverd wordt bij de process-engine (via een portaal of via een onafhankelijke applicatie), stelt de process-engine op basis van de procesplaat vast welke verwerkingsservices moeten worden aangeroepen. Vervolgens worden stap voor stap automatisch alle services afgelopen die onderdeel uitmaken van het i-proces dat bij de aangevraagde informatieverwerking hoort. Services kunnen gericht zijn op verschillende vormen van informatieverwerking. Denk hierbij aan analyses met als uitkomst een rapport of informatiebeveiliging met als resultaat ‘bevoegd’ of ‘niet bevoegd’. Een i-proces heeft vaak meerdere mogelijke uitkomsten, die afhankelijk van de aangeleverde informatie aan de orde zijn. Hieronder volgt een opsomming van typische i-processen. Deze opsomming is een momentopname en is daardoor niet compleet. Er kan, afhankelijk van de informatieketen die we in beschouwing nemen, sprake zijn van meer, minder of alternatieve i-processen.

- Opzetten van een beveiligde verbinding
- Aanleveren van berichten
- Afleveren van berichten
- Herafleveren
- Vastleggen audit trail
- Status opvragen
- Authenticatie
- Autorisatie
- Zekerstellen
- Archiveren
- Rapportgeneratie
- Validatie
- Conversie
- Extractie/filtering

Hieronder volgt een korte beschrijving van de i-processen.

Opzetten van een beveiligde verbinding
Een beveiligde verbinding dient om de client/server-applicaties te beveiligen tegen bijvoorbeeld afluisteren. De beveiliging dient zowel vanuit de rol van client als die van server te kunnen worden opgezet. Het hiervoor thans gehanteerde protocol is SSL/TLS (dubbelzijdig). Hiervoor moet de aanleverende partij (bedrijf of intermediair) in bezit zijn van een geldig Certificaat van een door de overheid erkende en vertrouwde Certificate Autority (CA), die voldoet aan de eisen van PKIoverheid of vergelijkbaar. Met dit Certificaat en het Certificaat van de aanleverservice wordt de verbinding versleuteld. Indien het opzetten van de beveiligde verbinding niet lukt, dan eindigt het proces.

Aanleveren van berichten
Het aanleveren zorgt ervoor dat een aangeboden bericht door de aanleverende partij wordt aangenomen, gecontroleerd, zeker gesteld en geregistreerd, en dat de aanleverende partij terugkoppeling krijgt van het resultaat van aanleveren. Aanleveren gebeurt middels een aanleververzoek. Bij het aanleveren wordt gecontroleerd of het bericht voldoet aan de specificaties (zoals vastgelegd in de koppelvlakspecificaties). Deze controle kan onder andere toezien op:

- De aanwezigheid van de verplichte elementen
- De afwezigheid van onbekende elementen
- De waarden die de elementen bevatten, juiste waarde en juiste lengte
- De maximale berichtomvang voor het koppelvlak
- De aanwezigheid van de digitale handtekening

Indien het aanleververzoek niet aan de eisen voldoet, dan treedt er een fout op.

Afleveren van berichten
Bij afleveren wordt een bericht op vertrouwelijke en betrouwbare wijze overgedragen aan de bedoelde ontvanger. Deze heeft daartoe een service geïmplementeerd, die in staat is berichten te ontvangen volgens de geldende koppelvlakspecificaties. Het bericht dient opgemaakt te worden volgens deze specificaties.

Herafleveren
Indien de service van de ontvanger niet beschikbaar is, wordt een bericht opnieuw afgeleverd. De time-out periode en het aantal pogingen zijn configureerbaar.

Vastleggen audit trail
Draagt er zorg voor dat alle relevante informatie over verwerking van een bericht traceerbaar, onweerlegbaar en onwijzigbaar wordt vastgelegd. De audit trail is er met name voor intern gebruik, zoals foutopsporing. Op basis van de audit trail kunnen rapportages gemaakt worden om de uitvragende partijen te informeren over het functioneren van Digipoort. Beschikbaarheid van de procesinfrastructuur, uitval op basis van foutieve berichtinhoud en doorlooptijden van berichten vormen interessante statistische informatie over het presteren van de i-processen.

Status opvragen
Stelt aanleveraars in staat om navraag te doen naar de verwerkingsstatus van hun aangeleverde berichten. De statusinformatie is een selectie van informatie uit de audit trail, die voor de aanleverende partij relevant en begrijpelijk is. De statusinformatie geeft aan welke stappen doorlopen zijn. De laatste stap is de actuele status van de verwerking. De statusinformatie wordt opgevraagd via de statusservice.

Authenticatie
Bij authenticatie wordt de identiteit van de aanleveraar van een verzoek vastgesteld met een bepaald betrouwbaarheidsniveau.

De identiteit van de aanleverende partij is in een betrouwbare registratie vastgelegd. Het kan hier gaan om:

- Een basisregistratie: NHR (KvK-nummer, RSIN); of GBA (BSN)
- De administratie van een dienstverlener (fiscaal nummer, BTW-nummer)
- Een gelijkwaardige buitenlandse registratie

Er zijn verschillende varianten denkbaar hoe de authenticatie praktisch kan geschieden:

- Variant 1: op basis van een Certificaat met daarin een OIN of een HRN opgenomen identiteit
- Variant 2: op basis van een Certificaat zonder identificerend nummer van de aanleverende partij
- Variant 3: op basis van een externe authenticatiedienst

Autorisatie
Bij autorisatie wordt gecontroleerd of de aanleverende partij geautoriseerd is gebruik te maken van een bepaalde dienst (het opvragen of aanleveren van informatie). Deze autorisatie is aanvullend op de autorisatie die wordt uitgevoerd bij het opbouwen van een beveiligde verbinding. Voorafgaand aan de autorisatie is altijd een authenticatie van de aanleverende partij uitgevoerd. De op basis daarvan vastgestelde identiteit wordt gebruikt bij de autorisatie. Er zijn verschillende varianten denkbaar hoe de autorisatie praktisch kan geschieden:

- Blacklist: de identiteit van de aanleverende partij komt NIET voor op een lijst van aanleveraars die niet vertrouwd worden.

- Whitelist: de identiteit van de aanleverende partij komt WEL voor op een lijst van aanleveraars die vertrouwd worden.
- Onvoldoende betrouwbaar: de identiteit van de aanleverende partij is vastgesteld met een betrouwbaarheidsniveau dat lager is dan het voor de dienst vereiste betrouwbaarheidsniveau.
- Bevoegdheidscontrole: de aanleverende partij is bevoegd om namens de in het bericht opgenomen belanghebbende te handelen. Controle vindt plaats via een register waarin bevoegdheden zijn vastgelegd, bijvoorbeeld een machtigingenregister.

Zekerstellen
Vastleggen van een identiek afschrift van een bericht. Hiermee is het bericht beschermd tegen verwerkingsfouten waarbij het bericht verloren zou kunnen gaan. In de basale vorm wordt een bericht zeker gesteld totdat verwerking en archivering zijn voltooid, en wordt daarna verwijderd. Op verzoek van de ketenverantwoordelijke kan een bericht langer worden zekergesteld.

Archiveren
Draagt er zorg voor dat archiefbescheiden in combinatie met de audit trail kunnen worden bewaard, totdat ze aan een volgende archiefvormer worden overgedragen of de archieftermijn is verstreken.

Rapportgeneratie
Relevante informatie uit de audittrail-database wordt verzameld en in een overzichtelijk format geplaatst.

Validatie
Een bericht (de payload) wordt gevalideerd aan de hand van een schema/model. Indien het bericht niet valide is bevonden, dan volgt een validatierapport dat als basis kan dienen voor het verdere verloop van het i-proces. Varianten die kunnen voorkomen, zijn bijvoorbeeld:

- Schemavalidatie: validatie op basis van een xml-schemadefinitie (xsd)
- XBRL-validatie: validatie op basis van business rules vastgelegd in XBRL
- Taxonomische validatie: inhoudelijke validatie aan de hand van een domeintaxonomie

Conversie
Een bericht dat is aangeleverd in een bepaald berichtschema wordt geconverteerd naar een equivalent bericht in een ander berichtschema, gebruikmakend van een set conversieregels.

Extractie/filtering
Alleen die gegevens uit berichten worden doorgegeven, die in een vervolgstap van het i-proces zijn toegestaan of nodig zijn.

Uit de bovenstaande procesbeschrijvingen kunnen we het volgende concluderen:

- De i-processen van de verschillende verantwoordingsstromen zijn op hoofdlijnen vrijwel identiek. De exacte configuratie kan wel per berichtsoort verschillen.
- De berichtsoort bepaalt het i-proces dat doorlopen wordt.
- Interne applicaties worden als services gemodelleerd, aangeroepen en geconfigureerd. Hierbij gaat het vrijwel alleen om interne services. Slechts bij autorisatie wordt een externe service aangeroepen.
- Het hergebruik van services is mogelijk. Hierdoor zijn deze bij een veranderende taxonomie nog steeds bruikbaar (configureerbaar).

We gaan in de volgende paragraaf nader in op een aantal services dat georkestreerd wordt.

7.4.5 *Welke services worden door Digipoort aangeroepen?*

De services die Digipoort biedt, hebben een 'generieke' interface. Dat wil zeggen dat ze kunnen worden gebruikt om verschillende 'berichtsoorten' mee uit te wisselen. Andere diensten kunnen gebruik maken van deze generieke services. Dat gebeurt bijvoorbeeld door het domein DigiInkoop en diens voorloper, E-factureren.

In deze paragraaf beschrijven we een aantal services dat in Digipoort wordt gebruikt in het kader van de i-processen voor verantwoordingsinformatie. Ook hier geldt dat dit overzicht een momentopname is. Voor specifieke informatieketens kunnen er ook andere services worden ontwikkeld en aangeroepen. We maken onderscheid tussen koppelvlakservices en verwerkingsservices. Koppelvlakservices (K) omvatten de aanleverservice, de afleverservice en de statussinformatieservice. De overige services zijn verwerkingsservices, uitgevoerd door de process-engine (V). De volgende services komen bij deze beschouwing aan bod:

1. Aanleverservice (K)
2. Statusinformatieservice (voor aanleverende partij) (K)
3. Zekerstel- en archiefservice (V)
4. Validatieservice (V)
5. Machtigingenservice (V)
6. Statusupdateservice (voor uitvragende partij) (V)
7. Afleverservice (K)

Opvallend is dat de genoemde services op 'business niveau' zijn benoemd. Hierdoor is hergebruik van services makkelijker. We kiezen voor een grove granulariteit (bundeling van meerdere enkelvoudige functionaliteiten), omdat we anders veel losstaande services moeten opsommen waarvan de samenhang niet geheel duidelijk is. Hierna volgt een beknopte uiteenzetting van de eerder opgesomde services.

1. Aanleverservice
Digipoort biedt voor het aanleveren van elektronische berichten door een bedrijf een 'Aanleverservice'. Via de koppelvlakken wordt de aanleverservice aangesproken door de aanleverende partij (bedrijf of intermediair). De aanleverservice doorloopt per aangeleverd bericht een heel aantal handelingen. Deze handelingen zijn in te delen in berichtcontrole, procesinitiatie en feedback.

De eerste stap die de aanleverservice doorloopt, is de berichtcontrole. Het koppelvlak kent een aantal specificaties – eisen – waaraan de aangeleverde berichten moeten voldoen. De basiscontrole bestaat uit de volgende elementen:

- Controle op aanwezigheid van een bekende berichtsoort. Zonder berichtsoort weet de aanleverservice bij de procesinitiatie niet welk i-proces doorlopen moet worden, waardoor er geen i-proces kan plaatsvinden.
- Controle op maximale berichtgrootte. De omvang van de aangeleverde berichten is gelimiteerd om de performance van Digipoort te garanderen.
- Controle op aanwezigheid van verplichte elementen en afwezigheid van verboden elementen.
- Authenticatie. Controle op geldigheid van het gebruikte PKIoverheidcertificaat. Controle of het certificaat voorkomt op een blacklist (lijst van te weigeren certificaten) of whitelist ('gastenlijst' van te accepteren certificaten).

Indien het bericht aan de specificaties van de basiscontrole voldoet, volgt de procesinitiatie. Het doel van de procesinitiatie is dat het bericht verder zal worden verwerkt door Digipoort en het af te leveren aan de uitvragende partij. Ten eerste wordt een berichtkenmerk aangemaakt om de verwerking van het bericht te kunnen traceren. Het zekerstellen van het originele bericht vindt ook in deze fase plaats – de bijbehorende service wordt in de volgende paragraaf beschreven. Op basis van de berichtsoort wordt het juiste type i-proces in de process-engine aangesproken. Het bericht wordt aan de process-engine overgedragen voor verdere verwerking.

De laatste stap in de aanleverservice is de feedback. De aanleverservice geeft ook direct feedback aan de aanleverende partij omtrent de controle op aanleverspecificaties. Dit is wenselijk vanuit het oogpunt van procesafhandeling. De directe feedback houdt in, dat wordt aangegeven of het aangeleverde bericht verder wordt verwerkt of dat er een fout is opgetreden. Bij een fout wordt een toelichting gegeven, zodat de aanleverende partij gericht acties kan ondernemen om een bericht aan te leveren dat wel geaccepteerd wordt. Bij gebruik van het SOAP2008 protocol wordt ook het resultaat van het gehele aanleverproces meegegeven. Bij WUS eindigt de sessie met acceptatie voor verdere verwerking of een fout. De status van de verdere verwerking moet apart worden opgehaald. Bij zowel SOAP2008 als WUS wordt het aangemaakte berichtkenmerk meegegeven, mits het bericht succesvol is ontvangen.

2. Statusservice (voor aanleverende partij)

De aanleverende partij kan van elk aangeleverd bericht de actuele status opvragen. Voor het opvragen van de status worden dezelfde koppelvlakken gebruikt als bij het aanleveren. Met een ander endpoint wordt de WSDL van de statusservice aangesproken. De aanleverende partij heeft bij het aanleveren van een bericht dat aan de aanleverspecificaties voldeed, een berichtkenmerk ontvangen. Onder dit kenmerk is ook de statusinformatie en audit trail binnen Digipoort opgeslagen. De respons van de statusservice is de statushistorie, ofwel een lijstje van de relevante handelingen (services) die het bericht heeft doorlopen alsmede het resultaat daarvan. De gebruiker van Digipoort kan hieruit het volgende concluderen:

- Het bericht is door de uitvragende partij geaccepteerd.
- Het bericht bevindt zich momenteel nog ergens in het i-proces.

- Ergens in het i-proces is een fout geconstateerd, met een toelichting op de inhoud van de fout.

3. Zekerstel-en archiefservice
Het zekerstellen houdt in dat een bericht dat de controle op de aanleverspecificaties succesvol doorlopen heeft, in originele staat – met WS-securityheader – wordt opgeslagen. Bij foutieve verwerking kan men het originele bericht gebruiken om de verwerking nogmaals te doorlopen. Ook bij onenigheid kan men terugvallen op het originele bericht zonder bewerking van Digipoort of de uitvragende partij. Hoofdstuk 5 (I-Processen) geeft meer inzicht in de rol van zekerstellen in proces-compliance. De zekerstelservice is een vast onderdeel binnen de aanleverservice. Aanvullend op de zekerstelservice is de archiefservice. De archiefservice archiveert berichten die de zekerstelservice aanbiedt voor een bepaalde periode. Het gebruik van de archiefservice is optioneel en hangt af van de afspraken tussen Digipoort en de uitvragende partij.

4. Validatieservice
De validatieservice controleert of de inhoud van het aangeleverde bericht in overeenstemming is met de Nederlandse Taxonomie en bijbehorende afspraken, waaronder het juiste gebruik van het XML-schema en de XBRL-standaard. In het bijzonder wordt gecontroleerd op:

- XBRL 2.1
- Dimensions 1.0
- Generic Links 1.0

Er wordt enkel gevalideerd op de Nederlandse Taxonomie. Digipoort is zodanig ingericht dat zij geen extensietaxonomie van buiten Digipoort kan ophalen of raadplegen. Zie hoofdstuk 6 (Gegevens) voor nadere toelichting op de XBRL-standaard en de Nederlandse Taxonomie.

De validatieservice draagt een bericht dat voldoet aan de Nederlandse Taxonomie over aan de afleverservice. Indien het bericht niet voldoet, wordt het niet afgeleverd. Afleveren en verdere verwerking heeft bij berichten met fouten immers geen zin, omdat het i-proces altijd in een fout zal resulteren. Bij de fouten wordt een heldere, doch vaak technische, toelichting gegeven. Wanneer de gebruiker de status van het aangeleverde bericht opvraagt, zal duidelijk worden waar de validatie mis is gegaan. De gebruiker kan de fout proberen te herstellen om vervolgens succesvol aan te leveren.

5. Machtigingenservice
De machtigingenservice bevraagt een vertrouwd register om vast te stellen of de partij die de aanlevering doet, ook daadwerkelijk bevoegd is de aanlevering te doen. De machtigingenservice verwerkt de respons van het vertrouwde register. Indien het register een respons met een bevoegdheidsverklaring geeft, geeft de machtigingenservice 'toestemming' om het aangeleverde bericht verder te verwerken. Wanneer de respons van het vertrouwde register geen bevoegdheidsverklaring bevat, wordt het bericht niet verder verwerkt. De aanleverende partij krijgt een foutmelding.

6. Statusupdateservice (voor uitvragende partij)
De statusupdateservice is relevant wanneer de uitvragende partij zelf nog een aantal (inhoudelijke) controles uitvoert, voordat de verantwoordingsinformatie voor verwerking wordt geaccepteerd. Het doel van de statusupdateservice is dat de aanleverende partijen kunnen worden geïnformeerd. De status dat een aangeleverd bericht door de uitvragende partij daadwerkelijk geaccepteerd is, zal voor veel processen het eindresultaat zijn. Zodra het aangeleverde bericht is afgeleverd bij de uitvragende partij, heeft Digipoort geen zicht meer op het procesverloop. Maar Digipoort is wel de plek waar de aanleverende partij de status zal opvragen over het al dan niet succesvol aanleveren van een bericht met verantwoordingsinformatie. De statusupdateservice stelt de uitvragende partijen in staat de status van de interne berichtcontroles toe te voegen aan de status die bij Digipoort per proceskenmerk wordt opgeslagen. Het gebruik van deze service is optioneel, aangezien niet iedere uitvragende partij een eigen berichtcontrole zal uitvoeren. In dat geval is het succesvol afleveren bij de uitvragende partij de eindstatus van het aangeleverde bericht.

7. Afleverservice
De process-engine draagt het bericht over aan de afleverservice voor aflevering aan de uitvragende partij. De afleverservice levert de berichten af aan de uitvragende partij die bij de berichtsoort hoort. Enkel gevalideerde berichten worden verstuurd. Hiermee wordt vervuiling – in de vorm van onverwerkbare of kwaadaardige berichten – van de systemen van de uitvragende partij geweerd. De afleverservice betreft het koppelvlak tussen Digipoort en de uitvragende partij. Ook bij de afleverservice kunnen de eerder genoemde koppelvlakken gebruikt worden. Hier geniet ebMS Digikoppeling de voorkeur, aangezien er hoogfrequent in beide richtingen grote aantallen berichten worden verstuurd. Dankzij de orkestrerende rol van de process-engine kunnen services alle gewenste procesconfiguraties doorlopen die invulling geven aan de procesinfrastructuur-rol van Digipoort. Bovenstaande lijst van services volstaat niet bij processen van andere aard dan verantwoordingsprocessen. Voor het ondersteunen van andere typen processen, die bijvoorbeeld om het converteren van een bericht vragen, moet in dat geval ook een conversieservice worden ontwikkeld.

7.4.6 *Wat zijn de implicaties voor gebruikers van de procesinfrastructuur?*

De beschreven keuzes in de architectuur van Digipoort hebben implicaties voor de gebruikersgroepen, namelijk bedrijven en uitvragende partijen. We bespreken hier de implicaties waar de gebruikers rekening mee moeten houden. Voor bedrijven (en eventueel de intermediairs) is Digipoort één digitaal loket voor verantwoordingsinformatie. Doordat deze procesinfrastructuur als een black box functioneert, hoeven bedrijven en intermediairs weinig kennis te hebben over de werking van Digipoort. De software van een bedrijf hoeft slechts een koppeling te kunnen leggen met Digipoort, waardoor het bericht automatisch goed wordt verzonden en ontvangen. Hierdoor stelt Digipoort bedrijven in staat op een eenvoudige en uniforme wijze informatie uit te wisselen met de overheid. Het conformeren aan de koppelvlakstandaarden is voor bedrijven/intermediairs het enige dat om inspanning vraagt. Koppelvlakstandaarden moeten zorgen voor maximale interoperabiliteit bij minimale ontwikkelingsinspanning. Om het voor marktpartijen zo snel en eenvoudig mogelijk

te maken om Digipoort te gebruiken, is ervoor gekozen zoveel mogelijk open standaarden en bestaande bouwstenen te gebruiken. De verwachting is, dat de gebruikte open standaarden zich de komende jaren verder zullen ontwikkelen en dat de communicatiebehoefte ook aan verandering onderhevig zal zijn. Het overleg met de markt dat nodig is om deze ontwikkelingen te accommoderen, is een governance thema waar we in de laatste hoofdstukken op terugkomen.

Voor de uitvragende partijen vormt Digipoort de verbinding met een grote en pluriforme groep bedrijven. Logius ondervangt met Digipoort een deel van de juridische, technische en ondersteuningsvraagstukken rond het aansluiten van bedrijven. Voor uitvragende partijen is Digipoort een procesinfrastructuur die bepaalde, goed afgebakende taken uit handen neemt. Handelingen zoals ontvangst, acceptatie en terugmelding worden door Digipoort uitgevoerd. Hierdoor kunnen de uitvragende partijen zich concentreren op taken die om veel inhoudelijke, domeingerichte expertise vragen. Daarnaast biedt Digipoort als SOA een flexibel procesverloop, waarbij eventuele (wets)wijzingen eenvoudig en eenduidig kunnen worden doorgevoerd. Tenslotte zorgt Digipoort ervoor dat de uitvragende partijen niet zelf een procesinfrastructuur hoeven te ontwikkelen, die aan de hoge eisen van betrouwbaarheid, beschikbaarheid en beveiliging voldoet. Dit bespaart in de kosten. Het conformeren aan de koppelvlakspecificaties is ook voor uitvragende partijen een randvoorwaarde.

7.5 Afsluiting

Het vervullen van de behoefte aan een procesinfrastructuur die gegevens neutraal zou kunnen opereren en flexibiliteit in procesverloop kon faciliteren, bleek ondanks de beschikbaarheid van bewezen technologische protocollen (SOAP, XML en webservices) geen gemakkelijke opgave. Redenen hiervoor zijn terug te vinden in deel 1 van dit boek. Denk hierbij aan onzekerheid inzake de behoefte en standaarden, wederzijdse afhankelijkheid, veranderdilemma's en het complexe besturingsvraagstuk van wijzigingen in ketens (zie hoofdstukken 2, 3 en 4). Binnen Digipoort geldt dat i-processen altijd vooraf gedefinieerd zijn en dat altijd in dezelfde volgorde de taken worden doorlopen. I-processen en activiteiten zoals aanleveren, gebruikersautorisatie, berichtvalidatie, archivering, zeker stellen en afleveren zijn typische voorbeelden van i-processen die voor alle uitvragende partijen relevant zijn en op dezelfde manier (lees: met dezelfde techniek) ondersteund kunnen worden. Dit onderstreept het belang van communicatie en het maken van afspraken. Er wordt dan ook wel gesteld, dat SOA slechts voor een klein deel met techniek te maken heeft en veel meer met het beschrijven van bedrijfsprocessen en met de communicatie over hoe tot standaardisatie binnen processen te komen. Het resultaat van de zoektocht is Digipoort, een gedeelde procesinfrastructuur ingericht conform de architectuurprincipes van flexibiliteit, open standaarden, loose coupling en platformonafhankelijkheid. In combinatie met de bouwblokken processpecificaties (hoofdstuk 5) en berichtspecificaties (hoofdstuk 6) komen we dichter bij het doel van SBR: een generieke overheidsoplossing voor de system-to-system (S2S) uitwisseling en gedeelde verwerking van verantwoordingsinformatie. We zeggen bewust 'dichterbij', omdat een belangrijk aspect van SBR tot nu toe nog niet is behandeld: de invulling van governance. Hier gaat hoofdstuk 9 op in. Voordat we daar aan toekomen, behandelen we een laatste belangrijk aspect van de techniek van SBR: de oplossingen die in het kader van informatiebeveiliging bij SBR zijn gerealiseerd (hoofdstuk 8).

8 Beveiliging van informatieketens

8.1 Inleiding

Personen en organisaties krijgen in de praktijk regelmatig te maken met identificatie, authenticatie en autorisatie, oftewel: beveiliging. Dit geldt voor private partijen onderling (kassamedewerker en klant, huisartsenpost en patiënt, werknemer die toegang heeft tot bepaalde dossiers), en in hun interactie met de overheid (denk aan de agent die iemand aanhoudt of bij het loket burgerzaken van de gemeente). Ook in het beveiligen van elektronisch verkeer – internetbankieren, belastingaangifte – zijn identificatie, authenticatie en autorisatie centrale elementen. In dit hoofdstuk ligt onze focus op het elektronisch berichtenverkeer tussen bedrijven en overheidspartijen.

Met de erkenning dat de overheid een belangrijke verantwoordelijkheid heeft bij het beveiligen van informatie die zij vraagt van en verstrekt aan bedrijven, heeft men in het kader van SBR bijzondere aandacht besteed aan het beveiligingsvraagstuk. Het gaat hier immers om informatie-uitwisseling en -verwerking waarbij

- de informatie bedrijfsgevoelig kan zijn (en dus vertrouwelijk);
- de informatie bestemd is voor specifieke overheidspartijen of specifieke ondernemingen;
- de overheidspartijen de informatie opvragen en verstrekken in het kader van de uitvoering van hun wettelijke taken;

- informatie verplicht door ondernemingen moet worden aangeleverd;
- informatie door gemachtigde tussenpersonen (bijvoorbeeld accountants) namens belanghebbenden kan worden aangeleverd en opgevraagd;
- op piekmomenten grote hoeveelheden informatie worden uitgewisseld en verwerkt;
- de uitwisseling geautomatiseerd plaatsvindt (tussen systemen oftewel system-to-system).

Kortom: het gaat om de geautomatiseerde afhandeling van grote hoeveelheden vertrouwelijke informatie. Voor de geautomatiseerde afhandeling gelden wettelijke eisen, die ook bepalend zijn voor de beveiligingsmaatregelen die er genomen kunnen worden. De Wet elektronisch bestuurlijk verkeer bijvoorbeeld bevat algemene regels betreffende elektronisch berichtenverkeer tussen burgers/bedrijven en bestuursorganen en tussen bestuursorganen onderling. Volgens deze en andere kaders (deze worden later genoemd) dienen de SBR-bouwblokken dusdanig te zijn ontwikkeld, dat zij op proportionele wijze voldoende zekerheid bieden voor een betrouwbare en vertrouwelijke berichtuitwisseling en -verwerking.

Tegen deze achtergrond geeft dit hoofdstuk antwoord op de vraag: *"Hoe is informatiebeveiliging in het kader van SBR geborgd?"* Het doel van dit hoofdstuk is om partijen (zowel publiek als privaat) die aan de slag willen met SBR, duidelijkheid te verschaffen over de beginselen, maatregelen en middelen waarmee ze te maken krijgen bij het aanleveren van berichten en het opvragen van informatie. Om verwarring te vermijden maken we bewust onderscheid tussen beginselen, maatregelen en middelen. 'Beginselen' liggen ten grondslag aan de wettelijke eisen en vormen de kaders voor informatiebeveiliging. Voorbeelden hiervan zijn authenticiteit en integriteit. Een 'maatregel' is een samenstel van middelen en regels dat wordt toegepast om aan de beginselen te kunnen voldoen. Voorbeelden zijn authenticatie en autorisatie. 'Middelen' duiden hier op technische en organisatorische instrumenten die gebruikt kunnen worden om beveiliging te realiseren. Voorbeelden zijn cryptografie, tijdstempels en een trusted third party. Al deze termen en voorbeelden komen in dit hoofdstuk aan de orde.

Informatiebeveiliging beslaat een breed spectrum van technische en organisatorische middelen, zoals het inrichten van firewalls, het versleutelen van berichten en het vaststellen van bevoegdheden. Maar ook het fysiek beschermen van hardware, het tijdig reageren op incidenten en het zorgen voor een uitwijkomgeving bij calamiteiten vallen onder informatiebeveiliging. Hoewel al deze middelen en processen relevant zijn voor de inrichting van elektronisch berichtenverkeer, zullen we ons hier beperken tot de specifieke beginselen, maatregelen en middelen die gezamenlijk door de samenwerkende ketenpartijen moeten worden ingevuld. Voor de bepaling van de scope zijn de volgende uitgangspunten leidend geweest:

- Het hoofdstuk dient de behoefte aan beveiliging van elektronisch berichtenverkeer tussen bedrijven en bestuursorganen expliciet te maken. Achterliggend aan die behoefte is de samenhang tussen de eisen uit de wetgeving, de risico's en de aard en doelstelling van de informatie-uitwisseling/ -verwerking.

- Het hoofdstuk dient inzicht te bieden in de functionele werking van de generieke bouwstenen die de basis vormen voor de 'end-to-end' beveiliging van informatieketens. Het gaat hier om een stelsel van beveiligingsmiddelen, dat gebruikt wordt voor identificatie (het claimen van een identiteit), authenticatie (ben je inderdaad wie je claimt te zijn?) en autorisatie (welke bevoegdheden heb je, al dan niet namens een ander?) van partijen die deelnemen aan het elektronisch berichtenverkeer. Deze bouwstenen verdienen extra aandacht aangezien deze niet door één organisatie geregeld kunnen worden, maar vragen om samenwerking over ketens[21] heen.
- Het hoofdstuk dient duidelijk te maken hoe de generieke bouwstenen in SBR worden toegepast en welke keuzes er bij de toepassing zijn gemaakt. Waarom of Vanuit welke praktische overwegingen en wettelijke beginselen zijn bepaalde keuzes gemaakt?

Naar bovenstaande uitgangspunten is de kern van het hoofdstuk in drie delen gesplitst. Het eerste deel (§ 8.2) beschrijft de behoefte en de relevante wettelijke kaders. Het tweede deel (§ 8.3) beschrijft de generieke bouwstenen die voorzien in de behoeften. Het derde deel (§ 8.4) gaat in op de keuzes die gemaakt zijn bij de beveiliging van SBR informatieketens. Het hoofdstuk sluit af met een reflectie op het ketenbeveiligingsvraagstuk (§ 8.5).

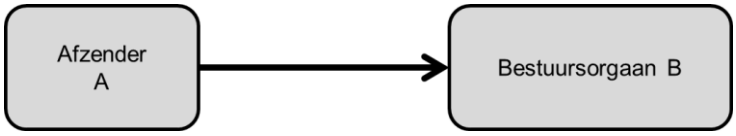
8.2 Behoefte en wettelijke kaders rond informatiebeveiliging

8.2.1 *Generiek model voor uitwisseling van informatie*

Wie zoekt op informatiebeveiliging (IT security management) komt tal van boeken, artikelen en richtlijnen tegen. Veelal krijgt de lezer lange lijsten van beveiligingseisen (vertrouwelijkheid, integriteit, beschikbaarheid etc.), maatregelen (identificatie, authenticatie, autorisatie etc.) en middelen (cryptografie, certificaten, machtigingenregister etc.) voor de kiezen. Deze begrippen krijgen echter pas betekenis als we de context - informatie-uitwisseling en informatieverwerking tussen twee partijen - onder de loep nemen.[22] We doen dit aan de hand van een generiek uitwisselingsmodel tussen twee organisaties: een afzender (A) en een bestuursorgaan (B).

[21] In hoofdstuk 2 hebben we al aangegeven dat het beschouwingsniveau 'keten' schakels als belanghebbende/intermediair – Digipoort – uitvragende partij omvat. Het beschouwingsniveau berichtenstroom omvat specifieke informatiestromen binnen een keten (bijvoorbeeld OB, VpB in de fiscale keten).

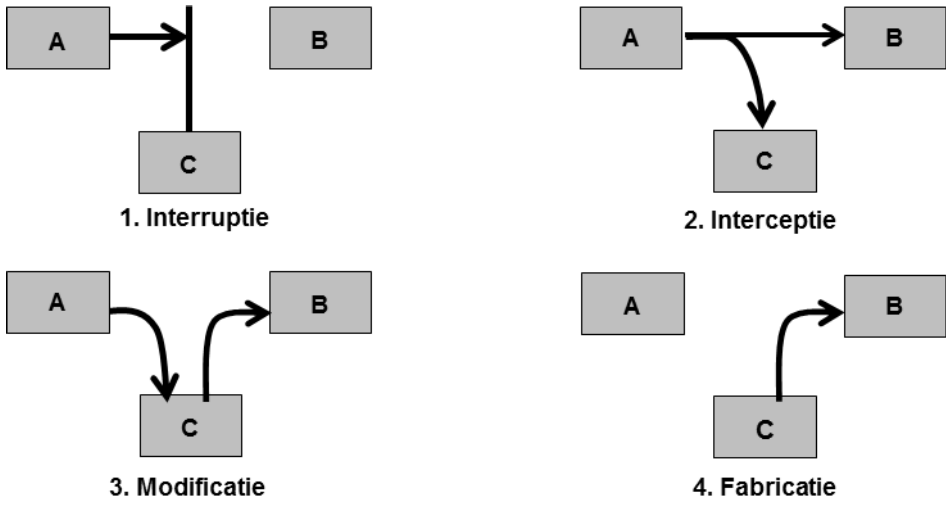
[22] We behandelen bewust niet alle mogelijke bedreigingen. Logische toegangsmaatregelen en andere beveiligingsmaatregelen (tegen brand, inbraak etc.) zijn belangrijk, maar vallen buiten de scope van het hoofdstuk. We focussen in dit hoofdstuk op de context van informatie-uitwisseling tussen twee partijen en informatieverwerking in een gedeelde procesinfrastructuur, en gaan daarom ook niet in op de risico's die binnen de organisatie van de afzender of de ontvanger kunnen bestaan.



Figuur 8.1 – Generiek uitwisselingsmodel tussen organisaties A en B

A wil zeker weten dat het bericht onderweg niet onderschept of gemanipuleerd is en alleen door B gelezen kan worden. B wil zeker weten dat het bericht van A afkomstig is en onderweg niet is gemanipuleerd, aangezien er op basis van het ingestuurde bericht van A beslissingen worden genomen die rechtsgevolgen hebben voor A.

De zekerheden die A en B willen, zijn echter niet vanzelfsprekend. Net als bij het uitwisselen van informatie op papier via de post is elektronische berichtuitwisseling niet zonder risico's. Een kwaadwillende, laten we deze hier partij C noemen, kan op diverse manieren de communicatie tussen A en B compromitteren. Dit wordt vaak aangeduid als een man-in-the-middle inbreuk. Partij C kan feitelijk ook een persoon binnen partij A of B zijn. Figuur 8.2 geeft een overzicht van een viertal man-in-the-middle inbreuken op de communicatie tussen A en B, die in de literatuur uitvoerig zijn beschreven (zie bijvoorbeeld Callegati, Cerroni, & Ramilli, 2009; Stallings, 2011).



Figuur 8.2 – Typologie van man-in-the-middle bedreigingen (vanuit een kwaadwillende partij C) die spelen bij elektronisch berichtenverkeer tussen organisaties A en B.

De eerste inbreuk – een interruptie – duidt op een aanval waarbij het bericht van A nooit aankomt bij B. De tweede inbreuk – een interceptie – duidt op een aanval waarbij een bericht wordt ingezien door partij C. De derde inbreuk – een modificatie – duidt op een aanval waarbij het oorspronkelijke bericht van A wordt onderschept en de inhoud hiervan wordt gewijzigd en doorgestuurd naar B. Tenslotte kan een be-

richt wel namens, maar zonder medeweten van A, door C worden opgesteld en gestuurd naar B. Men spreekt hier van een fabricatie. Hybride varianten zijn ook mogelijk en die vergroten het aantal potentiële beveiligingsinbreuken enorm. Deze hybride varianten worden niet verder uitgediept (zie hiervoor bijvoorbeeld Stallings, 2011).

Bovenstaande bedreigingen vormen onder meer de grondslag voor de wet- en regelgeving die normen stelt aan informatiebeveiliging bij uitwisseling van informatie met bestuursorganen, met name de Wet elektronisch bestuurlijk verkeer. De wetgever zag destijds (in 2002) het garanderen van voldoende veiligheid als een zwaarwegend probleem bij elektronische gegevensuitwisseling. "*Hoe kan men zeker weten dat de afzender degene is die hij zegt te zijn, en dat de inhoud van het stuk (onderweg) niet gewijzigd is? Hoe weet de afzender dat onbevoegden geen kennis kunnen nemen van de inhoud van het bericht?*"[23] Met het oog op deze vraagstukken is een wettelijk kader voor elektronisch verkeer gevormd.

8.2.2 *Wettelijk kader en beginselen voor informatiebeveiliging*

Met de Wet elektronisch bestuurlijk verkeer (in deze paragraaf: de wet) zijn bepalingen toegevoegd aan de Algemene wet bestuursrecht (Awb). Deze wet bevat algemene regels betreffende het verkeer langs elektronische weg tussen burgers/bedrijven en bestuursorganen. De wetgever licht toe dat het gebruik van papier bepaalde waarborgen met zich meebrengt, en wil dat aan elektronische berichten vergelijkbare eisen worden gesteld.[24] De wet formuleert een aantal abstracte normen met als centrale begrippen 'betrouwbaarheid' en 'vertrouwelijkheid'.
De wetgever licht deze begrippen als volgt toe:
"Berichten die langs elektronische weg door bestuursorganen worden verzonden, dienen in voldoende mate beveiligd te zijn. Eveneens dienen berichten die aan een bestuursorgaan worden gestuurd, door dat bestuursorgaan van de hand te kunnen worden gewezen indien het bestuursorgaan vermoedt dat het bericht in onvoldoende mate is beveiligd. In dit wetsvoorstel wordt deze eis tot uitdrukking gebracht door te spreken van betrouwbaarheid en vertrouwelijkheid."[25]

Betrouwbaarheid en vertrouwelijkheid zijn centrale begrippen die verwijzen naar een stelsel van nadere beginselen van beveiliging. Het is de bedoeling dat een bestuursorgaan rekening houdt met deze beginselen bij de concretisering van de begrippen:

- Authenticiteit
- Integriteit
- Onweerlegbaarheid
- Transparantie
- Beschikbaarheid

---

[23] Memorie van toelichting bij Wet elektronisch bestuurlijk verkeer, TK 2001-2002, 28 483, nr. 3, p. 14. (hierna: Memorie van toelichting)
[24] Memorie van toelichting, p. 14.
[25] Memorie van toelichting, p. 15

- Flexibiliteit
- Exclusiviteit

De beginselen zijn hierna op basis van de wetsgeschiedenis en de literatuur kort toegelicht. In de literatuur worden er verschillende definities aan gegeven. Ook worden de beginselen, vanwege de nauwe samenhang, vaak gecombineerd. Wij hanteren de hieronder gegeven interpretaties van de beginselen, en geven op basis daarvan invulling aan de begrippen betrouwbaarheid en vertrouwelijkheid.

8.2.2.1 Nadere uitwerking van beginselen

Met authenticiteit wordt volgens de wetgever gedoeld op de mate van zekerheid over de oorsprong van het document. Zijn de gegevens echt, is het bericht van de als afzender aangeduide persoon afkomstig? Authenticiteit kan ook betekenen dat de bron van (opgeslagen) gegevens bekend en geverifieerd is (Klingenberg, 2011). Indien een bestuursorgaan elektronisch een beschikking naar een bedrijf stuurt (bijvoorbeeld een toekenning van subsidie), is het van belang te kunnen (en te kunnen blijven) vaststellen dat het inderdaad van dat bestuursorgaan afkomstig is. In de praktijk zal voor een ontvangend bestuursorgaan het belang van zekerheid over de oorsprong vaak nog groter zijn.

Het beginsel van authenticiteit hangt nauw samen met integriteit en onweerlegbaarheid. En met transparantie: de authenticiteit moet ook achteraf en duurzaam vast te stellen zijn. In de literatuur wordt ook wel gesteld dat authenticiteit mede ziet op zekerheid over de identiteit van de afzender (Schellekens, 2004). Bij het streven naar een hoge mate van authenticiteit wil je inderdaad weten of de identiteit van de afzender 'klopt'. Een veelgebruikte maatregel hiervoor wordt authenticatie genoemd: het controleren van zowel de identiteit van de afzender als de oorsprong van het document. Let op: authenticatie is niet alleen aan het beginsel van authenticiteit gerelateerd, de maatregel dient meerdere functies (en beginselen). Wel willen we deze maatregel hier kort vanuit de theorie belichten. Over het algemeen vereist authenticatie de presentatie van 'credentials' (referenties) of items van waarde om te bewijzen dat je bent wie je beweert te zijn (Pipkin, 2000). De credentials of items van waarde zijn gebaseerd op unieke factoren die betrekking hebben op 'iets' wat je weet (kennis), iets wat je hebt (bezit) of iets wat je bent (persoonlijk kenmerk). Deze factoren worden soms in combinatie met elkaar gebruikt. De kennisfactor kan iets zijn dat alleen jij en degene die de authenticatie uitvoert kunnen weten, zoals een wachtwoord of een pincode. Dit is een factor die vaak wordt gebruikt in elektronisch berichtenverkeer, omdat het eenvoudig is te implementeren en te beheren. Het nadeel is dat een kennisfactor relatief gemakkelijk door een derde kan worden achterhaald (gekraakt). Dit komt met name doordat het in de aard van de mens zit om onzorgvuldig met zaken als een wachtwoord om te gaan. De bezitfactor verwijst naar een vorm van een identiteitsmiddel dat aan jou is toegewezen, bijvoorbeeld door een bedrijf of overheidsinstantie. Voorbeelden hiervan zijn een smartcard, een paspoort en een elektronisch certificaat. Het is op zich lastiger om een bezit goed na te maken en legitiem te doen voorkomen dan een kennisfactor. Tenslotte kun je door middel van een persoonlijk kenmerk zoals stem, vingerafdruk, iris patroon of andere biometrische kenmerken aantonen dat je inderdaad bent wie je claimt te zijn. De betrouw-

baarheid hier hangt af van het gekozen kenmerk. Bij multifactor-authenticatie gebruikt men een combinatie van bovenstaande factoren (bijvoorbeeld pincode op je smartcard) om de betrouwbaarheid te verhogen.
Met integriteit wordt gedoeld op de zekerheid dat gegevens volledig zijn en niet onbevoegd of door technische fouten of een storing zijn gewijzigd.[26] Met andere woorden, de mate waarin kan worden uitgesloten dat een document 'onderweg' wijzigt of onbevoegd gemanipuleerd wordt. Integriteit ziet ook op een goede werking van de ingerichte systemen: structurele juistheid en volledigheid van de verwerking en opslag van gegevens. Integriteit, net als authenticiteit en de andere genoemde beginselen, bevordert de rechtszekerheid (Klingenberg, 2011).

Onweerlegbaarheid wordt beschreven als de mate waarin niet door een afzender onterecht kan worden ontkend dat een bericht van hem is uitgegaan of de ontvanger onterecht kan ontkennen dat het bericht is ontvangen.[27]

Transparantie kan op twee manieren worden geïnterpreteerd: 1. transparantie over een gevolgd proces van informatieverwerking; 2. transparantie over de algemene werking van het systeem en welke middelen worden toegepast. Beide interpretaties sluiten elkaar overigens niet uit. De memorie van toelichting bij de wet volgt de eerste interpretatie en stelt dat transparantie staat voor de mogelijkheid dat wijzigingen van de gegevens achteraf kunnen worden opgespoord en inzichtelijk kunnen worden gemaakt. Dit impliceert eisen aan de opslag van gegevens en het mogelijk maken van controles (audit). In dat kader zijn archivering en het gebruik van audit trails in een systeem relevant. Ten aanzien van de tweede interpretatie wordt gesteld dat "*de werking van het systeem voor communicatie zichtbaar en begrijpelijk moet kunnen zijn*" (Klingenberg, 2011, p. 11). Het publiceren van informatie en documentatie door de overheid draagt bij aan deze vorm van transparantie. Voor het vervolg van dit hoofdstuk wordt de eerste interpretatie toegepast.

Archivering bij de overheid is geregeld in de Archiefwet 1995. De Archiefwet verplicht overheden om de 'archiefbescheiden' die zij ontvangen en creëren te archiveren.[28] De overheidspartij stelt in dat kader een selectielijst op, waarop staat wat niet bewaard hoeft te worden, wat wel, hoe lang, waar etc. In onderliggende regelgeving (Archiefbesluit en Archiefregeling) zijn eisen neergelegd waaraan archiefverantwoordelijke partijen dienen te voldoen bij het archiveren, met specifieke eisen voor elektronische archiefbescheiden. Bij elektronische processen is reconstrueerbaarheid van (de verwerking van) een ontvangen origineel bestand extra van belang, omdat elektronische bestanden eenvoudiger kunnen veranderen van inhoud, structuur en vorm. Er ontstaat een dubbele uitdaging: berichten dienen in hun oorspronkelijke vorm (zoals origineel ontvangen of gecreëerd) te worden gearchiveerd en tegelijkertijd moet de gearchiveerde en te archiveren informatie, mogelijk gevoelig en omvangrijk, beveiligd zijn. Het archief moet zijn afgeschermd voor toegang, inzage of

[26] Memorie van toelichting, p. 15.
[27] Memorie van toelichting, p. 15.
[28] Artikel 3 jo. 1 c Archiefwet 1995.

bewerking door onbevoegden (bijvoorbeeld door middel van versleuteling). Daarbij moet het voor bevoegde raadpleging wel beschikbaar blijven.

Beschikbaarheid refereert naar de bereikbaarheid en bruikbaarheid van de informatieverwerkingsdienst die wordt aangeboden door een bestuursorgaan, in relatie tot de eisen daaraan (bijvoorbeeld continu, 24/7). Er ligt voorts een relatie met toegankelijkheid van diensten van bestuursorganen voor burgers/bedrijven, in de zin dat het haalbaar moet zijn om de dienst te gebruiken met beschikbare en/of reguliere software.

Flexibiliteit is de mate waarin aan verschillende, veranderende en nieuwe eisen kan worden voldaan. Indien de technische mogelijkheden verbeteren, zou je het proces daarop kunnen aanpassen. Het is ook van belang om de mogelijkheden van inbraak in de systemen (door hackers) voor te blijven of op zijn minst bij te houden. Het bestuursorgaan dient zich in het kader van flexibiliteit de vraag te stellen of het haar systeem kan beschermen tegen nieuwe dreigingen. En of ze, in geval van verhoging van de eisen aan beveiliging van bovenaf (regels op Rijks- of Europees niveau ten aanzien van de vorm van identificatienummers; certificaatuitgifte etc.), deze gemakkelijk mee kan nemen in de bestaande inrichting van het elektronisch verkeer.

Exclusiviteit staat voor de exclusiviteit van een bericht en opgeslagen gegevens. Zijn de gegevens exclusief beschikbaar voor de geadresseerde, degene voor wie het bericht is bestemd? Dit hangt nauw samen met het bestuursrechtelijke beginsel van zorgvuldigheid. Men moet erop kunnen vertrouwen dat een overheidsorgaan op zorgvuldige wijze met haar gegevens omgaat (Klingenberg, 2011) en deze dus indien nodig vertrouwelijk behandelt, zoals bij persoonlijke of misbruikgevoelige gegevens. Bijzondere eisen aan exclusiviteit worden gesteld bij verwerking van persoonsgegevens. De basis voor deze eisen is te vinden in de Wet bescherming persoonsgegevens (Wbp).

Op de verantwoordelijke (verantwoordelijk voor de gegevens, bijvoorbeeld het ontvangende/verwerkende bestuursorgaan) rust een beveiligingsplicht, waaruit eisen voortvloeien aan de verwerking. De verantwoordelijke dient er zorg voor te dragen dat de beveiligingseisen tevens worden toegepast wanneer een bewerker (een andere partij namens de verantwoordelijke) verwerkingen verricht (artikelen 13 en 14 Wbp). Het College Bescherming Persoonsgegevens (CBP) geeft richtsnoeren voor de toepassing van de beveiligingsnormen uit de wet (Richtsnoeren beveiliging persoonsgegevens (CBP 2013), ter vervanging van AV 23 van 2001). Het document geeft aanwijzingen aan organisaties over hoe zij tot een ‘passend’ beveiligingsniveau kunnen komen. Het legt de nadruk op privacy-by-design, waarbij de bescherming van persoonsgegevens vanaf het begin in het informatiesysteem wordt ingebouwd, en het belang van risicoanalyses.

Niet alleen bij processen die primair gericht zijn op burgers en hun gegevens vindt verwerking van persoonsgegevens plaats. Ook indien de persoonsgegevens als neveninformatie onderdeel uitmaken van een bericht, geldt de Wbp. Bijvoorbeeld bij verwerking van verantwoordingsinformatie van ondernemers: namen van bestuurders in een jaarrekening die elektronisch wordt aangeleverd of adresgegevens van

eenmanszaken. Vertrouwelijke behandeling is tenslotte niet alleen bij persoonsgegevens aan de orde (afhankelijk van de categorieën en hoeveelheden). Ook andere gegevens in berichtenverkeer tussen personen/organisaties en bestuursorganen kunnen gevoelig zijn en maatregelen in het kader van exclusiviteit vereisen. Bijvoorbeeld concurrentiegevoelige informatie van bedrijven die wordt uitgewisseld met toezichthouders.

Bovenstaande beginselen zijn van belang voor het bevorderen van de rechtszekerheid. Hier is in het berichtenverkeer met bestuursorganen, waarin communicatie significante rechtsgevolgen kan hebben, met name behoefte aan.

8.2.2.2 Het geven van invulling aan betrouwbaarheid en vertrouwelijkheid

Aanvullend op deze beginselen van behoorlijk IT gebruik, heeft een bestuursorgaan altijd rekening te houden met de beginselen van zorgvuldigheid en evenredigheid. Zorgvuldigheid vraagt van een bestuursorgaan om een besluit zorgvuldig voor te bereiden, door het vergaren van de nodige kennis omtrent de relevante feiten en de af te wegen belangen. Bij het vaststellen van de maatregelen dient een bestuursorgaan rekening te houden met de eis van evenredigheid (proportionaliteit). Dit houdt in dat het te bereiken doel opweegt tegen eventuele geschonden belangen en dat het bestuursorgaan waar mogelijk de minst zware maatregelen of middelen gebruikt om het doel te bereiken (Ten Berge & Michiels, 2001).

Betrouwbaar en vertrouwelijk
In de wet is het als volgt geformuleerd:
Art. 2:14 lid 3 Awb
"*Indien een bestuursorgaan een bericht elektronisch verzendt, dan dient dit op een voldoende betrouwbare en vertrouwelijke manier te geschieden, gelet op de aard en inhoud van het bericht en het doel waarvoor het wordt gebruikt*."

Art. 2:15 lid 3 Awb
"*Een bestuursorgaan kan een elektronisch verzonden bericht weigeren voor zover de betrouwbaarheid en de vertrouwelijkheid van dit bericht onvoldoende is gewaarborgd, gelet op de aard en inhoud van het bericht en het doel waarvoor het wordt gebruikt*."

Uitgangspunt van de wet is dat het bestuursorgaan zelf invulling geeft aan het waarborgen van betrouwbaarheid en vertrouwelijkheid. Benadrukt wordt dat de invulling van de betrouwbaarheid en vertrouwelijkheid afhankelijk is van de stand der techniek. De wetteksten geven echter wel enkele suggesties voor de technische invulling. De memorie van toelichting bij de wet stelt bijvoorbeeld dat nuttige technieken om betrouwbaarheid en vertrouwelijkheid te bereiken, de elektronische handtekening, het tijdstempel en encryptie zijn. Er wordt een redelijk concrete toelichting gegeven op het versleutelen van berichten en Public Key Infrastructure (PKI).[29] Voor een op wilsuiting gerichte elektronische handtekening verwijst de wet naar het Burgerlijk Wetboek en de Telecommunicatiewet, waarin eisen aan gekwalificeerde certificaten zijn opgenomen.[30] Toch dient het bestuursorgaan uiteindelijk zelf te kiezen welke (combinatie van) concrete maatregelen zij hanteert.

[29] Memorie van toelichting, p. 16, 19, 21, 35.
[30] Artikel 2:16 Awb verklaart de regeling in artikel 15 van boek 3 van het Burgerlijk Wetboek en de Telecommunicatiewet t.a.v. (gekwalificeerde) certificaten van toepassing.

Het open karakter van de wettelijke normen zit met name in de genoemde mate van vertrouwelijkheid en betrouwbaarheid, namelijk 'voldoende' betrouwbaarheid en vertrouwelijkheid (niet maximaal of minimaal). De wet geeft aan hoe bepaald dient te worden wat voldoende is: "*gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt*". In geval van openbare informatie, bekendgemaakt door de gemeente, zal er een andere behoefte aan beveiliging zijn dan in geval van een belastingaangifte van een particulier. Daar zullen, afhankelijk van de stand der techniek, verschillende maatregelen voor getroffen worden.

Onze observatie is dat bestuursorganen, bij het invullen van waarborgen voor elektronische informatie-uitwisseling en -verwerking met burgers en bedrijven, met het volgende rekening dienen te houden:

- De genoemde beginselen
- De aard, inhoud en het doel van de uitgewisselde berichten
- De evenredigheid (proportionaliteit) van de te treffen maatregelen

In de wet wordt de gegeven invulling van de waarborgen van betrouwbaarheid en vertrouwelijkheid van een bericht aangeduid als het stellen van 'nadere eisen' door het bestuursorgaan.[31] De eisen en bijbehorende maatregelen kunnen technisch of organisatorisch van aard zijn, denk aan het verplichten van een digitale handtekening waarbij de certificaatuitgever aan bepaalde eisen voldoet. Daarbij is formele bekendmaking van de eisen en maatregelen wel noodzakelijk.[32] Indien er niet is voldaan aan de - door het bestuursorgaan kenbaar gemaakte - eisen, kan een bestuursorgaan weigeren om ontvangen berichten in behandeling te nemen. Het bestuursorgaan acht dan dat bijvoorbeeld de integriteit, authenticiteit of exclusiviteit niet is gewaarborgd. Dit kan bijvoorbeeld het geval zijn indien: "*de verzender niet voldoet aan de technische voorschriften die het bestuursorgaan stelt voor de ontvangst van bepaalde soorten berichten. De afzender maakt bijvoorbeeld gebruik van programmatuur waarmee het bestuursorgaan niet uit de voeten kan.*"[33]

Deelconclusie

De beginselen uit de wetsgeschiedenis geven blijk van bewustzijn van de man-in-the-middle-bedreigingen als interruptie, interceptie, modificatie en fabricatie, en van de vluchtigheid van elektronische communicatie, die mogelijk het intreden van de gewenste rechtsgevolgen kan verhinderen. Uitgaande van deze bedreigingen lopen bestuursorganen aan tegen de vraag hoe concrete invulling te geven aan de genoemde beginselen. Volgens de wet dient bij de invulling rekening te worden gehouden met de aard, de inhoud en het doel van de berichten. De wet vult dit verder beperkt in. Kortom, een bestuursorgaan zal in de praktijk zelf moeten bepalen welke technische en organisatorische invulling zij daaraan zal geven. Wel wordt in de memorie van toelichting verwezen naar in de praktijk gehanteerde middelen, zoals versleuteling van berichten, het gebruik van digitale handtekening en Public Key Infrastructuren. In SBR worden deze en andere middelen inderdaad toegepast voor de beveiliging

[31] Art. 2:15 lid 1 Awb. Memorie van toelichting, p. 16.
[32] P.J.J. van Buuren in Tekst en Commentaar Algemene wet bestuursrecht, 2009, p. 69.
[33] Memorie van toelichting, p. 31.

van informatieketens. Het gaat om generieke middelen en combinaties daarvan (bouwstenen), die voor meerdere toepassingen/processen gebruikt kunnen worden. In § 8.3 worden enkele middelen en bouwstenen onder de loep genomen. Dit doen we vanuit een functioneel perspectief: hoe werkt het en waarvoor dient het? In § 8.4 gaan we een stapje verder: hoe worden de bouwstenen in SBR gebruikt?

8.3 Generieke bouwstenen voor betrouwbaar elektronisch berichtenverkeer

8.3.1 *Scope*

In het eerste deel van dit hoofdstuk is een aantal beginselen van informatiebeveiliging beschreven waarmee rekening moet worden gehouden bij de inrichting van elektronisch berichtenverkeer. De beginselen zijn te relateren aan de man-in-the-middle bedreigingen en de noodzaak tot adequate (bestuurlijke) communicatie. Duidelijk is dat bestuursorganen bij het uitwisselen van gegevens, onderling en met burgers en bedrijven, rekening moeten houden met deze beginselen.

Uitgaande van deze beginselen kan de overheid gebruik maken van een algemeen middel voor informatiebeveiliging: cryptografie. We bespreken dit aan de hand van verschillende gerelateerde middelen:

- Encryptie en certificaten
- Toepassing van cryptografie op communicatielaag en de applicatielaag: SSL/TLS protocol, de hashfunctie en de digitale handtekening
- Public key infrastructure (PKI)

Op basis van deze middelen heeft een aantal bestuursorganen gezamenlijk enkele bouwstenen - combinaties van maatregelen en middelen - ontwikkeld, die moeten toezien op voldoende betrouwbare en vertrouwelijke elektronische informatie-uitwisseling en -verwerking. De bouwstenen zijn:

1. Een PKI voor de overheid
2. Een machtigingenvoorziening

In de volgende paragrafen worden de genoemde middelen en bouwstenen toegelicht. Hierbij wordt de bijdrage aan het waarborgen van de eerder beschreven beginselen expliciet gemaakt. De toelichting is functioneel en overstijgt de SBR context. Deze middelen worden breed gebruikt en ook de bouwstenen zijn niet alleen voor SBR ketens ontwikkeld. In § 8.4 volgt een beschrijving van de toepassing van de bouwstenen in SBR ketenprocessen.

8.3.2 *Cryptografie*

8.3.2.1 Encryptie: berichten onleesbaar maken voor onbevoegden

Bij het elektronisch berichtenverkeer wordt een verbinding tussen twee systemen opgezet. Voor bepaalde informatiestromen moet deze verbinding beveiligd worden. De infrastructuur die vaak wordt gebruikt voor communicatie – het internet – is volgens het oorspronkelijk ontwerp open en onveilig (zie kader).

Dit probleem wordt op technisch vlak vaak aangepakt door de toepassing van cryptografische technieken (Tel, 2002; Thomas, 2000). Het gaat hier met name om technieken voor encryptie en decryptie. Encryptie is een proces waarbij leesbare tekst (bijvoorbeeld 'plain tekst') wordt omgezet naar gecodeerde of vercijferde tekst ('cyphertext') die in deze vorm onbegrijpelijk is (Laudon & Laudon, 2010). Hierbij worden cryptografische algoritmen gebruikt. Voorbeelden hiervan zijn AES, 3DES en RSA (Stallings, 2011). Dergelijke algoritmen maken tekst onleesbaar door op de bits en bytes allerlei wiskundige operaties uit te voeren. Om gecodeerde gegevens te kunnen lezen moeten we het omgekeerde proces uitvoeren: van gecodeerde tekst naar leesbare tekst. Het omgekeerde proces wordt decryptie genoemd. Voor beide cryptografische processen (encryptie en decryptie) is een numerieke code nodig; een sleutel. Vandaar dat men bij encryptie vaak ook spreekt van versleuteling en bij decryptie van ontsleuteling.

De meest gangbare vormen van cryptografie zijn symmetrische en asymmetrische cryptografie (Paar & Pelzl, 2010). Symmetrische cryptografie maakt gebruik van een enkelvoudige sleutel (codereeks), waarbij dezelfde geheime sleutel (secret key) wordt gebruikt voor encryptie en decryptie. Het symmetrische aspect heeft betrekking op de gelijkheid van encryptiesleutel en decryptiesleutel. Aan deze vorm van cryptografie kleven echter twee belangrijke beperkingen:

1. Sleuteldistributie. Hoe dragen afzender en ontvanger de secret key aan elkaar over? Als de afzender de sleutel via het internet meestuurt met het gecodeerde bericht bestaat het risico dat bericht en sleutel gezamenlijk kunnen worden onderschept. Dit is vrijwel ondoenlijk als partijen elkaar niet (goed) kennen.
2. Geen onweerlegbaarheid. Aangezien afzender en ontvanger beschikking hebben over de secret key, kunnen beide partijen een bericht hebben gemaakt en versleuteld. Hierbij kan niet worden bewezen dat het bericht slechts door één partij zou zijn gemaakt (Paar & Pelzl, 2010).

In 1976 is een alternatief voor symmetrische cryptografie ontwikkeld: asymmetrische cryptografie (Diffie & Hellman, 1976). Dit is een 'twee-sleutel'-systeem dat twee mathematisch gerelateerde sleutels gebruikt: een publieke sleutel en een privé sleutel. Het asymmetrische aspect zit in het feit dat een sleutel slechts voor één functie – encryptie of decryptie – kan worden gebruikt en niet voor beide, zoals het geval is bij symmetrische sleutels. Het bijzondere aan asymmetrische cryptografie is dat een bericht dat met iemands privé sleutel is versleuteld, alleen met

Waarom is het internet van nature onveilig?
Het fundament van de internettechnologie is een stapel protocollen uit de jaren zeventig (Stallings, 2009). Deze protocollen zijn inmiddels standaard ingebouwd in elk gangbaar besturingssysteem (Brookshear, 2012). Het gaat hier hoofdzakelijk om het TCP/IP protocol; een samentrekking van het Transmission Control Protocol (TCP) en het internetprotocol (IP). Communicatie via het TCP/IP protocol is eenvoudig af te luisteren (Bosworth, Kabay, & Whyne, 2009). De te versturen data wordt in stukjes opgedeeld en als een set pakketjes naar de andere kant gestuurd, alwaar de stukjes weer in elkaar worden gezet. Elk pakketje wordt door een aantal tussenliggende nodes (servers) ontvangen en doorgegeven. Dit betekent dat elke node die de pakketjes doorgeeft, de inhoud ervan kan lezen.

diens publieke sleutel – de andere sleutel van het sleutelpaar – kan worden ontsleuteld. Een bericht dat met iemands publieke sleutel is versleuteld, kan alleen met diens privé sleutel worden ontsleuteld. Het is niet zo, dat de privé sleutel alleen bedoeld is om te versleutelen en de publieke sleutel alleen bedoeld is om te ontsleutelen. Omdat niet beide sleutels aan de wederpartij behoeven te worden gecommuniceerd, vermindert de kans op misbruik van de sleutels. Bovendien kan door het gebruik van twee verschillende sleutels voor encryptie en decryptie, uit de encryptie worden opgemaakt van wie het bericht afkomstig is en kan de decryptie worden beperkt tot uitsluitend degene voor wie het bericht bestemd is (Kleve, 2004).

Met asymmetrische cryptografie wordt weliswaar het probleem van sleuteldistributie opgelost, maar daar komt wel een ander probleem voor in de plaats. Wie betrouwbaar met iemand wil communiceren op basis van diens publieke sleutel moet vast kunnen stellen dat de betreffende sleutel ook echt bij die persoon hoort. De partij die garant staat voor deze koppeling wordt doorgaans aangeduid met de term trusted third party (TTP). Een omgeving die het mogelijk maakt om deze controle snel en betrouwbaar uit te voeren wordt aangeduid als een PKI. Meer hierover in § 8.3.4.

8.3.2.2 Certificaten

Certificaten worden gebruikt om asymmetrische sleutels aan gebruikers ter beschikking te stellen. Een certificaat is feitelijk een elektronisch document waarin onder meer de identificerende gegevens (naam) van een gebruiker (organisatie of rechtspersoon), zijn publieke sleutel, de naam van de certificaatuitgever en de geldigheidsduur van het certificaat zijn vastgelegd. Certificaten kunnen verschillende functies hebben. Drie van die functies zijn voor dit hoofdstuk relevant:

1. Het opzetten van een beveiligde verbinding, ten behoeve van exclusiviteit. Dit valt onder encryptie op de communicatielaag.
2. Het plaatsen van een digitale handtekening ten behoeve van authenticatie van de certificaathouder. Deze en de derde functie vallen onder encryptie op de applicatielaag.
3. Het plaatsen van een digitale handtekening met dezelfde rechtsgevolgen als een handgeschreven handtekening; een gekwalificeerde elektronische handtekening.

De term ‘elektronische handtekening’ is overigens een ruim concept, waaronder ook gescande handtekeningen, document imaging, een pincode, handtekeningen door middel van een elektronische pen, maar ook biometrische identificatiemethoden zoals gescande irissen en vingerafdrukken worden begrepen. Deze soorten (niet-digitale) ‘handtekeningen’ worden verder niet behandeld.

8.3.3 *Toepassing van encryptie*

Op het eerste gezicht lijkt encryptie een gemakkelijke keuze. Waarom zouden we immers vertrouwelijke gegevens blootstellen aan nieuwsgierige ogen als je het kunt beschermen door versleuteling (beginsel van exclusiviteit)? Conceptueel gezien kan encryptie op meerdere lagen van informatie-uitwisseling of –verwerking worden toegepast. Afhankelijk van het lagenmodel (bijvoorbeeld TCP/IP, OSI etc.) dat we hanteren, kunnen we bijvoorbeeld spreken van encryptie op de applicatielaag, de gegevenslaag en de communicatielaag. Het idee is dat dan het falen van encryptie op één

laag wordt opgevangen door de volgende laag. Dit wordt soms ook wel aangeduid als 'defence in depth'. De uitdieping van alle lagen voert hier te ver. De boodschap die we willen meegeven is dat over het algemeen geldt: hoe meer encryptie, hoe meer rekencapaciteit nodig is, hoe slechter de performance en hoe meer complexiteit (meerdere sleutels die beheerd moeten worden, afspraken die gemaakt moeten worden etc.). Hierdoor wordt encryptie in de praktijk slechts op enkele lagen toegepast. Meestal komen we encryptie tegen op de communicatie(transport)laag en de hoger liggende applicatielaag. We lichten encryptie op deze twee lagen toe.

8.3.3.1 Encryptie op de communicatielaag

Voor encryptie op de communicatielaag worden veelal protocollen als de Secure Socket Layer (SSL) en diens opvolger Transport Layer Security (TLS) gebruikt. Aangezien het verschil tussen beide minimaal is en SSL vaak als een synoniem voor een beveiligde verbinding wordt geïnterpreteerd (Thomas, 2000), worden beide afkortingen vaak samengetrokken tot SSL/TLS. SSL/TLS is een protocol (laag boven TCP/IP) dat door applicaties kan worden gebruikt om een sessie op te zetten tussen een client en een server, sleutels uit te wisselen en de data-uitwisseling te versleutelen. De door SSL/TLS geboden faciliteiten zijn onder andere encryptie (versleuteling van de sessie), authenticatie van de server en, als de server dat wenst, authenticatie van de client.

Een SSL/TLS-sessie begint met een zogenaamde 'handshake' – het uitwisselen van gegevens tussen client en server. De handshake stelt de server in staat zich via een publieke sleutel te identificeren bij de client (optioneel door het doorsturen van een certificaat). Dit kan ook de andere kant op: de server kan de client vragen om zich te identificeren. Indien zowel client als server zich moeten identificeren en elkaar authenticeren spreekt men van dubbelzijdige (two-way) authenticatie (Kizza, 2009). In eerste instantie wordt dus een asymmetrische versleuteling gebruikt om een verbinding op te zetten. Vervolgens kunnen client en server samen een symmetrische sleutel (secret key) afspreken voor snelle decryptie en encryptie van de rest van de sessie. Feitelijk worden de datapakketten bij het verlaten van de lokale applicatie/server versleuteld. Men noemt dit het opzetten van een 'tunnel'. De datapakketten worden vervolgens van de applicatie van de afzender via het internet naar de server van de ontvanger gestuurd, als ware het een directe (niet publiek toegankelijke) communicatieverbinding. De authenticatiemogelijkheden van asymmetrische encryptie worden gecombineerd met de efficiëntievoordelen van symmetrische encryptie. Een sessie wordt actief beëindigd of stopt na een time-out.

SSL/TLS is flexibel. Er kunnen diverse encryptie-algoritmen worden gebruikt. SSL/TLS is onafhankelijk van de applicatie, waardoor het tot op het niveau van webpagina (en eventueel webservice) geïmplementeerd kan worden. Door het gebruik van tunnels wordt versleuteling op transportniveau losgetrokken van de applicaties die daar gebruik van willen maken. Het is een generieke oplossing om applicaties versleuteld informatie uit te laten wisselen, op eenvoudige wijze. Deze applicaties en hun type gegevens kunnen sterk uiteenlopen, van webbrowsers, e-mail en system-to-system informatie-uitwisseling tot spraak en beeld. Naast applicatie-onafhankelijkheid heeft deze encryptielocatie het grote voordeel dat de kosten voor de verbindingen over grote afstanden laag zijn. Waar voorheen vaak relatief dure huurlijnen

noodzakelijk waren, kan nu worden volstaan met een verbinding over bijvoorbeeld het internet. Het gebruik van SSL/TLS voor alle communicatie heeft een nadeel: het vereist van zowel verzender als ontvanger extra rekenkracht voor het coderen en decoderen van de pakketten.

Samengevat biedt SSL/TLS ruimte voor een aantal afspraken voor de communicatie tussen afzender en ontvanger, waaronder het specificeren van een encryptie algoritme, de duur van de sessie en de rechten en de toegestane middelen voor identificatie. Hiermee wordt de exclusiviteit van de sessie beschermd. Om binnen een keten op gestandaardiseerde wijze gebruik te maken van tunnels kan men standaard koppelvlakspecificaties afspreken.

Een alternatief voor een tunnel is een Virtual Private Network (VPN). Deze optie is met name interessant als de communicerende partners vooraf bekend en vertrouwd met elkaar zijn (bijvoorbeeld bestuursorganen onderling), er veel vaker (frequenter) gecommuniceerd wordt en het om grote hoeveelheden berichten gaat. Een VPN is als het ware een afgeschermd netwerk binnen een bestaand open netwerk. Een VPN kan volledig softwarematig opgezet worden. Aanvullend kan gebruikt gemaakt worden van (fysieke) componenten in eigen beheer. Voor overheidsdoeleinden bestaat er in Nederland een eigen netwerk – Diginetwerk – met componenten in eigen beheer. Enkele van deze componenten bieden de mogelijkheid om berichten via een VPN tussen overheidsorganisaties uit te wisselen. Het voordeel van een VPN is dat er informatie tussen meerdere netwerkpartners uitgewisseld kan worden. Er dient wel rekening gehouden te worden met het feit dat zonder aanvullende maatregelen (bijvoorbeeld encryptie op applicatieniveau) alles te lezen is door de netwerkpartners binnen de VPN.

Tunnels lijken op een VPN, daar zij ook een eigen afgeschermde verbinding maken binnen een beschikbare open verbinding. Er zijn echter ook verschillen tussen beide. Een tunnel heeft point-to-point encryptie, een VPN heeft many-to-many encryptie. Over het algemeen is er bij een tunnel een tijdelijke (korte) sessieduur, bij een VPN is de sessieduur vaak langer. Van buiten de VPN is alles encrypted, binnen een standaard VPN lijkt alles op open communicatie. VPN en tunnels sluiten elkaar niet uit; het is mogelijk binnen een VPN tunnels te gebruiken, zodat andere partijen met (terecht of onterecht) toegang tot de VPN de uitgewisselde informatie niet kunnen inzien.

8.3.3.2 Encryptie op de applicatiecatielaag

Een belangrijke eigenschap van encryptie op de applicatielaag is dat het hiermee mogelijk is de beveiliging toe te passen tot op het kleinste element: de informatie zelf. Tot op detailniveau kan bepaald worden welke informatie wel of niet beveiligd hoeft te worden. Encryptie op de applicatielaag heeft als groot voordeel dat het mogelijk is integriteit op end-to-end-basis te bewerkstelligen. Dit houdt in dat de informatie vanaf het moment van verzenden continu op een bepaalde wijze beveiligd is. Alleen de ontvangende partij voor wie de informatie bedoeld is, kan de informatie ontsluiten. Ten behoeve van een succesvolle implementatie van een dergelijke beveiligingsapplicatie is het van belang dat alle communicerende partijen met de desbetreffende

applicatie overweg kunnen en dat de organisatie rondom het noodzakelijke sleutelbeheer goed vormgegeven is. Dit is ook de uitdaging van encryptie op de applicatielaag. Tussen de communicerende partijen dienen daar afspraken over gemaakt te worden, opdat de informatie gedeeld kan worden. Een belangrijke toepassing van encryptie op de applicatielaag is de digitale handtekening.

8.3.3.3 De digitale handtekening en de hashfunctie

We hebben de digitale handtekening genoemd als een van de functies waarvoor een certificaat wordt gebruikt. Het concept wordt hier nader toegelicht aan de hand van de volgende drie vragen:

1. Wat is een digitale handtekening?
2. Hoe wordt een digitale handtekening geplaatst?
3. Waarom/welke functies vervult een digitale handtekening?

1. Wat is een digitale handtekening?

Een digitale handtekening is een encrypted (versleuteld met een privé sleutel) hashwaarde van de te tekenen gegevens. De betekenis van de hashwaarde wordt onder vraag twee gegeven. In de context van dit hoofdstuk bedoelen we hier met gegevens de inhoud van (geselecteerde) velden van een certificaat of bericht.

Het feit dat een handtekening zowel over de velden in een certificaat als over de velden in een bericht kan worden geplaatst kan soms verwarrend zijn, al werkt dit feitelijk hetzelfde. Daarnaast lopen de termen 'tekenen' en 'ondertekenen' in diverse bronnen door elkaar. Om verwarring te voorkomen spreken we van 'tekenen' wanneer het gaat om het plaatsen van een digitale handtekening ten behoeve van authenticatie en om 'ondertekenen' als het gaat om het plaatsen van een specifieke vorm van de digitale handtekening: een gekwalificeerde elektronische handtekening (met dezelfde rechtsgevolgen als een handgeschreven handtekening). Tekenen en ondertekenen gaan uit van dezelfde techniek: de hashfunctie. Eén van de belangrijkste verschillen tussen ondertekenen en tekenen zit hem in het feit dat voor het zetten van een gekwalificeerde elektronische handtekening het certificaat onder de uitsluitende controle van de ondertekenaar moet staan (persoonsgebonden). Met een certificaat dat onder controle staat van een onderneming, maar door meerdere medewerkers gebruikt wordt (organisatiegebonden), kan een bericht dus wel getekend worden, maar niet ondertekend worden.

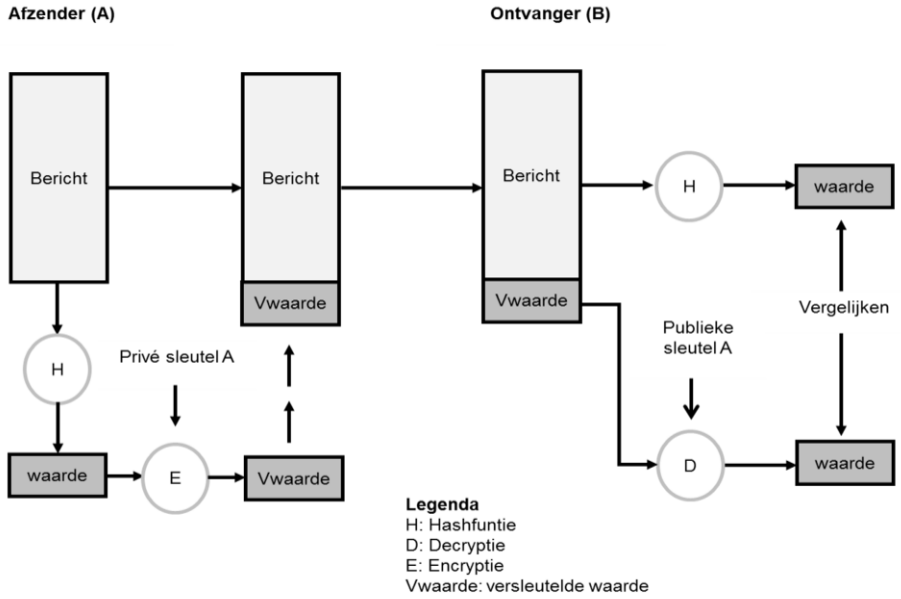
2. Hoe wordt een digitale handtekening geplaatst?

Een veelgebruikte techniek voor het plaatsen van een digitale handtekening is de hashfunctie (zie kader). Dit is een vorm van encryptie op de applicatielaag. Samengevat gaat het om het genereren van een unieke waarde op basis van geselecteerde velden uit een bericht (bepaalde velden in de header, in de body of de payload). De gegenereerde waarde wordt vaak aangeduid als hashwaarde,

Werking van de hashfunctie

Een hashfunctie zet de invoer uit een breed domein van waarden om in een (meestal) kleinere reeks van waarden. Hierbij geldt dat wanneer de hashwaarde H(b) van een ontvangen bericht wordt berekend met de hashfunctie, en deze waarde overeenkomt met de meegeleverde hashwaarde H(a), het ontvangen bericht dat ten grondslag lag aan de berekening hoogstwaarschijnlijk gelijk is aan het oorspronkelijk verstuurde bericht.

'fingerprint' of 'message digest'. De hashwaarde wordt vervolgens versleuteld met de privé sleutel van de afzender en wordt samen met de, al dan niet versleutelde, berichtinhoud verstuurd naar de ontvanger. Meestal wordt niet de gehele berichtinhoud versleuteld met de privé sleutel.[34] De hashwaarde is een vaste set van bits die bij encryptie en decryptie om minder rekencapaciteit vraagt dan de variabele en omvangrijkere set van bits in een bericht. De ontvanger kan bij ontvangst met behulp van de publieke sleutel van de afzender verifiëren of het bericht inderdaad van de afzender afkomstig is. Met andere woorden: na ontsleuteling door de ontvanger komt de hashwaarde weer te voorschijn. De ontvanger kan het bericht vervolgens door dezelfde hashfunctie halen en weet, als beide hashwaarden na vergelijking gelijk blijken, dat de geselecteerde gegevens gedurende het transport niet zijn gewijzigd. Een hashfunctie berekent op basis van het bericht een unieke waarde. Indien een element uit het bericht verandert, leidt dit tot een ander unieke (hash)waarde. Hieronder wordt de generieke werking van de hashfunctie afgebeeld.



Figuur 8.3 – Het plaatsen van een digitale handtekening ten behoeve van authenticatie door middel van een hashfunctie (gebaseerd op Stallings, 2011)

[34] Vaak wordt alleen de hashwaarde en niet het gehele bericht met de privé sleutel versleuteld. Als naast de hashwaarde ook de berichtinhoud met de privé sleutel wordt versleuteld dan kan dit als overbodig (dubbelop) worden beschouwd. Een wijziging zal altijd te detecteren zijn met behulp van de hashwaarde. Het kost minder rekencapaciteit van zowel de afzender als ontvanger als alleen de hashwaarde (een vaste set van bits) versleuteld en ontsleuteld hoeft te worden. Met name als de ontvanger een groot volume aan berichten moet verwerken (zoals bij SBR berichtstromen) is het qua hardware(kosten) raadzaam om alleen de hashwaarde te versleutelen/ontsleutelen in plaats van het gehele bericht. Indien echter de exclusiviteit beschermd dient te worden en aanvullende maatregelen voorzien daar niet in, dan zal versleuteling van het bericht overwogen worden.

Als de met de publieke sleutel van A ontsleutelde hashwaarde overeenkomt met de zelf berekende hashwaarde, kan met een bepaalde mate van zekerheid worden vastgesteld dat:

1. A de afzender is;
2. het bericht onderweg niet gewijzigd is.

De hashfunctie is gebaseerd op een algoritme. Een veelgebruikt algoritme is het Secure Hash Algoritme, afgekort als SHA (Burr, 2006). Inmiddels zijn er van SHA verschillende varianten beschikbaar met verschillende hashwaarden en kleine verschillen in ontwerp. SHA-1 creëert een hashwaarde van 160 bits. In februari 2005 hebben experts op cryptografisch gebied theoretische zwakheden gevonden in SHA1, die twijfel doen rijzen of dit algoritme nog langer bruikbaar is. Op dit moment is SHA1 nog veilig, maar de toekomstbestendigheid staat onder druk. Binnen het PKIoverheidstelsel is daarom besloten het advies van de Amerikaanse overheidsorganisatie National Institute for Standards and Technology (NIST) over te nemen en vanaf 1 januari 2011 certificaten uit te gaan geven op basis van het verbeterde en meer toekomstbestendige SHA-2 algoritme. SHA-2 is een verzamelnaam voor versies met verschillende grotere hashwaarden. Er zijn 224, 256, 385 en 512 bits versies beschikbaar. PKIoverheid hanteert het SHA-256 algoritme.

3. Waarom/welke functies vervult een digitale handtekening?

De digitale handtekening stelt de afzender van een bericht in staat om een unieke waarde aan het bericht of certificaat toe te voegen (Brookshear, 2012). Uniek betekent hier: gekoppeld aan het bericht en/of certificaat. Als het gaat om het tekenen van een certificaat, dan is de functie van de digitale handtekening het overdragen van vertrouwen. Als het gaat om het tekenen van een bericht vervult de digitale handtekening de volgende functies:

- **Authenticatie.** Aangezien de encrypted hashwaarde (de handtekening) alleen gelezen kan worden door deze te decrypten met de publieke sleutel van de afzender, kan de ontvanger er vanuit gaan dat het bericht alleen van de eigenaar van de bijbehorende privé sleutel kan zijn.
- **Borgen van berichtintegriteit.** Wanneer onderweg de inhoud van een bericht wijzigt, zal de meegestuurde (encrypted) hashwaarde altijd verschillen van de hashwaarde die de ontvanger na decryptie zelf met de hashfunctie berekent. Als beide hashwaarden identiek zijn, kan de ontvanger er zeker van zijn dat het bericht (of de geselecteerde velden) niet is gewijzigd.
- **Onweerlegbaarheid.** De hashwaarde kan alleen versleuteld worden met de privé sleutel van de afzender en ontsleuteld worden met de publieke sleutel van de afzender. Bij overeenkomende hashwaarden kan de afzender niet ontkennen het bericht te hebben opgesteld en getekend.

Bij het zogenoemd óndertekenen van een bericht vervult de digitale handtekening de volgende functie:

- **Wilsuiting.** Dit kan met een gekwalificeerde elektronische handtekening. Al in 1978 stelden onderzoekers dat "*If electronic mail systems are to replace the existing paper mail system for business transactions, signing an electronic message must be possible*" (Rivest, Shamir, & Adleman, 1978, p. 122). Dit citaat onderstreept de noodzaak voor een digitale handtekening

met een bepaalde mate van rechtsgeldigheid in elektronisch berichtenverkeer. Zoals gezegd is voor deze functie vereist dat het certificaat onder de uitsluitende controle van de ondertekenaar staat (persoonsgebonden). Deze en andere eisen zijn in wetgeving opgenomen.

Bovenstaande functies sluiten elkaar niet uit en kunnen gecombineerd voorkomen. De functies veronderstellen wel dat de publieke sleutel van de afzender daadwerkelijk de publieke sleutel van de afzender is en wiskundig gerelateerd is aan de privé sleutel van de afzender. Daarnaast gaan deze functies alleen maar op als de privé sleutel exclusief in handen is van de afzender. Om dat te bewerkstelligen moet de digitale handtekening gebaseerd zijn op een 'gekwalificeerd certificaat': een certificaat dat volgens strenge procedures en conform specifieke eisen is uitgegeven. Dit is het geval bij PKIoverheid certificaten. Hier komen we verderop in dit hoofdstuk op terug.

Deelconclusie
Eén van de doelen van cryptografie (encryptie en decryptie) is het realiseren van exclusiviteit (vertrouwelijkheid) van informatie. Het gebruik van sleutels – zowel symmetrisch als asymmetrisch – biedt de mogelijkheid om berichten onleesbaar te maken voor anderen dan de gewenste ontvanger. Afhankelijk van het gewenste beveiligingsniveau kan cryptografie op verschillende lagen worden toegepast. Vaak zien we toepassing op de communicatielaag, resulterend in het gebruik van tunnels tussen afzender en ontvanger. Daarnaast kan toepassing van cryptografie op de applicatielaag bijdragen aan wat men vaak aanduidt als een vorm van end-to-end beveiliging, aangezien de versleuteling al vanaf de bron (de gebruikersapplicatie) tot en met de ontvangende applicatie plaatsvindt. Het gebruik van encryptie stelt echter eisen aan het sleutelbeheer en de benodigde rekencapaciteit. Vandaar dat het inzetten van encryptiemiddelen vraagt om een goed afgewogen keuze, waarbij recht wordt gedaan aan alle aspecten die bij encryptie een rol spelen. Bij asymmetrische encryptie biedt een PKI een manier om deze en andere keuzes over ketens en organisaties heen te regelen. Hierover meer in de volgende paragraaf.

8.3.4 *Public key infrastructure*

Asymmetrische sleutels worden aan gebruikers meestal ter beschikking gesteld in de vorm van certificaten. Om certificaten te organiseren en beheren wordt gebruik gemaakt van een public key infrastructure. Met de 'infrastructure' wordt hier gedoeld op een stelsel van maatregelen en procedures om op praktische en betrouwbare wijze de publieke sleutel te delen. Een PKI maakt het daarmee mogelijk om partijen, zowel binnen één organisatie als partijen die niet van tevoren met elkaar zijn verbonden, op een betrouwbare manier elektronisch met elkaar te laten communiceren. In deze paragraaf wordt aan de hand van de onderdelen van een PKI generiek beschreven hoe een PKI werkt. We gaan daarna in op het bijzondere van PKIoverheid ten opzichte van een PKI in het algemeen.

8.3.4.1 Achtergrond

In de leerboeken wordt een PKI breed gedefinieerd als het samenstel van software, hardware, rollen, richtlijnen en procedures die nodig zijn voor het beheren (creëren, distribueren, gebruiken, bewaren en intrekken) van sleutels in de vorm van digitale

certificaten (zie bijvoorbeeld Ballad, Ballad, & Banks, 2010; Roebuck, 2011). Dit is een veelomvattende definitie die een aantal concepten aan elkaar verbindt. We beginnen hier met de relatie tot de hiervoor besproken encryptie en het gebruik van sleutels. De overige verbindingen zullen stapsgewijs worden beschreven.

De essentie van een PKI is een structuur rondom de functie van een trusted third party: een onafhankelijke derde partij die op afstand zaken rond identificatie en authenticatie tussen twee partijen (afzender en ontvanger) regelt. Deze structuur behelst het beheren van asymmetrische sleutels (Adams & Lloyd, 2002). Zoals eerder aangegeven gaat het hier om twee verschillende, doch wiskundig gerelateerde sleutels: een publieke sleutel en een privé sleutel. Anders dan bij het gebruik van symmetrische sleutels, waarmee zowel encryptie als decryptie met dezelfde sleutel wordt uitgevoerd, worden asymmetrische sleutels alleen voor één van de twee processen toegepast. Eén helft van het sleutelpaar doet de encryptie, de andere helft doet de decryptie. Laten we ter illustratie weer even communicatie tussen twee partners – A en B – onder de loep nemen. Hierbij is A de afzender en B de ontvanger. In een PKI heeft minimaal één van beide partners een publieke sleutel en een privé sleutel. De publieke sleutel wordt openbaar gemaakt en de privé sleutel houdt de communicatiepartner geheim. Voor encryptie en decryptie met asymmetrische sleutels zijn er in principe drie toepassingen te onderscheiden waarbij de communicatie van A richting B gaat:

1. A encrypt het bericht met de publieke sleutel van B. Dit bericht kan dan alleen met de privé sleutel van B worden geopend. Aangezien de privé sleutel geheim is en alleen B hierover beschikt, kunnen we ervan uitgaan dat alleen B het bericht kan decrypten.
2. A kan ook het bericht encrypten met zijn privé sleutel. B (maar ook andere partijen) kunnen het bericht decrypten met de publieke sleutel van A. In dit scenario weet B dat alleen A de afzender van het bericht kan zijn.
3. A encrypt het bericht eerst met zijn privé sleutel en daarna met de publieke sleutel van B. Bij dit scenario is er sprake van dubbele encryptie. Het gevolg is dat B eerst zijn privé sleutel nodig heeft om het bericht te decrypten. Het resultaat is een nog versleuteld bericht dat met de publieke sleutel van A gedecrypt kan worden. Deze vorm van dubbele encryptie geeft meer zekerheden dan de twee voorgaande scenario's. A en B hebben wederzijds de zekerheid dat de communicatie alleen tussen hen verloopt.

Bovenstaande scenario's gaan uit van een belangrijke randvoorwaarde: de sleutels worden op een degelijke manier beheerd. Beheren omvat hier een reeks activiteiten, waaronder het:

a. Creëren en uitreiken van sleutels
b. Bepalen van de levensduur van sleutels
c. Opslaan van sleutels
d. Distribueren (publiceren) van publieke sleutels
e. Intrekken van sleutels (bijvoorbeeld bij diefstal of misbruik)
f. Publiceren (bekend maken) van ingetrokken sleutels
g. Herstellen (recovery) van sleutels

8.3.4.2 Onderdelen van een PKI

In de praktijk zijn er verschillende commerciële en publieke PKI varianten in gebruik. Bij verdieping in PKI systemen zien we de volgende onderdelen steeds terugkomen:

- Certificaten
- Certification Authority (CA)
- Registration Authority (RA)
- Gebruikers (certificaathouders)
- Certificate Revocation List (CRL) en Online Certificate Status Protocol (OCSP)
- Certificate Policy (CP) en Certificate Practice Statement (CPS)
- Elektronische opslagplaats
- Vertrouwensketen, root CA en Policy Authority (PA)
- De digitale handtekening en de hashfunctie (zie 8.3.3)

Hierna worden deze onderdelen en aspecten verder uitgewerkt.

Certificaten in een PKI

We gaan hier nader in op de inhoud en werking van een certificaat. Meestal wordt gebruik gemaakt van de X.509[35] standaard voor het vastleggen van gegevens in een certificaat. De manier waarop een certificaat wordt opgezet, wordt ook wel certificaatprofiel genoemd. Een certificaatprofiel bestaat uit een aantal velden, oftewel attributen van het certificaat. Tabel 8.1 biedt een overzicht.

Tabel 8.1 – Certificaatprofiel: generieke attributen van een certificaat (gebaseerd op PKIoverheid 2012)

Attribuut (veld)	Toelichting
Basisattributen	
Version	Beschrijft de versie van het certificaat.
(certificate) SerialNumber	Een serienummer dat op unieke wijze het certificaat binnen het uitgevende CA domein identificeert.
Signature (Algorithm ID)	Bepaalt het algoritme (bijvoorbeeld SHA- 256 WithRSAEncryption), zoals deze door de PA is bepaald.
Issuer (Distinguished Name)	Bevat een Distinguished Name (DN) van de uitgever van het certificaat (de CA). Dit veld heeft minimaal de volgende subattributen: Issuer.countryName, Issuer.OrganizationName en Issuer.commonName.
Validity (not valid before… not valid after…)	Bepaalt de begin- en einddatum voor geldigheid van het certificaat conform het van toepassing zijnde beleid vastgelegd in het CPS.
Subject (Distinguished Name). Veld heeft de onderstaande attributen:	De attributen die worden gebruikt om het subject (eindgebruiker) te beschrijven. Dit veld heeft minimaal de volgende subattributen: Subject.countryName, Subject.OrganizationName en Subject.commonName.

[35] X.509: een IEFT standaard die een basis voor de elektronische opmaak van Certificaten definieert. Deze wordt ook door ISO als standaard erkend.

SubjectPublicKeyInfo	Bevat de publieke sleutel; identificeert het algoritme waarmee de sleutel kan worden gebruikt.
Subject.serialNumber	Identificerend nummer van de certificaathouder. Het Subject.serialNumber is ook bedoeld om onderscheid te kunnen maken tussen subjects met dezelfde commonName en dezelfde OrganizationName.
Extensies	
CRLDistributionPoints	Bevat de URI van een CRL distributiepunt.
AuthorityKeyIdentifier	Bevat de hashwaarde van de authorityKey (publieke sleutel van de CA).
SubjectKeyIdentifier	Bevat de hashwaarde van de subjectKey (publieke sleutel van de certificaathouder).
KeyUsage	Dit attribuut specificeert het beoogde doel van de in het certificaat opgenomen publieke sleutel. In de PKI overheid zijn per certificaatsoort verschillende bits opgenomen in the keyUsage extensie.
CertificatePolicies	Bevat de Object Identifier (OID) (rij getallen die op ondubbelzinnige wijze en permanent een object aanduidt) van de CP en de URI van het CPS.

Het aantal en de exacte indeling van velden hangt af van de afspraken die men hierover maakt. In het Programma van Eisen (PvE) van PKI voor de Overheid (Logius, 2011) spreekt men van verplichte, optionele, afgeraden en niet toegestane velden. Om verwarring door vertaling te voorkomen zijn voor aanduiding van de attributen de Engelstalige termen gebruikt. De PA eisen en de specifieke CA eisen voor een bepaald domein kunnen als additionele attributen in een certificaat zijn opgenomen. Om de betrouwbaarheid van een certificaat te garanderen vereist de X.509 standaard dat de uitgever van het certificaat – de CA – een digitale handtekening plaatst op het certificaat.

Certification authority als trusted third party

De Certification Authority (CA) is verantwoordelijk voor de uitgifte en het beheer van sleutelparen en digitale certificaten. Hierbij hoort het tekenen (signen) van een uitgegeven certificaat: het plaatsen van een digitale handtekening op/in het certificaat. Dit gebeurt door het genereren van een hashwaarde over bepaalde velden in het certificaat, die vervolgens met de private sleutel van de CA als vertrouwde partij wordt versleuteld. Hoe dit precies werkt is in § 8.3.3.2 toegelicht. Deze handtekening is nodig als bewijs van de echtheid van het certificaat. Het maakt het certificaat moeilijk te vervalsen en is door iedereen door middel van de bijbehorende publieke sleutel van de CA te controleren.

De privé sleutel van de CA dient bij voorkeur offline (niet op een apparaat dat via het internet toegankelijk is) te worden bewaard om compromittatie van deze privé sleutel te voorkomen. Compromittatie van deze sleutel brengt namelijk met zich mee dat geen enkel certificaat van deze CA meer te vertrouwen is. Dit kan verstrekkende gevolgen hebben, zoals het vervangen van alle uitgegeven certificaten.

De CA vervult binnen een PKI de rol van TTP. Hierbij heeft de CA een aantal belangrijke verantwoordelijkheden. Zo is het de verantwoordelijkheid van de CA om de identiteit van de (nieuwe) gebruiker te controleren voordat certificaten worden uitgegeven. Over het algemeen wordt deze controle uitbesteed aan de RA. We lichten deze rol hierna toe.

Registration Authority
De Registration Authority (RA) draagt zorg voor het aanbieden van gegevens (credentials) van gebruikers aan de CA ten behoeve van het uitgeven van (nieuwe) certificaten door de CA. De RA zorgt voor het vaststellen van de identiteit van de gebruiker (authenticatie). De RA ondertekent de certificaten niet en geeft ook geen certificaten uit; dit is een taak voor de CA. Dit betekent dat er een vertrouwensrelatie moet zijn tussen de RA en de CA. Ook moet worden voorkomen dat de door de RA aangeboden gegevens onderweg kunnen worden gemanipuleerd.

Gebruiker (certificaathouders)
Een gebruiker dient een aanvraag voor het verkrijgen van een certificaat in bij de RA. Hiertoe dient hij zich te identificeren. De methode van identificatie is afhankelijk van het soort certificaat dat wordt aangevraagd. Fysieke (persoonlijke) identificatie met geldig identiteitsbewijs gebeurt maar bij een klein deel van alle certificaten, maar wel vaak bij het type dat gebruikt wordt om met de overheid te communiceren (zoals bij PKIoverheid – dit wordt later toegelicht). Bij deze aanvraag geeft de gebruiker tevens aan voor welke toepassing het certificaat wordt aangevraagd, bijvoorbeeld voor het zetten van een digitale handtekening, het vercijferen van informatie etc. De gebruiker wordt geacht kennis te nemen van de Certification Practice Statement van de CA.

Certificate Policies en Certificate Practice Statements
Van CAs wordt verwacht dat ze expliciet zijn in de gehanteerde Certificate Policy (CP) en Certificate Practice Statement (CPS). Dit zijn twee documenten die inzicht geven in de werking van de CA. Een CP beschrijft de minimumeisen die zijn gesteld aan de dienstverlening - op het gebied van certificaten - van een CA binnen een PKI. Een CPS geeft aan op welke wijze invulling is gegeven aan deze eisen. Daarnaast beschrijft een CPS vaak ook de procedures en maatregelen die een CA in acht neemt bij de aanmaak, de uitgifte en het intrekken van certificaten.

Certificate Revocation List
Een geldig certificaat vormt de basis voor vertrouwen op elektronisch gebied. Om het risico van het gebruik van privé sleutels door onbevoegden te beperken hebben certificaten een beperkte geldigheid (enkele jaren). Als dit vertrouwen tussentijds verloren gaat dan zou – uitgaande van een goed werkende PKI - het certificaat moeten worden ingetrokken. Het is van groot belang dat de eigenaar van het certificaat een dergelijke situatie zo snel mogelijk meldt aan zijn CA. Via een zogenaamde Certificate Revocation List (CRL) maken CAs publiekelijk kenbaar welke certificaten niet meer vertrouwd mogen worden. Een CRL is een openbaar toegankelijke en te raadplegen lijst van ingetrokken certificaten, beschikbaar gesteld, ondertekend en onder verantwoordelijkheid vallend van de uitgevende CA. Het intrekken van een certificaat kan om verschillende redenen plaatsvinden, waaronder diefstal van de privé sleutel of verlies (bijvoorbeeld bij een server crash of upgrade). Ingetrokken certificaten waarvan de geldigheidsduur is verlopen worden niet meer in de CRL gepubliceerd. CAs dienen een CRL via een online voorziening opvraagbaar te maken. In veel PKI systemen gebeurt dit via het Online Certificate Status Protocol. Dit protocol maakt het mogelijk om elk certificaat direct (system-to-system) te controleren.

Elektronische opslagplaats

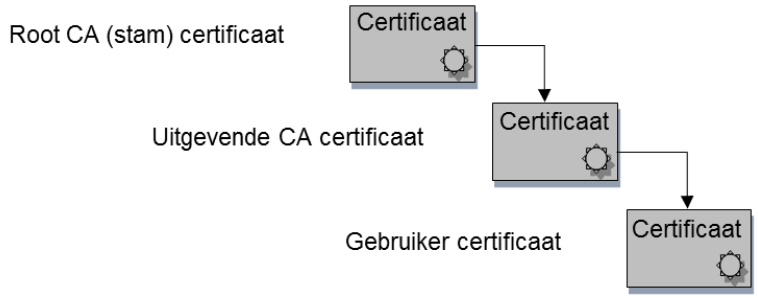
Binnen een PKI is er behoefte aan een toegankelijke elektronische opslagplaats, vaak ook repository genoemd. De opslagplaats dient de volgende zaken toegankelijk te maken:

- De CPS van de CA
- Overeenkomst en toepasselijke gebruiksvoorwaarden
- Certificaten van certificaathouders (deze bevatten alleen het publieke deel)
- CRL

De elektronische opslagplaats dient 24 uur per dag, 7 dagen per week voor een ieder beschikbaar te zijn, met uitzondering van onderhoudswerkzaamheden. De toegangscontrole tot de elektronische opslagplaats is zodanig ingericht dat alleen leesrechten zijn toegekend aan derden die deze informatie raadplegen. Uitsluitend de CA heeft schrijfrechten op de elektronische opslagplaats.

Vertrouwensketen, root CA en PA

Een PKI gaat uit van een vertrouwensketen. Dat betekent dat het vertrouwen in een keten doorgegeven wordt. Dit kan op basis van een certificatiepad. Een certificatiepad is een ononderbroken keten van vertrouwde punten tussen twee gebruikers om elkaar te authenticeren, via sub-certificaten naar het stamcertificaat. Onder het stam-certificaat worden namelijk verschillende groepen gebruikers (sub-CAs) gevormd die een vertrouwensrelatie hebben met de root CA. Een certificaat in de keten is betrouwbaar omdat een hogere CA dit zegt en borgt met een certificaat. Een eindgebruiker kan daarmee alle CAs en certificaten vertrouwen die onder dezelfde root CA (stamcertificaat) vallen.



Figuur 8.4 – Certificatiepad in een CA hiërarchie

Maar hoe weten we dat de root CA een betrouwbare partij is? Dit kan in principe op twee manieren: cross certificatie en self-signing.

Bij cross-certificatie tekenen root CAs elkaars certificaten. Hiervoor dienen de verschillende CPs en CPSs op elkaar te worden afgestemd. Dit is het meest complexe deel van de cross-certificatie. Als de ene root CA namelijk een hoger veiligheidsniveau hanteert voor de uitgifte van certificaten dan de andere root CA, kan certificaatinformatie niet zonder meer worden uitgewisseld. Zou dit wel gebeuren, dan zou dit

een inbreuk op het veiligheidsniveau van de root CA met het hoogste veiligheidsniveau tot gevolg hebben. Als de CPs en de CPSs op elkaar zijn afgestemd, dan hebben de CAs een vertrouwensrelatie. Bij self-signing tekent de root CA zijn eigen certificaat. Dit doen partijen, zoals overheden, die zelf niet afhankelijk willen zijn van commerciële partijen of andere overheden. In PKIoverheid heeft men ook voor deze optie gekozen.

Een afgeleid stelsel voor vertrouwen vinden we bij de browser c.q. softwareleveranciers, zoals Windows, Google of Apple. Root CAs worden opgenomen in de Certificate Store van een OS of browser. Een SSL certificaat van een root CA die wordt vertrouwd, levert dan geen foutmelding op. Anders gesteld: software leveranciers toetsen en bepalen ten behoeve van internetgebruikers of een root CA een betrouwbare partij is.

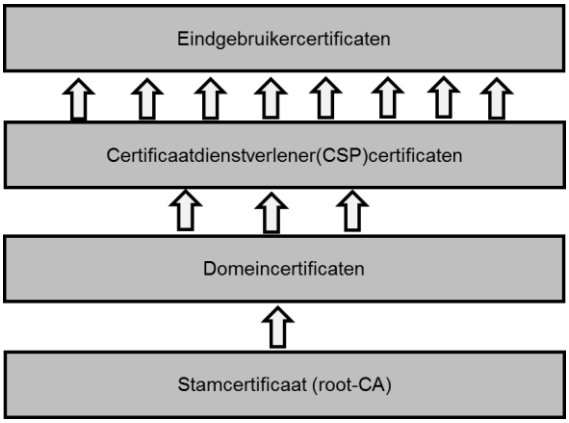
8.3.5 *Bouwsteen 1 – PKIoverheid*

Wat is het bijzondere aan PKIoverheid?
Op basis van de hiervoor besproken middelen heeft een aantal bestuursorganen de bouwsteen PKIoverheid (de PKI voor de Nederlandse overheid) ontwikkeld. PKIoverheid vormt een raamwerk met eisen en afspraken dat het gebruik van een digitale handtekening, elektronische authenticatie en vertrouwelijke elektronische communicatie mogelijk maakt, gebaseerd op certificaten met een hoog betrouwbaarheidsniveau. Technisch bestaan er veel overeenkomsten met andere PKI systemen. Er zijn echter wel enkele aspecten die PKIoverheid bijzonder maken:

1. De hoogste autoriteit is de Staat der Nederlanden.
2. Er wordt gebruik gemaakt van een gelaagde eisenstructuur.
3. De certificaten zijn functioneel gecategoriseerd.
4. Er gelden zorgvuldige uitgifteprocedures.
5. CSPs moeten aan strenge eisen voldoen om PKIoverheid certificaten te mogen uitgeven.
6. De PA van PKIoverheid houdt toezicht op de PKIoverheid leveranciers.

De optelsom van deze bijzonderheden maken PKIoverheid certificaten aantrekkelijk voor de identificatie en authenticatie in elektronisch berichtenverkeer. Bovenstaande verschillen worden hieronder toegelicht.

Bijzonderheid 1: De hoogste autoriteit is de Staat der Nederlanden
Een groot verschil met andere PKIs is de technisch hoogste autoriteit (root CA). In een commerciële PKI-variant is dat bijvoorbeeld een private partij. Bij PKIoverheid is dat de Staat der Nederlanden. De Nederlandse overheid is verantwoordelijk voor het stamcertificaat (root CA) en daarmee het eindpunt in de vertrouwensketen, waardoor PKIoverheid niet afhankelijk is van (buitenlandse) commerciële partijen waarvan de root niet te verifiëren is. Deze hiërarchische structuur wordt hieronder weergegeven in figuur 8.5.



Figuur 8.5 – Hiërarchische structuur PKIoverheid met de root CA van de Staat der Nederlanden

PKIoverheid is zo opgezet dat overheidsorganisaties en marktpartijen als certificatiedienstverlener (CSP) onder voorwaarden toe kunnen treden tot de PKI voor de overheid. Deelnemende CSPs zijn verantwoordelijk voor de dienstverlening binnen de PKI voor de overheid. De PA ziet toe op de betrouwbaarheid van de gehele PKI voor de overheid. De PA-functie wordt uitgevoerd door Logius.

Bijzonderheid 2: Er wordt gebruik gemaakt van een gelaagde eisenstructuur

Certificaten uitgegeven in het kader van PKIoverheid hebben een gelaagde eisenstructuur bestaande uit:

- Wettelijke eisen (abstracte eisen uit Richtlijn 99/93/EG, Besluit elektronische handtekeningen, Telecommunicatiewet)
- Technische niet-wettelijke eisen (ETSI, Europese en internationale standaarden van het European Telecommunications Standards Institute)
- Specifieke PKIoverheidseisen
- Specifieke domeineisen binnen PKIoverheid

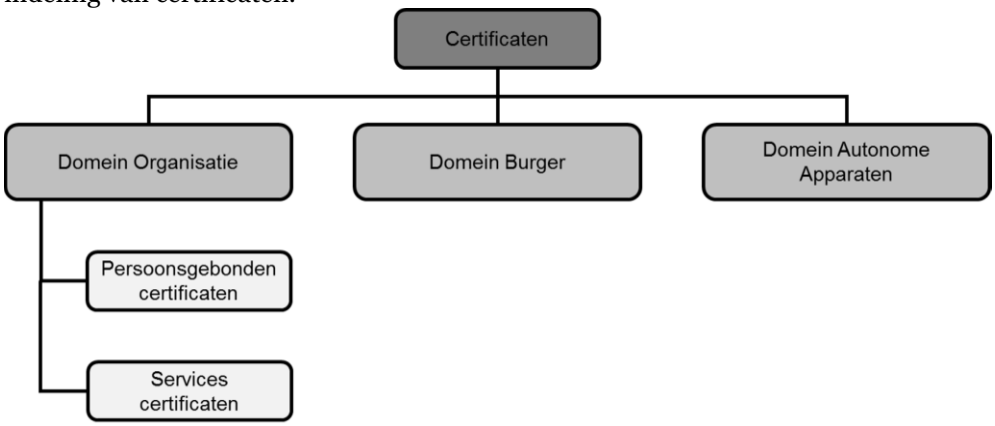
Alle gekwalificeerde certificaten van PKIoverheid moeten voldoen aan de wettelijke eisen voor gekwalificeerde certificaten. De richtlijn 99/93/EG[36] (inclusief bijlagen), de Telecommunicatiewet en het Besluit elektronische handtekeningen stellen specifieke eisen aan de certificaten en de certificatiedienstverleners die ze uitgeven. Volgens deze regelingen moet in gekwalificeerde certificaten het onderstaande opgenomen zijn:

- De vermelding dat het certificaat als gekwalificeerd certificaat wordt afgegeven.
- De identificatie en het land van vestiging van de afgevende CSP.

[36] Er is overigens een nieuwe verordening in de maak. Zie: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

- De naam van de ondertekenaar of een als zodanig geïdentificeerd pseudoniem.
- Ruimte voor een specifiek attribuut van de ondertekenaar, dat indien nodig en afhankelijk van het doel van het certificaat, kan worden vermeld.
- Gegevens voor het verifiëren van de handtekening, die overeenstemmen met de gegevens voor het aanmaken van de handtekening die onder controle van de houder staan.
- Begin en einde van de geldigheidsduur van het certificaat.
- De identiteitscode van het certificaat.
- De geavanceerde elektronische handtekening van de afgevende CSP.
- Voor zover van toepassing, beperkingen betreffende het gebruik van het certificaat.
- Voor zover van toepassing, grenzen met betrekking tot de waarde van de transacties waarvoor het certificaat kan worden gebruikt.

Bijzonderheid 3: De certificaten zijn functioneel gecategoriseerd
In het kader van PKIoverheid zijn certificaten opgesplitst in 3 domeinen: (1) Domein Organisatie, (2) Domein Burger en (3) Domein Autonome apparaten. Binnen ieder domein kunnen verschillende typen certificaten worden uitgegeven (waaronder voor de digitale handtekening, authenticatie en vertrouwelijkheid). De technische eisen verschillen per domein. Onderstaande figuur geeft een overzicht van de functionele indeling van certificaten.



Figuur 8.6 – Domeinen en typen certificaten in PKIoverheid; de technische eisen kunnen per domein en type verschillen.

Voor dit hoofdstuk zijn de certificaten onder het Domein Organisatie interessant. Binnen dit domein bestaan er twee typen certificaten: persoonsgebonden en services certificaten. Hieronder worden beide typen toegelicht.

Persoonsgebonden certificaten zijn gebonden aan een persoon. Een persoon kan meerdere persoonsgebonden certificaten hebben. Een variant van het persoonsgebonden certificaat is het beroepscertificaat (niet afgebeeld). Voor beroepscertificaten

dient een persoon ingeschreven te staan bij een erkende beroepsorganisatie. Erkende beroepen waarvoor een beroepscertificaat kan worden aangevraagd zijn onder andere: accountants/administratieconsulenten, advocaten en medici. Een accountant kan zich met een beroepscertificaat identificeren en authenticeren als zijnde een gekwalificeerde accountant die staat ingeschreven in het register. Tevens kunnen zij een digitale handtekening plaatsen onder een document of e-mail om zo onweerlegbaarheid te creëren, en indien gewenst een digitale handtekening met dezelfde waarde als een 'natte' handtekening –gekwalificeerde elektronische handtekening. Als laatste kunnen zij ook vertrouwelijkheid garanderen met deze certificaten door de berichten te versleutelen. Beroepscertificaten worden momenteel gebruikt in verschillende private processen. In het publieke domein worden ze (nog) niet gebruikt.

Services certificaten zijn niet gebonden aan een persoon, maar aan een systeem en worden soms ook als systeemcertificaten aangeduid. Deze certificaten kunnen ook gekoppeld zijn aan een functie. In § 8.4 komen we terug op het gebruik van services certificaten in SBR.

Bijzonderheid 4: Er gelden zorgvuldige uitgifteprocedures
PKIoverheid hanteert strengere voorwaarden voor uitgifte van certificaten dan PKI systemen die niet met gekwalificeerde certificaten werken. Eén van die voorwaarden die PKIoverheid hanteert voor de uitgifte van een gekwalificeerd certificaat is dat de gebruiker fysiek zijn gezicht moet laten zien (identificeren) bij de CSP. Deze voorwaarden gelden niet alleen voor de persoonsgebonden certificaten, maar ook voor de certificaten op organisatieniveau. PKIoverheid streeft naar één hoog betrouwbaarheidsniveau voor alle certificaattypen. PKIoverheid certificaten kunnen aangevraagd worden bij CSPs in Nederland.

De verschillende CSPs hanteren verschillende procedures voor het aanvragen van certificaten, maar globaal lopen ze drie stappen door:

1. Men moet de organisatie registreren bij de CSP als abonnee.
2. Men moet certificaatbeheerders aanwijzen als eerste aanspreekpunt voor de CSP.
3. Via een aanvraagformulier vraagt men bij de CSP een specifiek certificaat aan.

Voor het intrekken van een certificaat dient de certificaathouder de CSP die het certificaat heeft uitgegeven te benaderen en deze te verzoeken het certificaat in te trekken. De eisen die aan de CSP worden gesteld voor het uitgeven en beheren van deze certificaten, zijn beschreven in het PvE van PKI.overheid (http://www.logius.nl).

Bijzonderheid 5: CSPs moeten aan strenge eisen voldoen om PKIoverheid certificaten te mogen uitgeven
Binnen de PKIoverheid worden door CSPs certificaten aan eindgebruikers uitgegeven. Om PKIoverheid certificaten te kunnen uitgeven moet een CSP in de hiërarchie van de PKI voor de overheid worden opgenomen. Concreet betekent dit dat de publieke sleutel van een CSP wordt ondertekend door een Domein-CA van de PKI voor de overheid. Om de betrouwbaarheid van de PKI voor de overheid te waarborgen, moeten CSPs binnen PKIoverheid voldoen aan strenge eisen voor hun operationele

procedures, technische middelen, beveiliging van informatie, deskundigheid en betrouwbaarheid van personeel en informatieverstrekking aan hun doelgroep. De concrete eisen waaraan een CSP moet voldoen om certificaten binnen de PKI voor de overheid te mogen uitgeven, zijn opgenomen in het PvE PKIoverheid.

Om de betrouwbaarheid van de PKIoverheid blijvend te kunnen waarborgen, moeten de CSPs ook na toetreding tot de PKI voor de overheid blijven voldoen aan de gestelde eisen. Om dit vast te stellen, houdt de PA toezicht op de toegetreden CSPs en moeten de CSPs periodiek conformiteitbewijzen inleveren.

Bijzonderheid 6: De Policy Authority (PA) PKIoverheid houdt toezicht op de PKIoverheid leveranciers (CSPs)
De PA kijkt in hoeverre de CAs voldoen aan de eisen van de betreffende PKI. De PA wordt soms ook wel toezichthouder genoemd. Het gaat hier niet om een door de wet voorgeschreven rol van toezichthouder met dwangmiddelen/instrumenten (zoals de rol van de OPTA, opgegaan in de Autoriteit Consument en Markt (ACM)), maar om een controlerende rol die let op de naleving van afspraken en procedures binnen het PKI-afsprakenstelsel. Deze vorm van toezicht bestaat onder meer uit de volgende onderdelen:

- De PA PKIoverheid laat jaarlijks door een externe leverancier penetratietesten uitvoeren op de internet facing omgeving van de CSPs.
- Samen met de ACM (OPTA) bezoekt de PA PKIoverheid jaarlijks de CSPs naar aanleiding van bevindingen uit het auditrapport van de externe auditor.
- De PA PKIoverheid bezoekt een á twee keer per jaar de CSPs om onder andere te controleren of, en zo ja hoe, nieuwe eisen van het PvE zijn geïmplementeerd.

Deelconclusie
Het gebruik van encryptie en daarmee de effectiviteit van de hiermee te bereiken beveiliging staat en valt met een goed ingericht beheer van de sleutels en certificaten. Een PKI systeem is noodzakelijk voor het adequaat inrichten van het certificatenbeheer. Adequaat betekent hier in lijn met de relevante wettelijke, technische en domeineisen. In het geval van PKIoverheid zijn er strikte maatregelen genomen om aan de eisen te voldoen. Hierdoor garanderen PKIoverheid certificaten voor het elektronisch verkeer door en met de overheid een hogere veiligheidsnorm dan niet-PKIoverheid certificaten. Uitgaande van adequaat sleutelbeheer vormen certificaten een sterk middel voor identificatie en authenticatie: er kan dankzij de mogelijkheid voor het meesturen van een digitale handtekening met hoge mate van zekerheid worden vastgesteld dat A (uit figuur 8.3) de afzender van een bericht is. Ook wordt een hoge mate van integriteit en onweerlegbaarheid geborgd. Met andere woorden, we kunnen vaststellen dat het bericht onderweg niet gewijzigd is, en dat de (getekende) verzending in gang is gezet door de eigenaar van de privé sleutel, omdat die er als enige over beschikt. Ook hier is de mate van zekerheid afhankelijk van de kwaliteit van het sleutelbeheer. Een vraagstuk dat echter onvoldoende wordt opgelost met een PKI is autorisatie (en daarmee exclusiviteit, in het derde deel van dit hoofdstuk wordt uitgelegd waarom): is een persoon/organisatie bevoegd om een bericht in te sturen of om een reactie in te zien? De volgende paragraaf beschrijft een bouwsteen die in dit vraagstuk voorziet, een machtigingenvoorziening.

8.3.6 *Bouwsteen 2 – een machtigingenvoorziening voor autorisatie*

8.3.6.1 De behoefte aan een machtigingenvoorziening

Bij communicatie zijn er minimaal twee communicatiepartners: een verzender en een ontvanger. Vaak is er ook sprake van een tussenpersoon welke gemachtigd is om te handelen namens een van de communicatiepartners, hier ook wel intermediair genoemd. Intermediairs worden vaak zelf communicatiepartners in plaats van de oorspronkelijke belanghebbende namens wie zij handelen en waar de informatie betrekking op heeft. Dit brengt in de i-processen het autorisatievraagstuk naar boven: is een persoon bevoegd om bepaalde handelingen uit te voeren? In afwezigheid van de belanghebbende is dit lastig om vast te stellen. Het is omslachtig om bij elke informatie-uitwisseling bij de belanghebbende na te vragen of hij gebruikt maakt van een intermediair en zo ja, welke intermediair dat is en welke handelingen deze wel of niet namens belanghebbende mag uitvoeren. Tevens is het zeer belastend voor een belanghebbende, die middels een intermediair juist lasten uit handen wil geven. Het dilemma hier is dat we vanuit beginselen als exclusiviteit, authenticiteit en onweerlegbaarheid een machtigingsrelatie wel zouden moeten controleren. Dit moet op een proportionele wijze – passend bij de aard en het doel van een bericht. Het is geen optie om iedereen die claimt een intermediair te zijn namens een ander, te geloven zonder enig bewijs van een geldige machtigingsrelatie. Een kwaadwillende zou op deze wijze aan gevoelige informatie kunnen komen.

Maar hoe controleren we een machtigingsrelatie? Welke procedures en middelen zijn hiervoor nodig? Dit zijn slechts enkele vragen die het SBR Programma moest beantwoorden rond het machtigingenvraagstuk. Er was bij het inrichten van SBR berichtenstromen nog geen kant-en-klare bouwsteen beschikbaar die voldeed aan de gestelde eisen. Men heeft zelf een bouwsteen – een machtigingenvoorziening – ontwikkeld, die moest voorzien in de mogelijkheid de machtigingsrelatie tussen belanghebbende en intermediair(s) vast te leggen en deze wanneer nodig op te vragen. Deze bouwsteen moet echter wel generiek ingericht zijn, zodat het ook voor andere S2S i-processen kan worden ingezet. Het ontwerp van deze machtigingenvoorziening wordt hier beschreven. In § 8.4.3 wordt ingegaan op de vraag hoe de machtigingenvoorziening wordt ingezet in SBR berichtenstromen.

De rol van de intermediair in verantwoordingsketens
Een ondernemer kan ervoor kiezen om zijn administratie zelf te voeren en daarmee ook zelf aan de administratieve verplichtingen van de overheid te voldoen. Hij kan er ook voor kiezen om deze taken uit te besteden aan een (of meerdere) gespecialiseerde tussenperso(o)n(en). Een taak die vaak wordt uitbesteed is de salarisadministratie, naast de boekhouding en de aanvraag van subsidies. In het geval dat een ondernemer er voor kiest om taken uit te besteden, betekent dit dat de betrokken intermediair namens hem moet kunnen handelen. Het bedrijf 'machtigt' de intermediair (zie vertegenwoordiging door een gemachtigde, art. 2:1 Awb en volmacht, art. 3:60 BW). In dat geval moet de overheid in staat zijn om de intermediair te herkennen en vast te stellen of hij inderdaad gemachtigd is voor die handeling (autorisatie). Dit speelt zowel bij het aanleveren van gegevens als bij het ontvangen van retourinformatie van de overheid. Vanwege de vertrouwelijke aard van retourinformatie is het van belang dat de retourinformatie alleen voor de bevoegde intermediair beschikbaar is. Hiertoe is er in de keten behoefte aan functionaliteit, waarmee vastgesteld kan worden dat er daadwerkelijk een machtigingsrelatie bestaat tussen een intermediair en de belanghebbende waarop de aangeleverde of retourinformatie betrekking heeft.

8.3.6.2 Het ontwerp van de machtigingenvoorziening

De volgende vijf ontwerpaspecten van de machtigingenvoorziening worden nader toegelicht:

- De opzet: een centrale machtigingenvoorziening
- De machtigingsprocedures
- De reikwijdte van de machtiging
- De vastlegging van een machtiging
- De autorisatieprocessen

We beginnen met de opzet van een machtigingenvoorziening. In principe zijn er twee typen machtigingenvoorzieningen te onderscheiden: centraal en decentraal (Kizza, 2009). Decentrale machtigingenvoorzieningen zijn gedistribueerd qua opzet. Er zijn meerdere machtigingenregisters, die door verschillende organisaties beheerd worden. Gezamenlijk kunnen deze individuele registers één voorziening vormen. Het machtigingenregister is datgene wat in de literatuur op het gebied van 'authorization & access control' als 'access control list' wordt aangeduid. Dit is een lijst (database) van machtingsrelaties (autorisaties) die gekoppeld zijn aan een vertegenwoordigde en een gemachtigde (intermediair). In SBR is er vooralsnog niet gekozen voor een decentrale opzet, omdat er geen behoefte aan is. Daarnaast vraagt het ontwerpen en in stand houden van een decentrale opzet om veel afstemming. Er is daarom voor een centrale machtigingenvoorziening gekozen.

Een centrale machtigingenvoorziening kent één machtigingenregister en één beherende organisatie. Dit kent een simpele opzet, die snel en eenduidig te ontwerpen en in stand te houden is.

Het tweede ontwerpaspect betreft de machtigingsprocedures. Er zijn drie handelingen die bij deze machtigingenvoorziening terugkomen om wijzigingen in het machtigingenregister door te voeren:

- Het opvoeren van de machtiging
- Het verifiëren van de machtigingsrelatie
- Het intrekken van de machtiging

De eerste handeling is het opvoeren van een machtigingsclaim. De intermediair kan zich system-to-system opgeven als gemachtigde middels het aanleveren van een machtigingsclaim bij Digipoort. Hierna begint de tweede handeling: het verifiëren van de machtigingsrelatie. Deze verificatie bestaat uit een kennisgeving aan de vertegenwoordigde met een opt-out optie en een reactietermijn, tot de claim wordt omgezet naar een actieve machtiging. Wanneer de claim geverifieerd is, kan ook daadwerkelijk over een machtiging gesproken worden. De claim kan namelijk onterecht zijn. Het gaat hier om het vastleggen van een bestaande machtiging en niet om het creëren van een machtiging.

Ten derde is het mogelijk om een eerder opgevoerde machtiging in te trekken. De machtiging kan worden ingetrokken door beide partijen. De machtiging kan system-to-system worden ingetrokken door de partij die hem heeft laten registreren – de gemachtigde. De vertegenwoordigde heeft ook de mogelijkheid om de machtiging in te (laten) trekken, bijvoorbeeld bij een verstoorde relatie met zijn intermediair. Dit kan schriftelijk bij de beheerder van de machtigingenvoorziening.

Voor het opvoeren en intrekken van machtigingen bij Digipoort wordt gebruikt gemaakt van PKIoverheid services certificaten (bouwsteen 1) ten behoeve van identificatie en authenticatie. Voor verificatie van de machtiging en de vertegenwoordigde wordt gebruik gemaakt van authentieke registers, zoals het Handelsregister.

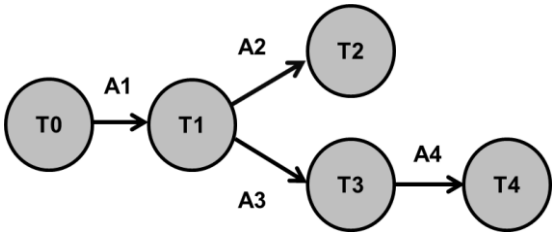
Het derde ontwerpaspect is de reikwijdte van de machtiging. De reikwijdte betreft onder meer aspecten als de dienst, de tijdspanne en de typen handelingen die verricht mogen worden. De dienst kan van breed (omvat bijvoorbeeld meerdere typen verantwoordingen of mededelingen) tot smal (één bepaald type verantwoording of mededeling) gedefinieerd worden. De tijdspanne van de machtiging kan uiteenlopen van eenmalig tot een bepaalde periode tot onbepaalde tijd. Een langere tijdspanne is eenvoudiger voor de gebruikers, maar maakt de tijd tussen wilsuiting voor het ontstaan van de machtiging en beëindiging van de machtiging langer; de belanghebbende kan de machtiging vergeten zijn. Voor een toepassing als bij SBR, waar met de overheid vertrouwelijke gegevens met (mogelijk) rechtsgevolgen worden uitgewisseld, ligt een beperkte looptijd en een afzonderlijke machtiging per type verantwoording voor de hand.

Het vierde ontwerpaspect is de vastlegging van de machtiging. Op het moment dat een intermediair namens een onderneming wil handelen, wordt gecontroleerd of hij door die onderneming is gemachtigd om deze handelingen uit te voeren. Door toepassing van een machtigingenvoorziening kan Digipoort geautomatiseerd controleren of bij elke handeling door de intermediair ook daadwerkelijk de benodigde machtiging aanwezig is. Een machtiging bestaat uit een combinatie van drie kenmerken (gemachtigde, vertegenwoordigde en de dienst) en kan in verschillende toestanden verkeren. De machtigingenvoorziening registreert, naar aanleiding van het opvoeren van een machtigingsclaim en de verificatie ervan, een machtiging als ‘actief’ (of ‘geldig’) en, naar aanleiding van een intrekking of het verlopen van de dienst, een machtiging als ‘niet actief’ (of ‘ongeldig’). Daarnaast zijn er de volgende toestanden: machtiging bestaat niet, machtiging in behandeling, machtiging afgekeurd. Hieronder zijn de mogelijke toestanden van een machtiging in een tabel weergegeven.

Tabel 8.2 – Vastlegging van een machtiging: mogelijke toestanden van een machtiging

Toestand	Beschrijving
T0	Bestaat niet in het register
T1	In behandeling
T2	Afgekeurd (eindtoestand)
T3	Actief
T4	Niet actief (eindtoestand)

Een machtiging kent de volgende toestandsovergangen:



Figuur 8.7 –Toestandsovergangen bij een machtiging naar aanleiding van bepaalde activiteiten

De overgang van de ene toestand naar de ander geschiedt langs een activiteit. Hieronder volgt een tabel met de activiteiten die een toestandstransitie tot gevolg hebben.

Tabel 8.3 – Activiteiten die leiden tot een wijziging van de toestand van een machtiging

Activiteit	Trigger
A1	Opvoeren van een machtigingsclaim
A2	Afkeuren van de machtigingsclaim n.a.v. het „niet verifieerbaar" zijn van de machtigingsclaim
	Afkeuren van de machtigingsclaim n.a.v. een brief van belanghebbende.
	Intrekkingsverzoek door gemachtigde
A3	Automatisch na 19 kalenderdagen geen reactie
A4	Dienst verlopen
	Intrekkingsverzoek door gemachtigde
	Intrekkingsverzoek van gemachtigde of vertegenwoordigde

Of de geclaimde relatie voorkomt in het machtigingenregister wordt door de machtigingenvoorziening met behulp van een getekend bericht medegedeeld aan de Digipoort. Digipoort stuurt alleen berichten door (aangeleverde informatie, bepaalde statusinformatie of mededelingen) wanneer de relatie vastgelegd is. Bovendien is het vastleggen van een tweede machtiging voor dezelfde dienst en dezelfde vertegenwoordigde niet mogelijk. Daarmee wordt een hogere mate van exclusiviteit van de berichten gerealiseerd; zeer wenselijk bij berichten met vertrouwelijke inhoud.

De machtigingen worden in een centraal en beveiligd register vastgelegd. Alleen specifieke processen hebben toegang tot dit register en hebben afhankelijk van hun functie specifieke rechten, waardoor bijvoorbeeld een controleproces slechts het register kan inzien en geen mutaties kan uitvoeren.

Het vijfde ontwerpaspect betreft de autorisatieprocessen. Dit zijn de geautomatiseerde handelingen die Digipoort uitvoert om te controleren of een specifieke machtiging actief is. De toepassing hiervan hangt af van het proces waarvoor de bouwsteen wordt ingezet. § 8.4 geeft nadere toelichting over de werking van de autorisatieprocessen in het kader van SBR. Een aandachtspunt bij de autorisatieprocessen is: welke informatie wordt verstrekt aan de gemachtigde? De richtlijn is dat je niet meer informatie verstrekt dan de gemachtigde al zou moeten weten. Dit betekent dat Digipoort de gemachtigde nooit 'nieuwe' informatie uit de machtigingenvoorziening meegeeft. Een voorbeeld hiervan is dat een gemachtigde die namens een vertegenwoordigde een mededeling wil opvragen waarvoor geen machtiging bestaat, alleen geinformeerd wordt dat de machtiging niet bestaat. En dus niet de informatie ontvangt welke partij dan wel gemachtigd is voor de betreffende vertegenwoordigde.

Deelconclusie
De ontwerpaspecten weerspiegelen een aantal keuzes, dat partijen hebben gemaakt bij het ontwikkelen van een machtigingenvoorziening ten behoeve van de betrouwbaarheid en vertrouwelijkheid in elektronisch berichtenverkeer. Hierin zien we de relatie tussen de machtigingenvoorziening als bouwsteen, autorisatie als maatregel en het beginsel van exclusiviteit (voorkomen dat informatie onterecht aan onbevoegden kan worden verstrekt). Deze keuzes rond de ontwerpaspecten hebben niet alleen een invloed op de bruikbaarheid, toegankelijkheid en kosten van de machtigingenvoorziening, maar ook op de informatiebeveiliging. Zwakheden in de opzet van de machtigingenvoorziening, of nalatigheid in gebruik of beheer, maken dat gevoelige informatie onterecht aan onbevoegden kan worden verstrekt of onterecht in naam van belanghebbende wordt opgevraagd.

8.4 Borging van informatiebeveiliging in SBR

8.4.1 *Scope*

Eerder in dit hoofdstuk hebben we generieke bouwstenen voor informatiebeveiliging besproken. In dit deel bespreken we hoe deze bouwstenen bij SBR worden toegepast. Hierbij wordt aandacht besteed aan de keuzes die ten aanzien van de toepassing zijn gemaakt om in de beginselen van beveiliging die in § 8.2 zijn uitgelegd, te voorzien.

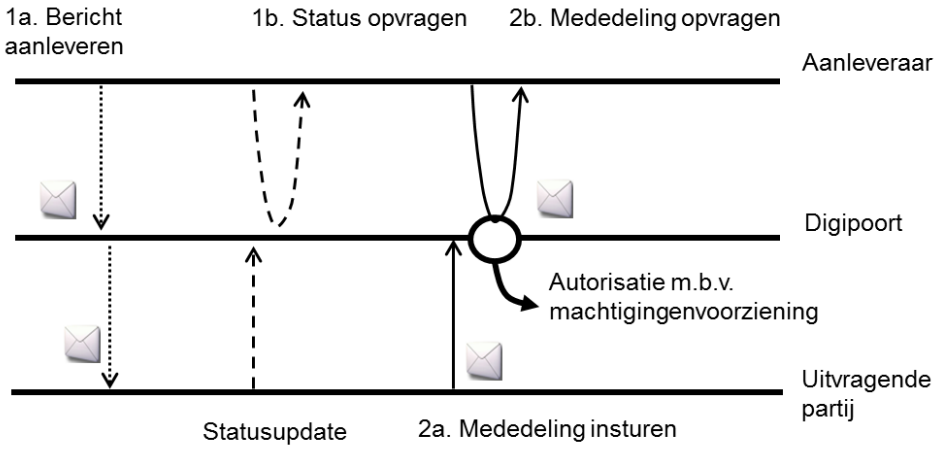
Om zo concreet mogelijk de toepassing van de bouwstenen te kunnen beschrijven wordt gebruik gemaakt van een vereenvoudigd overzicht van de i-processen waar aanleveraar (bedrijf/intermediair) en uitvragende partijen mee te maken krijgen bij het S2S uitwisselen en verwerken van berichten met verantwoordingsinformatie via Digipoort. Het gaat om twee hoofdprocessen:

1. Aanleveren, dit is te splitsen in:
   a. Het aanleveren van een bericht via Digipoort. Dit gebeurt aan de hand van een 'informatie push'.
   b. Het opvragen van een status (omtrent de aanlevering). Dit gebeurt aan de hand van een 'informatie pull'.

2. eMededelen, dit is te splitsen in:

a. Het insturen van een mededeling door de uitvragende partij (bijvoorbeeld een Service Bericht Aanslag). Dit gebeurt aan de hand van een 'informatie push'.
b. Het opvragen van een mededeling door een gemachtigde partij (inclusief autorisatie via de machtigingenvoorziening). Dit gebeurt aan de hand van een 'informatie pull'.

Onderstaand figuur biedt een vereenvoudigd beeld van deze i-processen, die elk via Digipoort verlopen. Een informatie push wordt weergegeven met een rechte pijl, een informatie pull met een gebogen pijl.



Figuur 8.8 – Vereenvoudigde weergave van de belangrijkste i-processen via Digipoort

Gezien vanuit de aanleveraar vindt er op twee manieren interactie plaats: een informatie push (insturen van een bericht) en een informatie pull (opvragen van een reactie op een ingestuurd bericht). De Belastingdienst, Kamer van Koophandel en Centraal Bureau voor de Statistiek zijn hierbij de uitvragende partijen die gebruik maken van Digipoort. De keuze voor gebruikmaking van een push of een pull, leunt op een aantal overwegingen. Zo is er voor een push een stabiel en vertrouwd afleveradres (een endpoint) met webservice nodig. We kunnen van de overheid verwachten dat zij de investeringen doet die hiermee gemoeid zijn; voor de duizenden aanleverende partijen ligt dat anders. Daarnaast wil je bij een push zeker weten, dat de ontvanger inderdaad degene is die hij of zij beweert te zijn. Als enkele uitvragende partijen (via Digipoort) naar duizenden aanleveraars een bericht moeten pushen, zouden de uitvragende partijen 'proactief' (voor de push) autorisaties moeten uitvoeren en de aanleveraars een vertrouwd adres moeten toekennen. Tenslotte is ook de aard van de uit te wisselen berichten een factor die meespeelt. De aanleverende partij neemt zelf het initiatief om een bericht (zoals een belastingaangifte) in te sturen en kiest de informatie en het moment dat ze het wil indienen; hierbij rekening houdend met eventuele wettelijke voorschriften t.a.v. kanaalvorm (IB of IB-winst, JRklein of JR groot) en/of termijn. Een aanleverende partij kan op elk gewenst moment een bericht naar Digipoort pushen. Omgekeerd - op elk moment pullen door Digipoort - is lastiger,

aangezien de aanleveraar geen berichtenbox heeft die altijd bereikbaar is, het om vele aanleveraars gaat (beheerlast) en het voor Digipoort niet is vast te stellen wanneer een bericht bij een aanleveraar 'klaar voor verzending' is. Wanneer het gaat om retourstromen –berichten gepusht door de uitvragende partijen naar Digipoort – is het onderscheid tussen push en pull ook van belang. Bij het klaarzetten van het retourbericht geldt dat Digipoort voortdurend beschikbaar is voor opvraagverzoeken. Het kan niet worden verwacht dat een ontvangend bedrijf op het moment dat het de overheid schikt – of permanent – een beveiligde verbinding opzet om zodoende een bericht te ontvangen. Een pull biedt hierbij de oplossing: de aanleveraar beslist zelf wanneer zij in de 'berichtenbox' van Digipoort gaat kijken of de uitvragende partij een bericht heeft ingestuurd. Kortom, de vorm van de interactie is van invloed op de behoefte aan maatregelen voor informatiebeveiliging.

Bovenstaande i-processen vormen de context waarbinnen we de bouwstenen gaan beschrijven. In de volgende paragrafen wordt aangegeven hoe de middelen en bouwstenen per i-proces worden gebruikt, teneinde betrouwbare en vertrouwelijke S2S-uitwisseling en -verwerking van verantwoordingsinformatie mogelijk te maken. Hierbij zullen we waar nodig een uitstapje moeten maken naar specifieke kenmerken van een bouwsteen die van belang zijn voor de beveiliging. We beginnen met het aanleverproces (inclusief statusopvraagproces), waarin nadruk wordt gelegd op het gebruik van PKIoverheid services certificaten als bouwsteen voor identificatie en authenticatie. Daarna wordt ingegaan op de beveiliging van het eMededelenproces, waarbij nadruk wordt gelegd op de machtigingenvoorziening als bouwsteen voor autorisatie.

8.4.2 *Beveiliging van het aanleverproces*

8.4.2.1 Het opzetten van een dubbelzijdige SSL/TLS-verbinding

Een bedrijf/intermediair (aanleverende partij) die een bericht wil aanleveren via Digipoort, moet hiervoor een beveiligde verbinding opzetten via het internet. Dit kan via een hiervoor geschikt softwarepakket. Aangezien berichten via het internet (TCP/IP) worden uitgewisseld en kunnen worden onderschept of gewijzigd, zijn met het oog op de aard van de berichten die tussen aanleveraar en uitvragende partijen worden uitgewisseld, additionele maatregelen noodzakelijk. In SBR is besloten om berichten via een dubbelzijdige SSL/TLS-verbinding (een tunnel) uit te wisselen. Dit onder andere omdat deze vorm van versleuteling de juiste balans bevat tussen het gewenste (hoge) beveiligingsniveau en de eenvoud van implementatie door aanleverende partijen. SSL/TLS zijn volwassen standaarden die breed toegepast worden en door de meeste softwaresystemen ondersteund worden. De benodigde kennis is breed beschikbaar. Een SSL/TLS-verbinding kan op verschillende manieren worden opgezet. In SBR is ervoor gekozen om dit door middel van PKIoverheid services certificaten te doen.

De toevoeging 'dubbelzijdig' verwijst hier naar een versleutelingsvorm, waarbij beide partijen (aanleveraar en Digipoort) over een certificaat beschikken. Dit houdt in dat zowel de aanleveraar als Digipoort zichzelf moeten identificeren (met het certificaat) en elkaar moeten authenticeren (controleren van elkaars certificaat), alvorens er tot uitwisseling en verwerking van informatie kan worden overgegaan. Dubbelzijdige SSL/TLS garandeert dat beide partijen zijn wie ze zeggen te zijn.

Beveiligde verbinding biedt de nodige waarborgen voor SBR berichten

Dankzij de beveiligde verbinding is het moeilijker voor een derde partij om interruptie te plegen. Dit is onder meer vanwege de termijngebondenheid van bepaalde verantwoordingsplichten van belang voor SBR. Neem bijvoorbeeld de jaarrekening. Indiening van de jaarrekening is wettelijk verplicht en dient binnen een bepaalde termijn te gebeuren. Indien indiening door interruptie (ongemerkt) niet plaats zou vinden, loopt de bestuurder van een onderneming kans dat hij hier achteraf op zou worden aangesproken. Ook bij belastingaangiften maakt het wettelijk verplicht en termijngebonden doen van aangifte dat de beginselen van beschikbaarheid, authenticiteit, integriteit en onweerlegbaarheid een belangrijke rol spelen. Indien indiening door interruptie of storing – onopgemerkt door de verzender – niet plaatsvindt, kan vanuit de fiscus een boete worden opgelegd. Overigens zijn de SBR i-processen zodanig ontworpen dat, indien er toch iets misgaat bij de aanlevering, dit aan de hand van de statusberichten in de sessie kan worden opgemerkt. Voorts zijn in de keten professionele accountantsorganisaties actief met een doorgaans volwassen automatisering. Zij kunnen eventuele vertragingen of onregelmatigheden in de keten snel opmerken en daar feedback over geven.

In hoofdstuk 7 (Technische inrichting SBR) wordt uitvoerig ingegaan op de verschillende functies van een koppelvlakspecificatie. Samengevat: een koppelvlakspecificatie beschrijft op welke manier en onder welke condities een verbinding tussen twee systemen kan worden opgezet en bevat (logistieke) afspraken om berichten juist te adresseren, leesbaar, uitwisselbaar en verwerkbaar te maken en veilig en betrouwbaar te verzenden.

Communicatie met Digipoort kan via verschillende koppelvlakspecificaties plaatsvinden, afhankelijk van de berichtsoorten en de partijen. Voor bedrijven is er bijvoorbeeld 'SOAP2008' en 'WUS voor bedrijven' (zie hoofdstuk 7). Overheidspartijen kunnen gebruik maken van de ebMS koppelvlakspecificatie. Deze koppelvlakspecificaties zijn gebaseerd op open internationale standaarden, wat ten goede komt aan de flexibiliteit van de elektronische communicatie. Ze leggen onder andere de volgende afspraken vast:

- Het beveiligingsprotocol waarlangs communicatie tussen client en server plaatsvindt (een versie van SSL/TLS).
- Het endpoint (aanspreekadres) dat moet worden ingevuld (een endpoint is in Digipoort gekoppeld aan een of meerdere berichtsoorten).
- De encryptiestandaard (bijvoorbeeld RSA) die gebruikt moet worden.
- Welk type PKIoverheid certificaten (uit welke domeinen en roots) worden geaccepteerd gedurende de verbinding.
- De berichtopzet met verplichte velden, waaronder de WS-Security header. Basis hiervoor is het web service security (WS-Security) protocol, dat onder meer beschrijft hoe een digitale handtekening in een SOAP bericht wordt vastgelegd (Bertino, Martino, Paci, & Squicciarini, 2010).

8.4.2.2 Gebruik van PKIoverheid certificaten in het aanleverproces

In SBR heeft men om een aantal redenen gekozen voor PKIoverheid certificaten. Relevant zijn bijzonderheden zoals een gelaagde eisenstructuur, strikte uitgifteprocedures van certificaten en de strenge voorwaarden waaraan de CSPs dienen te voldoen (zie § 8.3). Hierdoor borgen deze certificaten een hoge mate van betrouwbaarheid en vertrouwelijkheid in elektronisch berichtenverkeer. De keuze voor dit reeds bestaande en breder toepasbare stelsel past ook bij het streven van de partijen in SBR om waar mogelijk te kiezen voor het hergebruik van bestaande bouwstenen.

Digipoort voert bij aanlevering een controle uit op de berichtintegriteit, met andere woorden, op de geldigheid van de digitale handtekening. Tevens wordt er aan de hand van de CRL bij de CSP geverifieerd of een certificaat al of niet ingetrokken is. Digipoort verkrijgt door het gebruik van de certificaten de zekerheid dat de aanleveraar beschikt over een certificaat dat, na enkele controles op de door de aanleveraar geclaimde identiteit, verstrekt is door een betrouwbaar geachte CSP. Daar de huidige erkende CSPs er in het kader van het behoud van hun betrouwbare imago belang bij hebben certificaten slechts dan te verstrekken wanneer zij zich hebben vergewist van de door de aanvrager geclaimde identiteit, is er redelijke zekerheid over de authenticiteit van een certificaat en een daarmee getekend bericht.

Zoals in figuur 8.6 geïllustreerd zijn er verschillende typen certificaten die onder PKIoverheid worden uitgegeven. Voor het aanleveren bij Digipoort zijn zogenaamde 'Services' certificaten onder het domein 'Organisatie' noodzakelijk. Services certificaten vervullen grofweg drie functies in de beveiliging van berichtstromen in SBR:

1. Het opzetten van een dubbelzijdige SSL/TLS-verbinding met Digipoort.
2. Het zetten van een digitale handtekening in de WS-securityheader van een SOAP-bericht. Hiermee kan meer zekerheid worden gegeven over de authenticiteit en tijdigheid van een bericht.
3. Het zetten van een digitale handtekening in de XBRL-instance ter bewaking van de integriteit van het instance-document (ook wel enveloping signature genoemd). Hiermee kan de end-to-end integriteit worden versterkt. Deze wordt in de praktijk nog niet vaak toegepast.

Functies 1 en 2 zijn verplicht bij communicatie met Digipoort. Functie 3 is momenteel niet verplicht en er wordt bovendien weinig gebruik van gemaakt. Wanneer in de toekomst berichten met accountantsverklaringen via Digipoort zullen worden aangeleverd (bijvoorbeeld de jaarrekening van middelgrote en grote ondernemingen met wettelijk vereiste controleverklaring), zal deze functionaliteit wel worden gebruikt. Dergelijke verklaringen dienen namelijk te zijn voorzien van een handtekening van de accountant. De accountant zal dan voor de enveloping signature zijn persoonlijke beroepscertificaat kunnen gebruiken.[37] Het toevoegen van de enveloping signature wordt dan toegepast náást het verplichte tekenen van het bericht

[37] Omdat in zo'n geval de inhoud (enveloping signature) met een persoonsgebonden certificaat wordt getekend, vervult deze digitale handtekening van de accountant dan ook de functie van wilsuiting. En heeft dus dezelfde rechtsgevolgen als een handgeschreven handtekening.

(functie 2). We hebben in § 8.4.2.1 functie 1 behandeld. Functie 2 wordt hieronder toegelicht.

Een bericht dat aangeleverd wordt, dient altijd door de aanleveraar te zijn getekend met een PKIoverheid services certificaat. Het gebruik van dit type certificaten voor het tekenen van berichten is technisch gangbaar. Omdat het geen persoonsgebonden certificaten zijn, is er geen sprake van 'ondertekenen', maar van 'tekenen'. De digitale handtekening (versleutelde hashwaarde – zie § 8.3.3) wordt berekend over de volgende specifieke velden uit het SOAP bericht (zie hoofdstuk 7 voor een gedetailleerde beschouwing van het SOAP bericht):

- De body
- Het header-onderdeel Timestamp
- Het header-onderdeel WS-Addressing (alle elementen)

De handtekening wordt vervolgens als het WS-Security element in de bericht-header opgenomen.

Deze werkwijze levert het volgende op:

- Voor de ontvanger, de mogelijkheid tot controle van de integriteit van het bericht
- Zekerheid over de identiteit van de verzender van het bericht
- Zekerheid voor beide partijen over het moment van aanlevering

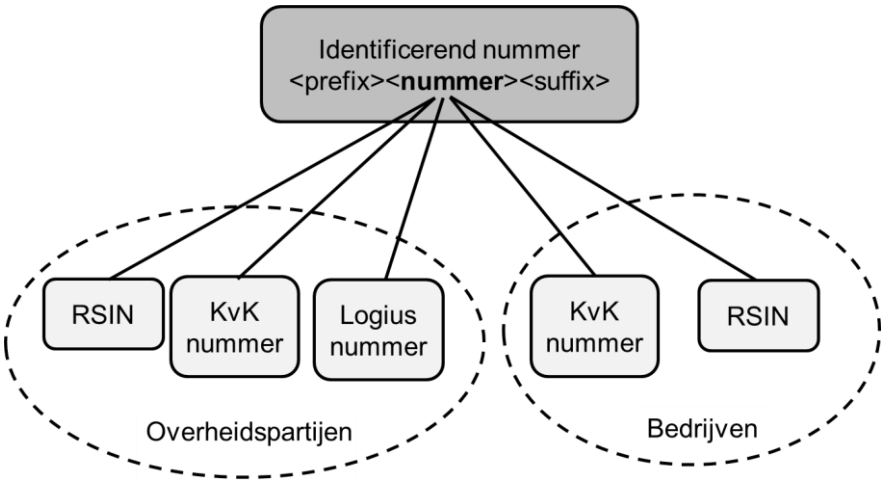
De publieke sleutel in het certificaat waarmee de handtekening gezet wordt, moet meegeleverd worden in de WS-Security header. Bij aflevering aan de uitvragende partij wordt het platte bericht (zonder WS-Security header) door Digipoort doorgestuurd. Dit scheelt extra berichtverwerkingscapaciteit. Digipoort zet een eigen digitale handtekening op het bericht. Dit betekent dat de integriteit van het bericht vanaf dat moment tot aan de aflevering aan de uitvragende partij weer geborgd is. Digipoort legt in het aanleverproces de identificerende gegevens van het certificaat waarmee het bericht is aangeleverd vast in de audit trail. Hierdoor kan achteraf altijd geverifieerd worden met welk certificaat (en dus door welke organisatie) een bericht is aangeleverd, en of rechtmatig of onrechtmatig verkeer heeft plaatsgevonden met een certificaat. De uitvragende partij kan eventueel dergelijke informatie achteraf opvragen. De audit trail wordt vijf jaar bewaard. Ook de verwerkingshandelingen van elk aangeleverd bericht worden vastgelegd. Digipoort legt de gegevens vast aan de hand van een uniek aangemaakt berichtkenmerk, dat de aanleveraar ook direct ontvangt (in dezelfde verbindingssessie). Deze reconstrueerbaarheid draagt bij aan de onweerlegbaarheid en transparantie van de aanleveringen.

8.4.2.3 Identificerend nummer in het certificaat: OIN en HRN

Identificatie en authenticatie van overheidspartijen en bedrijven via certificaten is geen vanzelfsprekendheid: hoe (in welk veld van een certificaat) en met welk identificerend nummer kunnen identificatie en authenticatie geautomatiseerd plaatsvinden? Als we ons verdiepen in deze vragen, zien we opnieuw een uitdaging waar men in SBR voor stond. Aangezien men in SBR meerdere typen stromen naar meerdere uitvragende partijen wil bedienen, is er behoefte aan een eenduidig identificerend nummer dat voortbouwt op bestaande nummers. Bovendien acht de overheid het

wenselijk dat, voor authenticatie in de communicatie tussen overheid en bedrijven, authentieke gegevens worden gebruikt die de overheid kan controleren. Authentieke gegevens zijn in beheer van de overheid, eenduidig geregistreerd en de kwaliteit ervan wordt bewaakt. Er werd besloten om aan te sluiten bij de systematiek die reeds bij certificaten voor overheidspartijen werd gehanteerd binnen Digikoppeling, voor het zogenaamde OverheidsIdentificatieNummer (OIN). In deze systematiek kunnen verschillende soorten nummers in één format onder worden gebracht, ten behoeve van het gebruik in certificaten. Dit gebeurt door middel van een <prefix> en een <suffix> waartussen een <nummer> uit het Handelsregister (HR) of – alleen voor overheidspartijen - een door Logius toegewezen nummer komt te staan. Het gehele identificerend nummer wordt opgenomen in het certificaat (subject.serialNumber veld).

Onderstaand figuur toont de opbouw van de identificerende nummers voor overheidspartijen en voor bedrijven.



Figuur 8.9 – De OIN/HRN systematiek: een eenduidig format voor een identificerend nummer van organisaties, gebaseerd op authentieke gegevens uit het overheidsdomein en het bedrijvendomein.

In de praktijk spreekt men bij een identificerend nummer voor een overheidspartij van een OIN en bij een identificerend nummer voor een bedrijf van een HRN (Handels Register Nummer). Dit kan verwarrend werken omdat het OIN ook gebaseerd kan zijn op een nummer uit het HR. Het onderscheid tussen OIN en HRN is echter nodig, omdat de aanvraagprocedure van het certificaat verschilt. Om verwarring te voorkomen spreken we in dit hoofdstuk van identificerende nummers (voor overheidspartijen of bedrijven). Hieronder wordt het verschil tussen beide nog verder uitgediept.

- Voor overheidspartijen die in het HR staan wordt het <nummer> (als onderdeel van het identificerend nummer) rechtstreeks afgeleid van het door de partij opgegeven RSIN (Rechtspersonen Samenwerkingsverbanden In-

formatie Nummer, vaak het voormalige fiscale nummer van de Belastingdienst) of het KvK-nummer.[38] Overheidspartijen die niet in het HR staan krijgen een <nummer> van Logius toegewezen. Alle overheidsorganisaties worden met hun identificerend nummer opgenomen in het Digikoppeling Service Register (DSR). Daarmee kunnen deze overheidsorganisaties onderling gegevens uitwisselen. Bij de aanvraag van het certificaat verifieert de CSP het nummer aan de hand van het DSR.

- Private organisaties worden geïdentificeerd op basis van een <nummer> in het HR: hun KvK-nummer òf door hun RSIN.[39] In deze variant wordt een identificerend nummer vastgesteld door de CSP, op basis van het door de aanvrager (bedrijf) opgegeven KvK-nummer of RSIN-nummer, dat door de CSP wordt gecontroleerd door middel van raadpleging van het HR.

De verificatie van het identificerend nummer door de CSP bij de aanvraag en uitgifte van het certificaat maakt de zekerheden die het gebruik van het certificaat in het proces biedt, groter. In het aanleverproces bij Digipoort wordt de aanleveraar geïdentificeerd aan de hand van het identificerend nummer in het certificaat, maar wordt dit nummer niet opnieuw geverifieerd. Wel kan het achteraf worden gebruikt voor reconstructie. Voorts vindt in het proces controle op de geldigheid van het certificaat plaats. Om vast te stellen of het certificaat nog steeds geldig gebonden is aan een bepaalde organisatie, wordt CRL-controle gehanteerd. Alle uitgevers van certificaten zijn verplicht om een CRL bij te houden, waarin gepubliceerd staat welke certificaten gerevoceerd zijn, dat wil zeggen niet meer geldig zijn. Die lijst moet binnen vier uur na een wijziging geactualiseerd worden door de CSP. Nieuwe (of extra) certificaten

BSN niet gebruikt bij SBR

Het Burgerservicenummer (BSN) wordt niet gebruikt als <nummer> voor het identificerend nummer op PKIoverheid certificaten in dit domein. Van eigenaren van eenmanszaken en personen die een rol spelen in een onderneming (bestuurders e.d.) wordt het BSN wel opgenomen in het HR, maar dit nummer is niet openbaar (Handelsregisterwet). Het BSN is bedoeld als een persoonsnummer binnen het publieke domein en is daarom in het HR alleen toegankelijk voor bestuursorganen (Wet algemene bepalingen burgerservicenummer). Een CSP zou (in kader van de Digikoppeling afspraken) het nummer dan ook niet kunnen verifiëren aan de hand van het HR of een ander register. Aan eenmanszaken is altijd een KvK-nummer toegekend, net als aan alle andere ondernemingen. Dit nummer wordt in SBR gebruikt voor het certificaat. Deze oplossing past ook bij de huidige functies van Digipoort, dat qua informatiebeveiliging en processen is ingericht op professionele/bedrijfsmatige aanleveraars, en niet op burgers.

[38] Het is niet duidelijk of er ook daadwerkelijk OIN's op basis van het KvK-nummer in omloop zijn. De systematiek biedt hier de mogelijkheid toe (er is een prefix voor KvK-nummers bepaald), echter de procedures binnen Digikoppeling voor overheidspartijen gaan uit van een RSIN of een door Logius te genereren nummer.

[39] In het HR zijn voor ondernemingen verschillende nummers in omloop:
KvK-nummer. Representeert de economische activiteit (de onderneming).
RSIN. Representeert de 'eigenaar' van een onderneming, in het geval de eigenaar een rechtspersoon is.
BSN. Representeert de 'eigenaar' van een onderneming, in het geval de eigenaar een eenmanszaak is, of representeert een persoon die een rol speelt in een onderneming. Het BSN is geen openbaar gegeven.
Vestigingsnummer. Elke vestiging van een onderneming heeft in het handelsregister één uniek vestigingsnummer van 12 cijfers.

voor dezelfde organisatie kunnen hetzelfde identificerend nummer hebben maar een ander serienummer. Zolang het certificaat geldig is (ondertekend door de CSP, geldigheidsdatum nog niet verstreken en niet ingetrokken), kunnen organisaties ervan uitgaan dat dit nummer correct is.

Door toepassing van de OIN/HRN systematiek is een certificaat herleidbaar tot de organisatie. Dit is een belangrijke invulling van het beginsel van onweerlegbaarheid in de SBR i-processen. Het heeft echter, in aanvulling op de concrete beveiligingsmaatregelen, ook een afwerend effect tegen misbruik. In principe kan iedereen die beschikt over een PKIoverheid certificaat aanleveren. Maar de herleidbaarheid op basis van de registratie van de certificaathouder en de gegevens in de audit trail waarborgen de mogelijkheid tot waarheidsvinding achteraf. Dit maakt het daarom minder aantrekkelijk om niet-professioneel te handelen of over te gaan tot malafide handelingen met SBR berichten, zoals modificatie of fabricatie, of het aanleveren van onterechte, corrupte of grote hoeveelheden berichten. Daarnaast zullen de professionele organisaties die zich bezighouden met aanleveren (intermediairs, accountantsorganisaties) hun eigen processen afdoende beveiligen, om te voorkomen dat vanuit hun naam misbruik kan worden gepleegd.

8.4.2.4 Tussen Digipoort en uitvragende partijen: Diginetwerk

In de communicatie tussen Digipoort en de uitvragende partijen worden specifieke Digikoppeling koppelvlakspecificaties gebruikt, waarbij berichtuitwisseling via Diginetwerk plaatsvindt. Digikoppeling bestaat uit, door het College Standaardisatie van de overheid vastgestelde, koppelvlakspecificaties. Diginetwerk is het besloten netwerk van de overheid dat overheidsorganisaties met elkaar verbindt. Via Diginetwerk kunnen overheden veilig gegevens uitwisselen met andere overheden. De rationale achter Diginetwerk is ervoor te zorgen dat overheidsorganisaties elkaar (en hun elektronische services) kunnen bereiken, ongeacht het fysieke overheidsnetwerk waaraan de organisaties verbonden zijn. Uitgangspunt hierbij is dat het om een bekend aantal uitvragende partijen gaat die professioneel werken en waarmee eenmalig beveiligingsafspraken kunnen worden gemaakt en doorgevoerd. De voordelen van het gebruik van Diginetwerk tussen Digipoort en uitvragende partijen bij SBR zijn:

- Hergebruik van Diginetwerk. Uitvragende partijen kunnen de aansluiting gebruiken voor meerdere e-overheidsdiensten (ook buiten SBR).
- Het biedt extra beveiliging. Niet aangesloten (overheids)partijen hebben geen toegang tot Diginetwerk. Deze extra beveiliging is wenselijk, omdat grote hoeveelheden berichten worden uitgewisseld.

Ook hier worden PKIoverheid certificaten gebruikt (met daarin opgenomen als identificerend nummer het OIN).

8.4.2.5 Beveiliging van het statusopvraag proces

Voor het opvragen van statusinformatie is hetzelfde type certificaat vereist als voor het aanleveren van een bericht. De opvrager tekent met dit certificaat het verzoek om informatie voor een bepaalde geadresseerde te ontvangen. In het opvraagproces wordt gecontroleerd of het identificerend nummer in het certificaat hetzelfde is als het identificerend nummer van het certificaat waarmee het betreffende bericht is

aangeleverd. Dit betekent dat een onbevoegde met een ander certificaat (een ander identificerend nummer) geen statusinformatie over aangeleverde berichten kan opvragen. Net als bij het aanleveren gaat Digipoort er op basis van het authentiek geachte certificaat vanuit, dat de identiteit van de opvrager bij de CSP te achterhalen is. De handelingen ten aanzien van statusinformatie (metadata) worden niet gelogd in de audit trail. De reden hiervoor is dat het mogelijk is om veelvuldig statusinformatie op te vragen over dezelfde aanlevering, en partijen dit ook daadwerkelijk doen. Het wordt niet noodzakelijk geacht om deze handelingen te loggen.

8.4.3 *Beveiliging van het eMededelenproces*

8.4.3.1 Gebruik van een machtigingenvoorziening

Het eMededelenproces (zie figuur 8.8) omvat het afleveren van een inhoudelijk bericht (bijvoorbeeld een service bericht aanslag (SBA)) door een uitvragende partij via Digipoort aan een bedrijf/intermediair. Uiteraard vindt hierbij een aantal interne deelprocessen plaats, zoals het verwerken en klaarzetten van een mededeling in Digipoort. Vanuit een end-to-end perspectief laten we de 'interne deelprocessen in Digipoort' buiten beschouwing en richten ons op de volgende deelprocessen:

1. Het aanleveren van de mededeling door de uitvragende partij.
2. Het opvragen van de mededeling door de daarvoor gemachtigde intermediair.

Bij het eerste deelproces gaat het om het uitwisselen van gegevens via Diginetwerk. De uitvragende partij stuurt op grond van haar wettelijke taak een mededeling, gericht aan een belanghebbende, naar Digipoort. De rest van deze paragraaf zal voornamelijk ingaan op het tweede deelproces. In dit proces wordt een machtigingenvoorziening toegepast, een bouwsteen waarvan enkele ontwerpaspecten al in § 8.3 zijn behandeld.

8.4.3.2 Autorisatie bij opvraagverzoeken

Het gaat bij mededelingen om informatie, afkomstig van de overheid, gericht aan één specifieke belanghebbende, met een vertrouwelijk karakter, met mogelijk gevoelige informatie over de bedrijfsvoering, en waaraan rechtsgevolgen verbonden zijn. Bijvoorbeeld aanslaginformatie, een voorlopige aanslag of kopie aanslag (SBA). Het is daarbij van groot belang om onderschepping (interceptie) te voorkomen. Ook al gebruikt men PKIoverheid certificaten, en krijgt de overheid een hoge mate van zekerheid over met welke partij ze te maken heeft, ze weet niet of een partij gerechtigd is om een SBA van een specifieke belanghebbende te ontvangen. Ten behoeve van een hoge mate van exclusiviteit is gekozen om bij de SBA het machtigingenproces te gebruiken. De overheid wil met oog op het zorgvuldigheidsbeginsel vooraf vaststellen of de partij die zich meldt de berichten inderdaad mag opvragen. Of een partij gemachtigd (geautoriseerd) is, zal moeten blijken uit een autorisatietoets waarbij - als onderdeel van het opvraagproces - wordt gecontroleerd of een machtigingsrelatie bestaat. De machtigingsrelaties zijn vastgelegd in een machtigingenregister.

Het opvraagproces van mededelingen bestaat uit twee stappen. Bij de eerste stap wordt aan de hand van het identificerend nummer in het certificaat gecontroleerd

voor welke belanghebbenden (Fi-nummers, BSNs of RSINs) de opvrager is gemachtigd. Vervolgens wordt een lijst met berichtkenmerken van gereed staande mededelingen die betrekking hebben op de bewuste belanghebbenden, samengesteld en aan de opvrager (gemachtigde) teruggezonden (in één sessie). Bij de tweede stap dient de gemachtigde een verzoek in, dat het berichtkenmerk bevat van de mededeling die hij wil opvragen. Vervolgens controleert de machtigingenvoorziening het bestaan van een geldige machtiging voor dit bericht aan de hand van het identificerend nummer van het certificaat van de opvrager. Indien dat goed gaat, ontvangt de opvragende partij de mededeling. Deze inrichting waarborgt dat een onbevoegde ten eerste niet kan opvragen voor willekeurige partijen of er berichten zijn, of wat voor machtigingen er bestaan, en ten tweede niet het bericht zelf kan opvragen. Ook behelst deze inrichting een 'real time check' op het bestaan van de machtigingen (dat ze niet tussentijds zijn ingetrokken), doordat de machtiging zowel bij het opvragen van de lijst als bij het opvragen van de mededeling wordt gecontroleerd.

Aanvullende waarborgen worden verkregen door enkele ontwerpprincipes. Bijvoorbeeld de regels ten aanzien van de reikwijdte van de machtiging: dat een machtiging voor een specifieke klant en een specifieke dienst wordt geregistreerd. Doet interceptie zich voor, dan gaat het maar om één of enkele berichten. De machtiging wordt per belastingjaar geverifieerd bij de vertegenwoordigde en loopt niet onopgemerkt door. De SBA kan slechts één keer worden opgehaald en is daarna niet langer beschikbaar. Zou er sprake zijn van onderschepping, dan komt dit naar boven zodra de gemachtigde accountant zich meldt voor de aanslag en het niet lukt om deze te verkrijgen. Aan de hand van het betreffende PKIoverheid certificaat zou de identiteit van de onderschepper kunnen worden achterhaald.

8.4.3.3 Audit trail

Zoals eerder al is aangegeven wordt het berichtenverkeer dat plaatsvindt in het kader van SBR, in een audit trail vastgelegd. Van iedere activiteit die in het kader van een aanlever- of opvraagproces wordt doorlopen, wordt vastgelegd wanneer deze plaatshad en wat het resultaat was. Dit geldt ook voor de uitkomst van de controle bij het machtigingenregister. De audit trail verhoogt de transparantie en onweerlegbaarheid van de handelingen ten aanzien van het machtigingenregister en het mededelingenproces.

8.4.3.4 Monitoring

Naast de vele preventieve maatregelen voor informatiebeveiliging speelt ook detectie een rol. Dat zagen we al bij de reconstructie, die op berichtniveau achteraf mogelijk is op basis van de audit trail en de certificaatgegevens. Op geaggregeerd niveau zorgt monitoring voor de detectie van (beveiligings)incidenten. Het SBR berichtenverkeer binnen Digipoort wordt continu gemonitord. Dagelijks wordt vastgesteld hoe het berichtenverkeer is verlopen. Een grote toename in berichtenverkeer kan argwaan wekken en vanuit betrokken partijen kan vervolgens bekeken worden of het legitiem berichtenverkeer betreft. In dat kader worden dagelijks rapportages opgesteld van alle door Digipoort verzonden en ontvangen berichten, en verstuurd naar de betreffende uitvragende partijen. De rapportage vermeldt ook foutmeldingen en afwijkende statusmeldingen. Afhankelijk van de eigenschappen van de berichten die het betreft, vereist de uitvragende partij een bepaalde frequentie en detailniveau van de

rapportage. Aan berichten die gedurende het hele jaar in lage aantallen worden opgeleverd, worden lagere rapportage-eisen gesteld dan aan bepaalde piekstromen (grote aantallen binnen een korte periode aangeleverd). Er wordt gewerkt aan een dashboard voor real-time monitoring van de i-processen om fouten direct te kunnen signaleren.

Voor continuïteit van ketenvoorzieningen zijn serviceniveaus afgesproken tussen de partijen in de keten. Logius bewaakt de serviceniveaus aan de hand van serviceniveau overeenkomsten (SNO/SLA) en zorgt dat deze ook worden gehaald.

8.5 Afsluiting

Informatiebeveiliging in ketens is niet zo eenvoudig als het misschien op het eerste gezicht lijkt. Beginselen zoals vertrouwelijkheid, beschikbaarheid of integriteit worden vaak genoemd in kader van informatiebeveiliging. Zo blijkt uit de opeenstapeling van richtlijnen waarin deze beginselen steeds worden herhaald. Maar de bouwstenen die in de praktijk noodzakelijk zijn om invulling te geven aan deze beginselen kunnen, zoals dit hoofdstuk laat zien, zeer complex zijn. Desalniettemin laat de SBR casus zien dat we met het gebruik van de bouwstenen aan alle beginselen invulling kunnen geven. Deze bouwstenen maken het mogelijk om de komende jaren meer ketens en grotere berichtvolumes op een veilige manier af te handelen. Een randvoorwaarde is wel dat de partijen die deelnemen aan het berichtenverkeer hun interne beveiligingsmaatregelen en -beleid op orde hebben. Dit betekent dat ook de alledaagse/generieke 'IT- controles' zoals firewalls, antivirus software en een beveiligingsplan in werking moeten zijn, ook met het oog op de beschikbaarheid (van services). De ketenpartners hebben hier dus zelf een rol in het bereiken van een toereikende informatiebeveiliging. Voorts omvatten de i-processen specifieke services (behandeld in de vorige hoofdstukken) die de informatiebeveiliging aanvullen. Bijvoorbeeld de validatie binnen het aanleverproces, waardoor alleen instances in XBRL of XML formaat gebaseerd op de Nederlandse Taxonomie daadwerkelijk het proces kunnen doorlopen. Dit maakt de kans dat malafide code binnenkomt en wordt verwerkt, een stuk kleiner.

De genericiteit van de bouwstenen leidt ertoe, dat de bouwstenen dienen te voldoen aan de hoogste eisen die er vanuit verschillende perspectieven aan worden gesteld. Een gedifferentieerd beveiligingsaanbod is slechts tot op zekere hoogte mogelijk, bijvoorbeeld in de keuze voor het wel of niet gebruiken van de machtigingenvoorziening. Dit betekent dat de i-processen waar in principe lichtere eisen voor gelden (bijvoorbeeld van niet-vertrouwelijke berichten), meeliften op de hoge mate van beveiliging die voor andere stromen vereist is. Een voorbeeld is het gebruik van PKIoverheid certificaten. Hier zien we de onderlinge afhankelijkheid tussen de ketens die gebruik maken van generieke bouwstenen. Dit vereist afstemming op strategisch, tactisch en operationeel niveau. Daarbij worden de belangen van de gebruikers meegewogen: er is een balans tussen beveiliging en gebruiksvriendelijkheid aangebracht. De keuze voor de toepassing van de bouwstenen bij SBR is gemaakt in combinatie met de keuzes om autorisatie bij aanlevering weg te laten, om de authenticatie op organisatieniveau en niet op het niveau van de handelende persoon te verrichten, en om geen voorafgaande registratie van gebruikers te vereisen.

Ondanks de bouwstenen moeten we benadrukken dat informatiebeveiliging nooit echt 'klaar' is. Honderd procent beveiliging bestaat niet. Daarom is het ook zo belangrijk om vroegtijdig te detecteren en adequaat daarop te reageren. Rapportages, dashboards en incidentmanagementprocedures kunnen als belangrijke aanvullende waarborgen worden getypeerd. Ook de interne en externe omstandigheden veranderen voortdurend, zodat 'afgeronde' bouwstenen regelmatig moeten worden bijgesteld. Tevens is het van belang om periodiek en na aanpassingen (updates, nieuwe koppelvlakken etc.) goed te toetsen of er geen (nieuwe) kwetsbaarheden zijn ontstaan (ten behoeve van de nodige flexibiliteit). Bij versterking van de beveiliging moet de balans tussen het doel van de beveiliging en de gebruiksvriendelijkheid (evenredigheidsbeginsel) niet uit het oog worden verloren. En soms moet die balans opnieuw gezocht worden als de realiteit verandert.

Tot slot willen we wijzen op een zwakke plek bij het gebruik van certificaten. In het recente verleden is gebleken dat verschillende bedrijven die zich als certificaatautoriteit opwierpen, minder betrouwbaar bleken dan noodzakelijk. Dat heeft het vertrouwen in deze aanpak en de waarde van de TTP-rol flink ondermijnd. Om deze zwakte op te vangen worden op diverse fronten maatregelen genomen, zoals verscherpt toezicht op CSPs. Uiteindelijk is het van groot belang dat alle partijen in de keten hun verantwoordelijkheid kennen, nemen en elkaar daarop aanspreken.

9 Govenance en beheer

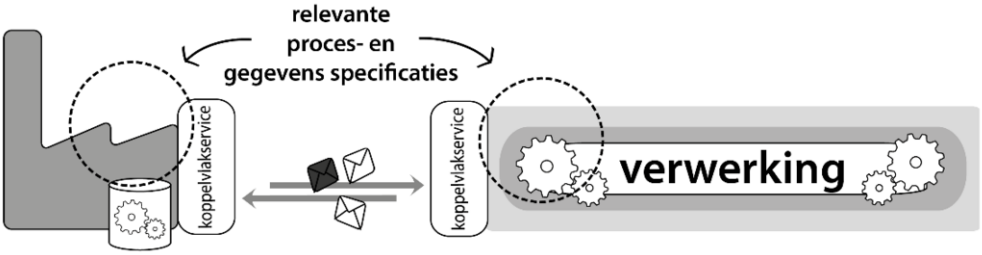
9.1 Inleiding

SBR koppelt systemen van verschillende organisaties binnen een verantwoordingsketen. De koppeling gebeurt in de SBR-verantwoordingsketens altijd op dezelfde manier. In de voorgaande hoofdstukken is beschreven hoe deze integratie voor SBR in de praktijk vorm heeft gekregen. Zoals uitvoerig in de inleiding van het boek aan bod is gekomen, vergroot system-to-system integratie de afhankelijkheden tussen partijen die betrokken zijn bij SBR. De conclusie van de inleiding was dat de organisatie van de noodzakelijke coördinatie van deze afhankelijkheden een onderbelicht deel betrof van de gewenste SBR-oplossing. Het gaat hier om de zogenaamde SBR-governance en de inrichting van Logius als gedeelde dienstverlener in het publieke SBR-domein. Dit hoofdstuk gaat in op dit deel van de SBR-oplossing. Het maakt hiervoor onderscheid in de drie integratievormen die wij zien bij de toepassing van SBR:

1. Horizontale integratie van SBR verantwoordingsketens door het leggen van organisatie-overschrijdende system-to-system koppelingen.
2. Verticale integratie door toepassing van een gedeelde dienstverlener (SSC), die als tussenschakel en middels een generieke dienstverlening betrokken is bij meerdere verantwoordingsketens.
3. Netwerkintegratie door toepassing van gedeelde standaarden bij het system-to-system integreren van verantwoordingsketens.

Alle drie integratievormen kennen verschillende afstemmingsvraagstukken. Het hoofdstuk heeft de toepassing van SBR bij verantwoordingsketens die hun basis hebben in wet- en regelgeving als primaire focus. Het gaat dus bij de horizontale en verticale integratie om de keten van uitvragende partijen, Logius en verantwoordingsplichtigen (met hun dienstverleners).

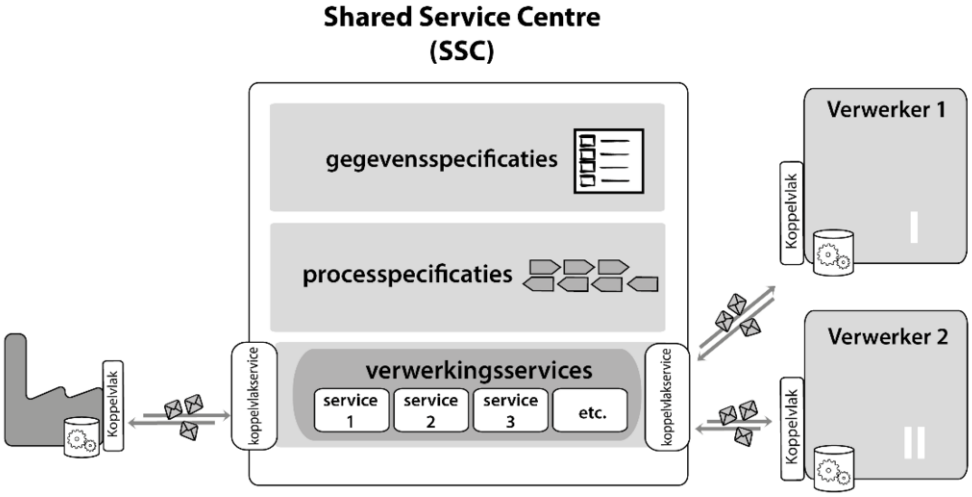
Ten eerste zien we een afstemmingsbehoefte bij de zogenaamde horizontale system-to-system integratie.



Figuur 9.1 – Horizontale integratie

Verantwoordingsplichtigen, softwareleveranciers en fiscalisten sluiten met hun systemen direct aan op de overheid om belastingaangifte te doen. Een dergelijke system-to-system koppeling kan alleen werken wanneer de aanleverende partijen tijdig de benodigde specificaties hebben geïmplementeerd. Een wijziging in de uitvraag, bijvoorbeeld door wijziging in de fiscale wetgeving, moet tijdig in alle systemen doorgevoerd kunnen worden. Het is voor een fiscalist, die mogelijk duizenden aangiften verwerkt, prettig vooraf op de hoogte te zijn over hoe een dergelijke wijziging in zijn werk gaat. Ditzelfde geldt voor de softwareleverancier. Een uitvragende partij heeft soms ruimte om invulling te geven aan een wetswijziging. Tevens geldt dat overal waar gewerkt wordt fouten gemaakt kunnen worden. Dus ook in de berichtspecificaties – in de vorm van bijvoorbeeld de taxonomie – kunnen zaken misgaan. De wijze waarop een wijziging wordt doorgevoerd kan een grote impact hebben op de partijen die betrokken zijn bij de aanlevering van de verantwoordingsinformatie. Het is in het belang van de uitvragende partij en van de partijen betrokken bij de aanlevering dat de aanlevering zo efficiënt mogelijk verloopt. Daarom is het logisch dat de Belastingdienst en belanghebbenden in de aanleverketen zo nu en dan om de tafel gaan zitten om een voorgenomen wijziging te bespreken óf het met elkaar te hebben over hoe zij invulling geven aan het wijzigingsproces. In de inleiding van het boek is ook aan bod gekomen dat de verantwoordingsplichtige, zijn softwareleverancier en zijn fiscalist als privaat systeem ook onderling zullen moeten afstemmen om SBR werkend te krijgen.

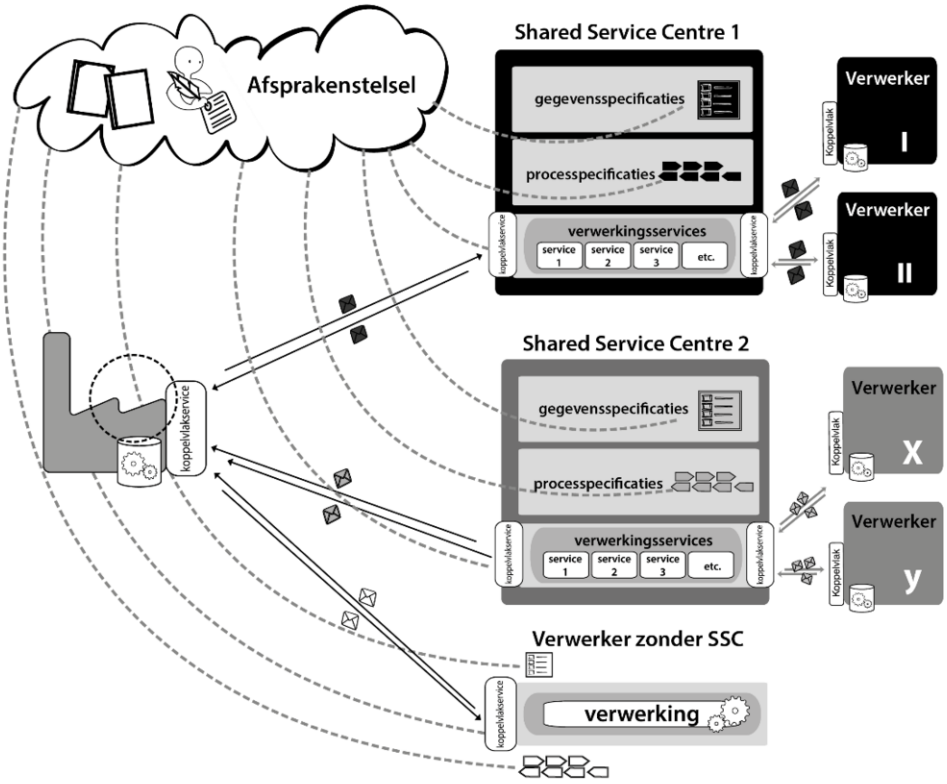
Ten tweede is er een afhankelijkheid voor partijen die voor de informatieverwerking gebruik maken van een gedeelde dienstverlener.



Figuur 9.2 – Verticale integratie

De afnemers van de gedeelde dienstverlener (in het plaatje verwerker 1 en 2, in SBR de uitvragende partijen) zijn system-to-system gekoppeld met de gedeelde dienstverlener. Dit neemt sowieso al de afhankelijkheden met zich mee van een horizontale integratie. Logius – de gedeelde dienstverlener bij SBR in het publieke domein - is echter efficiënter wanneer zij voor alle aanleveraars en afnemers maar één koppelvlak hoeft te onderhouden. Dit betekent dat de afnemers hier overeenstemming over moeten bereiken. Indien dit niet lukt, moet vastgesteld worden wie er opdraait voor de extra kosten. Vanzelfsprekend moeten de uitvragende partijen voor hun processen uit de voeten kunnen met de verwerkingsservices die Logius op de plank heeft liggen. Op welke wijze worden nieuwe verwerkingsservices ontwikkeld, welke serviceniveaus kan Logius bieden bij het afhandelen van verantwoordingsprocessen, hoe geeft Logius invulling aan de helpdeskfunctie etcetera? Logius kan kosteneffectiever opereren wanneer zij voor alle uitvragende partijen hetzelfde takenpakket op een standaard manier kan uitvoeren. Voor de uitvragende partijen kan maatwerk aantrekkelijk (of noodzakelijk) zijn. De afstemming in het kader van de verticale ketenintegratie zal vaak gaan over waar de standaard-dienstverlening voor de uitvragende partijen toereikend is en waar niet. Dan kan nog besloten worden een special te leveren of het standaard dienstenpakket uit te breiden. In alle gevallen geldt dat het noodzakelijk is vast te stellen wie voor welke kosten opdraait.

Ten derde is er SBR als netwerkstandaard. Het afsprakenstelsel van SBR bevat standaarden die partijen buiten het publieke domein kunnen toepassen bij het inrichten van verantwoordingsketens.



Figuur 9.3 – Netwerkintegratie

De brede toepassing van de SBR standaarden is prettig voor organisaties die zich niet alleen verantwoorden aan overheden. De zogenaamde 'ketenomkering' wordt hierdoor breder toegepast. De standaarden uit het afsprakenstelsel kunnen in een enkele horizontaal geïntegreerde verantwoordingsketen of binnen een privaat domein dat ook gebruik maakt van een generieke dienstverlener, worden toegepast. Het bancaire domein – met de Bancaire infrastructurele voorziening (BIV) als gedeelde dienstverlener – is een voorbeeld van de laatstgenoemde invulling. Alle SBR verantwoordingsketens gebruiken het afsprakenstelsel als basis voor de inrichting van de system-to-system integratie. Alle partijen betrokken bij de verantwoording zijn in dit kader belanghebbende bij het afsprakenstelsel. De afspraken op het niveau van het afsprakenstelsel bepalen in grote mate de vrijheid die partijen hebben bij het inrichten van hun eigen verantwoordingsketen. Dit stelt beperkingen aan voorschriften die gaan over de inhoud. Het afsprakenstelsel bepaalt bijvoorbeeld wel dat wanneer een partij een taxonomie maakt, deze zich houdt aan de voorgeschreven XBRL standaarden en de architectuur van de Nederlandse Taxonomie. Het geeft bijvoorbeeld niet aan welke elementen partijen uit moeten vragen. Desalniettemin kunnen het wat en het hoe in elkaar overlopen.

Uit het voorbeeld in de inleiding blijkt – om het makkelijk te maken – dat een wijzigingsbehoefte in een horizontale keten door kan werken in de andere integratievormen. Hetzelfde geldt ook omgekeerd, een besluit in het afsprakenstelsel kan grote gevolgen hebben voor de horizontale keten. Dit maakt dat de SBR-oplossing ketenbesturing behoeft op de verschillende integratievormen en vraagt om overkoepelend bestuur en coördinatie om de afhankelijkheden tussen de verschillende afhankelijkheidsgebieden te managen. Hoofdstuk 4 gaat uitgebreid in op ketengovernance: de afspraken tussen partijen over wie er op welke manier betrokken zijn bij beslissingen ten aanzien van aspecten die bepalend zijn voor de afhankelijkheidsrelatie binnen de keten. Dit hoofdstuk gaat in op de wijze waarop de governance op de SBR-onderdelen met publieke betrokkenheid concreet is georganiseerd. Het behandelt tevens hoe Logius als gedeelde dienstverlener organisatorisch invulling geeft aan het ketenbeheer. Wij hebben hiervoor het hoofdstuk opgedeeld in drie delen.

1. Uitgangspunten voor de governance bij de drie integratievormen:
   a. Generieke uitgangspunten voor ketengovernance voor alle integratievormen. De overheid dient zich bij al haar handelen, dus ook bij het inrichten van of deelname aan een governance, altijd te houden aan bepaalde spelregels. Dit zijn uitgangspunten die voortkomen uit de kaders en waarborgen voor behoorlijk bestuur.
   b. Specifieke uitgangspunten voor governance per ketenintegratievorm:
      - Horizontale integratie
      - Verticale integratie
      - Netwerkintegratie

      Per integratievorm gaan wij in op de aspecten waar betrokkenen – in het kader van SBR – over willen afstemmen. Dus 'wat staat er op de agenda?' Wij kiezen hier bewust voor het vage begrip 'aspect', omdat het niet perse gaat om vergelijkbare grootheden. De karakteristieken van SBR voor de drie integratievormen bepalen in grote mate welke onderwerpen voor de actoren van belang zijn in de afstemming. Op netwerkniveau is de vraag relevant: sluit SBR onvoorwaardelijk aan bij Digikoppeling of niet? Bij de verticale integratie gaat het om de vraag: welk prijsmodel hanteert Logius voor haar dienstverlening? Beide punten – van totaal andere orde - staan op agenda's van betrokken SBR-gremia en zijn relevant voor de implementatie van SBR. We zullen per integratievorm beschrijven welke uitgangspunten gezien de SBR karakteristieken gelden voor de ketengovernance.
   c. Samenhang tussen integratievormen. Afsluitend geven wij de samenhang weer van het bestuur op de verschillende integratievormen.

2. In het tweede deel van het hoofdstuk geven wij een beschrijving van de actuele SBR-governance. Deze SBR-governance heeft vorm gekregen door in te spelen op de behoeften die in de loop der tijd ontstonden over afstemming en afspraken. Hierbij is met name door agendazetting en differentiatie tussen het publiek/private en publieke deel rekening gehouden met de integratievormen. Het is belangrijk op te merken dat deze governance thans in beweging is.

3. In het derde deel van het hoofdstuk gaan wij dieper in op de centrale rol die Logius speelt bij het laten functioneren van de governance en hoe Logius binnen het publieke domein de samenhang bewaakt tussen de verschillende afstemmingsgebieden die door de toepassing van SBR ontstaan. Vanuit het SBR Programma is voor Logius een passende organisatie beschreven om kosteneffectief invulling te geven aan haar rol. Het hoofdstuk sluit af met een beschrijving van deze organisatie op hoofdlijnen.

9.2 Generieke uitgangspunten voor de governance

Voor alle onderdelen van de governance waar de overheid bij betrokken is, of die van overheidswege geïnitieerd zijn, gelden juridische kaders en waarborgen voor behoorlijk bestuur. Vanwege de betrokkenheid van de overheid bij SBR zijn de beginselen uit het bestuursrecht voor de verhouding tussen overheid en burgers / bedrijven en de waarborgen voor de bescherming van belangen van die burgers en bedrijven (algemene beginselen van behoorlijk bestuur) van belang.

Het gaat om de volgende beginselen:

- Zorgvuldigheidsbeginsel: bij de voorbereiding van besluiten vergaren bestuursorganen de nodige kennis omtrent de relevante feiten en af te wegen belangen (artikel 3:2 Awb). Het bestuursorgaan weegt de rechtstreeks bij het besluit betrokken belangen af (art. 3:4 lid 1 Awb). Een manier om hier invulling aan te geven is het inschakelen van vaktechnische experts voor advies bij het maken van keuzes ten aanzien van ontwerp en inrichting van de keten. Een ander manier is het mogelijk maken dat alle verschillende belangen(groepen) zich kunnen laten horen over de SBR ontwikkelingen.
- Evenredigheidsbeginsel / verbod van willekeur: de voor een of meer belanghebbenden nadelige gevolgen van een besluit mogen niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen (artikel 3:4 lid 2 Awb). Ook wel uitgelegd als evenredigheid van doel en middel. Daarnaast dient beleid consistent te zijn en niet gebaseerd op toevallige factoren. Evenredige vertegenwoordiging van de belangen van aanleveraars en andere bedrijvengroepen in de keten in de publiek-private SBR gremia draagt hier aan bij.
- Gelijkheidsbeginsel: gelijke gevallen worden gelijk behandeld. De bijeenkomsten en procedures van de gremia dienen te waarborgen dat elk lid zijn mening kan geven (gelijke behandeling in de afstemming). Om dit en bovengenoemde beginselen goed te borgen is het wenselijk om ook de overige belanghebbenden (minderheidsbelangen, kleinere groeperingen of eenheden) de kans te geven ‘mee te praten’, bijvoorbeeld door schriftelijk standpunten in te kunnen brengen. Deze ‘minderheidsbelangen’ dienen tevens toegang te hebben tot alle geboden toepassings- en aansluitondersteuning. De ondersteuning dient in dezelfde mate te beantwoorden aan de behoeften van deze belangen(groepen) als aan de belangengroepen die meer direct invloed uitoefenen in SBR gremia.
- Transparantie: transparantie vraagt om openbaarheid van overheidsdocumenten en de mogelijkheid tot inspraak. Besluitvorming en voorbereiding daarvan dient openbaar te worden gemaakt, bijvoorbeeld aan de hand van publicatie van verslagen.

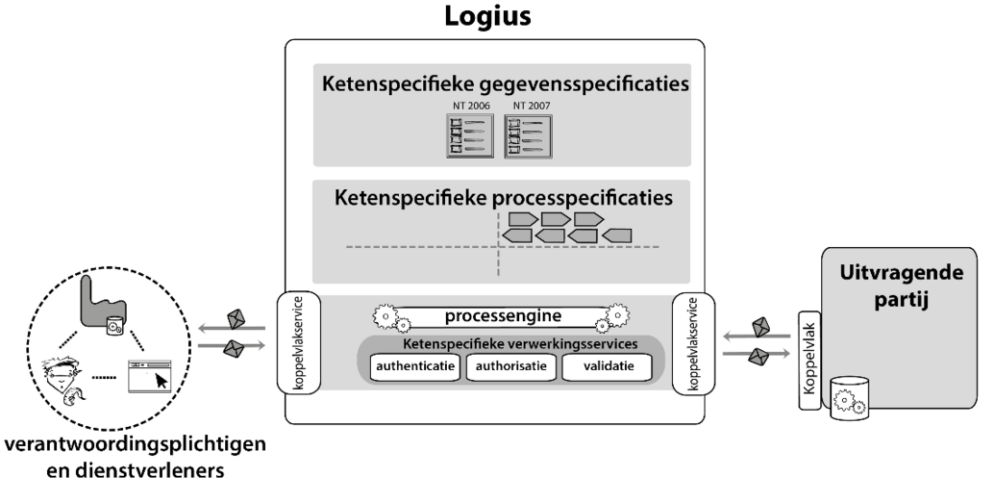
Bij het toebedelen van taken, verantwoordelijkheden en bevoegdheden aan de SBR gremia dient hier rekening mee te worden gehouden.

9.3 Governance op SBR verantwoordingsketens: horizontale integratie

Horizontale integratie treedt op wanneer de menselijke tussenkomst tussen organisaties binnen het keteninformatiesysteem beperkt wordt. Als we kijken naar verantwoording gaan wij uit van een machtsverhouding tussen de ketenpartijen waarbij een partij een duidelijke grondslag heeft om informatie op te vragen. Deze uitvragende partij stelt hiermee de eisen vast voor de verantwoording. De uitvragende partij moet zich hierbij houden aan wet- en regelgeving. Verschillende verantwoordingsketens kunnen hierdoor andersoortige eisen aan vorm en inhoud stellen. In het zogenaamde openstellingsbesluit staat op welke wijze een partij de verantwoordingsinformatie elektronisch bij de uitvragende partij kan aanleveren. Dit besluit kan verwijzen naar de Nederlandse Taxonomie en de koppelvlakken van Digipoort.

In onderstaande figuur is één horizontale keten binnen de SBR-oplossing weergegeven. We zien binnen deze figuur drie 'ketenkoppelingen'.

1. De ketenkoppeling tussen Logius en de uitvragende partij.
2. De ketenkoppeling tussen Logius en de aanleverende partij. Deze koppeling kan gezien worden als het juridische koppelvlak tussen de verantwoordingsplichtige partij en de uitvragende partij. Voor het gemak spreken wij hier over de koppeling tussen verantwoorder en uitvrager.
3. De ketenkoppeling tussen de partijen die betrokken zijn bij het opstellen en aanleveren van de verantwoordingsinformatie (weergegeven in de cirkel).



Figuur 9.4 – Horizontale SBR-keten en drie ketenkoppelingen

Voor de werking van een SBR verantwoordingsketen is eerst de ketenkoppeling tussen Logius en uitvragende partij van groot belang. Voor de SBR business case in de

markt is de laatste koppeling weliswaar relevant, maar de partijen betrokken bij aanlevering moeten zelf weten hoe zij hier invulling aangeven. Deze koppeling valt buiten het bereik van de regie van de overheid.

9.3.1 *Relevante aspecten voor de ketengovernance*

Iedere verantwoordingsketen (wel of niet geïntegreerd) kent in essentie dezelfde aspecten die om afstemming vragen. Verantwoordende partijen – en dienstverleners die hen ondersteunen bij de verantwoording, zoals softwareleveranciers en intermediairs – willen weten welke informatie op welk moment met welke kwaliteit moet worden aangeleverd. Wanneer er op een van deze punten veranderingen op komst zijn of wanneer er problemen dreigen te ontstaan willen de ketenpartners daarover met de uitvragende partij in gesprek. De uitvragende partij moet ervoor zorgen dat de verantwoordende organisatie op proportionele wijze aan zijn verantwoording kan voldoen. Bij een geïntegreerde keten betekent dit dat deze zorg ook uitgaat naar de ketenpartners. Voor de publieke verantwoording is de grondslag vastgelegd in het bestuursrecht. Natuurlijk heeft de uitvragende partij zelf ook belang bij een juiste aanlevering door verantwoordende partijen. Gezien de scope van dit hoofdstuk gaan wij alleen in op de ketengovernance van SBR verantwoordingsketens met een publieke uitvragende partij, met daarbij de opmerking dat de markt een groot aantal modellen biedt waarop de ketengovernance van een private verantwoordingsketen kan worden georganiseerd. De dominantie en macht van de private uitvragende partij in de ketengovernance wordt sterk bepaald door haar marktpositie.

In het kader van SBR – met de focus op de publieke verantwoording – is Logius beheerder van de systemen die geïntegreerd zijn met verantwoordingsplichtige organisaties en de uitvragende partijen. Logius heeft ten aanzien van de verantwoording geen zelfstandige bestuursbevoegdheden, maar treedt op namens achterliggende uitvragende partijen. Hierbij geldt dat een bericht door een bestuursorgaan is ontvangen wanneer het zijn systeem voor gegevensverwerking heeft bereikt. Hoewel de inhoudelijke beoordeling van het bericht door de Belastingdienst wordt uitgevoerd, vallen de technische controles van Logius juridisch onder ‘gegevensverwerking’. Het moment van ontvangst ligt bij SBR dus bij Digipoort.

Voor SBR zijn de volgende aspecten onderdeel van de afstemming bij de horizontaal geïntegreerde keten.

1. Het feit dat het afsprakenstelsel van SBR geldt als basis voor de inrichting van de verantwoordingsketen.
2. De Nederlandse Taxonomie als houder van de gegevensspecificaties voor een specifieke verantwoordingsketen.
3. Overige ketenspecificaties op berichtenniveau (bijvoorbeeld FRIS-regels).
4. De processpecificaties van het verantwoordingsproces.
5. Configuratie van de koppelvlakservices.
6. Ondersteuning bij implementatie en aansluiting.
7. Ondersteuning bij incidenten.
8. De serviceniveaus die gelden voor de opengestelde weg.
9. De governance op de relevante aspecten van de horizontaal geïntegreerde verantwoordingsketen.

9.3.1.1 SBR als basis voor de inrichting van de verantwoordingsketen

Wanneer een uitvragende partij aangesloten is bij SBR, neemt deze het afsprakenstelsel als basis voor de inrichting van de verantwoordingsketen. Dit betekent dat de verantwoordingsplichtige en zijn dienstverleners moeten kunnen werken met de SBR standaarden die relevant zijn voor de verantwoordingsketen waarin zij actief zijn. Zij moeten dus om kunnen gaan met een XBRL-taxonomie die is opgebouwd volgende de Nederlandse Taxonomie Architectuur. Zij moeten aangesloten zijn op de vastgestelde koppelvlakken die relevant zijn voor hun keten. Niet alle aspecten uit het afsprakenstelsel hoeven relevant te zijn voor alle partijen. Voor een softwarepartij die alleen maar rapportagesoftware voor de jaarrekening maakt, geldt bijvoorbeeld dat het eMededelen-koppelvlak niet relevant is omdat de Kamer van Koophandel geen mededelingen verstuurt. Het is voor de ketenpartners evenwel zeer relevant dat een uitvragende partij besluit SBR toe te passen als basis voor de verantwoordingsketen. Zeker wanneer dit de exclusieve methode voor de system-to-system aanlevering wordt. Deze stap is door de Belastingdienst in 2013 in het kader van het aanleveren van de IB/VPB genomen en veelvuldig vooraf met ketenpartners afgestemd. Hier ligt dus meteen de relatie tussen de ketengovernance voor de horizontale integratie en de governance op het SBR afsprakenstelsel.

9.3.1.2 Specifieke onderdelen uit de Nederlandse Taxonomie

De Nederlandse Taxonomie bevat naast generieke onderdelen ook een groot aantal ketenspecifieke onderdelen. Het gaat om de exacte specificatie van wat een uitvragende partij voor de verantwoordingsketen wil ontvangen. Dit gebeurt door een verwijzing naar generieke én specifieke elementen. System-to-system informatieverwerking is een kosteneffectieve oplossing wanneer de gevraagde elementen of de benodigde sub-elementen al tijdens de bedrijfsvoering worden verzameld en geadministreerd in softwareoplossingen. In dit kader zijn de ketenpartners graag tijdig op de hoogte van de inhoud van de berichtspecificaties. Daarnaast zijn alle betrokken partijen afhankelijk van de technische vorm en kwaliteit van dit specifieke deel van de taxonomie, omdat zij het moeten mappen aan de primaire bron. Mocht dit deel van de taxonomie onverhoopt een fout bevatten (dit kan technisch zijn, maar er kan ook een element missen) dan is het fijn als de ketenpartijen hier ruim voordat de daadwerkelijke berichtuitwisseling moet geschieden achter komen.

9.3.1.3 Overige ketenspecificaties op berichtniveau

Bovenop de Nederlandse Taxonomie stellen uitvragende partijen nog aanvullende eisen aan de berichten, zoals zogenaamde FRIS regels. De ketenpartners moeten dus ook weten welke aanvullende specificaties voor de berichten in de keten gelden.

9.3.1.4 Processpecificaties

Het verantwoordingsproces doorloopt een vooraf vastgelegde verwerking. Voor de betrokken ketenpartners is het van belang dat zij de procesuitkomsten die relevant zijn voor hun taak in het proces kennen en weten hoe zij hierop moeten reageren. Zo is het van belang dat de verantwoordingsplichtige weet wanneer deze aan zijn plicht heeft voldaan of wanneer zijn gegevens niet voldeden aan de daaraan gestelde eisen. Technische systemen moeten ingesteld zijn op de mogelijke procesoutput van de systemen waarmee zij system-to-system geïntegreerd zijn. Denk hierbij aan een ont-

vangstbericht of afkeurbericht en statusinformatie (waarbij een bericht ofwel uiteindelijk voor verwerking wordt geaccepteerd ofwel alsnog in het proces kan worden afgewezen). Verantwoordingsplichtigen en hun dienstverleners zijn voor de inrichting van hun werkzaamheden en producten afhankelijk van de wijze waarop de processen zijn opgesteld. Tevens geldt dat een deel van de geautomatiseerde verwerking plaatsvindt bij Logius. Voor Logius kun je de specifieke processpecificaties dan ook zien als functionele opdrachtbeschrijving.

9.3.1.5 Configuratie van de koppelvlakservices

De specificaties van de koppelvlakservices zijn voor SBR in principe beschreven op het niveau van het SBR-afsprakenstelsel (dat verwijst naar Digikoppeling en hier een inperking op maakt). De werking van de koppelvlakservices (dialoog) is daarnaast opgenomen in de processpecificaties. Omdat de technische implementatie op meerdere lagen geschiedt, zijn er voor koppelvlakservices zogenaamde koppelvlakbeschrijvingen beschikbaar. Voor specifieke ketens is het van belang te weten welke koppelvlakken voor de keten geïmplementeerd zijn en wat de adressering is van de koppelvlakken, welk typen certificaten (welke roots) geaccepteerd worden en wat het unieke identificerend kenmerk is voor de juiste verantwoording. Bij SBR gaat het hier over de zogenaamde berichtsoort. In het kader van SBR zijn er in de horizontale keten koppelvlakservices tussen Logius en de aanleverende partij en tussen Logius en de uitvragende partij.

9.3.1.6 Ondersteuning bij implementatie en aansluiting

Wanneer er wijzigingen worden doorgevoerd in de onderdelen van de verantwoordingsketen die verantwoordende partijen (of hun dienstverleners) moeten implementeren, willen deze partijen dit graag vooraf uitgebreid kunnen testen. Hier kunnen testvoorzieningen voor worden ingezet. Bij complexe aanpassingen kan er bij de aanleverende partijen behoefte bestaan aan andere vormen van kennisoverdracht over de implementatie.

9.3.1.7 Ondersteuning bij incidenten

Bij de lopende verantwoording kunnen ketenpartners fouten maken en machines kunnen stuk gaan. Wanneer de keten onverwacht stokt, moet er aanvullende ondersteuning aanwezig zijn. Aanleverende partijen moeten een melding kunnen maken van een verstoring en zij willen op de hoogte gesteld worden van verstoringen in het SBR-kanaal. Dit vraagt bij een ketenincident afstemming tussen de verschillende ketenpartners.

9.3.1.8 De serviceniveaus die nagestreefd worden voor de opengestelde weg

Voor alle voorgaande aspecten geldt dat de verantwoordende ketenpartners naast de vorm en inhoud zekerheid willen hebben over de kwaliteit die de overheid bij de opengestelde weg nastreeft. Wat is de beschikbaarheid van de koppelvlakservices waar zij vanuit mogen gaan? Wat is de beschikbaarheid van de taxonomie? Hoe vaak is er onderhoud? Hoe vaak kunnen wijzigingen verwacht worden? Voor Logius zijn de streefwaarden van de uitvragende partij van groot belang, omdat Logius voor een aantal van deze kwaliteitswaarden verantwoordelijk is. Voor een kosteneffectieve keten geldt dat kwaliteitsniveaus in de keten optimaal op elkaar afgestemd moeten

worden. De keten is immers zo sterk als de zwakste schakel. Het is niet handig wanneer de overheid 's-nachts een helpdesk bemant, wanneer de behoefte om hier gebruik van te maken voor de verantwoordende partij beperkt is. Anderzijds is het vervelend wanneer de aanleverservice standaard 's-nachts niet beschikbaar is wanneer bepaalde softwaresystemen dan efficiënt het berichtenverkeer van de dag zouden kunnen verwerken.

9.3.1.9 De governance op de relevante aspecten voor de horizontale integratie

De wijze waarop er over de inrichting van relevante aspecten van de opengestelde weg besloten wordt, is voor alle partijen vanzelfsprekend relevant.

9.3.2 *Uitgangspunten voor governance*

Bij de uitgangspunten voor de governance op de horizontaal geïntegreerde keten in SBR moet er een duidelijk onderscheid worden gemaakt tussen de drie genoemde ketenkoppelingen.

9.3.2.1 Ketenkoppeling tussen verantwoorder en uitvrager

De grondslag voor de ketengovernance op de ketenkoppeling tussen verantwoorder en uitvrager is gebaseerd op de wet- en regelgeving en beleidsuitingen van de overheid. De uitvragende partij dient de elektronische weg formeel open te stellen en zolang dit zorgvuldig gebeurt en niet in strijd is met gewekte verwachtingen, is de uitvragende partij feitelijk een beslisser met grote doorzettingsmacht. Wanneer een partij zich benadeeld voelt – omdat zij bijvoorbeeld niet op proportionele wijze aan haar plicht denkt te kunnen voldoen - kan deze een gang naar de burgerlijke rechter overwegen (met een beroep op onrechtmatigheid van het beleid). Wanneer een groot aantal ketenpartners zich benadeeld voelt, zal het onderwerp politiek worden en zullen de belanghebbenden via de politieke arena proberen de uitvragende partij tot anders handelen te bewegen.

Zeker dit laatste scenario spreekt niet tot de verbeelding van de uitvragende partij. De vraag die dan opkomt is of de uitvragende partij zonder consultatie van de verantwoordende partijen (en hun dienstverleners) op zorgvuldige wijze vast kan stellen of een taxonomie voor marktpartijen implementeerbaar is, of de onderhoudsmomenten van de opengestelde weg verstandig gepland zijn en of de storingscommunicatie toereikend is. In de praktijk zal de uitvragende partij – zeker bij grote wijzigingen - de aanleverende partijen willen consulteren en op zoek gaan naar draagvlak voor de gekozen weg. Dit begint al bij het vaststellen of een uitvragende partij SBR als basis voor de inrichting van de verantwoordingsketen moet gebruiken. Bij de consultatie betreedt de uitvrager de wereld van de pluriforme aanleverketen. Bij de consultatie moet deze rekening houden met de verschillende belangengroepen die in een verantwoordingsketen actief zijn. Denk hierbij aan het onderscheid tussen kleine en grote verantwoordende organisaties, maar ook organisaties die gebruik maken van een intermediair of zogenaamde zelfaanleveraars (zoals zelfaangevers). De dienstverleners in de keten – zoals intermediairs en softwareleveranciers – hebben ook eigen belangen. Ook hierin kan gedifferentieerd worden tussen verschillende partijen. Vaak zijn partijen met gedeelde belangen aangesloten bij een brancheorganisatie of koepel. Een stevige belangenorganisatie is in dat geval een logisch aanspreek-

punt voor de uitvragende partij. Toch vraagt een goede afstemming vaak om maatwerk binnen een keten. Zo moet altijd de vraag gesteld worden of alle relevante partijen voldoende vertegenwoordigd zijn en dient de uitvragende partij goed na te denken over de wijze waarop zij de consultatie organiseert. Wanneer bijvoorbeeld concurrerende softwareleveranciers bij elkaar in een zaaltje gevraagd worden of zij moeite hebben met de toepassing van een nieuwe techniek, kan het zijn dat zij niet het achterste van hun tong laten zien.

Dat een uitvragende partij als de Belastingdienst bij het vaststellen van haar beleid rond de openstelling van de elektronische weg rekening houdt met de belangen van de verantwoordingsplichtigen en hun dienstverleners, is bij SBR gebleken uit het feit dat zij op aanvraag van de marktpartijen de exclusieve toepassing van SBR heeft onderzocht. Vooruitlopend op de beschrijving van de actuele governance van SBR is het belangrijk op te merken dat de Belastingdienst voor een afstemming als deze ook haar eigen infrastructuur gericht op de verantwoordingsketens uit het fiscale domein onderhoudt. Op basis van het overleg met ketenpartners heeft de Belastingdienst bewust gekozen om de eerste exclusieve implementatie in de IB/VPB-keten uit te voeren, omdat het aantal softwareleveranciers dat in deze keten actief is beperkt is en de system-to-system aanlevering in deze keten voor het overgrote deel via intermediairs gaat. Hierdoor had zij bij de vuurdoop te maken met een overzichtelijke en goed georganiseerde groep belanghebbenden om mee af te stemmen en haar besluiten op te baseren.

Uitgangspunten voor de governance van de publiek/private horizontaal geïntegreerde keten:

- De uitvragende partij werkt in principe zelfstandig de kaders voor de governance uit, waarbij zij zelfstandig vaststelt in welke mate zij haar oordeel bij het inrichten van de keten baseert op ketenpartners. Hierbij dient de uitvragende partij zich te houden aan de wettelijke kaders rond openstelling en eventueel door de overheid gewekte verwachtingen.
- Verantwoordende partijen in de keten die vinden dat zij benadeeld worden kunnen zich altijd wenden tot de rechter of zaken politiek maken. Dit is een escalatie die door partijen overwegend als onwenselijk wordt gezien.
- De uitvragende partij heeft er belang bij partijen een tafel te bieden waar private partijen tijdig geïnformeerd en geconsulteerd worden over voorgenomen wijzigingen ten aanzien van de benoemde aspecten. Dit met als doel dat partijen:
    - tijdig hun werkwijze, dienstverlening en technologie kunnen aanpassen;
    - aan kunnen geven wat de impact is van de voorgenomen wijziging.
- De uitvragende partij heeft er belang bij aan te sluiten aan een tafel waar betrokken partijen ook suggesties en klachten over de bestaande inrichting van SBR-gerelateerde aspecten kunnen bespreken.
- De tafels die door een uitvragende partij geboden worden kunnen een grotere reikwijdte hebben dan SBR en hoeven dus niet onderdeel uit te maken van generieke SBR gremia.
- De uitvragende partij kan er belang bij hebben tijdens bepaalde besluitvorming de consultatie maatgericht vorm te geven.

- Branchеverenigingen en koepelorganisaties zijn logische aanspreekpunten om in de besluitvorming mee te nemen. De uitvragende partij dient altijd zelf de afweging te maken of met het betrekken van deze organisaties de verschillende belangen van ketenactoren voldoende zijn gediend.
- Voor een goed functionerende governance is het van belang dat de uitvragende partij vooraf zoveel mogelijk duidelijkheid verschaft over het doel van de afstemming. Bijvoorbeeld: worden partijen geconsulteerd of uitsluitend geïnformeerd?

9.3.2.2 Ketenkoppeling tussen Logius en uitvragende partij

De ketengovernance op de ketenkoppeling tussen Logius en de uitvragende partij is gebaseerd op een dienstrelatie: de uitvragende partij die een dienst afneemt bij Logius. De juridische kaders gaan hier thans uit van een sterke sturende rol van de bestuursdienst die de dienst afneemt en een volgende rol van Logius als dienstaanbieder. In een dergelijk model is een voorschrijvende rol van de uitvragende partij uitgangspunt en geldt dat Logius de specificaties van de uitvragende partij moet implementeren en uit moet voeren. Door de specialisatie van Logius op het gebied van de geautomatiseerde berichtuitwisseling ontstaat er echter een kennisafstand tussen opdrachtgever en opdrachtnemer, waarbij Logius een autoriteit verwerft op het gebied van de inrichting van de geautomatiseerde verwerking van verantwoordingsinformatie en S2S-integratie met aanleverende partijen. Op basis van deze autoriteit krijgt Logius vanzelf de vraag om – gezien de gestelde doelen van de uitvragende partij en de middelen die deze tot haar beschikking heeft – de uitvragende partij te adviseren over de wijze waarop het deel van de keten dat Logius onder haar hoede heeft, ingericht zou moeten worden. Logius kan ook eisen stellen aan de uitvragende partij, bijvoorbeeld op het gebied van beveiliging. Met de advisering en het stellen van eisen ontstaat er een verantwoordelijkheid voor de keten die op den duur zoveel gewicht krijgt, dat een governancemodel met een volledig voorschrijvende uitvragende partij niet past bij de gewenste verantwoordelijkheidsverdeling. Er ontstaat een behoefte bij de uitvragende partij dat Logius zich zelfstandig verantwoordt over haar handelen, omdat de uitvragende partij deze verantwoordelijkheid niet meer kan nemen. Deze behoefte wordt nog eens versterkt door de verticale ketenintegratie die in § 9.4 behandeld wordt. De uitvragende partij blijft verantwoordelijk voor de inrichting van de integratie tussen haar voorziening en die van Logius, maar mag zich bij haar keuze voor de inrichting hiervan deels verlaten op de oordelen en expertise van Logius. Hiermee heeft Logius als dienstverlener een grotere verantwoordelijkheid, die in de besturing op deze inrichting hand in hand moet gaan met grotere bevoegdheden. Hieruit volgen de volgende uitgangspunten voor de governance:

- De uitvragende partij is verantwoordelijk voor de keuze of zij Logius inzet bij de verwerking van verantwoordingsinformatie. Zij kan zich bij deze keuze deels verlaten op het feit dat Logius dit specialisme heeft toebedeeld gekregen binnen de overheid.
- Logius heeft als de specialist op het gebied van de geautomatiseerde verwerking van verantwoordingsinformatie en S2S-integratie en als gedeelde dienstverlener ten aanzien van de aanleverende partijen een zelfstandige verantwoordelijkheid. Vanuit deze autoriteitsrol kan zij voorwaarden stellen aan de samenwerking met uitvragende partijen en vindt de besluitvorming

over de relevante aspecten binnen de context van opdrachtgever en opdrachtnemer, op gelijkwaardige voet plaats.

9.3.2.3 Ketenkoppeling tussen verantwoordingsplichtige en zijn dienstverleners

Verantwoordende organisaties kunnen door de toepassing van SBR te maken krijgen met een verdere integratie van systemen. In principe is het aan de marktpartijen om zelf te bepalen op welke wijze zij hier de besluitvorming over willen inrichten. Het kan zijn dat intermediairs bepaalde software voorschrijven die de hele integratie tussen de verantwoordingsplichtige, de intermediair en de overheid ondersteunt. In dat geval is het aan de verantwoordingsplichtige om op deze wijze in zee te gaan met die intermediair of op een andere wijze aan zijn verplichting te voldoen. Als één van de vele klanten van de intermediair is de invloed van de verantwoordingsplichtige op de (door)ontwikkeling van het pakket in zo'n geval beperkt en vindt besluitvorming eigenlijk plaats via de tucht van de marktwerking. Wanneer een pakket ongebruiksvriendelijk is, kan dit een partij doen besluiten over te stappen naar een andere intermediair. Dit zal een teken zijn voor de intermediair die het pakket als standaard hanteert. In sommige verantwoordingketens hebben de intermediairs een inhoudelijke rol en zijn zij dermate gespecialiseerd dat zij hun eigen beroepsregels kennen. Dit geldt in zekere mate voor fiscalisten en nog meer voor accountants (RA's of AA's). In dit geval geldt dat de beroepsregels voor de governance meegenomen moeten worden bij de besluitvorming over de inrichting van de geïntegreerde keten. Het gevolg van dergelijke beroepsregels kan zijn dat een partij zich juist wel met een besluit wil bemoeien, of juist niet bij een besluit betrokken wil zijn. Een voorbeeld van een complexer besturingsvraagstuk in de markt is de vraag wie de inrichting van de administratie en de mapping van de elementen uit de taxonomie voor zijn rekening neemt. Dit kan de softwareleverancier zijn. In dat geval vertrouwen de intermediairs en de verantwoordingsplichtige op de expertise van deze leverancier. In de fiscale keten is dit mogelijk, maar er zijn genoeg fiscalisten die vanuit hun beroepsverantwoordelijkheid liever zelf de mapping voor hun rekening nemen. Een controlerend accountant zal mogelijk niet betrokken willen worden bij de keuze van de mapping, daar dit gezien kan worden als advisering over de inrichting. Deze rol kan conflicteren met zijn controlerende taak. Wanneer er problemen in de verantwoording ontstaan, zal vaak de verantwoordingsplichtige het eerste aangesproken worden. Deze kan echter een dienstverlener die nalatig is geweest aansprakelijk stellen voor de schade. Denk hierbij bijvoorbeeld aan een softwareleverancier die onterecht melding geeft van het succesvol aanleveren van een OB-aangifte, terwijl de koppelvlakservice een foutmelding als respons gaf.

- In principe bepalen verantwoordende partijen en hun dienstverleners zelf hoe zij besluiten over de ketenintegratie. Hier zijn verschillende modellen mogelijk.
- Partijen hebben een eigen verantwoordelijkheid om vast te stellen welke rol zij in de geïntegreerde keten hebben en welke eventueel uit wet- en regelgeving voortkomende verantwoordelijkheden hierbij horen. Waar verantwoordelijkheden liggen, dienen zij ook de bevoegdheden te claimen om bij de besluitvorming rond de inrichting betrokken te zijn of zich juist afzijdig te houden van besluiten die conflicteren met hun rol.

- Wanneer er onenigheid ontstaat naar aanleiding van de besluitvorming rond de ketenintegratie, kunnen partijen via het privaatrecht proberen hun gelijk te halen.

9.4 SBR bij verticale ketenintegratie

In het publieke domein neemt Logius voor SBR een centrale rol in als shared service center. Dit om een kosteneffectieve eOverheid mogelijk te maken. Hierbij voert Logius ten eerste de programmatische werkzaamheden uit die zich richten op de verdere ontwikkeling en implementatie van SBR als breed standaardisatie-initiatief. Daarnaast draagt Logius zorg voor het operationeel houden en de doorontwikkeling van generieke bouwstenen voor specifieke verantwoordingsketens. Door de inzet van generieke bouwstenen voor meerdere verantwoordingsketens is er sprake van verticale ketenintegratie. De partijen die gebruik maken van de gedeelde diensten zijn hiervan afhankelijk voor hun primaire proces en willen daarom betrokken zijn bij de besturing van de wijze waarop Logius zich als generieke dienstverlener gedraagt en ontwikkelt.

9.4.1 *Relevante aspecten*

De mate waarin uitvragende partijen hun verantwoordingsketen kunnen uitbesteden aan Logius wordt bepaald door wat Logius op de schappen heeft staan. De prijs van de Logius-dienstverlening is hierbij relevant, daar dit één van de redenen is om gebruik te maken van een shared service center. Ditzelfde geldt voor de kwaliteit. Het is voor de partijen van belang te weten welke (organisatorische en technische) maatregelen zij nog meer moeten nemen om gebruik te kunnen maken van de Logius dienstverlening. Ook zullen de betrokken partijen eruit moeten komen hoe zij sturen op de gedeelde dienstverlening en welke bevoegdheden en mandaten van de gedeelde dienstverlener hier liggen.

9.4.1.1 De diensten van Logius

De diensten van Logius in het kader van SBR laten zich opsplitsen in twee hoofddiensten:

1. Afstemmingsdiensten – gericht op het laten functioneren van SBR als oplossing
2. Reporting services – gericht op het leveren van diensten ten behoeve van specifieke verantwoordingsketens

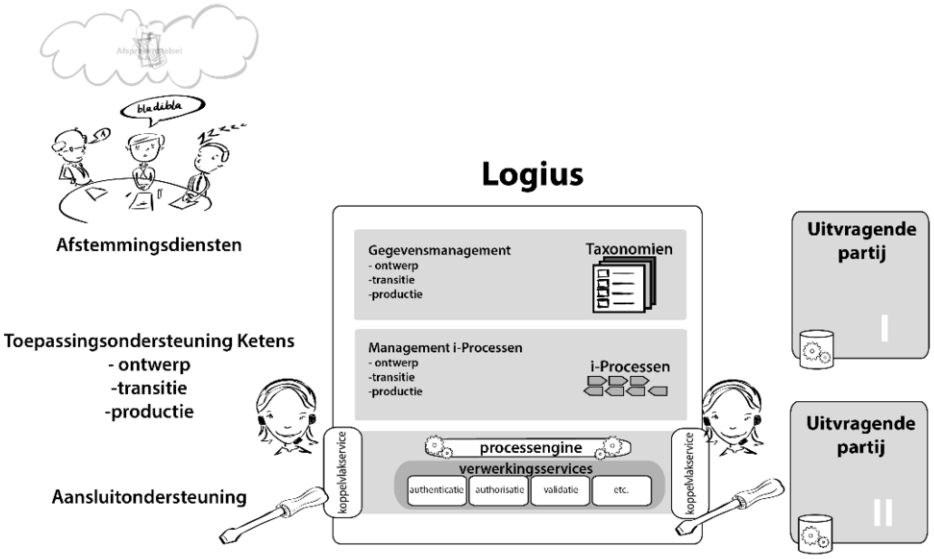
Ad 1. De eerste hoofddienst heeft betrekking op het beheer van het afsprakenstelsel van SBR, het promoten van de SBR oplossing binnen de overheid en het inhoudelijk en procesmatig faciliteren van de governance hierop.

Ad 2. De Reporting Services hebben betrekking op:

1. i-Procesmanagement: het ontwerpen, implementeren en beschikbaar houden van processpecificaties en onderliggende koppelvlak- en verwerkingsservices.
2. Gegevensmanagement: het ontwerpen, implementeren en beschikbaar houden van taxonomieën.

3. Toepassingsondersteuning: het ondersteunen van partijen bij de toepassing van de keten en de regievoering bij ketenincidenten (1e en 2e lijnsondersteuning).
4. Aansluitondersteuning: het ondersteunen van ketenpartners bij de implementatie van de onderdelen van SBR ten behoeve van de ketenintegratie.

In het onderdeel uit dit hoofdstuk over beheer wordt nader ingegaan op deze diensten. Voor deze diensten geldt dat belanghebbenden moeten besluiten hoe zij eruit zien, wat de reikwijdte is en in welke mate zij standaard zijn en waar ruimte is voor maatwerk. Hierbij geldt tevens de vraag: wat zijn SBR diensten? Welke diensten van Logius dienen primair vanuit SBR-perspectief benaderd te worden? Om onderscheid te maken tussen de bestuursverhoudingen ten aanzien van de twee diensten wordt voor de afstemmingsdienst gesproken over een opdrachtgeverschap aan Logius als dienstverlener, voor de Reporting Services worden de uitvragende partijen met de term 'afnemers' aangeduid. In figuur 9.5 is het afstemmingsgebied in het kader van SBR opgenomen.



Figuur 9.5 – Afstemmingsdiensten

Kwaliteit

De kwaliteit van de dienstverlening is van groot belang voor de afnemende uitvragende partijen, omdat deze grotendeels bepaalt of de geïntegreerde verantwoordingsketens in voldoende mate kunnen functioneren.

Prijs en bekostiging

De eerder genoemde aspecten, welke diensten met welke kwaliteit, worden met name relevant door het prijsperspectief. Kort door de bocht bepaalt de wijze waarop

invulling wordt gegeven aan de dienstverlening in sterke mate de prijs van de dienstverlening. Daarom sturen partijen niet op maximale kwaliteit, maar op voldoende kwaliteit. Hierbij geldt:

- Meer maatwerk in dienstverlening is overwegend duurder.
- Hogere beschikbaarheid is overwegend duurder.
- Flexibelere dienstverlening is overwegend duurder.
- Hoger beveiligingsniveau dienstverlening is overwegend duurder.

De kosten van de dienstverlener moeten worden verdeeld over de opdrachtgevers en afnemers. Hier kunnen verschillende modellen voor gekozen worden. Partijen kunnen de kosten bijvoorbeeld evenredig verdelen naar gebruik. Voorwaarde is dat wel vastgesteld moet kunnen worden welke kosten toe te rekenen zijn aan welk gebruik. Dit is niet altijd gemakkelijk. Waar het gaat om ontwikkeling kan een partij er ook voor kiezen de volledige kosten van de ontwikkeling van een dienst voor haar rekening te nemen om vervolgens in de exploitatie de kosten van de dienstverlening te delen met meerdere gebruikers van de dienst.

9.4.2 *Uitgangspunten voor governance*

De uitgangspunten voor de governance op de gemeenschappelijke dienstverlening binnen het publieke domein zijn gebaseerd op het algemene belang: uiteindelijk gaat het om één overheid die doelmatig invulling moet geven aan haar totale takenpakket. Tevens geldt dat het uitgangspunt voor de besturing op de generieke dienstverlener sterk bepaald wordt door de formele positie van de dienstverlener. Logius is een baten-lastendienst met dientengevolge een beperkt eigen vermogen. Feitelijk komt het erop neer dat Logius ook voor de doorontwikkeling van haar dienstverlening een of meerdere overheidspartijen moet vinden die bereid zijn in de ontwikkeling te investeren. Dit heeft effect op de besturing. Bij trajecten die nog een grote onzekerheidsfactor kennen en waarvan de toepassing nog beperkt is, zal de betrokkenheid van de opdrachtgevers voor de ontwikkeling en dienstverlening groot zijn. De betrokken overheden (waaronder de beleidsministeries en uitvragende partijen in de rollen van opdrachtgever/afnemer) zullen een besturing vereisen die recht doet aan hun investering (en belang). Hier geldt ook het adagium wie betaalt, bepaalt.

Een programma als SBR kent een dubbele onzekerheid. Ten eerste wordt de business case voor uitvragende partijen bepaald door de bruikbaarheid binnen de eigen verantwoordingsketens. Wanneer de dienstverlening van Logius ontoereikend blijkt, heeft de uitvragende partij die hierin heeft geïnvesteerd een probleem. Ten tweede wordt de business case van de gedeelde dienstverlener bepaald door de bredere adoptie van SBR. Wanneer de toepassing van SBR beperkt blijft tot enkele verantwoordingsketens is het hele circus rond de netwerkstandaardisatie en de complexe organisatorische inrichting rond generieke bouwblokken niet rendabel. Vanuit het belang van de algehele lastenvermindering voor de BV Nederland en de verzilvering van gedane investeringen, treden het Ministerie van Economische Zaken en de Belastingdienst gezamenlijk sturend op bij de positionering van de verdere inrichting van de verticale ketenintegratie. Doordat de dienstverlening van Logius voor de SBR-verantwoording steeds volwassener wordt, neemt het risico voor nieuwe aansluitende partijen af. Voor hen is het juist aantrekkelijk aan te sluiten op een generieke

dienst waarmee verschillende compliance vraagstukken uit handen worden genomen. Zij willen zich niet verdiepen in de materie die nodig is voor de operationele besluitvorming, maar dit over laten aan hun dienstverlener. Het is prettig wanneer een uitvragende partij in de horizontale afstemming ervan uit kan gaan, dat het gebruik van Logius in het kader van SBR automatisch betekent dat de belangrijkste verantwoordelijkheden rond de Wet op het elektronisch bestuurlijk verkeer zijn ingevuld. Deze partijen zullen veel minder frequent bij de besluitvorming betrokken willen worden, althans zolang de verwachte kwaliteit geleverd wordt. Bij voorgaande constatering hoort wel een grote 'maar'. Een uitvragende partij in de rol van afnemer moet zeer bewust zijn welke rol Logius speelt in de keten waar zij verantwoordelijk voor is. De uitvragende partij moet altijd op de hoogte blijven over hoe haar eigen verantwoordingsketen functioneert. Dit vraagt om een uitvragende partij die zeker op tactisch niveau een zeer sterke inhoudelijke en conceptuele basis heeft.

Voor de ketengovernance op de gedeelde dienstverlener in het kader van de SBR aspecten gelden in ieder geval de volgende uitgangspunten:

- De volwassenheid van de gedeelde dienst bepaalt sterk de wijze waarop de ketengovernance georganiseerd is. Launching customers, die risico lopen, zullen intensief betrokken willen worden bij de besluitvorming rond de inrichting van de gedeelde dienstverlening. Bij een volwassen dienstverlening is voor partijen een governancemodel waarmee zij ontzorgd worden juist aantrekkelijk.
- Een efficiënte en evenwichtige besturing op Logius als gedeelde dienstverlener blijft gebaat bij een level playing field waar het gaat om kennis over het domein van verantwoording en de integratie van informatiesystemen.
- Wie betaalt, bepaalt is een belangrijk uitgangspunt bij ketengovernance. Doordat Logius een baten-lastendienst is, is de launching customer vaak de bepalende partij bij de inrichting van de dienstverlening.

9.5 SBR bij netwerkintegratie

Netwerkintegratie door toepassing van standaarden treedt op wanneer meerdere partijen besluiten op eenzelfde wijze koppelingen te bouwen voor hun informatieuitwisseling, zonder dat alle informatieketens in de praktijk met elkaar verbonden zijn. Deze vorm van standaardisatie zien we bijvoorbeeld bij het internet. In theorie kan je vanuit je browser, door toepassing van de verschillende standaarden, iedere website bereiken en de benodigde informatie uitwisselen. In de praktijk zul je de meeste bestaande sites nooit bezoeken. Voor SBR kunnen wij ook zo'n beeld oproepen. Stel dat een uitvragende partij (publiek of privaat) het SBR koppelvlak hanteert en gebruik maakt van een 'discoverable' taxonomie. Eentje die opgezet is volgens de Nederlandse Taxonomie Architectuur. Wanneer deze uitvragende partij vraagt om begrippen die in de database van een verantwoordingsplichtige reeds gemapt zijn, is volledig automatische system-to-system verantwoording mogelijk. Het is vanzelfsprekend nodig om het endpoint van het koppelvlak op te geven en de berichtsoort te benoemen. Dat is in dit geval vergelijkbaar met de URL van een website.

In de praktijk zijn verantwoordingsketens (vanuit het verleden en vanwege wet- en regelgeving) dusdanig vormgegeven dat de integratie van het informatiesysteem

vanuit het ketenperspectief gestalte krijgt. Voor het boek is deze concrete ketenbenadering (met de horizontale en verticale integratievormen) daarom als uitgangspunt genomen. Het perspectief van de netwerkbenadering is voor de ketengovernance weldegelijk relevant. In de eerste plaats omdat (componenten van) SBR in de praktijk wel als netwerkstandaard wordt toegepast, waardoor er sprake is van een zekere netwerkintegratie. In de tweede plaats omdat voor de uiteindelijke realisatie van een open en flexibel verantwoordingsstelsel (en het ideaal van eenmalig inrichten, meervoudig rapporteren) het netwerkperspectief een steeds dominantere positie kan gaan innemen.

Het succes van 'standaarden' om als standaard voor netwerkintegratie te dienen wordt onder andere bepaald door de volgende elementen:

1. **Beschikbaarheid**: De mate waarin de standaarden toegankelijk (vindbaar, betaalbaar) zijn voor toepassers.
2. **Effectiviteit**: De mate waarin standaarden bruikbaar zijn voor het doel waar zij voor worden toegepast.
3. **Doelmatigheid**: De mate van toepasbaarheid van de standaarden waar het gaat om het benodigde geld, inspanningen en kennis bij implementatie en toepassing.
4. **Relevantie**: De relevantie van het adoptiegebied.
5. **Stabiliteit**: De mate waarin standaarden onderhevig zijn aan wijzigingen.

Hoe een standaard op genoemde punten scoort moet relatief bezien worden ten opzichte van concurrerende specificaties die een oplossing bieden voor dezelfde behoefte. In de praktijk blijkt dat doelmatigheid (eenvoud) het bijna altijd wint van effectiviteit. Zo won VHS het van Betamax (standaard van videobanden, waarbij de tweede technisch beter was, maar de eerste eenvoudiger toepasbaar) en Ethernet van Token Ring (netwerkstandaard, waar hetzelfde fenomeen zichtbaar was).

9.5.1 *Relevante aspecten*

Het relevante item bij SBR als netwerkstandaard is het zogenaamde SBR-afsprakenstelsel. Dit afsprakenstelsel beschrijft welke standaarden je toepast bij het inrichten van een verantwoordingsketen. Het bestaat in de praktijk uit verschillende deelafspraken, die voornamelijk terug te vinden zijn in de besluiten van de gezamenlijke overleggen. Kijken we naar de onderdelen uit het afsprakenstelsel binnen SBR, dan dient er onderscheid gemaakt te worden tussen SBR-specifieke specificaties en niet-SBR-specifieke specificaties. Deze laatste 'specificaties' zijn op zichzelf al standaarden die breder dan SBR worden toegepast. De SBR-specifieke specificaties verwijzen vaak naar een set of een deelverzameling van niet-SBR specifieke specificaties.

In het volgende figuur is een beeld van het werkingsgebied van het afsprakenstelsel in de praktijk weergegeven.

SBR-specifieke specificaties:

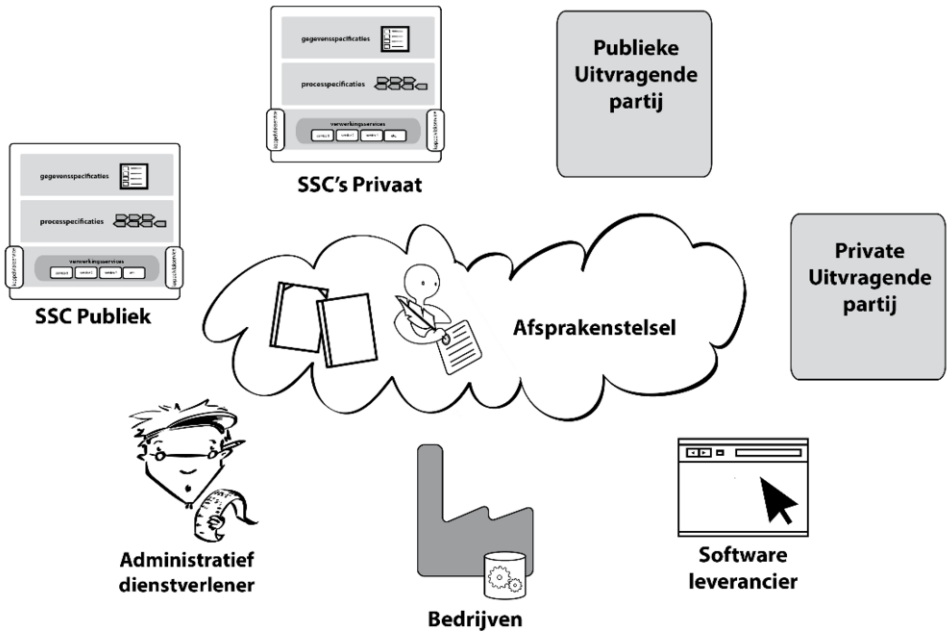
- Nederlandse Taxonomie Architectuur
- SBR Proces Architectuur
- SBR Technische Architectuur
- Nederlandse Taxonomie
- SBR Governancebeschrijving

Niet-SBR-specifieke specificaties waar SBR gebruik van maakt:

- TCP/IP
- XBRL 2.1 (en een hele set aanvullende XBRL-specificaties die aan de orde zijn geweest in het hoofdstuk Gegevens)
- TLS
- WUS (Digikoppeling 3.0)
- PKIoverheid

Voorgaande standaarden kennen ieder hun eigen wijze van doorontwikkeling en bestuur. SBR maakt zoveel mogelijk gebruik van open standaarden (specificaties die voldoen aan bepaalde vormen van beheer en wijziging en beschikbaarheid) om de acceptatie van SBR te vereenvoudigen. De inmiddels veelbesproken afhankelijkheid die hierdoor ontstaat moet vanuit de actoren verbonden aan SBR gemanaged worden. De wijze waarop dit gebeurt verschilt per standaard. Op sommige vlakken zijn de actoren verbonden aan SBR volgend. Zo zullen zij in principe geen energie steken in de doorontwikkeling van de internetstandaarden, terwijl een duidelijke participatie bij de doorontwikkeling van Digikoppeling voor de hand ligt.

Ook ontwikkelingen op het gebied van XBRL worden door de architecten die te maken hebben met SBR nauwgezet in de gaten gehouden. De SBR-specifieke specificaties (die gezamenlijk de SBR-standaard vormen) bestaan voor een deel uit voorschriften over welke open standaarden moeten worden toegepast bij de inrichting van een verantwoordingsketen en een beschrijving van de wijze waarop een open standaard moet worden toegepast. Een ander deel heeft betrekking op inhoudelijke aspecten van de verantwoording (rond begrippen en processen). Alle actoren die aangesloten zijn op een SBR-verantwoordingsketen zijn stakeholder van het SBR-afsprakenstelsel en op een zekere wijze betrokken bij de afstemming rond de relevante aspecten.



Figuur 9.6 – Stakeholders SBR-afsprakenstelsel

In onderstaande paragrafen wordt een korte toelichting gegeven op de verschillende onderdelen.

De Nederlandse Taxonomie Architectuur
Dit is het meest duidelijke en meest op netwerkniveau geaccepteerde object. Wanneer je voor een verantwoordingsketen een taxonomie maakt en je wilt conform SBR werken, dan pas je de Nederlandse Taxonomie Architectuur toe (zie voor details het hoofdstuk Gegevens). Door de naam wordt mogelijk de suggestie gewekt dat er geen andere taxonomiearchitecturen in Nederland bestaan. Dit is niet het geval. Betrokkenen bij de gegevensstandaard geven aan dat de aanduiding Nederlandse SBR Taxonomie Architectuur (of de SBR Taxonomie Architectuur) meer recht doet aan de positie van de NTA.

SBR Proces Architectuur
Er zijn twee afspraken die onder de SBR Proces Architectuur geplaatst kunnen worden. Ten eerste zijn er afspraken gemaakt over de wijze waarop de SBR processen met de betrokkenen gedeeld moeten worden. Hier wordt de standaard BPMN voor gehanteerd. In de praktijk hanteert men deze afspraak voor de procesonderdelen van gemeenschappelijke voorzieningen (Digipoort en de Bancaire Infrastructurele Voorziening). De tweede afspraak heeft betrekking op de wijze waarop met statusinformatie wordt omgegaan. Een deel van de statusinformatie en de foutmeldingen zijn geharmoniseerd, waarbij opgemerkt moet worden dat softwareleveranciers hier met de uitvragende partijen verdergaande afspraken over willen maken. Zij vragen de uitvragende partijen op dit gebied hun uitvraag verder te harmoniseren. Uitvragende

partijen hebben in dit kader al afgesproken duidelijk te communiceren wat de eindstatus van een aanleverproces is, zodat partijen weten wanneer zij aan hun verplichting hebben voldaan. Er is door diverse partijen geopperd te komen tot een standaard voor een uitbreidbare en discoverable taxonomie voor statusinformatie. Het voordeel hiervan is dat partijen bepaalde nieuwe controleservices kunnen implementeren zonder dat de softwareleveranciers aanpassingen hoeven te doen in hun software in verband met 'nieuwe' statusmeldingen.

SBR Technische Architectuur
Feitelijk beschrijven de 'toegestane' koppelvlakspecificaties van SBR de technische afspraken en vormen hiermee gezamenlijk de technische architectuur van SBR. Inmiddels vormt Digikoppeling 3.0 de basis binnen het afsprakenstelsel, waarbij de overheidspartijen in het SBR afsprakenstelsel alleen WUS 2.0 versie 1.2 als koppelvlak willen toestaan. Digikoppeling 3.0 betreft een overheidsstandaard en de banken hebben – als private uitvrager – in eerste instantie aangegeven hier de overheid te willen volgen. Inmiddels blijken de banken niet tevreden over de ontwikkelingen van Digikoppeling. Omdat zij niet de noodzaak zien de koppelvlakken door te ontwikkelen, zien zij graag dat een eerdere versie van het koppelvlak onderdeel blijft van het SBR-afsprakenstelsel. Daarnaast is er nog een vraagstuk over portalen. SBR voorschrijft geen specificaties voor invoerportalen. Dit wil niet zeggen dat portalen niet gebruikt kunnen worden voor aanleveringen in SBR. Het portaal functioneert in dat geval als 'software' die SBR compliant is. Voor gegevens die niet standaard in de administratie opgenomen zijn kan een dergelijke human-to-system koppeling interessant zijn. Logius als gedeelde dienstverlener kan voor ketens een dergelijk portaal verzorgen en door het gebruik van de SBR standaarden kunnen de wijzigingen in een dergelijk portaal snel doorgevoerd worden. Ook de banken onderhouden een gemeenschappelijk portaal. De human-to-system interface valt echter buiten het afsprakenstelsel. Een uitvragende partij kan er ook voor kiezen om voor een bepaalde doelgroep een eigen portaal met een achterliggende niet-SBR-koppeling te onderhouden.

De Nederlandse Taxonomie
De Nederlandse Taxonomie kan als standaard op netwerkniveau gezien worden omdat partijen hun extensies baseren op de Nederlandse Taxonomie. Zij hergebruiken dan begrippen uit de taxonomie voor hun eigen rapportage. In de praktijk blijkt dit hergebruik met name effectief binnen zogenaamde verantwoordingsdomeinen. De verschillende fiscale verantwoordingsrapportages kennen overlap in gegevens. Hetzelfde geldt voor rapportages uit het jaarrekeningendomein. In tegenstelling tot wat men misschien zou verwachten geldt met name voor wat geavanceerdere jaarverantwoording ten behoeve van het maatschappelijke verkeer dat begrippen weliswaar een grote overeenkomst hebben met fiscale begrippen, maar dat ze niet volledig samenvallen. Doordat hergebruik van begrippen domeingebonden blijkt, dient eventuele afstemming ook op dit niveau georganiseerd te worden. Omdat partijen in meerdere domeinen kunnen opereren, is het van belang dat er geen homoniemen ontstaan. De reports in de Nederlandse Taxonomie betreffen de ketenspecifieke specificaties en de extensies komen derhalve terug als object bij de horizontale ketenintegratie.

SBR Governance
De governance van het afsprakenstelsel voor SBR is een belangrijk aspect binnen het afsprakenstelsel waar alle partijen mee te maken hebben. De betrokkenen bij SBR beschrijven hier hoe zij afspraken op een systematische wijze kunnen herzien of tot nieuwe afspraken kunnen komen. Idealiter beschrijft de governance ook de wijze waarop de governance gewijzigd kan worden. Zo beschrijft de Grondwet ook de procedure voor het wijzigen van de Grondwet. In de SBR-governance is voorzien in een periodieke evaluatie. Hoe de besluitvorming rond wijzigingen verder verloopt is niet beschreven.

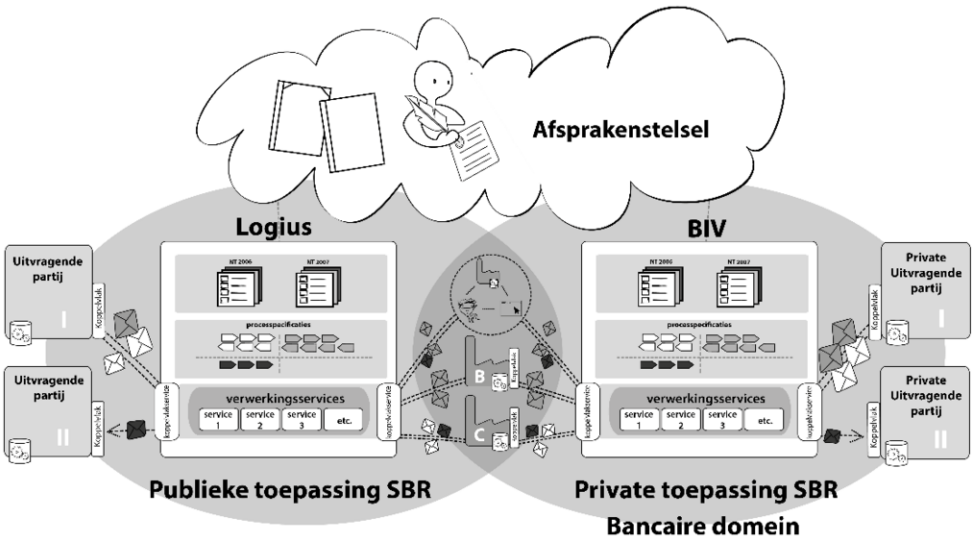
9.5.2 *Uitgangspunten voor de governance van SBR bij netwerkintegratie*

De uitgangspunten voor de governance van SBR als standaard voor netwerkintegratie (publiek/privaat) zouden via twee uiterste modellen kunnen worden geformuleerd. Bij het ene uiterste is één partij verantwoordelijk voor de governance op de netwerkstandaard. Deze partij onderhoudt de specificaties vanuit zijn eigen behoeften en maakt deze vervolgens openbaar. Andere partijen kunnen de specificaties vervolgens ook in hun verantwoordingsketens toepassen. Dit is een valide model, zolang hiermee wordt voldaan aan eerdere succescriteria voor adoptie van een specificatie om als netwerkstandaard te worden geadopteerd. Een ander uiterst model gaat uit van volledige participatie waarbij alle (potentiële) toepassers van de specificaties gezamenlijk verantwoordelijk zijn voor de governance op de specificatie. Het is van belang op te merken dat ook in het model van één bepalende partij, deze partij de behoefte kan hebben om wijzigingen in de specificaties met (belangrijke) ketenpartners te bespreken om de continuïteit in de eigen informatievoorziening te waarborgen. Cruciale beperking is dat bij de afweging van de bepalende partij in dit model de toepassing binnen de eigen keten centraal staat.

Tussen de uitersten zijn hybride modellen denkbaar, waarbij het aantal partijen dat verantwoordelijk is voor de governance en de besluitvorming beperkt is, maar waar consultatie niet alleen plaatsvindt vanuit de toepassingsmogelijkheden binnen de eigen keten, maar ook rekening houdt met de toepassing van de specificaties in andere informatieketens. In dat geval spant een partij zich in voor het algemeen nut. Dit model zal eerder geadopteerd worden door publieke partijen.

Binnen het SBR Programma is het beleid gevoerd om de adoptie van het afsprakenstelsel door publieke en private partijen hand in hand te laten verlopen. Met de toepassing van SBR door grootbanken is de scope van de toepassing van SBR dan ook gewijzigd van het publieke domein naar het publiek/private domein, maar dit betekent iets voor de reikwijdte van gedeelde specificaties. Door de toetreding van de banken wordt het netwerkperspectief weliswaar een stuk relevanter, maar de tegenstelling in de eisen aan de informatieverwerking in het publieke en private domein stelt grenzen aan de diepgang van het overkoepelende afsprakenstelsel. Voor private partijen geldt dat differentiatie een noodzaak is die de marktomgeving vereist. Daarom zijn marktpartijen beperkt in de mate waarin deze zich kunnen conformeren aan bepaalde afspraken. Wanneer de betrokken banken gezamenlijk de volledige informatieverwerking bij het kredietverstrekkingsproces zouden uniformeren zou de ruimte voor differentiatie sterk afnemen. Dit model past bij een franchise, waarbij

de Autoriteit Consument en Markt het waarschijnlijk niet acceptabel zou vinden dat drie grootbanken in Nederland defacto op die manier zouden opereren. Voor publieke partijen is het juist goed wanneer zij vergelijkbare onderdelen (functies) uniform inrichten en op deze wijze de efficiëntie en controleerbaarheid vergroten. Dit past bij een doelmatige overheid. Op dit vlak kunnen de overheden verder harmoniseren. Het publieke domein is zodoende te beschouwen als een domein met nadere standaardisatie-afspraken. Kijken we naar inhoudelijke harmonisatie rond begrippen, dan hebben publieke partijen vaak te maken met wettelijke voorschriften waardoor een participatief governancemodel met andere uitvragers lastiger wordt. Zij moeten zich immers bij hun uitvraag baseren op de wet en kunnen niet zomaar en zelfstandig een wettelijke definitie aanpassen. Private partijen kunnen hier weer gemakkelijker standaardiseren en vormen op dit gebied een domein met nadere standaardisatie-afspraken. Onderstaande figuur geeft een gevoel bij de reikwijdte van het afsprakenstelsel binnen SBR.



Figuur 9.7 – Beeld van de reikwijdte van het afsprakenstelsel

Voor de governance van SBR als standaard voor netwerkintegratie kunnen de volgende uitgangspunten geformuleerd worden:

- De reikwijdte van het publiek/private afsprakenstelsel en de hierin opgenomen governance moeten aansluiten bij de adoptiemogelijkheden in het volledige domein. In de praktijk betekent dit dat met name de inhoudelijke keuzes op dit niveau beperkt blijven. Binnen een toepassingsdomein van SBR kunnen inhoudelijke onderdelen nog nader gestandaardiseerd worden.
- Een model van één dominante partij die vanuit het eigen ketenperspectief de volledige specificatieset vaststelt, sluit niet aan bij de huidige opzet van SBR. Dit betekent dat voor het hoogste niveau er een afstemmingsstructuur op basis van 'onderlinge gelijkwaardige afstemming' moet worden ingericht in plaats van een consultatiestructuur.

- Waar partijen mogelijkheden hebben om verder te harmoniseren kunnen zij dit binnen een bepaald toepassingsdomein doen. De SBR-bankentaxonomie is hier een voorbeeld van. De betrokkenen uit het domein hanteren voor de besluitvorming over de gezamenlijke specificaties een eigen governance. Merk op dat hierdoor een nieuwe afstemmingstafel ontstaat. De overheidspartijen (publieke uitvragers) stellen voor hun toepassing van SBR ook aanvullende eisen. In principe zouden er ook weer dwarsverbanden (verticale domeinen) kunnen ontstaan, wanneer bijvoorbeeld publieke en private partijen die te maken hebben met uitvragen rond beloning gezamenlijk aanvullende afspraken over de toepassing van de netwerkstandaarden zouden maken.

9.6 Samenhang tussen de governance op de drie integratievormen

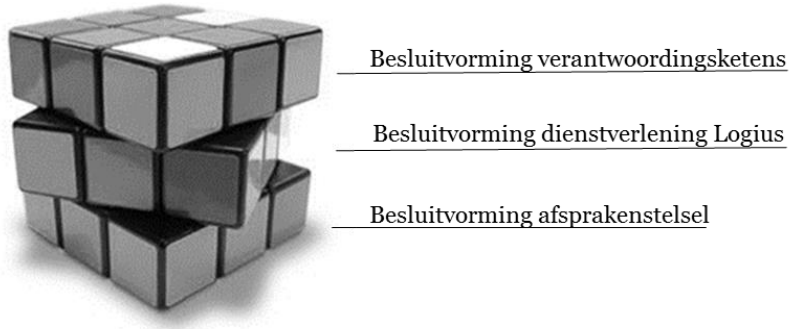
De samenhang tussen de ketengovernance op de drie integratievormen is enerzijds heel eenvoudig maar tegelijkertijd ook zeer complex.

De eenvoudige benadering ziet de besturingsvormen als losstaande onderdelen, met ieder een duidelijk afgebakend gebied. Een uitvragende partij conformeert zich voor de inrichting van de verantwoordingsketen wel of niet aan het SBR-afsprakenstelsel. Voor de uitvragende partijen die dit wel doen is het afsprakenstelsel dan het uitgangspunt voor de nadere inrichting van de verantwoordingsketen. Los hiervan stellen de uitvragers die gebruik maken van een gedeelde dienstverlening de scope en reikwijdte vast van de gedeelde dienstverlening. Het spreekt voor zich dat de gedeelde diensten voor de SBR-ketens compliant moeten zijn met het afsprakenstelsel. Verder is binnen de eigen kaders alles mogelijk. Hoe meer je regelt op netwerkniveau, hoe gemakkelijker de besturing is op de relevante aspecten bij de horizontale en verticale integratie. Wanneer het SBR-afsprakenstelsel zegt dat een taxonomie altijd dimensioneel opgebouwd moet zijn, hoeft deze keuze niet meer gemaakt te worden door een uitvragende partij die zijn verantwoordingsketen inricht. Logius, als generieke dienstverlener, zorgt er dan voor dat haar diensten op het gebied van gegevensmanagement altijd uitgaan van een dimensionele taxonomie. Een extremer voorbeeld: wanneer het SBR-afsprakenstelsel zou zeggen dat een SBR-compliant koppelvlakservice altijd een minimale beschikbaarheid moet hebben van 99,8%, weten de verantwoording-verwerkende organisaties, waaronder Logius, dat voor iedere bestaande en nieuwe SBR-keten haar serviceorganisatie voor dit serviceniveau moet worden ingericht. Zoals al aan de orde kwam bij SBR als netwerkstandaard zitten er echter grenzen aan de one size fits all benadering. Partijen kunnen niet met één verantwoordingsketen uit de voeten omdat het doel van de verantwoording verschilt of omdat zij vanuit hun eigen verantwoordelijkheid anders aankijken tegen de inrichting van vergelijkbare verantwoordingsstromen. Het is van belang dat partijen die zich willen conformeren aan de SBR-kaders op netwerkniveau kunnen inschatten of zij bij de inrichting van hun verantwoordingsketen met de standaard uit de voeten kunnen. En hier ontstaat de complexiteit.

De complexe benadering houdt rekening met het sneeuwbaleffect dat op kan treden wanneer een probleem in één keten doorwerkt op alle andere integratievormen. Dit is weergegeven in het voorbeeld in de inleiding (tekstbox). Voor de uitvragende partijen geldt dat, wanneer zij zich conformeren aan een bepaald besluit over verdere standaardisatie, zij direct hun verantwoordelijkheid ten aanzien van hun dienstverlener en verantwoordende partijen uit de eigen keten in ogenschouw moeten nemen. Hier wordt de besluitvorming over aspecten voor netwerkintegratie afhankelijk van de besluitvorming over aspecten die gelden voor de horizontale en verticale ketenintegratie. Doordat de verschillende ketenpartners – en de gedeelde dienstverlener – in meerdere verantwoordingsketens actief zijn, zullen zij bij de inschatting van de mogelijkheden van standaardisatie ten aanzien van een verantwoordingsketen hun belangen vanuit een breder perspectief benaderen. Hier raakt de besluitvorming dus verweven.

De verweven besluitvorming leidt in de praktijk tot actoren die bij de afstemming vanuit verschillende perspectieven zullen spreken. In een overleg waar eigenlijk nut en noodzaak van een aanpassing in een specifieke verantwoordingsketen op de agenda staat, beginnen zij over de noodzaak om deze aanpassing integraal voor alle SBR-ketens door te voeren. Dit is natuurlijk een valide gedachte, maar het kan betrokkenen die toevallig eendimensionaal in de wedstrijd zitten en die het bredere belang van een partij niet herkennen, verwarren. De besluitvorming wordt ook gecompliceerd doordat de aspecten die zich richten op integratie van ketens bijna altijd zeer technisch/inhoudelijk van aard zijn. Niet iedere uitvragende partij heeft de ruimte om zich te verdiepen in de technische materie en de impact van standaardisatie op de eigen keten. Niet iedere organisatie heeft automatisch de kennis in huis om vast te stellen of een enveloping signature, enveloped signature of een externally detached signature een standaard is waarmee zij in alle gevallen of in sommige gevallen of nooit uit de voeten zullen kunnen. Partijen zullen bij twijfel huiverig zijn om iets tot standaard te verklaren en in het afsprakenstelsel ruimte willen houden voor afwijkingen. Hierbij moet worden opgemerkt dat met name rond fundamentele wijzigingen de afhankelijkheden tussen de verschillende afstemmingsgebieden het grootst zijn (zie ook hoofdstuk 4).

Om voortgang te kunnen boeken bij de standaardisatie rond dergelijke aspecten is het daarom van belang dat er in het spel actoren aanwezig zijn die enerzijds voldoende specialisme in huis hebben om op heldere wijze de technische impact van besluiten vanuit verschillende perspectieven te ontrafelen en anderzijds het vertrouwen genieten van andere partijen dat zij hierin in zekere mate handelen vanuit het gedeelde belang. Deze actor kan de hele puzzel overzien en bijdragen aan het leggen van een consistent geheel.



Figuur 9.8 – Samenhang governance op de drie integratievormen

Een partij moet dit gezag verdienen en de rol kan door meerdere partijen in het speelveld worden ingevuld. Doordat de gedeelde dienstverleners zich kunnen specialiseren in de materie en doordat zij belangrijke onderdelen van de keten onder hun hoede hebben, zijn zij bij uitstek een partij die het complexe speelveld kan overzien. In de praktijk zal het succes van de standaardisatie afhangen van de mate waarin deze dienstverlener in staat blijkt de benodigde autoriteitspositie te verwerven. Bij SBR heeft de Belastingdienst, als grote uitvragende partij met veel expertise op het gebied van system-to-system informatieverwerking, met haar investeringen in kennisdeling en als launching customer van Logius, onder uitvragende partijen gezag op het gebied van SBR opgebouwd. Het vertrouwen van de Belastingdienst helpt Logius bij het verwerven van haar autoriteitstatus. Tot slot is de Rijksregisseur SBR (zie de inleiding of onderstaand) een belangrijke actor in SBR gebleken qua regie en stroomlijning van de besluitvorming op verschillende niveaus.

9.7 Actuele governance SBR

9.7.1 *Opbouw en verbinding*

Momenteel zijn er in het kader van SBR diverse publiek/private gremia ingericht die gezamenlijk opereren in een beschreven stelsel. Kenmerkend is dat de aspecten die aan de orde komen enerzijds betrekking hebben op de toepassing van SBR voor netwerkintegratie, anderzijds gebruiken de uitvragende partijen en Logius de gremia voor de afstemming over horizontaal geïntegreerde ketens. De publiek/private gremia behandelen vanzelfsprekend niet de vraagstukken die gelden voor horizontale en verticale integratie van publieke schakels. Deze zijn belegd bij een publieke governance binnen SBR, die ingesteld is om te:

- besluiten over de wijze waarop de overheid in het kader van SBR optreedt binnen de publiek/private governance;
- besluiten over de wijze waarop de diensten die zij gedeeld afnemen (door)ontwikkeld en beheerd moeten worden (verticale integratie);
- besluiten over de horizontale integratie tussen Logius en de uitvragende partijen.

Op verschillende vlakken is er verbinding tussen de publiek/private governance en de publieke governance. Zo wordt zowel het SBR Beraad als de SBR Stuurgroep (de

hoogste organen uit de governance) voorgezeten door de DG Belastingdienst. Tevens is er een Rijksregisseur aangesteld. De Rijksregisseur schakelt tussen de publieke SBR partijen, andere overheidsorganisaties en marktpartijen om uitleg te geven over de betekenis van SBR voor de overheid en de markt, draagvlak te creëren en eventuele bredere vraagstukken te beleggen. Door zijn vrije rol en aanspreekbaarheid is de Rijksregisseur tevens belangrijk in de agendazetting. Hij bewaakt dat zaken op de juiste plaats voor besluitvorming aan de orde komen en voert de regie over verdere standaardisatie.

9.7.2 *Publiek/private gremia SBR*

SBR Beraad
De bestuurders van marktpartijen en de overheid stellen in het Beraad de gezamenlijke kaders en strategische lijnen voor de toepassing van SBR als netwerkstandaard op de lange termijn vast. Het Beraad creëert daarmee het nodige draagvlak bij alle betrokkenen voor de besluitvorming in andere gremia en invulling van het beheer van de generieke voorzieningen door de overheid en door de private partijen aan hun zijde. Op een geaggregeerd (nationaal / sector) niveau nemen alle belanghebbenden deel (zowel die in het Platform zijn vertegenwoordigd als de overige – kleinere belanghebbenden). Bijvoorbeeld: een vertegenwoordiger van alle intermediairs en koepelverenigingen gezamenlijk; een vertegenwoordiger van alle dienstverleners / softwareleveranciers gezamenlijk; VNO NCW et cetera.

SBR Platform
Het Platform is het gremium waarin de verschillende belangen van de bij SBR betrokken partijen vertegenwoordigd zijn. Dit was in de begindagen van het SBR Programma een belangrijke functie: het goed aftasten en betrekken van de markt. Met de groei van SBR naar een vanuit de overheid geformaliseerde, meer permanente methode, dragen de vertegenwoordigers in het Platform er vooral aan bij dat eventuele knelpunten voor de voortgang van SBR vroegtijdig worden gesignaleerd en dat kansen om SBR verder te brengen worden geagendeerd. De brede vertegenwoordiging van belangen is in lijn met het zorgvuldigheidsbeginsel en het evenredigheidsbeginsel. Echter, teneinde een werkbaar gremium te realiseren en belanghebbenden gelijk te behandelen is het van belang om een aanvullende voorwaarde te stellen: deelnemers dienen een substantieel belang te vertegenwoordigen. Voor wat 'substantieel belang' is dienen heldere en expliciete criteria geformuleerd te worden. Het betekent in de praktijk dat de deelnemers namens belangenverenigingen deelnemen.

Expertgroepen
In de expertgroepen voor respectievelijk gegevens, processen & techniek en marketing & communicatie, nemen vakexperts van de marktpartijen en overheid deel. Zij werken onder leiding van experts van Logius aan de ontwikkeling van op expertise gebaseerde voorstellen en adviezen over de inrichting en het beheer en onderhoud van standaarden. Ook signaleren zij nieuwe of nog niet adequaat geadresseerde trends en problemen en adviseren over hoe de SBR-partijen vastgestelde standaardisatiedoelen kunnen realiseren. Expertgroepen vereisen een actieve inbreng van de deelnemers en specifieke expertise (afhankelijk van de expertgroep binnen het domein gegevens, processen & techniek of marketing & communicatie). Via openbare

consultatie van bijvoorbeeld de taxonomie wordt input uit de brede community verkregen. De inbreng van expertise ten behoeve van de besluitvorming in SBR draagt bij aan de zorgvuldigheid in de uitvoering. De resultaten, verslagen, documenten en dergelijke zijn publiek en worden op de SBR site gepubliceerd voor overige belanghebbenden.

Overige betrokkenheid
De kleinere groeperingen en eenheden binnen een in het Platform vertegenwoordigde belangengroep moeten (met oog op zorgvuldigheid, evenredigheid en gelijkheid) ook de kans hebben om mee te praten. Dit kan bijvoorbeeld worden geregeld door middel van een 'loket' en/of een jaarlijkse 'SBR-dag', waarop zij hun inbreng en belang kunnen verwoorden en een oordeel meegeven over de output van het Platform vanuit hun perspectief. Notulen van het Platform zijn in het kader van transparantie openbaar.

Zelfstandige sessies in het kader van besturing
Uitvragende partijen en andere belanghebbenden beleggen zelfstandig sessies met belanghebbenden binnen het eigen verantwoordingsdomein, vanuit hun verantwoordelijkheid voor de inrichting van de horizontale integratie in hun eigen verantwoordingsketens.

9.7.3 *Publieke gremia SBR*

Stuurgroep SBR
In de Stuurgroep SBR besluiten de overheidspartijen over de strategische lijnen ten aanzien van het SBR-afsprakenstelsel (de inbreng in het Beraad) en ten aanzien van de gedeelde dienstverlening. Elk van de bij SBR betrokken overheidspartijen is vertegenwoordigd: de beleidsverantwoordelijke ministeries van V&J, Financiën, EZ en BZK; de uitvragende partijen (waaronder KvK, CBS, Belastingdienst) en Logius. De Stuurgroep wordt voorgezeten door de DG Belastingdienst.

Projectleidersoverleg
Vanuit het Projectleidersoverleg (PLO), bestaande uit de uitvragende partijen, EZ en Logius, wordt uitvoering gegeven aan de in de Stuurgroep uitgezette lijnen voor SBR. Het PLO stelt jaarlijks een tactisch plan en een begroting voor SBR op. Zij bereidt de bekostigingsmethodiek voor en houdt toezicht op de uitvoering van de plannen en werkzaamheden op operationeel niveau.

Werkgroepen SBR
Op operationeel niveau bestaan werkgroepen voor respectievelijk processen & techniek, gegevens, marketing & communicatie en compliance: overheidswerkgroepen waarin vakexperts van de uitvragende partijen, EZ en Logius zich bezighouden met het identificeren van behoeften; het ontwerp van processen / taxonomieën/ communicatie-instrumenten / procedures; afstemming op doorontwikkeling en beheer van de voorzieningen; het bepalen van de impact op de keten en het oplossen van vraagstukken ten aanzien van de voorzieningen.

Project board verbreding en internationaal
In de Project board kijken de opdrachtgevers voor verbreding – onder voorzitterschap van de Rijksregisseur – samen met Logius naar de wijze waarop de dienstverlening van Logius in het kader van SBR breder binnen de Rijksdienst ingezet zou kunnen worden. Werkzaamheden voor partijen in de interessefase (zie ook hoofdstuk 10) worden vanuit deze Project board aangestuurd. Verder bespreken partijen de relevante kansen en bedreigingen voor de internationale standaardisatie op het gebied van verantwoording.

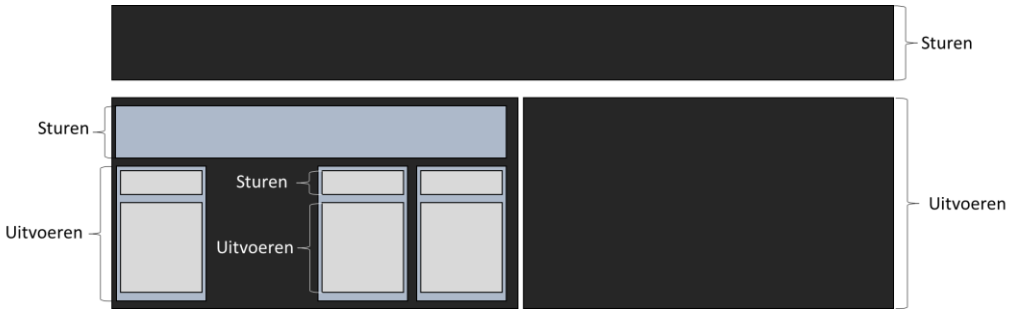
9.7.4 *Relevante ontwikkelingen*

Met de recente ontwikkelingen, met name de groeiende berichtaantallen en de verplichtstelling van SBR voor system-to-system aanleveringen, is er behoefte aan een meer permanente structuur voor SBR. Steeds meer aspecten van de standaarden, de ketens en de generieke dienstverlening zijn stabiel en kennen een brede toepassing. Deze aspecten vragen voor een kosteneffectieve toepassing (zie hoofdstuk 4) meer en meer om een procedurele besturing. De besturing zal een lagere frequentie kennen en veel van de besluitvorming kan op het operationele of tactische niveau plaatsvinden. Dit geldt echter niet voor alle aspecten van SBR. Verdere differentiatie tussen de besturing op business as usual en zaken in ontwikkeling, zoals het stimuleren van de SBR toepassing, is daarom voorzien.

9.8 De centrale rol van Logius binnen SBR

9.8.1 *De relatie tussen governance en beheer*

Het onderscheid tussen de organisatie van de governance en de organisatie van het beheer is die van beslissen bij sturen en beslissen bij uitvoeren. Voor de differentiatie tussen ketengovernance en ketenbeheer is het echter nodig een duidelijk afgebakend frame of reference vast te stellen. De grens tussen bestuur en uitvoering is arbitrair en recursief. Dit is in onderstaand model weergegeven. Twee organisaties kennen een overkoepelend bestuur. Deze organisatie kent een eigen bestuur dat meerdere afdelingen aanstuurt. Deze afdelingen worden weer bestuurd door het afdelingsmanagement etc.



Figuur 9.9 – Grens tussen bestuur en uitvoering

Afhankelijk van de organisatorische opzet (professionele organisatie of machinebureaucratie / business unit of franchise) kan de beslissingsbevoegdheid van een onderliggend deel groot of klein zijn. De uitvoeringsrol van Logius vindt plaats in het kader van de opdrachten die zij formeel krijgt van de verschillende beleidsopdrachtgevers en uitvragende partijen.

9.8.2 *De opdracht aan Logius in het kader van SBR*

De diensten die Logius levert in het kader van SBR zijn feitelijk tweeledig:

1. **Afstemmingsdiensten**: Organisaties uit het publieke domein willen op een standaard wijze system-to-system verantwoordingsinformatie verwerken die zij nodig hebben voor het uitvoeren van hun publieke taak. Deze standaard leggen zij onder de naam SBR vast in een afsprakenstelsel. De besluitvorming (ketengovernance) rond dit stelsel en de coördinatie van de samenhang met de andere governancegebieden moet inhoudelijk gefaciliteerd worden. Versies van het stelsel moeten voor betrokkenen beschikbaar zijn. Logius heeft de opdracht in dit kader een groot deel van de technisch/inhoudelijke en administratieve ondersteuning te leveren.
2. **Reporting services**: Voor de generieke geautomatiseerde afhandeling van de verantwoordingsinformatie zijn de uitvragende partijen op zoek naar een gedeelde dienstverlener. Hiervoor is het noodzakelijk dat een aantal bouwstenen op generieke wijze geoperationaliseerd wordt, te weten: berichtspecificaties, specificaties rond de i-processen, koppelvlakservices en services voor het verwerken van berichten. De organisaties dienen – wanneer bij de verantwoording verstoringen optreden of zaken onduidelijk zijn – door Logius ondersteund te worden. Tevens moet Logius de infrastructuur in stand houden om partijen te ondersteunen bij het doorvoeren van wijzigingen.

Uit deze rol vloeit voort dat Logius een autoriteit moet zijn op het gebied van standaardisatie en actief moet monitoren welke ontwikkelingen op het gebied van standaardisatie relevant zijn voor SBR. Daarnaast moet zij actief de vraag van de verschillende uitvragende partijen managen en steeds de koppeling maken tussen de behoefte en de architectuur, waarmee de specifieke behoefte met generieke bouwblokken vormgegeven kan worden. Hoe Logius partijen in staat stelt om een geheel nieuwe keten conform SBR in te richten wordt nader behandeld in hoofdstuk 10.

9.8.2.1 De dienstgeoriënteerde architectuur

Logius is een baten-lastendienst die werkt voor meerdere opdrachtgevers. De consequentie hiervan is dat Logius haar dienstverlening zo moet inrichten dat de kosten voor haar diensten toe te rekenen zijn aan de juiste opdracht en bijbehorende opdrachtgever(s). Een dienstgerichte benadering is daarom het uitgangspunt voor de gedeelde dienstverlening. De wijze waarop diensten afgebakend worden en het gehanteerde aggregatieniveau is bepalend voor de acceptatie en de werkbaarheid van het systeem. Bij een fijnmazige indeling is een specifieke dienstverlening mogelijk en is de specifieke toerekenbaarheid groot, maar kan het zo zijn dat de opdrachtverstrekking en verantwoording een grote bureaucratie teweeg brengt. Dit komt de tijdigheid en doelmatigheid niet ten goede. Bij een grofmazige indeling is het verantwoordingsmodel eenvoudig, maar kan het zijn dat opdrachtgevers onvoldoende specifiek bediend kunnen worden en de verantwoording over de dienstverlening niet

aansluit bij hun kaders. Logius definieert een dienst als een clustering van functionaliteiten met een vaste input en output, die afzonderlijk kan of moet worden afgenomen door een opdrachtgever. De dienst voldoet aan de eisen die Logius aan een dienst stelt en aan de eisen die het SBR-afsprakenstelsel eraan stelt. De eisen aan de herbruikbaarheid, flexibiliteit en kostenefficiëntie alsmede de architecten bepalen hoe een dienst wordt gedefinieerd en wat de reikwijdte van een dienst is.

Van iedere dienst moet nauwkeurig zijn vastgelegd wat de karakteristieken zijn. Hierbij is het van belang dat de volgende onderdelen zijn beschreven:

- De voorwaarden die gelden voor het afnemen van de dienst in de vorm van inputeisen.
- De resultaten die door de dienst opgeleverd worden in de vorm van outputeisen.
- De wijze waarop de dienst kan worden besteld.
- De eenheden waarin de dienst geleverd kan worden en de kosten die hiermee gepaard gaan.
- De doorlooptijden waarbinnen een dienst kan worden geleverd.
- De KPI's die voor de dienst gelden.
- De methode en technieken die bij de dienstverlening worden gevolgd.
- De wijze waarop het kwaliteitsmanagement over de dienstverlening is vormgegeven.
- De wijze waarop verstoringen in de dienstverlening (h)erkend worden en worden opgelost.
- De wijze waarop escalatie plaatsvindt bij ernstige afwijkingen in de dienstverlening.
- De wijze waarop behoefte aan wijzigingen in de dienstverlening (h)erkend wordt en kan worden ingewilligd.
- De wijze waarop de financiële controle op de dienstverlening georganiseerd wordt.
- De wijze waarop er over de dienstverlening gerapporteerd wordt.
- De wijze waarop de geleverde diensten geëvalueerd worden.

De diensten die Logius in het kader van SBR aanbiedt houden verband met de twee opdrachten waar Logius als gedeelde dienstverlener invulling aan geeft. In onderstaande paragrafen worden zij kort toegelicht.

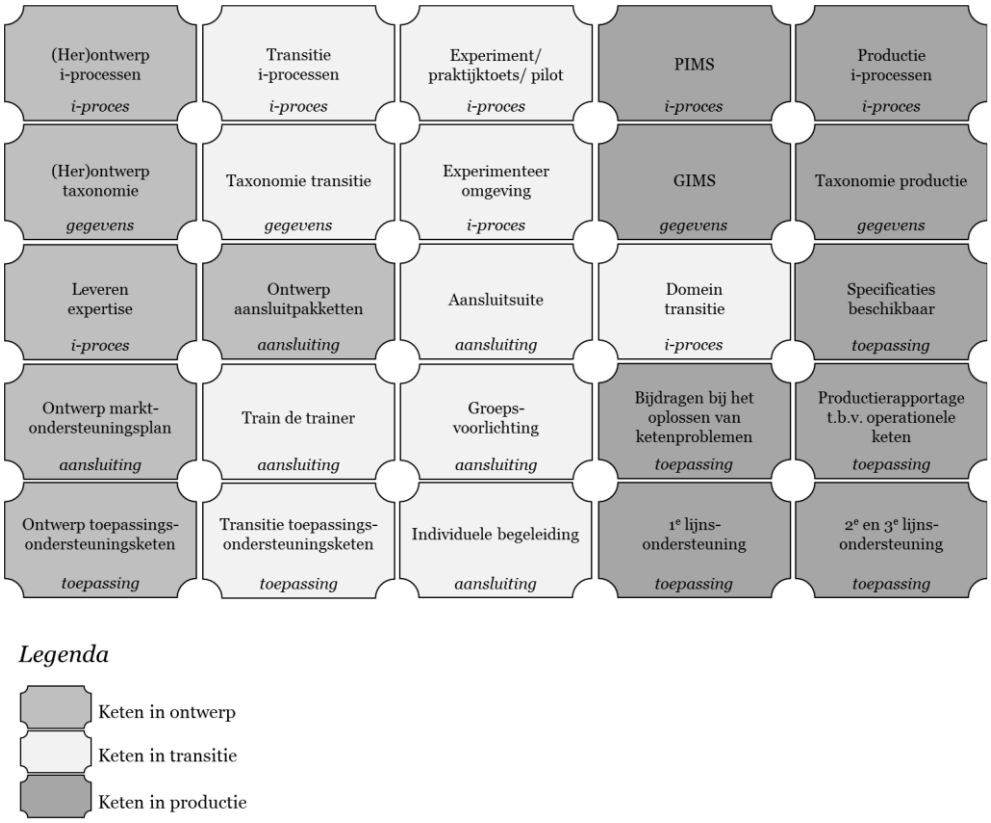
9.8.2.2 Afstemmingsdiensten

Voor het faciliteren van de ketengovernance levert Logius mensen, middelen en expertise voor de volgende diensten:

- Voorbereiden, coördineren en inhoudelijk faciliteren van overleggremia van SBR.
- Algemene ondersteuning bij PR en communicatie rond het SBR-afsprakenstelsel.

9.8.2.3 Ontwikkeling en operationeel houden van bouwstenen voor verantwoording

Voor het ontwikkelen en operationeel houden van de SBR-verantwoordingsketens (Reporting Services) onderhoudt Logius een uitgebreide dienstencatalogus. Deze is weergegeven in onderstaande figuur.



Figuur 9.10 – Dienstencatalogus Logius

De diensten zijn ingedeeld in een van de volgende vier basisfuncties:

1. i-Procesmanagement
2. Gegevensmanagement
3. Toepassingsondersteuning
4. Aansluitondersteuning

Ad 1. i-Procesmanagement richt zich op de totstandkoming en operatie van de i-processen (informatieverwerking). Berichten die bij een koppelvlak worden aangeboden, moeten op een gestructureerde manier verwerkt worden. Het i-Procesmanagement zorgt er voor dat de verwerking per berichttype exact is vastgelegd, dat zowel de koppelvlakservices als de verwerkingsservices operationeel zijn en dat deze op de juiste wijze functioneren. De (door)ontwikkeling van een i-proces start met het bekijken hoe de bestaande koppelvlakservices en verwerkingsfunctionaliteit ingezet

kunnen worden bij het invullen van de behoefte. Indien het nodig is wordt nieuwe functionaliteit (een nieuwe service) beschreven en gerealiseerd. Samengevat is het i-Procesmanagent verantwoordelijk voor de ontwikkeling en werking van de volgende bouwblokken voor de system-to-system informatieverwerking:

- Gegevensverwerkingsprocessen
- Koppelvlakservices
- Verwerkingservices

Ad 2. Gegevensmanagement richt zich op de totstandkoming en de beschikbaarheid van taxonomieën. In een taxonomie zijn de exacte definities van gevraagde begrippen horend bij een bericht gestructureerd beschreven, bijvoorbeeld het begrip 'winst'. Door de structurering van de beschrijving is het mogelijk software zo in te richten dat met behulp van informatie uit een pakket op een gemakkelijke manier berichten gegenereerd kunnen worden die voldoen aan de gevraagde specificaties. Taxonomieën kunnen naast de specificaties van de gegevens die in een bericht moeten worden opgenomen ook eenvoudige en complexe regels over de inhoud bevatten. Wanneer een organisatie heeft aangegeven dat er inkomsten uit nevenactiviteiten zijn, kan vereist worden dat de omvang van deze activiteiten ook is ingevoerd. Samenvattend is het gegevensmanagement verantwoordelijk voor de ontwikkeling en werking van de taxonomie die toegepast wordt bij een i-proces.

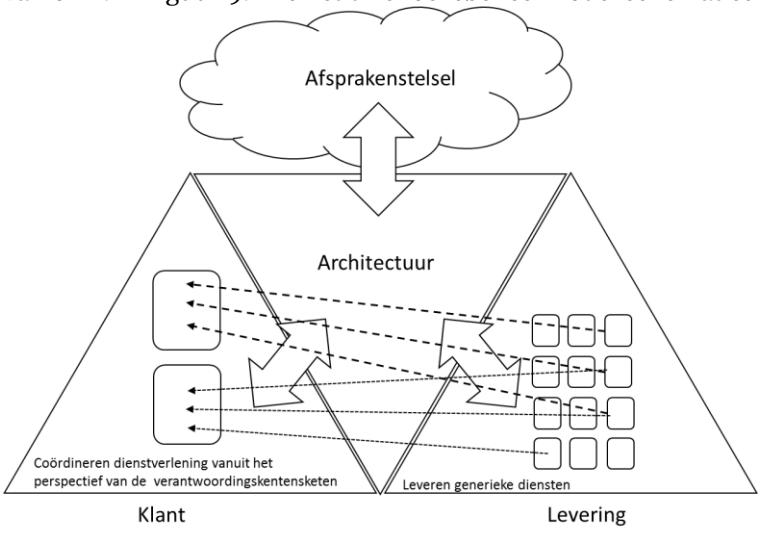
Ad 3. Toepassingsondersteuning is gericht op de totstandkoming en uitvoering van de ondersteuning van organisaties (incl. softwareleveranciers) betrokken bij een system-to-system informatieverwerking. De toepassingsondersteuning houdt voor de betrokkenen een 'doe het zelf' component in stand en kent daarnaast een interactieve component. De 'doe het zelf' component bevat de informatie en de voorzieningen die nodig zijn om eventuele vragen of mogelijkheden van de toepassing te bestuderen en te testen. De interactieve component is een loket waar gerichte vragen over de toepassing gesteld kunnen worden of problemen met de toepassing kunnen worden gemeld. Wanneer er sprake is van een verstoring die voor meerdere organisaties problemen kan opleveren, biedt toepassingsondersteuning hier proactief informatie over aan. Vanuit toepassingsondersteuning kan de incidentoplossing en eventueel benodigde 2e/3e lijns-ondersteuning gestart worden.

Ad 4. Aansluitondersteuning biedt intensieve interactieve en 'doe het zelf' ondersteuning bij de aansluiting van organisaties op de (door)ontwikkelde system-to-system informatieverwerking. Aansluitondersteuning is met name van belang indien de kennis voor het toepassen van de system-to-system informatieverwerking of gerelateerde technieken onvoldoende beschikbaar is voor de betrokken organisaties, wanneer er nog sprake is van een onvolwassen keten of ketenfunctionaliteit en/of indien de overheid een bijzondere zorgplicht voor ondersteuning heeft. Dit laatste geldt bijvoorbeeld indien partijen de facto verplicht worden voor hun communicatie met de overheid aan te sluiten op de system-to-system informatieverwerking. De aansluitondersteuning betreft een tijdelijke intensivering van de ondersteuning voor een bepaalde doelgroep.

Uiteindelijk worden de generieke diensten ingezet om de system-to-system informatieverwerking te ondersteunen die nodig is voor verschillende verantwoordingsketens. Al eerder is opgemerkt dat meerdere i-processen een rol kunnen spelen bij één verantwoordingsketen. Dit betekent automatisch dat er ook meerdere berichtspecificaties voor dezelfde taak in gebruik zijn en onderhouden moeten worden (bijvoorbeeld serviceberichten aanslag, aangiftes, uitstelverzoek etc.). Omdat de informatieverwerking veelal betrekking heeft op een bepaalde periode kan het zo zijn dat dezelfde i-processen berichtspecificaties over meerdere jaren ondersteunen. Men kan via hetzelfde proces VPB-aangifte doen over de periode 2011 maar ook over de periode 2012. Toepassingsondersteuning en aansluitondersteuning moeten hierbij ingericht zijn op de belevingswereld van de organisaties die betrokken zijn bij de specifieke publieke taak. Een gebruiker die meldt problemen te ondervinden met de winstaangifte kan net zo goed doelen op het feit dat hij een foutmelding krijgt bij het aanvragen van uitstel van de aangifte. Ook wanneer problemen in de system-to-system verwerking bij de aangesloten overheidsorganisatie plaats kunnen vinden is Logius een logisch aanspreek-/ of communicatiepunt. Logius dient daarom de specifieke toepassing van de generieke diensten te coördineren vanuit het perspectief van de horizontaal geïntegreerde keten, zodat deze herkenbaar wordt voor de verantwoordingsplichtige organisaties en de uitvragende partij. De organisatie van Logius moet hier op ingericht zijn.

9.8.3 *Het driehoeksbeheermodel*

Om invulling te kunnen geven aan de verschillende functies hanteert Logius een driehoeksbeheermodel. Centraal in dit model staat de architectuurfunctie, waar de verbinding wordt gelegd tussen de drie vormen van ketenintegratie onder invloed van SBR. In figuur 9.11 is het driehoeksbeheermodel schematisch weergegeven.



Figuur 9.11 – Driehoeksbeheermodel

De klantenkant (in de figuur links) richt zich allereerst op het stroomlijnen van de actuele vraag naar system-to-system informatieverwerking. Het perspectief van de horizontaal geïntegreerde verantwoordingsketens is aan de klantenkant dominant.

Deze kant geeft vanuit deze behoefte richting aan de vraag naar (door)ontwikkeling van de system-to-system informatieverwerking voor specifieke verantwoordingsketens. Vraagmanagement richt zich ten aanzien van de verantwoordingsketen op een adequate vraag-fulfillment.

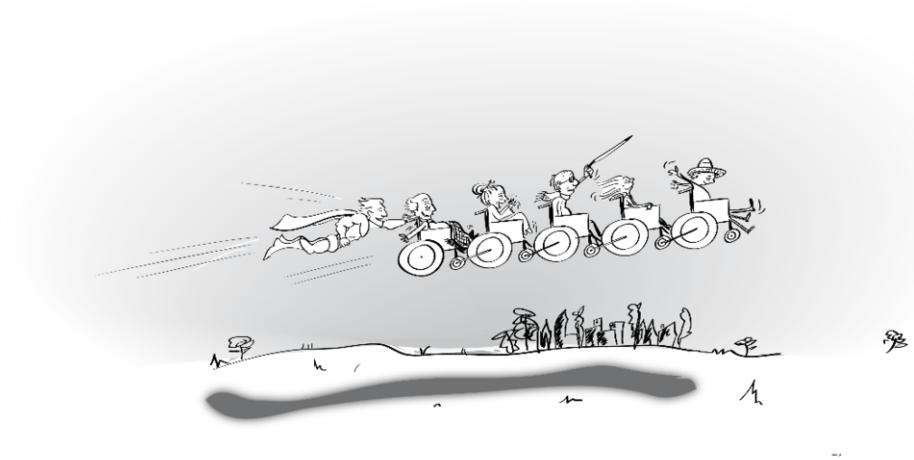
De leveringskant (in de figuur rechts) richt zich op het conform opdracht leveren van de generieke basisfuncties van de system-to-system informatieverwerking. Aan deze kant staat het perspectief van de verticale ketenintegratie centraal. Levering zorgt dat er een serviceorganisatie en infrastructuur operationeel is, die nodig is om voor verschillende verantwoordingsketens de system-to-system informatieverwerking te ondersteunen. De opdrachten voor dienstverlening worden verstrekt vanuit de klantenorganisatie en zijn altijd gekoppeld aan een specifieke (horizontaal geïntegreerde) verantwoordingsketen. De oplossing voor een verantwoordingsketen is opgebouwd uit generieke diensten (figuur 9.11 laat dit zien door de stippellijnen vanuit de verschillende diensten richting de klantenkant). Wanneer de system-to-system informatieverwerking in de keten verstoord wordt draagt leveringsmanagement bij aan het zo snel mogelijk normaliseren van de dienstverlening. Hierbij volgt levering de door de horizontaal geïntegreerde verantwoordingsketens gestelde kaders.

Architectuur zorgt ervoor dat de werkwijze van de hele beheerorganisatie beschreven is en aansluit bij het SBR afsprakenstelsel. Het aansluiten gebeurt enerzijds door het adopteren van deze standaarden, anderzijds wordt door het onderdeel architectuur ook actief geparticipeerd en een bijdrage geleverd in de standaardisatiegremia die van belang zijn voor SBR. Het onderdeel architectuur monitort de mate waarin de beschreven werkwijze en standaarden uit het kader gevolgd worden en maakt inschattingen van de consequenties van afwijkingen.

9.9 Afsluiting

Kijkend naar de SBR-context zien we drie vormen van integratie van keteninformatiesystemen: netwerkintegratie, horizontale integratie en verticale integratie. De verschillende vormen van integratie leiden tot verschillende afhankelijkheden waardoor er een behoefte ontstaat aan ketengovernance. Voor iedere vorm van integratie zijn andere uitgangspunten voor de ketengovernance aan de orde. Doordat de verschillende ketenpartners – en de gedeelde dienstverlener – in meerdere verantwoordingsketens actief zijn en dus een belang hebben bij de verschillende integratievormen, kan de besluitvorming verweven raken. Met name rond fundamentele wijzigingen doet deze vermenging zich voor. Doordat Logius zich kan specialiseren in de materie en doordat zij belangrijke onderdelen van de geïmplementeerde SBR-ketens onder haar hoede heeft, is zij bij uitstek een partij die het complexe speelveld kan overzien en kan orkestreren. In de praktijk zal het succes van de standaardisatie afhangen van de mate waarin Logius in staat blijkt te zijn om de benodigde autoriteitspositie te verwerven. De organisatie van de gedeelde dienstverlener moet dan wel op deze rol zijn ingericht. Logius heeft in het kader van SBR een driehoeksbeheermodel uitgewerkt, met een centrale rol voor architectuur om aan dit aspect invulling te geven. Verder maakt zij een duidelijk organisatorisch onderscheid in het klantenperspectief, waar de horizontaal geïntegreerde ketens centraal staan in de vorm van oplossingen, en het leveringsperspectief, waar vanuit de generieke diensten worden ontwikkeld en geleverd.

10 De SBR-verbredingsmethodiek



10.1 Inleiding

10.1.1 *Aanleiding*

SBR heeft zich ontwikkeld tot een standaard overheidsoplossing voor system-to-system verantwoording, waarmee publieke en private partijen onderdelen van hun verantwoordingsketen op efficiënte en effectieve wijze kunnen afhandelen. In de inleiding van dit boek zijn de voordelen van het breed toepassen van SBR in meerdere verantwoordingsketens benoemd. Zoals we in hoofdstuk 4 hebben gezien bestaat de ketenwijziging voor partijen die overgaan op SBR uit twee componenten. (I) Technologie: de ketenpartijen moeten voor de verantwoordingsketen gebruik gaan maken van de SBR-technologie (II) Governance: de ketenpartijen dienen aan te sluiten bij de ketengovernance op de verschillende integratievormen van SBR. Het wijzigingstraject van interesse in SBR tot een werkende SBR keten in productie vraagt om een methodische aanpak. Gedurende het traject dienen partijen onder andere gestructureerd inzicht te krijgen in de voordelen en kosten van SBR binnen hun verantwoordingsketen en de implementatie dient gecoördineerd te worden. Vanuit het SBR Programma is voor het traject een methodiek ontwikkeld, die in dit hoofdstuk besproken wordt. De SBR-verbredingsmethodiek is in eerste instantie bedoeld voor partijen die vanuit een overheidstaak geïnteresseerd zijn in de toepassing van SBR, maar heeft zeker relevante aspecten voor private ketens die met SBR aan de slag willen. Als basis voor dit hoofdstuk geeft deze inleiding allereerst een schets van de te realiseren B-situatie van SBR. De B-situatie is de gewenste te realiseren situatie, zie

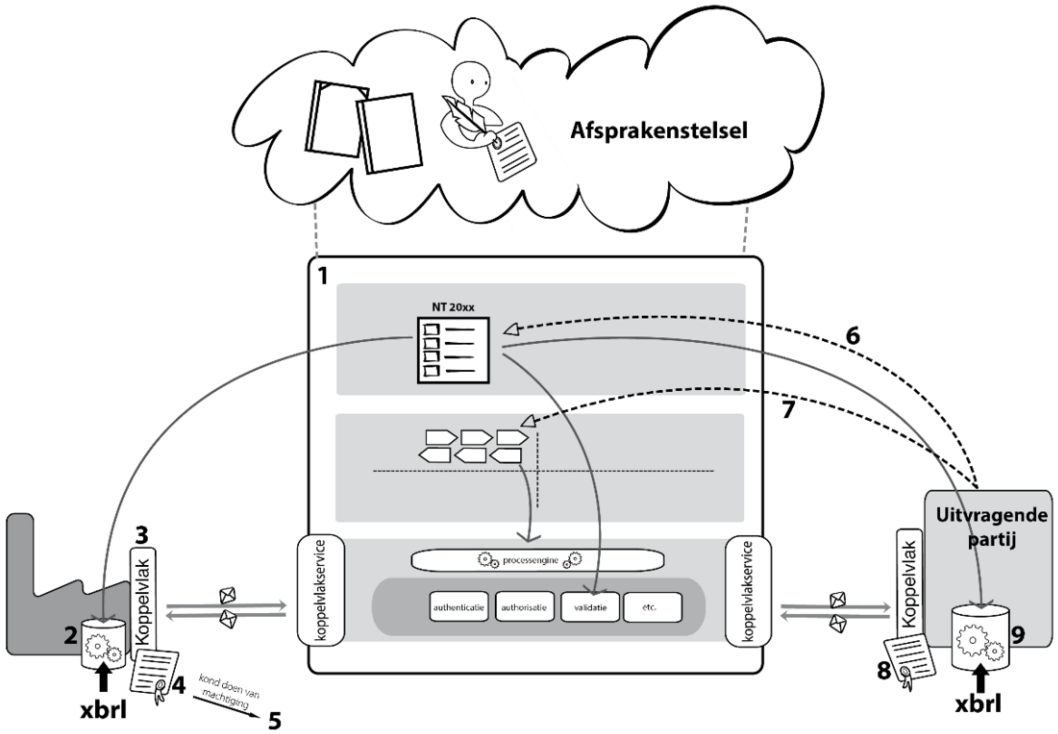
voor een uitgebreide toelichting van dit begrip hoofdstuk 3 en 4. De schets geeft de lezer direct gevoel over de reikwijdte van de methodiek. Na de geschetste B-situatie geeft de inleiding gestructureerd inzicht in het doel en de opzet van de methodiek en geeft het een leeswijzer voor de volgende onderdelen uit het hoofdstuk.

10.1.2 *Schets van de te realiseren B-situatie SBR*

De B-situatie voor een verantwoordingsketen die (mogelijk) gaat aansluiten op SBR is op voorhand al enigszins bekend. De verantwoordingsketen moet ingericht worden conform het SBR-afsprakenstelsel. Voor publieke uitvragende partijen levert Logius de gedeelde diensten die nodig zijn voor de generieke onderdelen van verantwoordingsketens gebaseerd, op wet en regelgeving. Voor zowel de SBR-technologie als de SBR-ketengovernance kan de toetreding van nieuwe ketens naast een uitbreiding ook een 'inhoudelijke' wijziging teweegbrengen. Stel je voor dat een partij er bijvoorbeeld op staat om inline XBRL te ondersteunen, iets dat thans nog niet past binnen de Nederlandse Taxonomie Architectuur (NTA). In dat geval worden de actoren die reeds aangesloten zijn op SBR ook geconfronteerd met een transitievraagstuk. Uitgangspunt is om zeker bij de initiële implementatie de inhoudelijke transitie van de generieke SBR onderdelen beperkt te houden.

10.1.3 *Te implementeren SBR-technologie*

Onderstaande figuur geeft de componenten weer die relevant zijn voor de implementatie van de SBR-technologie. Zij worden vervolgens nader toegelicht.

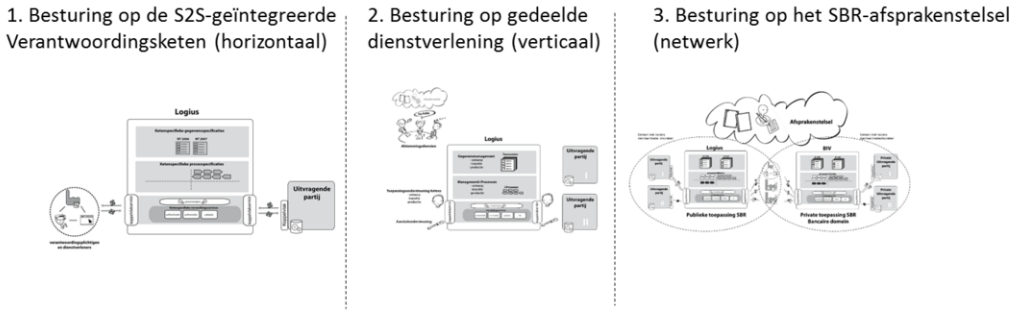


Figuur 10.1 – De B-situatie voor een verantwoordingsketen die (mogelijk) gaat aansluiten bij SBR

1. Logius, als Shared Service Center (SSC), levert de diensten om een partij te faciliteren bij het ontwerp en de implementatie van de verantwoordingsketen. Deze ondersteuning kan projectmatig geleverd worden.
2. De software aan de kant van de verantwoordingsplichtige moet aangesloten zijn op de gegevensstandaarden uit SBR. Wanneer software voor andere ketens al SBR toepast kan de impact van deze wijziging zeer beperkt zijn. Daarnaast moet er een mapping plaatsvinden van de onderdelen uit de Nederlandse Taxonomie (NT) die voor de specifieke verantwoordingsketen, bronsystemen van de aanleveraar/ontvanger van de verantwoordingsinformatie en mededelingen gelden. Wanneer een keten met name gebruik maakt van gegevens die al door anderen worden uitgevraagd heeft deze wijziging een beperkte impact.
3. De software aan de kant van de verantwoordingsplichtige moet aangesloten zijn op de SBR koppelvlakken die relevant zijn voor zijn verantwoordingsketen. Wanneer deze software voor andere ketens al aangesloten is op SBR koppelvlakken kan de impact van deze wijziging zeer beperkt zijn.
4. De partij die de verantwoordingsinformatie aanlevert en mededelingen hierover ontvangt moet in het bezit zijn van een PKIoverheidscertificaat. Wanneer de aanleverende/ontvangende partij voor andere ketens al aangesloten is op SBR koppelvlakken kan de impact van deze wijziging zeer beperkt zijn.
5. Indien er mededelingen van vertrouwelijke aard in een verantwoordingsketen worden uitgewisseld kan het zijn dat de aanleverende partij een machtigingsclaim moet opvoeren bij de Digipoort. Logius kan deze claim verifiëren bij de verantwoordingsplichtige partij. Dit is een specifieke handeling binnen de verantwoordingsketen.
6. De uitvragende partij dient een (extensie)taxonomie te maken voor de specifieke berichten uit de verantwoordingsketen. Deze extensie wordt in principe onderdeel van de Nederlandse Taxonomie en maakt waar mogelijk gebruik van elementen die reeds opgenomen zijn en voegt de elementen toe die nog geen onderdeel uitmaken van de Nederlandse Taxonomie.
7. De uitvragende partij dient in BPMN de i-processen te definiëren die Logius af gaat handelen. Hierbij vormen de bestaande koppelvlakservices en verwerkingsservices, alsmede de bestaande SBR referentieprocessen voor aanleveren en het ontvangen van mededelingen de basis.
8. De uitvragende partij moet in het bezit zijn van een PKIoverheidscertificaat. Wanneer de uitvragende partij voor andere ketens al aangesloten is op SBR koppelvlakken kan de impact van deze wijziging zeer beperkt zijn.
9. De verwerkingssoftware van de uitvragende partij moet aangesloten zijn op de gegevensstandaarden uit SBR. Wanneer de verwerkingssoftware al voor andere ketens toepast wordt, kan de impact van deze wijziging zeer beperkt zijn. Daarnaast moet er een mapping plaatsvinden van de onderdelen uit de Nederlandse Taxonomie die gelden voor de specifieke verantwoordingsketen en de verwerkingssystemen van de uitvragende partij.

10.1.4 *Te implementeren SBR-ketengovernance*

Onderstaande figuur illustreert de verschillende ketengovernance structuren waar de ketenpartijen uit een SBR-verantwoordingsketen mee te maken krijgen. Deze structuren zijn uitgebreid aan bod gekomen in hoofdstuk 9.



Figuur 10.2 – De ketengovernance structuren waar ketenpartijen uit een SBR-verantwoordingsketen in de B-situatie mee te maken krijgen

1. De voor de verantwoordingsketen verantwoordelijke uitvragende partij die over wil op SBR moet in principe de lead nemen op de inrichting van de besturing op de S2S-geïntegreede verantwoordingsketen. De implementatie van SBR zal met name vanuit deze besturingsstructuur vorm moeten krijgen. Bij een bestaande verantwoordingsketen zullen er al afstemmingsstructuren bestaan met ketenpartijen. Bij een papier-gebaseerde of H2S-gebaseerde keten zal een aanpassing in de besturing en agendapunten in het kader van de implementatie het logische gevolg zijn van de implementatie van SBR. De uitvragende partij moet beseffen dat sommige partijen uit de keten reeds betrokken kunnen zijn bij SBR-gremia voor andere verantwoordingsketens waar zij in deelnemen. In dit kader is het goed om gedurende het traject de samenhang tussen deze besturing op de verantwoordingsketen en de overige afstemming in het kader van SBR goed in de gaten te houden. Logius kan hierbij ondersteunen.
2. De uitvragende partij zal voor een deel van de verantwoordingsketen gebruik gaan maken van diensten van Logius. Dit doet iets met de business case van Logius als SSC en heeft hoogstwaarschijnlijk een positief effect op andere deelnemers. Wanneer de partij echter voor zijn keten een grote aanpassing wil in deze dienstverlening komen de andere afnemers in de hele opdrachtgeversstructuur ook met transitievraagstukken te zitten. De uitvragende partij zal als één van de afnemers in het afnemersoverleg van Logius plaatsnemen (thans nog het PLO SBR en de werkgroepen SBR) en daar op gelijkwaardig niveau kunnen deelnemen aan de besluitvormingsstructuren die hier thans voor gelden.
3. Als stakeholders van het afsprakenstelsel zal de uitvragende partij, maar wellicht ook andere ketenpartners, willen deelnemen aan de besturing op de doorontwikkeling van het SBR-afsprakenstelsel. Alle ketenpartijen kunnen deelnemen aan de expertgroepen en hun vertegenwoordiging regelen in het SBR-platform of het SBR-beraad. De uitvragende partij kan via de publieke ketengovernance (thans de SBR-Stuurgroep, PLO en Werkgroepen) met de overheidspartijen afstemmen over nadere standaardisatieafspraken in het kader van de publieke toepassing van SBR. Daarnaast wordt in deze gremia de beleidslijn ten aanzien van de publiek/private samenwerking afgestemd.

10.1.5 *Doel en opzet van de SBR-verbredingsmethodiek*

De SBR-verbredingsmethodiek (of: de methodiek) stelt partijen in staat om:

- gestructureerd de informatie boven water te krijgen die nodig is voor een gedegen besluitvorming over de implementatie en toepassing van SBR;
- duidelijke go/no go momenten te identificeren voor een verantwoord en gefaseerd programma om bij SBR aan te sluiten;
- SBR gecontroleerd te implementeren (technologie en ketengovernance) in de desbetreffende verantwoordingsketen, waarbij gebruik kan worden gemaakt van diensten die aangeboden worden door de gedeelde dienstverlener Logius;
- voort te bouwen op reeds aanwezige kennis en ervaring over de route die dient te worden afgelegd bij de (her)inrichting van verantwoordingsketens.

Het startpunt van een verantwoordingsketen die (mogelijk) gaat aansluiten bij SBR is altijd anders. Denk hierbij onder andere aan de technische, politiek-bestuurlijke, historische, wettelijke en organisatorische kenmerken van de bestaande keten. Voor iedere verantwoordingsketen dient er een uniek traject doorlopen te worden. De methodiek laat dan ook ruimte voor deze keten-specifieke aanpak doordat partijen zelfstandig de route kunnen bepalen die voor hun keten doorlopen wordt. Wel biedt de methodiek een viertal fasen, waarmee voor iedere fase go/no go beslissingsmomenten zijn geïdentificeerd en ketenpartijen de kwaliteit van de voortgang kunnen waarborgen langs checkpoints. Tevens reikt de SBR-verbredingsmethodiek een inhoudelijke leidraad aan waarlangs partijen de fasen doorlopen. Bovendien worden voor iedere fase do's en don'ts aangegeven. We raden ketenpartijen aan bij het bepalen van de route gebruik te maken van bestaande projectmanagement methodieken (Prince2) en programmamethodieken (Managing Successful Programmes).

Het is belangrijk om aan te geven dat het aflopen van de methodiek niet als 'winnend kant-en-klaar recept' kan worden beschouwd voor de betrokkenen bij het verbredingstraject. Het valt te verwachten dat het traject gepaard gaat met complexe vraagstukken. Kritische succesfactor in het traject is of de betrokken personen in staat blijken te zijn dergelijke vraagstukken te doorgronden en op een goede manier weten op te lossen. Van hen wordt gevraagd dat zij een uitmuntende prestatie leveren wanneer zij acteren in de diverse domeinen (onder andere bestuurlijk, organisatorisch, technisch en juridisch zowel publiek als privaat). Dit vereist dat zij verstand van zaken hebben, elkaar weten te vinden en een beroep kunnen doen op elkaars professionaliteit, gevoel van eigenaarschap, creativiteit en doorzettingsvermogen.

Dit hoofdstuk zet als volgt voort. De volgende paragraaf beschrijft de SBR-verbredingsmethodiek op hoofdlijnen. Vervolgens wordt iedere fase die ketenpartijen doorlopen afzonderlijk in meer detail behandeld. Dit zijn de interessefase, de detailanalyse- en herontwerpfase, het experiment en de opschaling. Ten slotte vindt er reflectie plaats op de methodiek en trekken we conclusies.
De in dit hoofdstuk gehanteerde begrippen worden toegelicht, maar voor zover ze betrekking hebben op onderdelen van SBR verwijzen we voor een bredere uiteenzetting naar de daarvoor geëigende, specifieke hoofdstukken. Tot slot raden wij de lezer die geïnteresseerd is in de hierna behandelde materie om ook de hoofdstukken 3, 4

en 9 tot zich te nemen, aangezien deze hoofdstukken complementaire inzichten bevatten die voor dit hoofdstuk relevant zijn.

10.2 De SBR-verbredingsmethodiek op hoofdlijnen

In de SBR-verbredingsmethodiek geven ketenpartijen zelf invulling aan de route die zij doorlopen teneinde SBR te implementeren. De route die ketenpartijen afleggen doorloopt wel altijd vier fasen. Dit wordt beschreven in § 10.2.1. Tevens reikt de SBR-verbredingsmethodiek een inhoudelijke leidraad aan waarlangs partijen de fasen doorlopen. Dit wordt beschreven in § 10.2.2.

10.2.1 *De route doorloopt vier fasen*

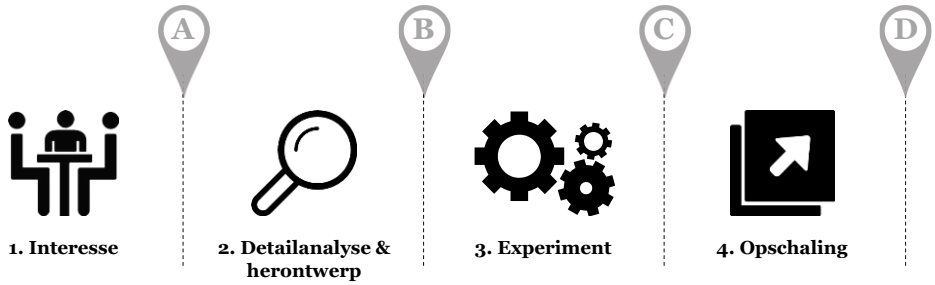
De route die ketenpartijen afleggen ten einde SBR te implementeren doorloopt altijd vier fasen; de interessefase, de detailanalyse- en herontwerpfase, experimentfase en opschalingsfase. De eerste fase is de interessefase. De interessefase vangt aan wanneer partijen interesse tonen in SBR en in dit kader contact hebben met functionarissen van de gedeelde dienstverlener Logius. De interessefase beoogt laagdrempelig inzichtelijk te maken of een verantwoordingsketen geschikt is voor de toepassing van SBR. Dit gebeurt aan de hand van een Quick Scan. Uit de Quick Scan volgt een advies om al dan niet een gedetailleerde analyse en herontwerp uit te voeren. Indien het antwoord ja is - wordt tevens de SBR-ambitie voor één of meerdere verantwoordingsketens vastgesteld. De ambitie wordt in de volgende fase vertaald in een roadmap met een duidelijke doelstelling.

De tweede fase is de detailanalyse- en herontwerpfase. De fase vangt aan wanneer uit de Quick Scan blijkt dat de toepassing van SBR in potentie voordelen met zich meebrengt. Op basis van de Quick Scan kan er een herontwerp gemaakt worden van de gewijzigde verantwoordingsketen. Het herontwerp bestaat in ieder geval uit een extensietaxonomie, een procesontwerp van een i-proces in BPMN, een toepassingsondersteuningsketen en een marktbewerkingsplan. Voor dit plan is het essentieel dat de uitvragende partij vaststelt welke rol de SBR-verantwoordingsketen (in de tijd) gaat spelen in de totale verantwoordingsbehoefte van een uitvragende partij. Het is goed denkbaar dat een uitvragende partij SBR alleen voor een bepaalde groep verantwoordingsplichtigen in wil zetten. Wat betreft de ketengovernance is het van belang dat de partijen in de verantwoordingsketen ook komen tot een visie op een goede aansluiting bij de SBR gremia en de eigen besturing voldoende toereikend vormgeven (in opzet). Door het uitvoeren van de detailanalyse, het opstellen van een implementeerbaar herontwerp van de verantwoordingsketen(s) en een concrete roadmap is de benodigde informatie voor een gedegen besluitvorming verzameld. Tevens zijn de ketenpartijen klaar om het herontwerp te testen.

Het besluit om te starten met de derde fase (het experiment) is binnen de methodiek het meest cruciale. De verantwoordende en dienstverlenende partijen die gaan werken volgens SBR in het experiment zullen in toenemende mate vragen om duidelijkheid over het toekomstige beleid om de te maken investeringen te kunnen verantwoorden. Om verwachtingen goed te managen, dient het uitgangspunt bij aanvang van het experiment te zijn dat *als het experiment zonder substantiële problemen verloopt, de toepassing van SBR binnen de verantwoordingsketen de aankomende*

jaren wordt doorgezet met als doel SBR binnen één tot drie jaar toe te passen conform de ambitie die voor de keten(s) gesteld is. Dit vraagt om een visie én het betekent dat er in feite in dit stadium voldoende draagvlak dient te zijn voor de toepassing van SBR binnen de verantwoordingsketen onder de belangrijkste ketenpartijen (met als voornaamste partij de uitvragende partij en eventuele beleidsopdrachtgevers). Binnen de methodiek is dit de eerste van de twee acceptatiedrempels die ketenpartijen tegenkomen. Als er voldoende acceptatie voor de toepassing van SBR onder de belangrijkste ketenpartijen is, voeren ketenpartijen het experiment uit. Dit is de derde fase. Het experiment wordt gebruikt om het herontwerp te testen. Partijen die voor de keten voor het eerst op SBR aangesloten zijn kunnen testen of de aansluiting op SBR is gelukt. Indien er nieuwe technische services zijn ontwikkeld voor de procesinfrastructuur van Logius, kunnen deze ook getest worden. In deze fase kunnen de laatste 'kinderziektes' in de nieuwe keten verholpen worden. Door het experiment tonen ketenpartijen aan dat de verantwoordingsketen technisch functioneert. Als het experiment probleemloos verloopt dan ligt het in de lijn der verwachting dat de toepassing van SBR binnen de verantwoordingsketen conform ambitie geïmplementeerd kan worden. Gedurende de fase van het experiment dient de besturing op het implementatieprogramma langzaam maar zeker over te gaan in de ontworpen ketengovernance.

Tijdens de vierde en laatste fase – de opschaling – worden de beoogde gebruikers stapsgewijs aangesloten bij SBR. Het aansluiten van gebruikers vormt de tweede acceptatiedrempel die ketenpartijen tegenkomen. Zoals in hoofdstuk 4 is toegelicht, dienen alle partijen die tot de beoogde doelgroep horen SBR te implementeren om een ambitie waar te maken. Een reeds functionerende keten vanuit het experiment speelt een belangrijke rol om aan te tonen dat de toepassing van SBR mogelijk is. Net zo belangrijk is dat de gedeelde dienstverlener – Logius – de partijen die nog niet aangesloten zijn op SBR ondersteunt bij de aansluiting op SBR. Het SBR-verbredingstraject is ten einde wanneer de ambities voor de keten gerealiseerd zijn. De vier te doorlopen fasen zijn weergegeven in figuur 10.3.



Figuur 10.3 – De vier te doorlopen fasen en bijbehorende checkpoints ten einde SBR te implementeren in een keten

Voor iedere fase zijn specifieke doelen en een aanpak vastgesteld (zie § 10.3 t/m § 10.6). Gedurende de route komen ketenpartijen checkpoints tegen. De checkpoints zijn in de bovenstaande figuur weergegeven als zijnde A t/m D. Een checkpoint markeert zowel de afronding van de fase als het startpunt van de volgende fase. Een checkpoint dient de volgende twee functies:

1. De eerste functie van een checkpoint is om binnen elke fase (met uitzondering van de laatste fase) binnen de SBR-verbredingsmethodiek te komen tot een **go/no go** beslissing om de route al dan niet voort te zetten. De inzet van dergelijke keuzemomenten helpt de ketenpartijen om te toetsen of de ingezette koers het beoogde resultaat heeft opgeleverd en gaat opleveren.
2. De tweede functie van een checkpoint is om voor aanvang van de aankomende fase ervan verzekerd te zijn dat de vorige fase met de juiste diepgang, scope en kwaliteit is doorlopen. Ook kan het checkpoint 'zachtere' eisen stellen. Checkpoint B stelt bijvoorbeeld als vereiste dat vóór aanvang van het experiment er voldoende draagvlak is onder de belangrijke ketenpartijen voor de geambieerde toepassing van SBR.

Naast de vier fasen biedt de SBR-verbredingsmethodiek tevens een inhoudelijke leidraad. De inhoudelijke leidraad zal in de volgende paragraaf worden besproken.

10.2.2 *Inhoudelijke leidraad gedurende de route*

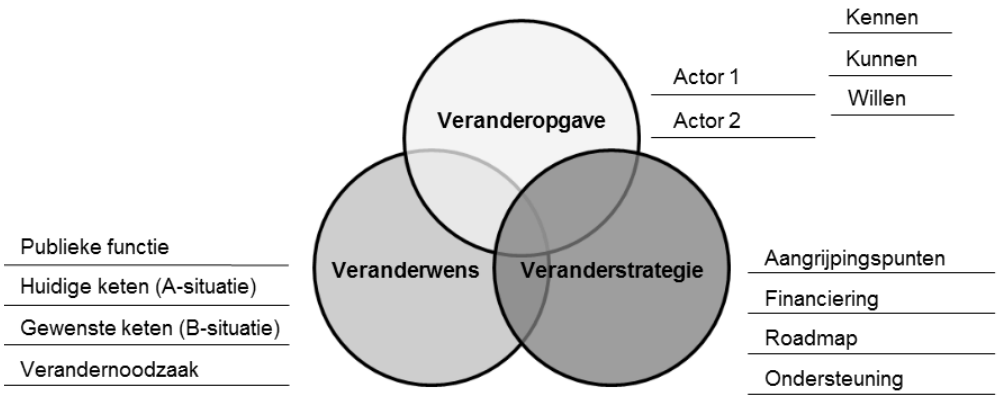
De ketenpartijen doorlopen de route teneinde SBR te implementeren langs een inhoudelijke leidraad. Deze inhoudelijke leidraad dient twee doelen. Ten eerste, zorgt de leidraad ervoor dat de informatie die nodig is voor een gedegen besluitvorming boven water komt. Ten tweede zorgt de leidraad ervoor dat de informatie die nodig is voor een gecontroleerde implementatie voorhanden is. Naast een ontwerp dat voldoet aan de gestelde eisen doelen we daarmee tevens op het verkrijgen van acceptatie van de betrokken partijen.

Voor een uitgebreide behandeling van het thema acceptatie verwijzen we naar hoofdstuk 3 en hoofdstuk 4. Waar in deze hoofdstukken de concepten uit de literatuur meer theoretisch zijn behandeld, hebben in dit hoofdstuk de concepten hun weerslag in de inhoudelijke leidraad die meer praktisch van opzet is. De inhoudelijke leidraad bestaat uit een set van karakteristieken van ketenverandering. Dit zijn:

1. De veranderwens. De veranderwens bestaat uit het verschil tussen de A-situatie en de B-situatie bij de invulling van de publieke functie van de verantwoordingsketen. Het verschil wordt inzichtelijk gemaakt langs de lijnen: processen (hoofdstuk 5) –gegevens (hoofdstuk 6) –techniek (hoofdstuk 7/8), gezamenlijk de dimensie technologie en de dimensie ketengovernance (hoofdstuk 9). Ook wordt er gekeken naar ontwikkelingen en factoren die van invloed zijn op de verandernoodzaak. De ambitie voor de B-situatie is vervolgens het centrale richtpunt. Het gaat hier om de vraag: hoeveel van de verantwoordingsinformatie uit welke ketens wordt op welk moment via SBR ontvangen?
2. De veranderopgave. De veranderopgave wordt per actor bekeken waarbij er onderscheid wordt gemaakt in het kennen, kunnen en willen langs de dimensies technologie en ketengovernance (zie tevens hoofdstuk 4). Tevens wordt er rekening gehouden met de opgave volgend uit de coördinatie van de inspanningen van de actoren.
3. De veranderstrategie. De veranderstrategie bestaat uit de strategie om de gewenste ketenverandering te realiseren. Daartoe wordt onderscheid gemaakt in:
    a. Aangrijpingspunten om de verandering in te zetten, bijvoorbeeld een specifieke verantwoordingsstroom of te betrekken partijen waarlangs de verandering kan worden aangevangen.

b. De financiering van de verandering.
c. De roadmap, het plan waarin de implementatie van SBR in een aantal plateaus en bijbehorende doorlooptijden kan worden gerealiseerd.
d. De ondersteuning van actoren ten aanzien van het kennen en kunnen (zie hoofdstuk 4) en de aangeboden diensten door de gedeelde dienstverlener Logius.

Deze karakteristieken van ketenverandering zijn weergegeven in de onderstaande figuur.



Figuur 10.4 – Set van samenhangende karakteristieken van ketenverandering als inhoudelijke leidraad bij de route

De ketenpartijen onderzoeken steeds de set van karakteristieken zoals weergegeven in figuur 10.4 in samenhang. Voor een succesvolle implementatie is het noodzakelijk dat de veranderwens in verhouding staat tot de opgave die is gemoeid met de ketenverandering per actor en dat de ketenpartijen de gekozen veranderstrategie toereikend achten om de ketenverandering te realiseren.

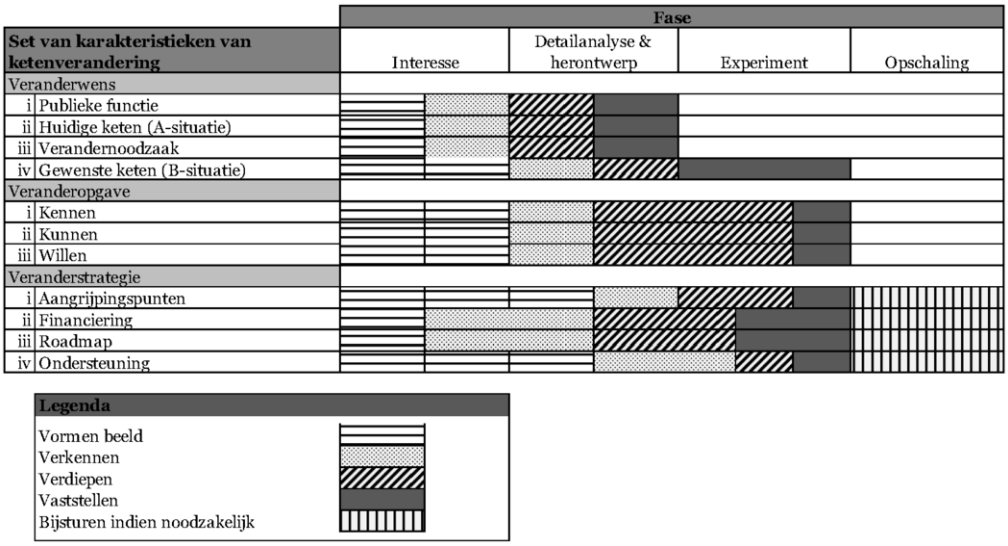
Door keuzes te maken (denk hierbij aan de scope, de functionaliteiten, de betrokken partijen, de aangeboden ondersteuning, de gekozen doorlooptijden en de samenhang met andere projecten) kunnen partijen de veranderwens, de veranderopgave en de veranderstrategie voortdurend op elkaar afstemmen teneinde de samenhang te waarborgen. Dergelijke keuzes zijn op voorhand onmogelijk te voorspellen en kunnen dus een groot beroep doen op de betrokken personen (zie tevens de inleiding van dit hoofdstuk).

Door de veranderwens, veranderopgave en veranderstrategie zo expliciet mogelijk te bespreken, wordt impliciet aanwezige kennis over de keten van experts expliciet gemaakt. Bijkomend voordeel is dat de betrokken ketenpartijen vanaf de eerste dag hun ketenbewustzijn vergroten.

Iedere fase – zoals die in de vorige paragraaf zijn besproken – legt de nadruk op andere karakteristieken. De interessefase richt zich op het verkennen van de pu-

blieke functie, de huidige situatie (A-situatie) en de verandernoodzaak. De detailanalyse- en herontwerpfase richt zich op het vaststellen van de A-situatie, het verdiepen van de B-situatie, de veranderopgave en enkele onderdelen van de veranderstrategie (zoals de financiering). Gedurende het experiment wordt de gewenste keten, de veranderopgave en de veranderstrategie vastgesteld. In de opschaling houden de ketenpartijen zich in principe aan de vastgestelde veranderstrategie, tenzij uitzonderingen en/of onverwachte gebeurtenissen het noodzakelijk maken om bij te sturen.

De onderstaande figuur geeft een overzicht van de nadruk die iedere fase legt op de verschillende karakteristieken.



Figuur 10.5 – De nadruk per fase op de karakteristieken van ketenverandering

In iedere fase onderzoeken de ketenpartijen met meer detail en diepgang de karakteristieken van de ketenverandering. De onderstaande tabellen geven een beeld van generieke vragen aangaande de karakteristieken waar ketenpartijen naar op zoek gaan gedurende het traject. Met iedere fase kunnen ketenpartijen meer vragen beantwoorden. Ook kunnen zij gedetailleerder antwoord geven op de vragen. Het aantal generieke vragen voor de karakteristieken veranderopgave en veranderstrategie is beperkt, omdat de vragen die gesteld zouden moeten worden sterk afhangen van de verkregen inzichten gedurende het traject en op voorhand dus lastig te voorspellen zijn.

Gedurende een verbredingstraject kan er worden voortgebouwd op reeds aanwezige kennis vanuit andere verbredingstrajecten. Zo kan bijvoorbeeld voor ketens waarbij sprake is van een accountantscontrole (waarbij de big 4 en de Raad van de Jaarverslaggeving terugkerende partijen zijn) de actoranalyse deels hergebruikt worden.

Ten aanzien van de publieke functie van verantwoording als onderdeel van de veranderwens dienen ketenpartijen te zoeken naar antwoorden op onder andere de onderstaande vragen.

Tabel 10.1 – Relevante vragen omtrent de veranderwens

Veranderwens		
Onderdeel		Relevante vragen
Publieke functie verantwoording	Functie verantwoording	• Welk doel dient het aanleveren van verantwoordingsinformatie? • Welke eisen stelt het doel van het aanleveren van verantwoordingsinformatie aan de kwaliteit, tijdigheid en betrouwbaarheid van verantwoordingsinformatie?
	Wettelijke grondslag verantwoording	• Wat is de wettelijke grondslag van de verantwoordingsverplichting van aanleverende partijen? • Welke wettelijke basis ligt er ten grondslag aan de uitvraag van verantwoordingsinformatie door uitvragende partijen?
	Compliance vereisten	• Welke vereisten volgen uit de Wet elektronisch bestuurlijk verkeer? • Welke vereisten volgen uit de (ongeschreven) Algemene beginselen van behoorlijk bestuur? • Welke vereisten volgen uit de Archiefwet 1995 en onderliggende regelingen? • Welke vereisten volgen uit de Wet bescherming persoonsgegevens? • Welke vereisten volgen uit de Dienstenwet? • Welke vereisten volgen uit de Mededingingswet en het Besluit markt en overheid? • Welke vereisten volgen uit de Telecommunicatiewet? • Welke vereisten volgen uit de wet algemene bepalingen burgerservicenummer? • Welke vereisten volgen uit de Richtlijnen voor de Jaarverslaggeving en BW2? • Welke vereisten volgen uit normenkaders t.a.v. assurance? • Welke vereisten volgen uit de voorschriften voor informatiebeveiliging voor de overheid? • Welke vereisten volgen uit sector-specifieke wet- en regelgeving?

Ten aanzien van de huidige keten als onderdeel van de veranderwens dienen ketenpartijen te zoeken naar antwoorden op onder andere de vragen in tabel 10.2.

Tabel 10.2 – Relevante vragen voor de huidige keten (A-situatie)

Veranderwens	
Onderdeel	Relevante vragen omtrent de huidige keten (A-situatie)
Ketenorganisatie	• Wie zijn de uitvragende partijen in de verantwoordingsketen? • Wie zijn de beleidsverantwoordelijken? • Wie zijn de aanleverende partijen in de verantwoordingsketen? • Welke dienstverleners en intermediairs zijn actief in de verantwoordingsketen (accountants, softwareleveranciers, administratiekantoren)? • Welke overige publieke partijen zijn betrokken (inspectie, uitvoeringsinstantie, etc)? • Welke koepelorganisaties zijn betrokken (brancheverenigingen, etc)? • Welke overige partijen zijn betrokken (Raad voor de Jaarverslaggeving, etc.)? **Voor (semi-)publieke partijen:** • Wat is de (publieke) taak van de organisatie? • Welke wet- en regelgeving ligt er ten grondslag aan het uitvoeren van de publieke taak? • Wat is de financiële en maatschappelijke impact van de bedrijfsvoering van de organisatie? • Hoe zeker is de taakstelling en het budget van de overheidspartijen? • Wat zijn relevante historische gebeurtenissen van waaruit de A-situatie verklaard kan worden? • Welke aanvullende (publieke) taken zijn er ten aanzien van de verantwoording? • Hoe groot is de pluriformiteit in termen van o.a. cultuur, omvang (budget, FTE)? • Is informatieverwerking de 'core business'? **Voor private partijen:** • Van welke marktvorm is er sprake (monopolie, oligopolie, polypolie / aantal aanbieders en afnemers)? • Welke eisen worden gesteld aan toetreders (technisch, juridisch)? • Wat is het verloop van actoren? • Hoe groot is de pluriformiteit in termen van o.a. cultuur, omvang (omzet, FTE), strategie, verdienmodel, klanten? • Is informatieverwerking de 'core business'? • Nemen er aanleverende partijen deel welke in het buitenland gevestigd zijn, of zelf een buitenlandse entiteit zijn?
Keten governance	• Is er sprake van een centrale ketengovernance of formele overlegstructuren? • Welke actoren en belanghebbenden maken deel uit van de ketengovernance of de formele overlegstructuren? • Welke informele overlegstructuren zijn er? • Hoe worden wijzigingen in de keten doorgevoerd? • In hoeverre worden beslissingen in samenspraak genomen of van bovenaf opgelegd? • Hoe zijn de machtsverhoudingen binnen de keten? • Zijn de gemaakte afspraken informeel/zacht of formeel/hard? • Wat zijn de consequenties als actoren zich aan de gemaakte afspraken onttrekken? • In hoeverre zien de actoren dat zij deel uit maken van een keten of is hun blik meer beperkt tot de schakel? • In hoeverre zijn er convenanten of overeenkomsten van toepassing? • In hoeverre spelen (internationale) normenkaders of afsprakenstelsels een rol? • Waar zien de afspraken op (standaarden, techniek, proces, gegevensmodel)? • Welke wederzijdse afhankelijkheden zijn er binnen een keten en hoe worden deze geborgd? • In hoeverre worden processen en wijzigingen op elkaar afgestemd? • Wie ziet er toe op de naleving van de verantwoordingsverplichting van aanleverende partijen? • Welke partij regelt de openstelling van het elektronische aanleverkanaal?

Processen	• Welke berichtenstromen zijn er te onderscheiden? • Hoe hangen de berichtenstromen met elkaar samen (incorporeer tevens andere verantwoordingsdomeinen)? • In hoeverre maken de berichtenstromen gebruik van dezelfde schakels binnen de keten? **Per berichtenstroom:** • Hoe worden de te rapporteren gegevenselementen vastgesteld? • Hoe worden de te rapporteren gegevenselementen gepubliceerd? • Hoe worden de aanlevermodaliteiten beschikbaar gesteld? • Bestaan er verschillende routes voor dezelfde informatie-uitvraag? • Op welke manier wordt er toegang verleend tot de elektronische weg? • Op welke manier worden de uitgevraagde gegevens geregistreerd, opgeslagen en verzameld binnen de aanleverende partij? • Welke handelingen worden daarbij uitgevoerd door medewerkers, en welke door IT-systemen? • Hoe verloopt de samenwerking met de accountant (indien van toepassing)? • Wie zijn de verschillende proceseigenaren? • Hoe komt de beveiligde verbinding tot stand? • Is er sprake van een enkelvoudige stroom of een conversatie/dialoog? • Worden er ook mededelingen gedaan? • Worden retourstromen gepusht of door de ontvanger geïnitieerd/ opgehaald? • Volgen mededelingen op een aangeleverd bericht of is er een andere ontstaansreden? • Welke stappen bij de gegevensverwerking worden doorlopen? • Zijn er schakels of stappen in de keten die optioneel zijn? • Hoeveel berichten zijn er per jaar te verwachten? • Wat is de frequentie van berichten? • Zijn er bepaalde piekmomenten of deadlines? • Worden er in de keten business rules uitgevoerd en zo ja, op welke momenten? • Wat gebeurt er als er fouten in de aanlevering blijken te zitten? • Wat gebeurt er als er een fout in het proces optreedt? • Worden de verantwoordingsgegevens ter beschikking gesteld aan het maatschappelijk verkeer, en zo ja, op welke wijze? • Wat gebeurt er als aanleverende partijen hun verantwoordingsverplichting niet nakomen?
Gegevens	• Wat is de inhoud van de aangeleverde berichten en op welke punten is de inhoud voor meerdere verantwoordingsstromen (soort)gelijk? • Welke informatie wordt op papier aangeleverd en welke informatie digitaal? • In welk format worden digitale gegevens aangeleverd? • Kennen de rapportages een vaste berichtopzet? • Gebruiken alle actoren dezelfde berichtopzet? • Is er een centraal gegevensmodel en door wie wordt dit beheerd? • Kennen de digitale berichten een vaste syntax? • Biedt deze syntax de gewenste mate van standaardisatie enerzijds en vrijheid anderzijds? • Met welke regelmaat verandert de syntax? • Hechten alle actoren dezelfde betekenis aan dezelfde definities (semantiek)? • Worden definities onderling afgestemd en uitgewisseld? • Met welke regelmaat verandert de set van gebruikte definities? • Is het mogelijk geautomatiseerd de berichten te controleren op volledigheid en syntax? • Worden er elementen uitgevraagd die reeds in de NT zijn opgenomen?

Techniek	• Verwerken aanleverende partijen de verantwoordingsgegevens reeds geautomatiseerd? Zo nee, ligt er in de branche een business case voor de geautomatiseerde verwerking? • Verwerken uitvragende partijen de verantwoordingsgegevens reeds geautomatiseerd? • Bestaat reeds de mogelijkheid tot het system-to-system uitwisselen van verantwoordingsgegevens? • Hoe komt de (beveiligde) verbinding tot stand? • Wat is de omvang van de uitgewisselde berichten (aantal en grootte)? • Welke eisen worden er gesteld aan de berichtuitwisseling in termen van aanlevertijdvakken, verwerkingstijden en juistheid van verwerking? • Kunnen meerdere entiteiten waarover verantwoording moet worden afgelegd in een bericht opgenomen worden of moeten deze apart worden aangeleverd? • Hoe omvangrijk en volwassen is de IT-ondersteuning en bijbehorende procedures? • Hoe zijn waarborgen m.b.t. informatiebeveiliging genomen? • Wat is de kwaliteit van de in de verschillende schakels gebruikte software? • Is de gebruikte software in eigen ontwikkeling of ingekocht? • Hoe stabiel (in control) is de huidige IT-ondersteuning van de actoren?
Kosten-effectiviteit	• Hoe groot zijn de uitvoeringslasten van de verantwoordingsketen bij publieke partijen (bij benadering)? • Is er inzicht in de kostenstructuur en zo ja, welke inspanningen worden er gedefinieerd en hoe weerhouden de kosten voor beheer, doorontwikkeling en niet- toegeschreven kosten zich tot elkaar? • Vanuit welke partij(en) wordt het budget verschaft? • Hoe groot zijn de nalevingskosten van verantwoording bij aanleverende partijen (bij benadering)? • Hoe groot zijn de totaalkosten binnen verantwoordingsketen (bij benadering)? • In welke mate stelt de verkregen informatie in de huidige verantwoordingsketen de uitvragende partijen in staat om hun taken uit te voeren en geeft de verantwoordingsketen invulling aan de publieke functie in brede zin (effectiviteit)? • In welke mate worden binnen de verantwoordingsketen mensen en middelen doelmatig ingezet (efficiëntie)? • Staat het huidige doelbereik in redelijke verhouding tot de huidige kosten (kosteneffectiviteit)? • Valt te verwachten dat het toekomstige doelbereik in redelijke verhouding staat tot de toekomstige kosten?

Ten aanzien van de verandernoodzaak als onderdeel van de veranderwens dienen ketenpartijen te zoeken naar antwoorden op onder andere de onderstaande vragen.

Tabel 10.3 – Relevante vragen omtrent de verandernoodzaak

Veranderwens		
Onderdeel		Relevante vragen
Verandernoodzaak	Push-factoren	• In hoeverre is er momenteel sprake van een kosteneffectieve keteninrichting? • Zijn er substantiële knelpunten binnen de huidige keteninrichting die veranderingen binnen de verantwoordingsketen noodzakelijk maken? • Zijn er ontwikkelingen op nationaal niveau die veranderingen binnen de verantwoordingsketen noodzakelijk maken (maatschappelijke ontwikkelingen, omgevingsontwikkelingen, politieke ontwikkelingen, economische ontwikkelingen)? • Is er gewijzigde (sectoroverstijgende) wet- en regelgeving die veranderingen binnen de verantwoordingsketen noodzakelijk maakt? • Staat dit domein (tijdelijk) onder politieke of maatschappelijke aandacht? (e.g. als gevolg van gebrek aan transparantie)? • Bestaat er draagvlak voor de verantwoording of staat deze ter discussie? • Bestaat uit vanuit bepaalde actoren een verandernoodzaak (e.g. onhoudbaar business model)?
	Pull-factoren	• Is het domein aan inhoudelijke veranderingen onderhevig, bijvoorbeeld door vorderingen in technologie (e.g. opkomst ERP, SaaS, open data)?

		• Kan er synergie worden behaald door het voeren van regie over meerdere verantwoordingsstromen (verlaging administratieve lasten)? • Hoe groot zijn de voordelen voor uitvragende partijen door het gebruik van shared services bij de gedeelde dienstverlener Logius (o.a. kostendeling, volwassen dienstverlening, compliance by design, waarborgen op informatiekwaliteit door geautomatiseerde controles vroeg in de keten)? • Welke potentiele kansen ontstaan voor marktpartijen (e.g. introductie diensten en producten)? • Welke overige potentiele baten zijn er (o.a. vergelijkbaarheid data)?

Ten aanzien van de B-situatie als onderdeel van de veranderwens dienen ketenpartijen te zoeken naar antwoorden op onder andere de onderstaande vragen.

Tabel 10.4 – Relevante vragen voor de gewenste keten (B-situatie)

Veranderwens	
Onderdeel	Relevante vragen gewenste keten (B-situatie)
Ketenorganisatie	• Uit welke schakels en betrokken partijen bestaat de toekomstige verantwoordingsketen? • Wat zijn de overige relevante betrokken partijen rondom de keten?
Ketengovernance	• Welke partijen worden op welke wijze opgenomen in de SBR-ketengovernance?
Processen	• Hoe gaan de verantwoordingsprocessen lopen in de toekomstige keten?
Gegevens	• Welke elementen staan in de toekomstige taxonomie?
Techniek	• Van welke verwerkingsservices gaat gebruik worden gemaakt?
Kosten-effectiviteit	• Hoe groot zijn de uitvoeringskosten van SBR (bij benadering)? • Wat is de kostenstructuur van de uitvoeringskosten (bij benadering)? • Vanuit welke partij(en) gaat het budget worden verschaft?

Ten aanzien van de veranderopgave dienen ketenpartijen te zoeken naar antwoorden op onder andere de onderstaande vragen.

Tabel 10.5 – Relevante vragen omtrent de veranderopgave

Veranderopgave	
Onderdeel	Relevante vragen
Kennen (per actor)	• Is de ketenactor bekend met de technologie die gebruikt wordt binnen SBR? • Is de ketenactor bekend met de afstemmingsgremia van SBR? • Is de ketenactor bekend met S2S-integratie van informatieketens/verantwoordingsketens? • Heeft de ketenactor zekerheid over de interne voorwaarden en impact van de implementatie van de technologie van SBR? • Heeft de ketenactor zekerheid over de interne voorwaarden en impact van de implementatie van de ketengovernance van SBR?
Kunnen (per actor)	• Benodigde competenties en capaciteit: • Is de actor reeds actief in ketens waar SBR bestaat of geïntroduceerd wordt? • Heeft de actor in het verleden verandertrajecten doorlopen van vergelijkbare omvang en wat waren de resultaten van voorgaande verandertrajecten? • Kan de actor de benodigde capaciteit vrijmaken? • Benodigde middelen: • Hoe verhoudt de benodigde investering zich tot het budget of omzet? • Kunnen de benodigde middelen beschikbaar worden gemaakt?
Willen (per actor)	• Welke doelen heeft de ketenpartij zichzelf gesteld? • Levert de implementatie van SBR een bijdrage aan het behalen van deze doelen? • Welke alternatieven zijn er voorhanden om de doelen te bereiken? • Draagt de implementatie van SBR bij aan het kosteneffectief behalen van de door de ketenpartij gestelde doelen?

Actoroverstijgend	• Welke afhankelijkheden bestaan er tijdens de implementatie waarmee rekening gehouden moet worden? • Welke activiteiten van ketenactoren moeten tijdens de implementatie achtereenvolgens of parallel plaatsvinden? • Wie coördineert de activiteiten van actoren?

Ten aanzien van de veranderstrategie dienen ketenpartijen te zoeken naar antwoorden op onder andere de onderstaande vragen.

Tabel 10.6 – Relevante vragen omtrent de veranderstrategie

Veranderstrategie	
Aangrijpingspunten	• Is er een verantwoordingsstroom die zich bij uitstek leent voor de toepassing van SBR? • Welke partijen willen een koploper-positie innemen? • Voor welke onderdelen van de keten is de verandernoodzaak hoog? • Waar kunnen door de implementatie van SBR snelle opbrengsten worden geboekt tegen minimale inspanningen (quick-wins)? • Op welke punten is iedereen het over eens en welke punten zijn omstreden?
Financiering	• Wat is de (verwachte) investering voor de implementatie van SBR? • Hoe zijn de kosten verdeeld over tijd? • Vanuit welke partijen kan budget beschikbaar worden gesteld voor de implementatie?
Roadmap	• Langs welke lijn kan de implementatie van SBR worden gerealiseerd? • Welke plateaus vallen hierin te onderscheiden? • Hoe hangt de implementatie van SBR samen met andere projecten / programma's waarmee synergie kan worden behaald? • Welke doorlooptijden zijn realistisch?
Ondersteuning	• Welke ketenactoren dienen op welke manier ondersteund te worden bij het kunnen? • Welke ketenpartijen dienen op welke manier tegemoet te worden gekomen ten aanzien van het willen? • Welke diensten worden afgenomen bij de gedeelde dienstverlener Logius?

Bovenstaande karakteristieken van ketenverandering en bijbehorende te onderzoeken vragen vormen de inhoudelijke leidraad waarlangs ketenpartijen de verantwoordingsketen onderzoeken. De vragen dienen als richtlijn en zijn geen limitatieve opsomming. In de vragen zien we de inzichten uit hoofdstuk 3 en hoofdstuk 4 terugkomen. Om een zo rijk mogelijk beeld van de verantwoordingsketen te verkrijgen hebben we ervoor gekozen om de vragen veelal open te formuleren. Een checklist (ja/nee) biedt wel systematiek in de beantwoording en beoordeling van vragen, maar biedt beperkt ruimte voor diepgang en context. Het 'nadeel' is dat open vragen een groter beroep doen op de deskundigheid van de uitvoerder van de scan, waarmee de scan minder laagdrempelig is. Het is een bredere discussie, gevoed door de SBR-Quick Scan, die tot waardevolle inzichten leidt.

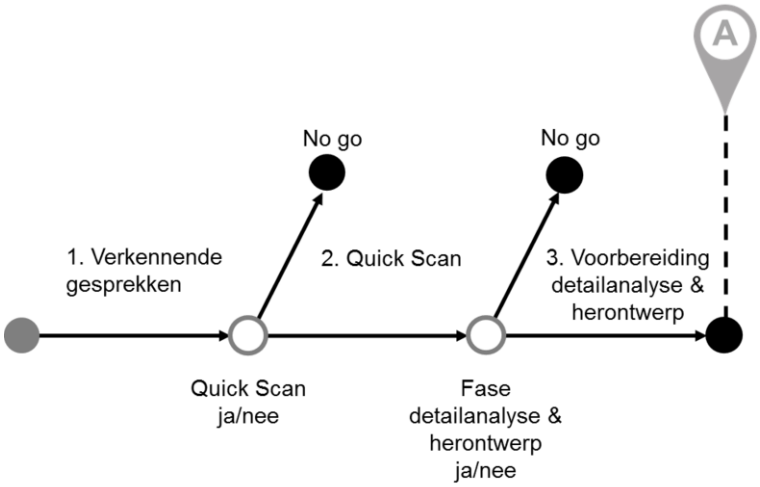
10.3 De interessefase

De interessefase vangt aan wanneer één of meerdere ketenpartijen interesse tonen in SBR en in dit kader contact hebben met de gedeelde dienstverlener Logius. Denk hierbij bijvoorbeeld aan beleidsverantwoordelijke(n), aanleverende partij(en), uitvragende partij(en) en/of dienstverlener(s). De interessefase beoogt de volgende doelen te bereiken:

- Geïnteresseerde partijen hebben inzicht in de mogelijkheden en grenzen van de toepassing van SBR en de SBR-verbredingsmethodiek.

- Geïnteresseerde partijen hebben gestructureerd inzicht in het functioneren van de huidige verantwoordingsketen en eventuele knelpunten.
- Geïnteresseerde partijen hebben een goede indicatie of de verantwoordingsketen geschikt is voor de toepassing van SBR.
- Geïnteresseerde partijen zijn voorzien van een onderbouwd advies over het al dan niet uitvoeren van de detailanalyse- en herontwerpfase als onderdeel van de Quick Scan.
- De (beoogde) uitvragende partij en/of beleidsopdrachtgever die verantwoordelijk zijn voor een verantwoordingsketen hebben een duidelijke ambitie voor SBR binnen de verantwoordingsketens voor ogen.
- De programmaorganisatie en bijbehorende gremia voor het aankomende traject zijn ingericht.
- De detailanalyse & herontwerpfase is voorbereid.

Er zijn drie onderdelen in de interessefase: de verkennende gesprekken, de SBR-Quick Scan en de voorbereiding van het vervolgtraject. Ketenpartijen doorlopen de onderdelen sequentieel. De verkennende gesprekken en de Quick Scan sluiten af met een besluitvormingsmoment.



Figuur 10.6 – Drie onderdelen en twee besluitvormingsmomenten in de interessefase

10.3.1 *Verkennende gesprekken*

Bij aanvang van de interessefase voeren geïnteresseerde partijen verkennende gesprekken met bijvoorbeeld de Rijksregisseur SBR of de manager vraag van Logius. Deze gesprekken kunnen geïnitieerd zijn door de Rijksregisseur/Logius of de geïnteresseerden zelf. In de verkennende gesprekken krijgen de geïnteresseerde partijen een eerste inzicht in de mogelijkheden en grenzen van SBR. Logius kan in samenspraak met geïnteresseerden aan de hand van de gesprekken en een eventuele deskstudy een eerste beeld van de huidige verantwoordingsketen schetsen.

De functionaris van Logius attendeert de geïnteresseerde partijen op de mogelijkheid tot het uitvoeren van de Quick Scan. In de Quick Scan verkennen de ketenpar-

tijen de mogelijkheden van SBR binnen de verantwoordingsketen verder op een gestructureerde wijze. Als de ketenpartijen interesse hebben om de Quick Scan uit te voeren, formaliseren zij de opdracht, stellen ze de uitgangspunten vast en doen zij een voorstel voor de scope en de te betrekken partijen bij de Quick Scan.

Het onderdeel verkennende gesprekken wordt afgesloten met een besluitvormingsmoment voor het al dan niet uitvoeren van een SBR-Quick Scan.

10.3.2 *SBR-Quick Scan*

Door de SBR-Quick Scan krijgen geïnteresseerde partijen een onderbouwd inzicht in het functioneren van de huidige verantwoordingsketen en wat de toepassing van SBR in de verantwoordingsketen betekent. Op basis van de bevindingen van de SBR-Quick Scan stellen de functionarissen van Logius een advies op over het al dan niet uitvoeren van een diepgaande analyse. Ook maken zij (hoog over) de business case, met hierin in ieder geval de ambitie met SBR. De Quick Scan vangt aan met een kick-off met de partijen zoals die vanuit de verkennende gesprekken zijn voorgesteld. Tijdens de Quick Scan geven de functionarissen van Logius uitleg over SBR en de aanpak tijdens de Quick Scan. Doel van de kick-off is om gezamenlijk met de betrokken partijen de scope en de te betrekken partijen definitief vast te stellen. Daarbij is het zaak zo snel mogelijk tot 'namen en rugnummers' te komen, zodat de benodigde afspraken en bijeenkomsten ingepland kunnen worden.

Na de kick-off houden afgevaardigden van de betrokken partijen en de functionarissen van Logius interviews en workshops. Het aantal workshops, de exacte invulling van de workshops en de samenstelling van deelnemers is afhankelijk van de keten, het aantal betrokken partijen en de doorlooptijd. Als richtlijn: twee workshops zijn minimaal noodzakelijk en meer dan acht workshops lijken het doel van de Quick Scan voorbij te schieten. Tijdens de workshops beschrijven de partijen de B-situatie. De partijen schatten de potentie van de toepassing van SBR, de verandernoodzaak en de veranderopgave in. Er is ook ruimte om na te denken over de veranderstrategie.

De verzamelde informatie zet een functionaris van Logius op papier. Hierdoor kan er 'closure' (ofwel, het vaststellen van deelproducten) plaatsvinden met de partijen. Tevens biedt het de geïnteresseerde partijen – gezamenlijk met het advies dat wordt gegeven – inzicht in de mogelijkheden van SBR binnen de verantwoordingsketen.

De deliverables die volgen uit de Quick Scan zijn in Tabel 10.7 weergegeven.

Tabel 10.7 – Overzicht deliverables Quick Scan

1	Startnotitie	Een gedragen startnotitie door de deelnemers van de Quick Scan van 2 A4 met daarin in ieder geval een beknopte en duidelijke beschrijving van de volgende elementen: 1) De maatschappelijke opgave volgend uit de publieke functie van verantwoording; 2) De resultaten van een onderbouwde analyse van het functioneren van de huidige verantwoordingsketen; 3) Een beeld van de verantwoordingsketen met toepassing van SBR; 4) Verandernoodzaak; 5) Aandachtspunten in de veranderopgave; 6) De voorgestelde strategie in termen van mogelijke aangrijpingspunten en roadmap.

2	Quick Scan	Een gedragen document door de deelnemers van de Quick Scan met daarin in ieder geval een uitgebreide en duidelijke beschrijving van de volgende elementen: 1) Aanleiding, doelstelling, scope, leeswijzer; 2) De maatschappelijke opgave volgend uit de publieke functie van verantwoording; 3) Relevante actoren; 4) Ketengovernance; 5) Processen; 6) Gegevens met daarin bijzonder aandacht voor (soort)gelijke gegevens binnen verschillende stromen; 7) De techniek; 8) De kosteneffectiviteit van de keten; 9) Verandernoodzaak; 10) Een beeld van de B-situatie voor alle onderdelen; 11) Een beeld van de veranderopgave; 12) Een beeld van de veranderstrategie; 13) Een advies over het al dan niet voortzetten van het traject; 14) Aandachtspunten voor de detailanalyse & herontwerpfase; 15) Managementsamenvatting; 16) Lijst met afkortingen en verklarende woordenlijst.
3	Business case (outline)	Een inschatting op hoofdlijnen van: 1) De ambitie voor de B-situatie (welke rol moet SBR gaan spelen binnen het verantwoordingsdomein. 2) De huidige kosten (administratieve lasten en uitvoeringslasten); 3) De toekomstige kosten (administratieve lasten en uitvoeringslasten) en baten bij toepassing van SBR (incl. kansen); 4) Investeringskosten en investeringsrisico's; 5) Alternatieven

Het onderdeel SBR-Quick Scan wordt afgesloten met een besluitvormingsmoment voor het al dan niet starten van de fase detailanalyse & herontwerp. Ook is het mogelijk dat de keten wel geschikt is voor de toepassing van SBR, maar dat de aanvang van de volgende fase 'on hold' wordt gezet. Als er wordt besloten tot het ingaan van de volgende fase, is het laatste onderdeel binnen de interessefase de voorbereiding van het vervolgtraject.

10.3.3 *Voorbereiding detailanalyse- en herontwerpfase*

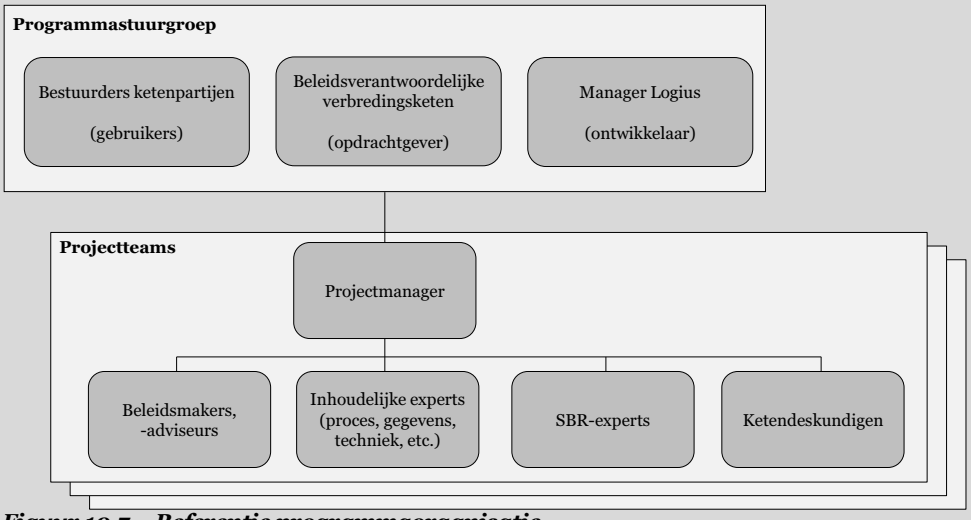
In de voorbereiding naar de volgende fase is het met name van belang dat de betrokken ketenpartijen de benodigde capaciteit en middelen beschikbaar weten te stellen voor een uitvoerige analyse. Hiertoe dient het plan van aanpak een exact beeld te geven van de benodigde activiteiten en bijbehorende planning om de beoogde resultaten op te leveren. Daarnaast geeft het plan van aanpak duidelijkheid over onder andere de uitgangspunten voor de programma-organisatie. Voor de resterende drie fasen dient er een programmaorganisatie te worden ingericht. Figuur 10.7 illustreert een referentie programmaorganisatie.

Tabel 10.8 – Overzicht van deliverables voorbereiding detailanalyse- en herontwerpfase

1	Programmaplan	Een document met daarin een beschrijving van: 1) Aanleiding, programmadoelstellingen, scope, uitgangspunten; 2) Raming van kosten, tijd van projecten en het afhankelijkheidsnetwerk tussen projecten; 3) Overall tijdschema en integrale opleverdata deliverables; 4) Weergave en toelichting gehanteerde plateaus; 5) Kwaliteitsbeheersing en risicobeheersing.
2	Plan van aanpak detailanalyse & herontwerpfase (per project)	Een document met daarin een beschrijving van: 1) Aanleiding, projectdoelstellingen, deliverables, scope, uitgangspunten; 2) Hoofdlijnen aanpak, fasering en besluitvorming, activiteiten, af te nemen diensten, projectplanning, projectorganisatie; 3) Kwaliteitsbeheersing en risicobeheersing.

In de voorbereiding naar de volgende fase maken de betrokken ketenpartijen de benodigde capaciteit vrij volgens het plan van aanpak en het programmaplan.

De referentie programmaorganisatie bestaat uit een stuurgroep (strategisch niveau) en onderliggende projectteams. Merk op dat de programmaorganisatie wat betreft actoren bij voorkeur een afspiegeling is van besturing op de in te richten keten. Gezien het programmatische karakter zal er een hoger bestuurlijk niveau intensief bij de organisatie betrokken worden, dan het geval zou zijn wanneer de keten in productie is. De referentie programmaorganisatie is bewust 'plat' gehouden. Communicatielijnen dienen kort te zijn. Een relatief klein aantal personen met 'commitment' valt sterk te prefereren boven een groot aantal personen waarvan de bijdrage die zij kunnen leveren teveel afhankelijk zal zijn van andere/externe werkzaamheden. Ketenpartijen kunnen kiezen om af te wijken van de referentie programmaorganisatie. Indien partijen afwijken, wordt wel aangeraden de wijziging programmatisch te besturen. De reden hiervoor is toegelicht in hoofdstuk 4. De referentie programmaorganisatie is weergegeven in onderstaand figuur.



Figuur 10.7 – Referentie programmaorganisatie

In de referentie stuurgroep is de beleidsverantwoordelijke van de verbredingsketen de opdrachtgever van het programma. Afgevaardigden van de betrokken ketenpartijen (dit zullen in ieder geval de uitvragende en aanleverende partijen betreffen, en eventueel dienstverleners) nemen de rol van gebruiker op zich. Een manager vanuit Logius (de manager Klant) vervult de rol van de ontwikkelaar. Het is de verantwoordelijkheid van de stuurgroep om de verschillende projecten te managen teneinde een integrale (geplande en beheerste) aanpak te waarborgen. De afgevaardigden in de stuurgroep sturen op de doelen van het verbredingsprogramma. Dit bevat in ieder geval het sturen op het ontwerpen, testen, accepteren en in productie nemen van de technologie en op de realisatie van de ketengovernance. De voornaamste taken van de stuurgroep zijn de periodieke beoordeling van de voortgang (budget en termijnen) van het traject en het bewaken van de zakelijke rechtvaardiging van het traject. De belangrijkste bevoegdheden van de stuurgroep zijn het nemen van de go/no besluiten voor de overgang naar de volgende fase en het aanbrengen van wijzigingen of vroegtijdig staken van projecten. De voorgenomen aanpak van de stuurgroep vindt zijn weerslag in een programmaplan. Omdat de volgende fasen tijd en capaciteit van alle betrokken ketenpartijen zullen vragen, kan het stuurgroep ervoor kiezen een programma-overeenkomst te sluiten tussen de betrokken ketenpartijen. De projectteams bevatten afgevaardigden vanuit verschillende organisaties en achtergronden om tot ee heterogeen projectteam te komen. Typische rollen die binnen de projectteams voorkomen zijn weergegeven

in de onderstaande tabel. Een rol bestaat uit een specifiek geheel van taken, verantwoordelijkheden en bevoegdheden die kan worden toegewezen aan één of meerdere personen. In de onderstaande tabel is tevens weergegeven vanuit welke partijen de personen afkomstig zijn die de rol kunnen vervullen. De lijst van rollen is niet uitputtend.

Tabel 10.9 – Overzicht van rollen

Rol	Beschrijving	Afkomstig van
Oplossings-eigenaar (projectleider)	De oplossingseigenaar is verantwoordelijk voor de dagelijkse leiding van projecten. De oplossingseigenaar is een 'meewerkend voorman'. Naast managen, voert hij dus tevens inhoudelijk taken uit. De projectleider speelt een voortrekkersrol bij het doorgronden en oplossen van complexe vraagstukken die gedurende het verbredingstraject naar boven kunnen komen. De oplossingseigenaar is betrokken van ontwerp naar experiment naar productie en coördineert tevens de verschillende diensten die vanuit Logius worden afgenomen.	Logius
Beleidsmaker, -adviseur	De beleidsmakers en –adviseurs zijn verantwoordelijk voor de aansluiting van het SBR en het gehanteerde beleid, zowel door het SBR-traject te vormen naar de beleidscontext, alsmede de beleidscontext te vormen naar SBR.	Publieke partijen
Ketendeskundigen	Ketendeskundigen geven input gedurende de analyse en het ontwerp van de verantwoordingsketen. In de latere fasen dienen zij als klankbord voor het voortdurend toetsen van de behaalde resultaten. Er kan ook om betrokkenheid van 'buitenstaanders' (bijvoorbeeld notoire criticasters) worden gevraagd.	Publieke en private partijen, 'buitenstaanders'
Procesdeskundige	De procesdeskundigen zijn verantwoordelijk voor de analyse, het ontwerp en de transitie van de huidige naar de toekomstige verantwoordingsprocessen.	Publieke en private partijen, Logius
Gegevensexpert	De gegevensexperts zijn verantwoordelijk voor de analyse, het ontwerp en de transitie van de huidige gegevenselementen naar de toekomstige Extensietaxonomie en de reports.	Publieke en private partijen, Logius
Technisch expert	De technisch experts zijn verantwoordelijk voor het gestructureerd opheffen van de technische roadblocks die de implementatie van SBR in de weg staat.	Publieke en private partijen, Logius
Juridisch specialist	De juridisch specialisten zijn verantwoordelijk voor de compliance toets. Daarnaast lossen juridisch specialisten eventuele juridische vraagstukken op.	Logius, publieke en private partijen
Ketengovernance-experts	De experts op het gebied van ketengovernance zijn verantwoordelijk voor de analyse, het ontwerp en de begeleiding bij de transitie van de huidige naar de toekomstige ketengovernance.	Logius en publieke partijen
Marktanalist	De marktanalist brengt de aanleverende partijen en betrokken dienstverleners grondig in beeld en maakt een analyse van de ondersteuning die zij nodig hebben om bij de verantwoordingsketen aan te kunnen sluiten.	Logius
SBR-experts	SBR-experts zijn afkomstig van de gedeelde dienstverlener Logius en geven procesbegeleiding of leveren een inhoudelijke bijdrage gedurende het traject, anders dan de bovenstaande expertise langs de lijnen proces, gegevens, techniek en ketengovernance.	Logius

10.3.4 *Af te nemen diensten bij de gedeelde dienstverlener Logius*

In principe begeleidt de gedeelde dienstverlener Logius de ketenpartijen bij het uitvoeren van de Quick Scan. De begeleiding is echter geen verplichting. Geïnteresseerde ketenpartijen kunnen ook zelfstandig aan de slag gaan en aangeven op welke punten zij input nodig hebben vanuit SBR. Partijen dienen er dan uiteraard wel vertrouwen in te hebben dat zij kunnen voldoen aan de eisen die het checkpoint stelt voor aanvang van de volgende fase.

10.3.5 *Kostensoort*

Er is bij de interessefase geen sprake van substantiële directe kosten. De investering vraagt om het beschikbaar stellen van tijd voor de verkennende gesprekken, het uitvoeren van de Quick Scan en de voorbereiding voor het vervolgtraject. De benodigde middelen beperken zich tot zaken als het organiseren van bijeenkomsten. Over het algemeen zullen de bijeenkomsten vanuit de gedeelde dienstverlener georganiseerd worden, tenzij betrokken partijen om praktische redenen anders prefereren.

10.3.6 *Do's en don'ts bij de interessefase*

Vanuit de literatuur en de ervaringen vanuit het SBR is er een aantal do's en don'ts te benoemen bij de interessefase.

- Besluitvorming over verbreding is strategisch van aard. Het is derhalve wenselijk om de ambtelijke top zo snel mogelijk te betrekken bij de verkennende gesprekken, mocht dit bij aanvang niet het geval zijn.
- De meeste vragen uit de Quick Scan kunnen op basis van desk study en enkele workshops met betrokkenen uit de keten worden ingevuld. Ervaring leert dat gebruikers van de Quick Scan met verschillende achtergronden (juridisch, bedrijfskundig, technisch etc.) gedeeltelijk een andere/complementaire invulling geven aan de vragen in de scan. Om tot een rijk beeld te komen kunnen derhalve experts vanuit verschillende disciplines worden geraadpleegd om vervolgens de uitkomsten met elkaar te verbinden.
- De wettelijke kaders rond de verantwoordingsketen kunnen een barrière vormen voor de implementatie van SBR (en de business case). Voor veel ketens is het aantrekkelijk op termijn volledig over te gaan op SBR, maar hier moet wel een wettelijke grondslag voor zijn. Besteed voldoende aandacht aan dit vraagstuk.
- Verantwoordingsketens zijn legio in aantal, maar kennen onderling vaak diverse raakvlakken. SBR kan interessante verbanden tussen verantwoordingsketens aan het licht brengen. Het verdient aanbeveling in de interessefase het contact met andere (uitvragende) partijen op te zoeken. Zeker de partijen die al aangesloten zijn op SBR zullen nuttige bijdragen kunnen leveren. Gebruik hier ook de SBR gremia voor.
- Volg een plateaubenadering bij het inrichting van het programma. Ieder plateau is een herkenbare stap op weg naar de gewenste situatie. Deze overtuiging vloeit voort uit onderzoek op het gebied van de proces herinrichting en de lerende organisatie (Kettinger & Grover, 1995). Hierbij wordt de plateaubenadering als tegenhanger van de blauwdrukbenadering aangedragen. De essentie van de plateaubenadering is dat men niet verandert op basis van

een blauwdruk die zich over een aantal jaren uitstrekt, maar dat men verandert op basis van een globale visie die gaandeweg en al lerende kan worden aangepast aan omstandigheden die men nooit had kunnen plannen of voorzien (Huizing & de Vries, 1997).
- Pas kwaliteitsmanagement toe. Onder kwaliteit verstaan we 'fitness voor use', oftewel het voldoen aan afspraken, eisen en verwachtingen van de betrokken partijen. Geschiktheid voor ketendoeleinden is het essentiële criterium voor de acceptatie van resultaten. Een hulpmiddel hierbij is bijvoorbeeld een checklist met kwaliteitscriteria aan de hand waarvan resultaten uit het aansluittraject kunnen worden beoordeeld.

10.4 De detailanalyse- en herontwerpfase

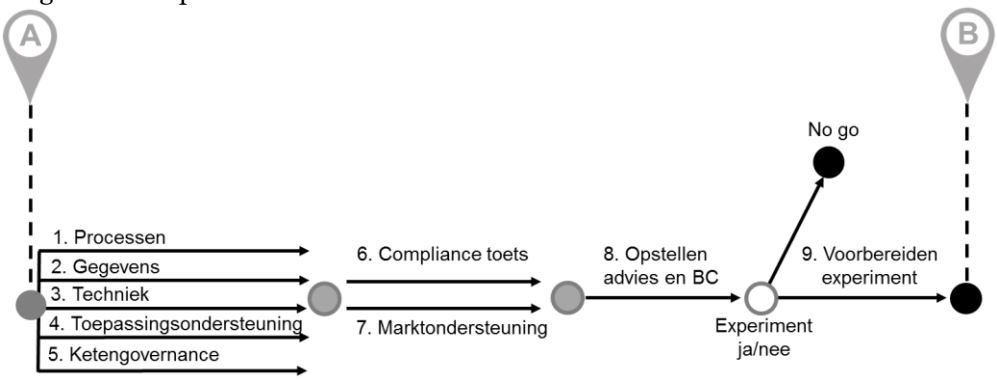
De detailanalyse- en herontwerpfase is de tweede fase van de SBR-verbredingsmethodiek. Wij spreken over een herontwerp omdat er meestal al sprake zal zijn van een reeds bestaande verantwoordingsketen. Ketenpartijen hebben reeds de interessefase doorlopen. De analyse & herontwerpfase kan aanvangen wanneer aan de volgende criteria is voldaan (als onderdeel van checkpoint A):

- De beleidsverantwoordelijke of uitvragende partij geeft opdracht tot het uitvoeren van de detailanalyse en het herontwerp van een of enkele verantwoordingsketens.
- Er is een business case aanwezig waarin een duidelijke ambitie ligt voor het verandertraject dat ingegaan wordt, waarbij duidelijke doelen zijn gesteld die binnen een overzichtelijke termijn te behalen moeten zijn.
- Vanuit de gedeelde dienstverlener Logius ligt er een positief advies tot het uitvoeren van de detailanalyse en het herontwerp.
- De publieke functie, de actuele situatie (A-situatie) en de verandernoodzaak zijn verkend en heeft zijn weerslag gevonden in een document dat wordt gedragen door de betrokken partijen.
- Er is een beeld gevormd van de gewenste keten (B-situatie), de veranderopgave en de veranderstrategie en dit beeld heeft zijn weerslag gevonden in een document dat wordt gedragen door de betrokken partijen.
- De programmaorganisatie en bijbehorende gremia zijn ingericht.
- Het plan van aanpak voor de detailanalyse & herontwerpfase is opgesteld en wordt toereikend geacht door de stuurgroep.
- De ketenpartijen kunnen de benodigde capaciteit beschikbaar maken.

De detailanalyse & herontwerpfase beoogt de volgende doelen te bereiken:

- De publieke functie, A-situatie en verandernoodzaak is gedetailleerd in kaart gebracht en vastgesteld door de betrokken partijen.
- De gewenste keten (B-situatie) is ontworpen door de betrokken partijen.
- Het marktondersteuningsplan is opgesteld.
- De stuurgroep heeft een gedetailleerde onderbouwing over de kosten en baten van de toepassing van SBR binnen de verantwoordingsketen.
- De stuurgroep is voorzien van een advies over het al dan niet uitvoeren van het experiment.
- Het experiment is voorbereid.

Er zijn negen onderdelen in de detailanalyse & herontwerpfase. De eerste vijf onderdelen zijn de detailanalyse en het herontwerp langs de lijnen processen-gegevens-techniek en ketengovernance. Ook wordt de toepassingsondersteunings-keten ontworpen. Ketenpartijen doorlopen deze vijf onderdelen parallel, waarbij de projectleden de samenhang tussen de onderdelen in het herontwerp waarborgen. Hierin is ook een belangrijke taak weggelegd voor de projectleider. Gedurende de analyse en het ontwerp, als de vijf onderdelen zijn voltooid, vindt er een integrale compliance toets plaats en wordt de marktondersteuning bepaald. Op basis van de bevindingen worden het advies en de business case opgesteld. Onderdeel negen is de voorbereiding van het experiment.



Figuur 10.8 – Negen onderdelen en het besluitvormingsmoment in de detailanalyse- en herontwerpfase

De volgende paragrafen lichten de afzonderlijke onderdelen nader toe.

10.4.1 *Procesanalyse en –ontwerp*

In het onderdeel processen onderzoeken procesdeskundigen in detail de huidige verantwoordingsprocessen en ontwerpen zij de toekomstige verantwoordingsprocessen. Er zijn procesdeskundigen van zowel de verantwoordingsketen als vanuit SBR betrokken. Met behulp van procesbeschrijvingen in Business Process Modelling Notation (zie hoofdstuk 5) maken de procesdeskundigen de huidige verantwoordingsprocessen inzichtelijk van registratie tot uiteindelijke verwerking. De analyse is grondig. Procesdeskundigen houden rekening met de pluriformiteit van aanleverende partijen, bijvoorbeeld door het opstellen van enkele archetypen. Denk hierbij aan verschillen in het aanleverproces van kleine partijen, die gebruik maken van een dienstverlener bij de verantwoording tot een multinational die system-to-system aanlevert bij SBR.

Door het inzichtelijk maken van de A-situatie komen er in de meeste gevallen mogelijke verbeterpunten naar voren. Vanuit SBR zijn generieke verwerkingservices voor de i-processen (inclusief bijbehorende procesbeschrijvingen) reeds voorhanden. Op basis van de A-situatie en de bouwblokken starten betrokken partijen een herontwerptraject. Daarbij kunnen de betrokkenen een beroep doen op de methode, toolbox en kennis zoals deze binnen SBR voorhanden is. De procesdeskundige vanuit Logius analyseert de impact van het ontwerp op de diensten van Logius. Het ontwerp

resulteert in een volledige beschrijving van implementeerbare i-processen in BPMN en met bijbehorende toelichting in tekst. De scope van het ontwerp strekt zich uit van het IT-systeem van de aanleverende partij tot de backoffice van de uitvragende partij.

Tabel 10.10 – Overzicht van deliverables procesanalyse en –ontwerp

1	Procesanalyse	Een beschrijving van de huidige verantwoordingsprocessen in BPMN met aandacht voor bijzonderheden. Naast de 'happy flow' zijn tevens afwijkingen in het proces en de bijbehorende oorzaken vastgelegd.
2	Procesontwerp	Een volledige beschrijving van implementeerbare i-processen in BPMN en bijbehorende toelichting in tekst, in overeenstemming met de opgestelde kaders en in samenhang met gegevens-techniek. De scope van het ontwerp strekt zich van het IT-systeem van de aanleverende partij tot de backoffice van de uitvragende partij.
3	Impactanalyse	De impact van het herontwerp op de aangeboden diensten van Logius. Hierin ligt de nadruk op eventueel noodzakelijke (door)ontwikkeling van verwerking- en koppelvlakservices of benodigde servicelevels.

10.4.2 *Gegevensanalyse en –ontwerp*

In het onderdeel gegevens onderzoeken gegevensexperts in detail de huidige set van uitgevraagde gegevens (elementen en definities) en aanwezige brongegevens. De detailanalyse kan een trigger zijn voor de beleidsmakers om de uitgevraagde set van gegevens kritisch onder de loep te nemen. Dit kan door het verrichten van een informatiebehoeftenanalyse. De informatiebehoeftenanalyse valt buiten de scope van de verbredingsmethodiek, maar door het gelijktijdig plaatsvinden van beide trajecten kan er synergie worden bereikt.

De gegevensexperts onderzoeken de relaties tussen de diverse gegevenselementen. Ook kijken zij welke (soort)gelijke gegevens reeds in de Nederlandse Taxonomie en de Extensies zijn opgenomen. Op basis van hun analyse stellen zij vast welke elementen er toegevoegd dienen te worden aan de NT door middel van een extensietaxonomie en hoe de reports eruit komen te zien. De betrokkenen kunnen een beroep doen op de methode en tooling zoals deze binnen SBR voorhanden is. De gegevensexpert vanuit Logius analyseert de impact van het ontwerp op de diensten van Logius.

Tabel 10.11 – Overzicht deliverables gegevensanalyse en –ontwerp

1	Huidig gegevens-model	Een weergave van de uitgevraagde elementen, bijbehorende definities en de relatie tussen de uitgevraagde elementen.
2	Extensie-taxonomie en reports	Het ontwerp van een extensietaxonomie in XBRL waarin alle uitgevraagde elementen en bijbehorende definities bevat. Het ontwerp van de reports voor aanleverende en uitvragende partijen met daarin de relevante koppelingen naar de Nederlandse Taxonomie en bijbehorende extensies.
3	Impactanalyse	De impact van het herontwerp op de aangeboden diensten van Logius en de architectuur van de NTA.

10.4.3 *Analyse en ontwerp techniek*

In het onderdeel techniek onderzoeken technisch experts de consequenties van de processen en gegevens in de B-situatie binnen de geldende technische architecturen. De experts stellen de technische specificaties op van de nieuwe services. Op basis van de analyse en het ontwerp stellen zij de impact van de technische implementatie van SBR voor de diverse partijen vast.

Tabel 10.12 – Overzicht van deliverables analyse en ontwerp techniek

1	Business en technologie files	Technische specificaties en verkennende impactanalyse

10.4.4 *Analyse en ontwerp toepassingsondersteuningsketen*

In een werkende SBR-verantwoordingsketen moeten partijen zicht kunnen hebben op de specificaties van deze keten. Ook moeten zij ergens ketenincidenten kunnen melden, of moeten zij op de hoogte gehouden worden van verstoringen. Hier is een toepassingsondersteuningsketen nodig. Logius speelt een centrale rol in deze keten, maar het is de uitvragende partij die als afnemer verantwoordelijk is voor de gehele keten. Tevens is Logius voor de toepassingsondersteuning afhankelijk van de positie die de uitvragende partij bij de toepassingsondersteuning wil innemen. Aan de hand van de bestaande toepassingsondersteuning en de beschikbare dienstverlening van Logius op dit gebied ontwerpen de ketenpartners een nieuwe toepassingsondersteuning.

Tabel 10.13 – Overzicht van deliverables analyse en ontwerp toepassingsondersteuningsketen

1	Toepassings-ondersteunings-keten	Het ontwerp van de toepassingsondersteuningsketen van de verantwoordingsketen in de B-situatie.

10.4.5 *Analyse en ontwerp ketengovernance*

In het onderdeel ketengovernance analyseren de deskundigen de huidige ketengovernance en ontwerpen zij de toekomstige ketengovernance. Bij aanvang onderzoeken zij welke ketenactoren de huidige verantwoordingsketen besturen (zowel formeel als informeel) en of zij op basis van de bestaande afspraken de verantwoordingsketen naar tevredenheid kunnen besturen. Vervolgens onderzoeken de deskundigen de afhankelijkheden die ontstaan (of wijzigen) als gevolg van horizontale integratie, verticale integratie en netwerkintegratie.

Ten aanzien van de horizontale integratie maken ketenpartijen zoveel mogelijk gebruik van de reeds aanwezige governance van de keten. Als er een governance aanwezig is die naar behoren functioneert, kan deze in principe vrijwel één op één worden overgenomen. Uiteraard dienen eventuele nieuw toegetreden partijen in de keten (dit betreft in ieder geval Logius) wel een plek te krijgen in de ketengovernance. Als de huidige ketengovernance afwezig is (bijvoorbeeld omdat de verantwoordingsketen nog niet geïntegreerd is) of niet naar tevredenheid functioneert (het is bijvoorbeeld lastig om een wijziging door te voeren in de keten), dan stellen de deskundigen gezamenlijk een herontwerp op. Mochten er in de B-situatie van de ketengovernance

partijen zijn opgenomen die momenteel niet betrokken zijn bij de besturing van het verbredingstraject, dan geeft dit stof tot nadenken. Volgend uit hoofdstuk 4, valt het aan te raden deze partijen zo snel mogelijk bij de wijziging te betrekken.

Als gevolg van de verticale integratie ontstaan er afhankelijkheden met de andere uitvragende partijen. De rol die de toetredende ketenactoren gaan spelen in de ketengovernance is afhankelijk van de impact op de diensten van Logius die zij graag willen afnemen. De proces-, gegevens-, en techniekexperts vanuit Logius stellen de impact gedurende het ontwerp vast. Als er sprake is van een lage impact (ofwel: de dienst wordt afgenomen conform de wijze waarop Logius de dienst aanbiedt) dan kunnen zij een *'laisser faire'* houding aannemen in de ketengovernance. Het grote voordeel van het op zijn beloop laten van de verticale afstemming is dat het ketenpartijen meer ruimte geeft voor andere (belangrijkere) aspecten van de ketenverandering. Als de keten eenmaal in productie is, bestaat er immers altijd nog de mogelijkheid tot doorontwikkeling. Eventuele wensen die om een wijziging in de generieke dienstverlening en/of specificaties vragen kunnen ketenpartijen voorstellen nadat zij enige ervaring hebben opgedaan binnen en over SBR. Wij raden af om een wijziging in de generieke dienstverlening voor te stellen zolang de keten nog niet in productie is. Het maakt het wijzigingstraject een stuk complexer voor de aansluitende keten, niet in de laatste plaats omdat er tevens draagvlak verkregen dient te worden bij de andere uitvragende partijen. De proces-, gegevens- en techniekexperts zullen gedurende het ontwerp dit dan ook aansturen op een zo laag mogelijke impact.

Als gevolg van netwerkintegratie ontstaan er afhankelijkheden door het gebruik van de SBR standaarden. De partijen bekijken hoe zij het beste deel kunnen gaan nemen aan de ketengovernance op het afsprakenstelsel. Hetgeen dat geldt voor verticale integratie geldt eigenlijk nog sterker voor netwerkintegratie. Een wijzigingsvoorstel in de specificaties namens een toetredende partij dat significante impact heeft voor het stelsel maakt de wijziging tot een zeer complex programma. In dat geval moeten er van de toepassing binnen de nieuwe keten wel hele grote baten verwacht worden.

Tabel 10.14 – Overzicht deliverables analyse en ontwerp ketengovernance

1	Ketengovernance-beschrijving A-situatie	Een detailbeschrijving van de huidige ketengovernance inclusief een onderbouwd oordeel over de kosteneffectiviteit van de ketengovernance.
2	Ketengovernance-beschrijving B-situatie	Een detailbeschrijving van de toekomstige ketengovernance langs de lijnen horizontale integratie, verticale integratie en netwerkintegratie.
3	Wijzigingsvoorstel ketengovernance	Een wijzigingsvoorstel in de ketengovernance van SBR, ter formele toetreding van de afgevaardigden van de betrokken ketenpartijen in de SBR gremia.

10.4.6 *Compliance toets*

Processen-gegevens-techniek zijn in samenhang ontworpen. De compliance toets is de finale check op de geldende en relevante wet- en regelgeving. Ook wordt gecontroleerd of het integrale ontwerp voldoet aan alle gestelde eisen en standaarden (denk hierbij aan de regels van de Nederlandse Taxonomie Architectuur, proces- en technische standaarden en eventuele aanvullende kaders en eisen vanuit Logius). Er is speciale aandacht voor informatiebeveiliging (zie tevens hoofdstuk 8).

Tabel 10.15 – Overzicht deliverables analyse en ontwerp ketengovernance

1	Compliance toets	Een gestructureerd oordeel over de compliance van het integrale ketenontwerp en eventuele aanbevelingen.

10.4.7 *Marktondersteuning*

Met een gedetailleerd ontwerp in handen, is de marktanalist in staat om, in overleg met deskundigen en experts, de gevolgen van de toepassing van SBR voor de verschillende marktpartijen inzichtelijk te maken. Vanuit de stuurgroep zal in dit stadium duidelijkheid verkregen dienen te worden over de beoogde gebruikers van SBR. Denk hierbij aan een specificatie van aantallen (bijvoorbeeld: 80% van de verantwoordingsverplichtigen levert per 2015 aan met SBR) en doelgroep (bijvoorbeeld: SBR richt zich op de grote aanleverpartijen). Het vervolgens vaststellen welke ondersteuning gebruikers bij de toepassing van de verantwoordingsketen in de volgende fase kunnen krijgen (marktondersteuningsplan) gebeurt altijd in nauw overleg met de opdrachtgever en de publieke deelnemers van de verantwoordingsketen. Logius biedt een heel aantal diensten aan dat zich richt op de aansluitondersteuning van marktpartijen. Het gaat onder andere om:

- Aansluitsuite (testvoorziening)
- Aansluitpakketten
- Individuele begeleiding

Tabel 10.16 – Overzicht deliverables marktondersteuning

1	Marktonder-steuningsplan	Een document met daarin een beschrijving van de beoogde gebruikers en de wijze waarop beoogde gebruikers van de verantwoordingsketen ondersteuning ontvangen aan de hand van bijvoorbeeld aansluitpakketten, individuele begeleiding en/of groepsvoorlichting.

10.4.8 *Opstellen advies en business case*

Voor de besluitvorming wordt op basis van de gedetailleerde analyse van de huidige situatie en het ontwerp de business case nader gespecificeerd en het bijbehorende advies opgesteld. De stuurgroep ontvangt het advies en de onderliggende business case ten behoeve van de besluitvorming.

Tabel 10.17 – Overzicht deliverables voorbereiden besluitvorming

1	Advies en Roadmap	Een advies om SBR al dan niet binnen één tot drie jaar conform de vastgestelde toepassingsdoelstelling in de verantwoordingsketen toe te passen, gegeven de baten en benodigde investeringen vanuit de diverse betrokken partijen. Een Roadmap waarin aangegeven staat hoe dit doel gerealiseerd kan worden.
2	Business case	Een zo meetbaar en financieel mogelijke inschatting van: 1) De huidige kosten (administratieve lasten en uitvoeringslasten); 2) De toekomstige kosten (administratieve lasten en uitvoeringslasten) en baten bij toepassing van SBR (incl. kansen); 3) Investeringskosten en investeringsrisico's; 4) Alternatieven

10.4.9 *Besluitvorming*

Binnen het SBR-verbredingstraject is het besluitvormingsmoment aan het einde van de detailanalyse & herontwerpfase (als onderdeel van checkpoint B) de meest cruciale. Er ligt een op papier integraal en implementeerbaar ontwerp, dat voldoet aan de gestelde kaders en eisen. Daarmee zijn de ketenpartijen klaar om het ontwerp te testen. De stuurgroep is voorzien van een advies. Het advies is onderbouwd met de detailanalyse en de business case. Daarmee is de benodigde informatie voor een gedegen besluitvorming verzameld. Het kenbaar maken van de visie op SBR binnen de verantwoordingsketen komt nu centraal te staan.

Door de activiteiten die hebben plaatsgevonden zullen (betrokken en niet-betrokken) marktpartijen inmiddels de gekozen beleidslijn goed in de gaten houden. Met het uitvoeren van het experiment zullen de verwachtingen van marktpartijen verder toenemen. De partijen die daadwerkelijk gaan werken volgens SBR – weliswaar als experiment – zullen in toenemende mate vragen om duidelijkheid over het toekomstige beleid om de investeringen te kunnen verantwoorden. Om verwachtingen goed te managen, dient het uitgangspunt bij aanvang van het experiment te zijn dat *als het experiment zonder substantiële problemen verloopt, de toepassing van SBR binnen de verantwoordingsketen de aankomende jaren wordt doorgezet met als doel SBR binnen één tot drie jaar SBR conform de ambitie die voor de keten(s) gesteld is, toe te passen.* Het marktondersteuningsplan en het aankomende experiment maken onderdeel uit van de visie op SBR binnen de verantwoordingsketen.

Dit betekent dat er in feite voldoende draagvlak dient te zijn voor de toepassing van SBR binnen de verantwoordingsketen onder de belangrijkste ketenpartijen. Onder belangrijkste ketenpartijen worden in ieder geval de beleidsverantwoordelijke, de uitvragende partijen alsmede enkele toonaangevende aanleverende partijen en dienstverleners verstaan. Als er voldoende draagvlak aanwezig is dan lijkt de toepassing van SBR in de nabije toekomst een feit. Merk op dat het experiment daardoor fundamenteel verschilt met het uitvoeren van bijvoorbeeld een pilot. Indien er onvoldoende draagvlak blijkt te zijn voor de toepassing van SBR onder de belangrijkste ketenpartijen dan verwijzen we naar hoofdstuk 3 en 4 voor een nadere behandeling van het thema acceptatie en de manier waarop acceptatie beïnvloed kan worden.

10.4.10 *Voorbereiden experiment*

Bij de afronding van de detailanalyse & herontwerpfase vinden de voorbereidingen plaats voor het experiment. Deze bestaan uit het opstellen van het plan van aanpak, het inrichten van de experimenteeromgeving en het vrijmaken van capaciteit en middelen. In de voorbereiding naar de volgende fase is het van belang dat de betrokken ketenpartijen de benodigde capaciteit en middelen beschikbaar weten te stellen. Hiertoe dient het plan van aanpak een exact beeld te geven van de benodigde activiteiten en bijbehorende planning (inclusief de gevraagde capaciteit van omgevingen en voorzieningen) om de beoogde resultaten op te leveren. Het experiment dient te worden begroot – met daarin de kosten uitgesplitst naar de verschillende partijen – om de financiering vorm te geven.

Tabel 10.18 – Overzicht deliverables voorbereiding experiment

1	Plan van aanpak experiment	Een document met daarin een beschrijving van: 1) Aanleiding, projectdoelstellingen, deliverables, scope, uitgangspunten; 2) Hoofdlijnen aanpak, fasering en besluitvorming, activiteiten, projectplanning, af te nemen diensten, capaciteitsplanning IT-services en infrastructuur en bijbehorende serviceniveaus, projectorganisatie; 3) Kosten en financiering; 4) Kwaliteitsbeheersing en risicobeheersing

De gedeelde dienstverlener Logius biedt een dienst aan voor het uitvoeren van experimenten. Om te kunnen waarborgen dat de benodigde IT-services en infrastructuur beschikbaar zijn, dienen voor aanvang van het experiment de nodige voorbereidingen getroffen te worden en de experimenteeromgeving te worden ingericht. In de voorbereiding naar de volgende fase maken de betrokken ketenpartijen de benodigde capaciteit vrij volgend uit het plan van aanpak. Voor het uitvoeren van het experiment zijn substantiële middelen nodig, welke vrijgemaakt dienen te worden.

10.4.11 *Af te nemen diensten bij de gedeelde dienstverlener Logius*

In hoofdstuk 9 is toegelicht dat de diensten vier basisfuncties vervullen, te weten: i-procesmanagement, gegevensmanagement, toepassingsondersteuning en aansluitondersteuning. Voor iedere basisfunctie zijn er diensten die betrekking hebben op ontwerp, transitie en productie. De diensten die Logius aanbiedt tijdens de detailanalyse & herontwerpfase, hebben met name betrekking op het ontwerp. Zo kan het ontwerpen van de verantwoordingsketen plaatsvinden binnen de diensten (her)ontwerp i-processen en (her)ontwerp taxonomie. Logius levert één dienst die de coördinatie tussen de verschillende diensten van ontwerp naar experiment naar productie voor zijn rekening neemt. Dit is de dienst domeintransitie. Verder kan Logius expertise leveren ter ondersteuning van de besluitvorming, zoals procesbegeleiding of een inhoudelijke bijdrage.

10.4.12 *Kostensoort*

De detailanalyse en het herontwerp vragen om een substantiële tijdsinvestering van de betrokken ketenpartijen. De benodigde middelen zijn beperkt en kunnen worden aangeboden vanuit de diensten van Logius, zoals bovenstaand beschreven.

10.4.13 *Do's en don'ts bij de detailanalyse & herontwerpfase*

Vanuit de ervaringen vanuit SBR zijn er een aantal do's en don'ts bij de detailanalyse & herontwerpfase.

- De projectteams dienen gemachtigd te zijn om besluiten te nemen. De projectorganisatie is 'plat' van opzet waarmee er een grote verantwoordelijkheid op de projectleden komt te liggen. De verantwoordelijkheden dienen gepaard te gaan met bevoegdheden.
- Betrek de beleidsministeries bij het opstellen van de definitieve ambitie van SBR en stel samen vast of er aanpassingen moeten komen in de wettelijke kaders die gelden voor de verantwoording.
- De scope, functionaliteit en kwaliteit dient actief gemanaged te worden aan de hand van 'time boxing'. Dit uitgangspunt komt uit de literatuur over agile ontwikkeling en zorgt voor closure (Richards, 2007). Timeboxing zoekt een

balans tussen een tijdige oplevering van (deel)producten en het kunnen implementeren van eisen of randvoorwaarden die als 'voortschrijdend inzicht' kunnen worden aangemerkt. Bij timeboxing wordt de gehele projectperiode opgedeeld in meerdere korte perioden: de zogenaamde timeboxes of iteraties. Een timebox is kort. Aan het einde van een timebox wordt geëvalueerd of het juiste product nog op de juiste manier geproduceerd wordt. Hierdoor is bijsturing van het project mogelijk. Ongeacht het resultaat wordt er door het ontwikkelteam na iedere iteratie opnieuw bekeken wat de prioriteiten van het project zijn.

- Gebruik de roadmap als 'drukventiel'. Doe geen concessies op het eindplaatje, maar stuur op de snelheid van de transitie. Harde deadlines kunnen partijen motiveren het traject serieus te nemen. Weerstand kan juist worden verminderd door verschuivingen in de tijd.
- Zorg ervoor dat SBR niet gezien wordt als technisch of ICT project. De verleiding kan groot zijn voor ketenpartijen om SBR te beschouwen als ICT project, aangezien een groot deel van SBR vraagt om een wijziging in de processen, gegevens en techniek. Ervaring leert dat projecten die als technisch worden bestempeld vaak onvoldoende bestuurlijke betrokkenheid krijgen. Ze verdwijnen al gauw van de bestuurlijke radar die vooral scant naar oplossingen voor bredere – sociaal maatschappelijke – problemen. Houd genoeg oog voor de inrichting en realisatie van de governance.
- Ga het experiment organiseren als publiek-private samenwerking. De Nederlandse implementatie wijze van SBR wordt gekenmerkt door de inspraak die marktpartijen hebben in het totstandkomingsproces. Vanaf het begin is het SBR Programma een publiek-private samenwerking geweest die het doel had om de acceptatie en adoptie van SBR door marktpartijen te bevorderen.

10.5 Het experiment

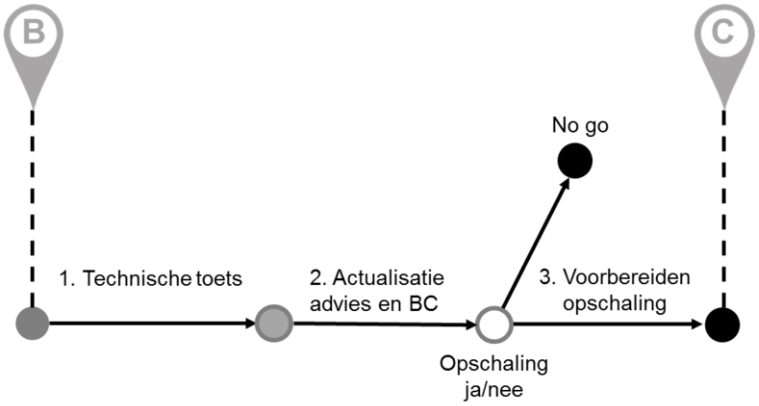
Het experiment is de derde fase van de SBR-verbredingsmethodiek. Ketenpartijen hebben de detailanalyse & herontwerpfase doorlopen. Het experiment kan aanvangen wanneer aan de volgende criteria is voldaan (als onderdeel van checkpoint B):

- Vanuit de belangrijkste ketenpartijen is er een gedragen roadmap om SBR binnen één tot drie jaar conform de gestelde doelen binnen het verantwoordingsdomein toe te passen.
- Vanuit de gedeelde dienstverlener Logius ligt er een positief advies over de toepassing van SBR binnen één tot drie jaar.
- Het ontwerp van de verantwoordingsketen is opgesteld, voldoet aan de eisen en de betrokken partijen hebben het vertrouwen dat met het ontwerp de test goed zal verlopen.
- Het plan van aanpak voor het experiment is opgesteld.
- De experimenteeromgeving is ingericht.
- Ketenpartijen kunnen de benodigde capaciteit vrijmaken en er is financiering voor het uitvoeren van het experiment.
- Er is voldoende beeld over de wijze waarop partijen zinvol kunnen participeren in de verschillende besturingsgremia.

Het experiment beoogt de volgende doelen te bereiken:

- Het ontwerp is technisch getoetst en de eventuele laatste 'kinderziekten' zijn verholpen.
- Het advies en onderliggende business case zijn geactualiseerd.
- Het plan voor opschaling is opgesteld.

Het experiment bestaat uit drie onderdelen. Het eerste onderdeel bestaat uit de technische toets van het ontwerp, ofwel de gecontroleerde implementatie van de situatie-B processen, gegevens en techniek in de beperkte en veilige experimenteeromgeving. Het tweede onderdeel bestaat uit de actualisatie van het advies en de business case. Het derde onderdeel bestaat uit de voorbereiding van de opschaling.



Figuur 10.9 – Drie onderdelen en het besluitvormingsmomenten in het experiment

10.5.1 *Technische toets*

De technische toets van het ontwerp vindt plaats op de experimenteeromgeving die Logius aanbiedt. De experimenteeromgeving is een flexibele voorziening die uitgaat van dezelfde architectuur als het platform waar i-proces,- en gegevensproductie in plaatshebben. In de experimenteeromgeving kunnen alternatieve configuraties worden getest en kan door middel van workarounds een bepaalde functionaliteit of interactie worden gesimuleerd. Daarmee kunnen eventuele laatste 'kinderziektes' in de nieuwe toepassing van de bouwblokken worden opgelost. In de meeste gevallen zal de experimenteeromgeving op basis van 'best-effort' servicelevels beschikbaar worden gesteld. Met het testen stellen de functionarissen binnen Logius vast of de processen, de taxonomie, de IT-services en infrastructuur voldoen aan de gespecificeerde eisen. Zo ja, dan accepteren zij de technologie voor productie.

Tabel 10.19 – Overzicht deliverables technische toets

1	Definitief ontwerp	Het definitieve ontwerp van de i-processen, de extensietaxonomie en reports voor de verantwoordingsketen.
2	Werkende keten	Een functionerende verantwoordingsketen met de toepassing van SBR in de experimenteeromgeving.
3	Impactanalyse	Een definitieve impactanalyse voor de dienstverlening (i-processen, gegevens, aansluitondersteuning en toepassingsondersteuning) van Logius.

10.5.2 *Actualisatie advies en business case*

Voor de besluitvorming wordt op basis van de gedetailleerde analyse van de huidige situatie en het ontwerp de business case nader gespecificeerd en het bijbehorende advies opgesteld. De stuurgroep ontvangt het advies en de onderliggende business case ten behoeve van de besluitvorming.

Tabel 10.20 – Overzicht deliverables actualisatie advies en business case

1	Advies (geactualiseerd)	Een actualisatie van het advies om SBR al dan niet binnen één tot drie jaar grootschalig in de verantwoordingsketen toe te passen
2	Business case (geactualiseerd)	Een actualisatie van de business case.

10.5.3 *Besluitvorming*

Als het experiment probleemloos is verlopen dan ligt het in de lijn der verwachting dat de stuurgroep bij het besluitvormingsmoment aan het einde van het experiment de grootschalige toepassing van SBR binnen de verantwoordingsketen doorzet. De stuurgroep bepaalt welke marktondersteuning er geboden gaat worden en stelt de definitieve veranderstrategie vast.

Alleen als er sprake is van substantiële problemen tijdens het experiment, met een grote invloed op de business case, worden de leden van de stuurgroep voor een daadwerkelijk te maken keuze gesteld. De stuurgroep wordt daarbij ondersteund door het advies. Binnen het advies zal tevens rekening worden gehouden met eventuele ketenoverstijgende effecten van de te nemen beslissing. Het besluit om voor een (technisch) probleem binnen deze verantwoordingsketen tot een degelijke oplossing te komen kan immers ook baten hebben voor andere verantwoordingsketens.

10.5.4 *Voorbereiding van de opschaling*

Gedurende het experiment kunnen ketenpartijen het ontwerp definitief vaststellen. Daarmee kan het plan voor de opschaling worden vastgesteld. Merk op dat met het doorlopen van het experiment de ketenpartijen een antwoord hebben gevormd op de vragen vanuit de inhoudelijke leidraad. Op basis van de verkregen inzichten (met name met betrekking tot de veranderopgave) stellen zij de veranderstrategie vast voor het vervolg. Cruciale onderdelen van de voorbereiding betreffen in ieder geval:

- De transitie van de verantwoordingsketen naar productiedienstverlening
- De implementatie van de ondersteuningsketen

Op basis van het plan voor opschaling maken de partijen capaciteit en middelen vrij.

Tabel 10.21 – Overzicht deliverables voorbereiding van de opschaling

1	Plan voor opschaling	Een document met daarin een beschrijving van: 1) Aanleiding, projectdoelstellingen, deliverables, scope, uitgangspunten; 2) Gedetailleerde veranderopgave per actor en bijbehorende veranderstrategie die toereikend wordt geacht door de betrokken partijen om de verandering te realiseren 3) Af te nemen diensten en bijbehorende serviceniveaus; 3) Kosten en financiering; 4) Kwaliteitsbeheersing en risicobeheersing.

10.5.5 *Af te nemen diensten bij de gedeelde dienstverlener Logius*

Logius biedt een aantal diensten aan in deze fase van de methodiek. Vanuit de dienst domeintransitie worden de diensten transitie i-processen en taxonomie transitie gecoördineerd. Logius stelt de experimenteeromgeving – en bijbehorende begeleiding – beschikbaar. Tevens bestaat de mogelijkheid tot het afnemen van aansluitingsondersteuning en toepassingsondersteuning.

10.5.6 *Kostensoort*

Het experiment vraagt afhankelijk van de uitgangspositie van betrokken ketenpartners om een substantiële investering van de betrokken partijen, zowel in termen van tijd als middelen. De uitvragende partij is afnemer van de diensten van Logius.

10.5.7 *Do's en don'ts bij het experiment*

Vanuit de ervaringen vanuit SBR zijn er een aantal do's en don'ts bij het experiment.

- Zorg dat er voldoende tijd is ingepland voor het werken met de experimenteeromgeving en dat er ruimte is voor uitloop in de planning. Het testen van technologie kan meer tijd in beslag nemen dan partijen op voorhand denken en wensen (Brooks, 2006).
- Zorg voor een projectmatige ondersteuning van de keten.
- Zorg dat samen met de beheerder van de experimenteeromgeving (Logius) het gebruik ervan tijdig wordt ingepland, rekening houdend met de benodigde capaciteit.

10.6 De opschaling

De opschaling is de vierde fase van de SBR-verbredingsmethodiek. Ketenpartijen hebben het experiment doorlopen. De opschaling kan plaatsvinden wanneer er aan de volgende criteria is voldaan (als onderdeel van checkpoint C):

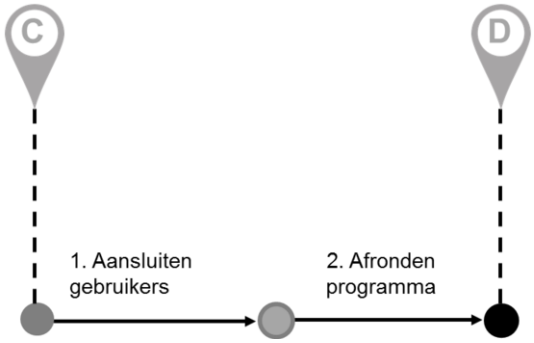
- De technische toets heeft geresulteerd in een functionerende verantwoordingsketen binnen de experimenteeromgeving.
- Afgevaardigden van de ketenpartijen participeren formeel in de structuren en gremia van de SBR-governance.
- Het plan voor opschaling is opgesteld en wordt toereikend geacht door het PLO.
- De ketenpartijen kunnen de benodigde capaciteit en middelen beschikbaar maken.
  De technologie is (na ontwerp en transitie) intern geaccepteerd voor productie.
- De ondersteuningsketen is geïmplementeerd.

De opschaling beoogt de volgende doelen te bereiken:

- De gebruikers van de verantwoordingsketen zijn aangesloten op SBR.
- Het verbredingstraject is afgesloten.

Er zijn twee onderdelen tijdens de opschaling. Het eerste onderdeel betreft de stapsgewijze aansluiting van de gebruikers op SBR, in overeenstemming met het markt-

ondersteuningsplan en het plan voor opschaling. Als de beoogde gebruikers zijn aangesloten op SBR is de keten in productie. Het tweede onderdeel betreft de afsluiting van het verbredingstraject.



Figuur 10.10 – Twee onderdelen bij de opschaling

10.6.1 *Aansluiten van gebruikers*

De opschaling heeft als doel om beoogde gebruikers stapsgewijs aan te laten sluiten bij SBR. Het is mogelijk dat hierbij een acceptatiedrempel overwonnen dient te worden. Immers, in navolging van de voorlopers dienen alle betrokken partijen in de verantwoordingsketen tot de implementatie van SBR over te gaan. Een reeds functionerende keten vanuit het experiment speelt een belangrijke rol om aan te tonen dat de toepassing van SBR mogelijk is. Net zo belangrijk is dat de gedeelde dienstverlener Logius partijen ondersteunt bij de aansluiting op SBR. Ketenpartijen zijn al gestart met de voorbereiding van de opschaling tijdens de interessefase, door het bespreken van de veranderopgave en veranderstrategie. Gedurende de detailanalyse & herontwerpfase is de veranderstrategie voortdurend onder de aandacht geweest. Met het experiment konden de gevolgen van de implementatie van SBR definitief worden bepaald en daarmee de veranderstrategie vastgelegd.

De opschaling verloopt in principe volgens het plan van opschaling. Alleen als er sprake is van uitzonderingen of onverwachte gebeurtenissen, kunnen ketenpartijen ervoor kiezen om bij te sturen.

Inmiddels wordt er een aantal productiediensten afgenomen bij Logius. De deliverables gedurende de opschalingsfase bestaan uit de geleverde output van de productiediensten. Denk hierbij bijvoorbeeld aan het beschikbaar stellen van alle relevante specificaties (zoals FAQ's) en productie- en monitoringsrapportages. Afhankelijk van de gekozen aansluitingsondersteuning levert Logius tevens zaken als een aansluitsuite en aansluitpakketten.

10.6.2 *Afronding programma*

Gedurende het SBR-verbredingstraject zijn de beoogde gebruikers aangesloten op SBR. De ketenpartijen zijn in staat gebleken om gedurende de route de checkpoints te passeren en eventuele (complexe) vraagstukken op te lossen. De bij aanvang projectmatige diensten van Logius worden na het doorlopen van de fasen ontwerp-tran-

sitie-acceptatie-productie inmiddels vanuit de lijn aangeboden. Doordat het programma stapsgewijs volledig overgegaan is in de structuren en diensten van de gedeelde dienstverlener Logius kan de programmatische besturing overgaan in de ketengovernance.

De stuurgroep voltooit het programma, draagt de resultaten en geleerde lessen (denk aan de gevonden oplossingen voor de technische roadblocks) over aan de gedeelde dienstverlener en heffen de stuurgroep en projectteams definitief op. Als het goed is, kijken de betrokken partijen met een tevreden gevoel terug op de route die gezamenlijk is afgelegd en de resultaten die daaruit voort zijn gekomen.

Tabel 10.22 – Overzicht deliverables afronding programma

1	Lessons learned	Een beschrijving van de geleerde lessen ter aanscherping en verbetering van onder andere de SBR-verbredingsmethodiek.

10.6.3 *Af te nemen diensten bij de gedeelde dienstverlener Logius*

Tijdens de opschaling wordt er een groot aantal diensten afgenomen. In aanvulling op de diensten die afgenomen kunnen worden tijdens het experiment zijn dat diensten in het kader van aansluitondersteuning (zoals het eventueel leveren van een aansluitsuite, trainingen, begeleiding en voorlichting) en productiediensten (zoals de productie i-processen, de taxonomie productie, bijbehorende managementinformatiesystemen, en 1e, 2e en 3e lijnsondersteuning).

10.6.4 *Kostensoort*

In de fase van opschaling maakt de uitvragende partij als afnemer bij Logius kosten voor de productiedienstverlening. De mate waarin de uitvragende partij ketenpartners wil ondersteunen bij het aansluiten op SBR bepaalt de andere kostenpost. De verticale ketenpartners zullen het belangrijk vinden dat de ketenambitie gehaald wordt en zullen bij de uitvragende partij erop aandringen dit deel niet te veronachtzamen. Afhankelijk van de mate waarin de ketenpartners al aangesloten zijn op SBR vraagt de opschaling om grotere of minder grote investeringen van de verantwoordingsplichtigen en hun dienstverleners.

10.6.5 *Do's en don'ts bij de opschaling*

Vanuit de ervaringen vanuit SBR zijn er een aantal do's en don'ts bij de opschaling.

- Het is begrijpelijk dat partijen weerstand kunnen bieden tijdens de opschaling. In hoofdstuk 3 en hoofdstuk 4 is al uitgebreid ingegaan op acceptatie. Het is van belang om voortdurend de veranderopgave van de betrokken partijen inzichtelijk te hebben en door middel van de geboden ondersteuning de drempel om SBR te implementeren te verlagen.
- Het heeft weinig zin veel tijd en energie in aansluitondersteuning te steken wanneer partijen geen uitzicht hebben op de voordelen van SBR of de 'verplichtstelling' van SBR.

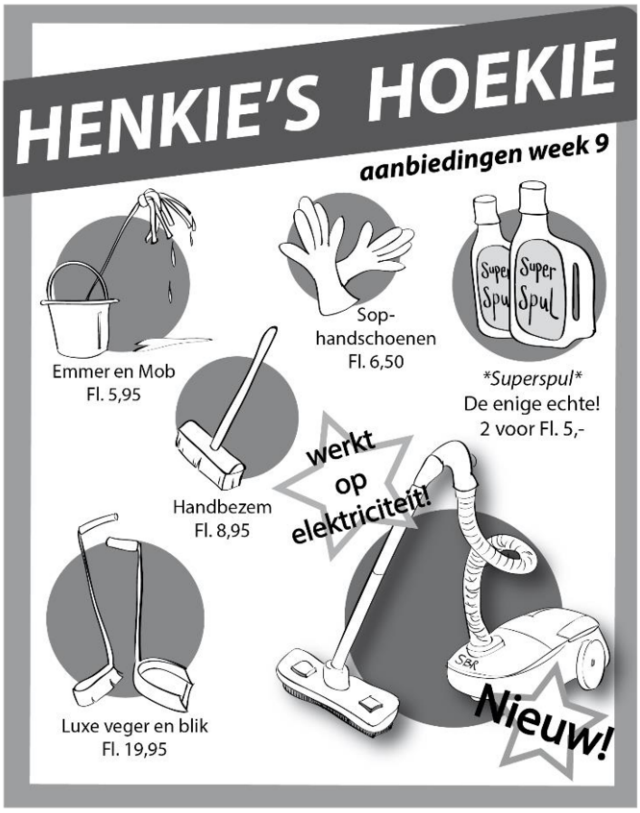
10.7 Reflectie op de SBR-verbredingsmethodiek

De SBR-verbredingsmethodiek is een generieke aanpak die kan worden gehanteerd voor uiteenlopende verantwoordingsketens. Ketenpartijen die de methodiek hanteren voor een uitermate complexe verandering zouden behoefte aan meer handvatten kunnen hebben. Ketenpartijen die de methodiek hanteren voor een relatief simpele verandering vinden enkele elementen waar de methodiek op hamert wellicht al wat overdreven. Wij realiseren ons dat er vele invulopties voor de methodiek mogelijk zijn. Ondanks dat de betrokkenen bij SBR deze aanpak 'the way to go' vinden, zijn wij er ons terdege van bewust dat de methodiek nog niet de status van 'best practice' kan worden toegerekend. Er is simpelweg te weinig ervaring met verbreding om erachter te komen op welke zaken juist meer of minder nadruk moet komen te liggen. Het meest duidelijk lijkt dit naar voren te komen, wanneer we de gevolgen van de aanname dat de toekomstige situatie bij aanvang bekend is in de praktijk ervaren. Zoals uitgebreid is toegelicht in hoofdstuk 4 is de grens tussen wel of niet bekend niet altijd duidelijk af te bakenen. In een verbredingstraject kunnen in praktijk 'scoping issues' ontstaan, omdat het bijvoorbeeld niet duidelijk is of een ketenpartij geraakt wordt indien de verantwoordingsketen mogelijk aanvullende functionaliteiten vereist. Ook kan het zijn dat na aanvang van het traject langzaam maar zeker het gedeelde beeld op de governance afneemt. De betrokken partijen dienen in beide gevallen te sturen en passende maatregelen te nemen. Welke do's en don'ts hiervoor gelden komt pas in de loop der tijd boven water. De functionarissen van Logius kunnen op basis van de opgedane ervaringen de methodiek verder aanvullen en bijschaven.

10.8 Afsluiting

Het wijzigingstraject van interesse in SBR tot een werkende SBR keten in productie vraagt om een methodische aanpak. Voor dit traject is de SBR-verbredingsmethodiek ontwikkeld. De SBR-verbredingsmethodiek kan partijen die aan de slag gaan met verbreding waardevolle informatie en inzichten bieden. De gefaseerde aanpak met go/no go momenten en checkpoints stelt partijen in staat om het programma verantwoord te doorlopen. Aan de hand van de inhoudelijke leidraad kunnen ketenpartijen de set van samenhangende karakteristieken van ketenverandering onderzoeken en zijn zij zich bewust van de relatie tussen de veranderwens, de veranderopgave en de veranderstrategie. Ketenpartijen zijn zich er met de methodiek in handen bewust van dat om verwachtingen naar marktpartijen goed te managen, er bij aanvang van het experiment voldoende draagvlak dient te zijn onder de belangrijkste ketenpartijen voor de toepassing van SBR. Tevens zijn ketenpartijen zich ervan bewust dat vanaf de interessefase er aandacht dient te zijn voor de brede acceptatie binnen de keten door het bespreken van de veranderopgave en de veranderstrategie, iets dat in de opschaling zijn vruchten gaat afwerpen. Ook zijn er do's en don'ts aangereikt. Hoe waardevol de methodiek ook mag zijn, er ligt nog veel ruimte tussen de methodiek op papier en datgene dat er in praktijk nodig is om een verbredingstraject tot een succes te maken. Zelfs als over enkele jaren de SBR-verbredingsmethodiek gemeengoed is en de status van 'best practice' toebedeeld kan krijgen, blijft een verbredingstraject mensenwerk waarvoor verstand van zaken, een professionele houding, gevoel van eigenaarschap, creativiteit en doorzettingsvermogen binnen het team is vereist.

11 Slotbeschouwing



In dit boek is SBR beschreven als opgave en als oplossing. Om inzicht te geven in de opgave werd een drietal hoofdstukken gewijd aan de aspecten die komen kijken bij het wijzigen van informatieketens. De hoofdstukken over de oplossing betreffen een grondige ontleding van de diverse onderdelen van SBR. De analyse – of het nu gaat over een uitgebreide beschrijving van XBRL of het stappenplan om aan te sluiten bij SBR – is een instrument om de wereld begrijpelijk te maken. Het heeft de lezer hopelijk voorzien van behapbare brokjes die gezamenlijk een werkende oplossing vormen. Voor een werkende oplossing is synthese nodig. Alleen door alle brokjes op de juiste manier bij elkaar te brengen, ontstaat een nuttig instrument. De toepasbaarheid – de voor- en nadelen – en de mogelijkheden van een instrument, laten zich echter moeilijk beschrijven via haar onderdelen. Een review van een stofzuiger zal zich meestal niet richten op het type plastic dat is gebruikt. Wel of geen 'krachtige motor' is nog een inwendig aspect waar u over geïnformeerd wordt. De review zal

zich met name richten op of het handvat lekker in de hand ligt, voor welke doelgroep hij geschikt is (hotels, thuisgebruik) etc. In deze slotbeschouwing willen wij SBR als oplossing op vergelijkbare wijze onder de loep nemen. Wat is de kracht van SBR als oplossing voor system-to-system verantwoorden? Welke barrières zien wij nog voor de oplossing? Welke perspectieven lonken en zijn er ook bedreigingen te onderkennen? We gaan hierbij uit van een tijdspanne van ongeveer vijf jaar.

De kracht van de SBR-oplossing

Kijken we naar de toepassing van SBR in het fiscale domein, dan kunnen we constateren dat het huidige SBR een werkende oplossing voor verantwoording biedt. De aanleverketen voor IB/VPB is grootschalig in productie. De Belastingdienst heeft voldoende vertrouwen in SBR om te sturen naar een situatie waarin voor de fiscale verantwoording SBR als enige system-to-system modaliteit overblijft. Dit is voor SBR als oplossing essentieel. Ten eerste omdat de fiscale keten hoge eisen aan een oplossing stelt. Als een oplossing voldoende scoort voor belastingaangifte zit het in de basis wel goed. Ten tweede geldt dat doordat bijna iedere organisatie te maken heeft met de Belastingdienst veel partijen zijn aangesloten op SBR. Dit biedt potentie voor andere verantwoordingsketens. Voor de verplichtstellingsagenda van de KvK geldt hetzelfde, maar dan op het niveau van gegevens. Veel uitvragende partijen zijn geïnteresseerd in de jaarrekening die relevant is voor hun sector. De implementatie van SBR in andere verantwoordingsketens wordt ook door de verplichte toepassing in het jaarrekeningendomein een stuk gemakkelijker.

De uitbreidbaarheid van het concept is een belangrijke kracht van SBR. Basisfuncties worden op een standaard manier ingevuld, waardoor de aandacht in de verantwoordingsketen uit kan gaan naar de elementen die juist voor die keten van belang zijn. De uitwisseling van gegevens wordt bij SBR geautomatiseerd met behulp van internationaal geaccepteerde standaarden.

Voor de politiek is SBR interessant. SBR kan verantwoording naar de overheid goedkoper maken. Een overheid die er voor kiest verantwoordingsketens op een standaard wijze in te richten, zorgt er voor dat zij zelf en de verantwoordingsplichtigen hier vroeg of laat de vruchten van gaan plukken. Waar de verantwoordingsketen nog veel handmatige bewerkingen kent of uitgaat van een niet-gestructureerde aanlevering van gegevens, zal SBR de verantwoording ook verbeteren. De transitie die in zo'n geval van verantwoordingsketens gevraagd wordt is substantieel en hier moet dan ook niet lichtzinnig over gedacht worden. Er kunnen bij een ketenwijziging altijd partijen de dupe worden van de invoering van een nieuwe systematiek. Doordat SBR een methodiek biedt gericht op deze transitie, is SBR waarschijnlijk wel de meest efficiënte wijze om een verantwoordingsketen system-to-system te integreren.

Logius kan de gehele levenscyclus van een SBR-verantwoordingsketen vanuit een vast omlijnde dienstcatalogus ondersteunen. Logius helpt bij een eerste aansluiting, levert productiediensten en verzorgt eventuele (door)ontwikkeling. Hiermee is een volwassen SBR-serviceorganisatie gecreëerd. Deze werkwijze geeft een hoge mate van inzicht in de kwaliteit en kosten van het beheer en onderhoud van generieke onderdelen van de verantwoording. Deze volledige dienstverlening kan voor uitvragende partijen een comfortabele gedachte zijn. In de praktijk zien we voor de SBR

oplossing nog wel een aantal barrières die uitvragende partijen moeten overwinnen, voordat zij toegeven aan deze positie in de keten.

Barrières voor toepassing

Met de toepassing van SBR verliest een uitvragende partij autonomie. Met name op aspecten die buiten zijn core business zouden moeten liggen. Over het SBR-concept bestaan echter nogal wat misverstanden. Misverstanden die deels door weerstand tegen veranderingen – maar soms ook door onhandigheid – in leven worden gehouden. SBR zal moeten blijven investeren om deze misverstanden uit de wereld te helpen. Onderstaand een paar in het oog springende onderwerpen waar vaak verwarring over bestaat:

- SBR is niet alleen nuttig voor de verwerking van financiële gegevens. Ieder gegeven kan met behulp van SBR verwerkt worden. In het voedseldomein bestaat een XBRL-taxonomie voor microbiologische criteria.
- Store once, report many, moet vertaald worden als éénmalig inrichten, meervoudig aanleveren en niet als eenmaal aanleveren, meervoudig gebruik. Het SBR concept gaat dus niet uit van een grote database waar een verantwoordingsplichtige al zijn informatie in kiepert, die vervolgens door verschillende uitvragende partijen geleegd wordt.
- SBR heeft niet alleen zin wanneer uitvragende partijen dezelfde of ongeveer dezelfde gegevens uitvragen. Het hergebruik van begrippen levert niet de meeste en zeker niet de enige winst op bij SBR. De standaardisatie van SBR bevat zeer veel aspecten, bijvoorbeeld het gebruik van dezelfde koppelvlakken en een gedeelde dienstverlener. Bovendien kan SBR ook winst opleveren doordat de keten verder geautomatiseerd wordt.
- SBR heeft niet alleen voordelen voor de overheid. De winstverwachtingen voor het bedrijfsleven waren bij aanvang van SBR overspannen. Ook zijn potentiële en gerealiseerde winsten moeilijk meetbaar. Dit wil niet zeggen dat zij er niet zijn. Het is gemakkelijk te beredeneren dat een grootschalige standaardisatie door brede toepassing van SBR voor BV Nederland een efficiëntere verantwoording betekent.
- Nee, SBR bevat niet net zoveel calorieën als een pakje boter![40]

Misverstanden kunnen blijven bestaan door gebrek aan kennis. Hier ligt misschien de grootste barrière die SBR moet overwinnen. Om werkelijk in te kunnen schatten wat de SBR-oplossing kan betekenen binnen een verantwoordingsketen, moet de verantwoordingsketen als totaalsysteem overzien worden. Dit boek toont aan hoeveel aspecten hierbij komen kijken. Verantwoordingsketens zijn overwegend reactief ingericht. Zij zijn dus vaak laagje voor laagje opgebouwd en niet vanuit een integrale architectuur vormgegeven. Personen in de keten hebben zich gespecialiseerd in één aspect van de keten en zullen SBR vanuit dit perspectief beoordelen. Hier geldt de

[40] Dit om aan te geven dat misverstanden schadelijk kunnen zijn en serieus genomen moeten worden. De fabrikant van een bekend ijsje kwam serieus in de problemen door de mythe dat het ijsje net zoveel calorieën zou bevatten als een pakje boter: De feiten: het ijsje = 283 Kcal (80 gram) en het pakje boter waar mensen aan denken 1838 Kcal (250 gram). Zowel per 100 gram als per eenheid was de bewering onjuist.

metafoor van de blinde mannen die gezamenlijk de olifant beschrijven.[41] Bestuurders die zich afvragen of SBR voor hen nuttig kan zijn, consulteren terecht de partijen die actief zijn in de verantwoordingsketen. Een ieder richt zich op het eigen stukje van de verantwoordingsketen en op SBR en komt terug met een oordeel over SBR. Met een beetje pech blijft de totaaloplossing en de toegevoegde waarde van het geheel op deze wijze buiten beeld. Als het geheel wel overzien wordt, zal men de potentie juist inschatten, maar ook met een dilemma geconfronteerd worden. SBR gaat uit van een integraal ontwerp. Dit betekent fundamentele en structurele baten op langere termijn. Hier hoort overwegend een fundamentele transitie bij, waarbij niet het aansluiten op SBR maar het uitschakelen van bestaande modaliteiten ketenpartijen serieus pijn kan doen. Ondanks de business case voor de keten kan het verkrijgen van draagvlak voor de verbetering moeilijk zijn. Dit draagvlak is vaak gemakkelijker te verkrijgen wanneer ketens al voor een transitie staan – een grootschalige verbouwing in het huis kan hét moment zijn om over te gaan op een ander verwarmingssysteem.

Perspectieven

Voor SBR is het dus gunstig dat veel verantwoordingsketens momenteel in beweging zijn. In de afgelopen jaren is veel te doen geweest over de verantwoording van maatschappelijke ondernemingen. Scholen, zorginstellingen, ziekenhuizen en woningbouwcorporaties verantwoorden zich stuk voor stuk aan de overheid over substantiële publieke gelden. De overheid heeft desalniettemin onvoldoende grip gehad op deze sectoren. SBR kan een bijdrage leveren aan een betere verantwoording in de nieuw in te richten verantwoordingsketens. De beheersing van overheidsfinanciën is een van de speerpunten in het beleid. Beheersing begint met inzicht in de uitgaven. Met de verschuiving van bestuursbevoegdheden naar het decentrale veld (gemeenten), zal de keten van verantwoording complexer worden en is er behoefte aan de herinrichting van verantwoordingsketens ontstaan. Deze transitie brengt zeker kansen voor SBR met zich mee.

Ook het domein van financieel toezicht is in beweging. In dit laatste domein liggen er zeker mogelijkheden voor SBR, omdat XBRL internationaal snel terrein wint als enige standaard voor digitale verantwoording. Hierbij is het wel van belang dat er gestuurd wordt op een complementaire toepassing van deze standaard in plaats van een conflicterende inrichting. Dit vraagt om een centrale regie op de afstemming met de internationale ketens, wat één van de uitdagingen is waar SBR mee geconfronteerd wordt.

Uitdagingen

Een bredere toepassing van SBR zal gepaard blijven gaan met nieuwe governancevraagstukken. Zoals uitgebreid aan de orde is geweest, is het vormgeven van de ketengovernance eerder de opgave dan dat de techniek dit is. Het implementeren van het e-ID stelsel binnen het SBR domein is een concrete opgave die thans voor de deur

[41] Iedere blinde wijze pakt een stukje van de olifant en probeert vanuit dit stukje de hele olifant te beschrijven. De olifant is als een slang (voor de wijze bij de slurf), als touw (de staart), als een boom (de poot), als een muur (de zij), als een waaier (het oor).

staat. Hoe SBR binnen de eOverheid gepositioneerd wordt, bepaalt uiteindelijk de business case van SBR binnen het publieke domein. We hebben al gezien dat er soms wetswijzigingen nodig zijn om een efficiënte keten af te dwingen. Hier is dus de wetgever aan zet. Wanneer er politiek draagvlak ontstaat voor een overheid die uitgaat van sterk geautomatiseerde verantwoordingsketens en SBR hier als de oplossing ziet, kunnen ontwikkelingen snel gaan. Afbreukrisico's zijn er ook in het geval dat er niet gekozen wordt en een heldere integrale visie op verantwoording uitblijft. Verantwoordingsketens blijven dan leunen op verschillende modaliteiten voor dezelfde vormen van verantwoording en SBR – noch substituten voor SBR – levert in zo'n geval de potentiële winsten op. Dit speelt ook wanneer partijen gaan 'cherrypicken', oftewel alleen één onderdeel van de SBR-oplossing toepassen. Een beetje standaardiseren is als een beetje zwanger zijn.

Conclusie

Het lijkt het erop dat SBR zich als nuttige oplossing heeft gekwalificeerd. Zeker waar dit het fiscale domein betreft en waar het gaat om het deponeren van de jaarrekening. Als je het ons vraagt, denken wij dat dit een waardevolle ontwikkeling is. Of wij hierin objectief genoeg zijn moet nog blijken. Bij de invulling van dit boek is er alles aan gedaan zo'n eerlijk mogelijk beeld te geven van alle facetten van SBR, zodat de lezer in staat is zelf te oordelen. Hoe SBR zich ook verder ontwikkelt, de reikwijdte van SBR is inmiddels groot en het domein van verantwoording en digitalisering is nog volop in beweging. De voortgang van deze casus blijft vanuit diverse oogpunten dus uitermate interessant. Centrale vraag blijft welke titel een volgende of herziene versie van een integraal werk over SBR zal dragen: SBR van opgave naar oplossing naar…

Bijlagen

Bijlage A – Achtergrond SBR

Inleiding
Standard Business Reporting (SBR) is een oplossing voor verantwoording. De overheid wil dat verantwoording efficiënter en effectiever verloopt, zowel voor haarzelf en voor andere uitvragende organisaties als voor ondernemingen die verantwoording moeten afleggen.

Deze bijlage geeft de lezer van dit boek de nodige achtergrond over SBR. De beschrijving geeft hiertoe inzicht in de historie en de onderliggende beleidsdoelstellingen van SBR en de betrokken partijen. Ook krijgt de lezer inzicht in enkele kenmerken van SBR die van belang zijn voor een goed begrip van SBR. Achtereenvolgens komen aan bod:

- Het speelveld van financiële verantwoording en de spelers
- De voorgeschiedenis van SBR: XBRL, het NTP en het SBR Programma
- Belangrijke kenmerken van SBR

In deze achtergrondbeschrijving komt een aantal technische en organisatorische elementen van het huidige SBR naar voren. Voor meer details verwijzen we naar de hoofdstukken van deel B. Hier leggen we de nadruk op de betrokken partijen en de denktrends binnen de keten die voor het SBR-initiatief een rol spelen.

Het speelveld en de spelers
Ondernemingen en andere organisaties moeten zich over hun handelen verantwoorden naar de samenleving, naar overheden en naar andere organisaties. Voorbeelden zijn het publiceren van jaarverslagen, aangiften bij de Belastingdienst en kredietrapportages naar banken. In dit pluriforme speelveld van financiële verantwoording zijn verschillende ketens en stakeholders te onderscheiden.

Voordat we ingaan op de verschillende verantwoordingsketens lichten we twee rollen kort toe: intermediairs en softwareleveranciers. Intermediairs zijn de accountants, boekhouders, financieel adviseurs, belastingconsulenten en fiscaal adviseurs die door ondernemers worden ingehuurd. In de praktijk zijn het voornamelijk de intermediairs, en niet de ondernemers zelf, die te maken hebben met het daadwerkelijk aanleveren van verantwoordingsinformatie naar banken en overheid.

De softwareleveranciers zijn de partijen die de administratieve softwarepakketten voor bedrijven maken. Ondernemers en intermediairs gebruiken dergelijke pakketten om de bedrijfsadministratie of boekhouding in bij te houden, vaak met aparte pakketten of aparte functionaliteiten voor fiscale zaken (opstellen aangiften) en voor het opstellen van jaarverslaggeving.

Eén van de verantwoordingsketens in het speelveld is de belastingketen. Verschillende (rijks)belastingwetten verplichten ondernemingen om belasting af te dragen, en vaak ook om in dat kader aangifte te doen bij de Belastingdienst. Een ondernemer krijgt daar meerdere keren per jaar mee te maken. De periode waarover de ondernemer aangifte doet (de frequentie) verschilt per belastingsoort. Zo doet de ondernemer in principe jaarlijks de VPB-aangifte (op grond van de Wet op de vennootschapsbelasting 1969) en aangifte inkomstenbelasting voor ondernemers 'IB-winst' (Wet op de inkomstenbelasting 2001). Veel ondernemers doen elk kwartaal OB-aangifte (Wet op de omzetbelasting). Afhankelijk van de hoogte van de omzet kan de aangifteplicht ook maandelijks of jaarlijks zijn. De opgave ICP (IntraCommunautaire Prestaties, voorheen ICL) wordt ook maandelijks, per kwartaal of jaarlijks gedaan. Sinds 1 januari 2005 zijn bedrijven verplicht deze aangiften en opgave elektronisch te doen.[42]

Ondernemers kunnen zelf aangifte doen, maar de meeste (kleinere) ondernemers schakelen een intermediair in. De boekhouding is een van de onderdelen binnen bedrijven waar automatisering al langere tijd breed wordt toegepast (Jans, 1991). Veel intermediairs gebruiken boekhoudsoftware van waaruit zij de IB aangifte en de OB aangifte genereren, en specifieke software voor het samenstellen van de VPB aangifte. Vanuit de software kan de aangifte system-to-system worden aangeleverd. Dit betekent dat de software en systemen via een koppelvlak met elkaar communiceren, in principe zonder menselijke interactie. Een alternatief is het invullen van de aangifte op een formulier op de site van de Belastingdienst, waar met name de kleine groep zelf-aangevende ondernemers gebruik van maakt. De Belastingdienst ontvangt jaarlijks miljoenen elektronische aangiften van ondernemingen.

Naast belastingaangiften, hebben ondernemers te maken met publieke jaarverslaggeving. De in Nederland gevestigde ondernemingen hebben de wettelijke verplichting om jaarlijks een jaarrekening op te maken en te deponeren bij de Kamer van Koophandel. Niet voldoen aan die plicht kan leiden tot een (strafrechtelijke) boete en bestuurdersaansprakelijkheid.[43]

De jaarrekening geeft een jaarlijks overzicht van de financiële situatie van een bedrijf. De jaarrekening bestaat uit de balans, de winst- en verliesrekening en de toelichting.[44] Middelgrote en grote ondernemingen zijn verplicht om een controleverklaring van een accountant bij de jaarrekening te publiceren.[45] Kleine ondernemingen hoeven alleen een (vereenvoudigde) jaarrekening te deponeren.
Naar aanleiding van Europese ontwikkelingen kunnen ondernemingen - doorgaans zijn dat hun intermediairs namens hen - sinds 2005 de jaarrekening elektronisch deponeren, bijvoorbeeld in PDF.[46] Met behulp van een 'rapportgenerator' wordt de

[42] Artikel 8 Awr, gewijzigd door Het Belastingplan 2004, Staatsblad 526 van 29 december 2003.
[43] Artikel 2:394 BW; artikel 2:248 BW; artikel 1 ad 4 Wet op de economische delicten.
[44] Artikel 2:361 BW en Richtlijn 78/660/EEG, artikel 2 lid 1.
[45] Artikel 2:392 BW en Richtlijn 78/660/EEG, artikel 47.
[46] Artikel 3 lid 2 van richtlijn 68/151/EEG; artikel 3 lid 3 van het Handelsregisterbesluit. Ingevoerd met het Besluit tot wijziging Handelsregisterbesluit 1996 en Besluit modellen jaarrekening van 22 december 2005, Stb. 2005, 729.

jaarrekening door de intermediair uit de boekhouding gegenereerd. Ook is het nog steeds mogelijk om op papier te deponeren.

Een derde vorm van financiële verantwoording wordt uitgevraagd door het Centraal Bureau voor de Statistiek (CBS). Het CBS doet bij ondernemers steekproefsgewijs verschillende uitvragen, op verschillende momenten. Zo vraagt CBS maandelijks bij een selectie bedrijven (steekproef) kortetermijnstatistieken uit, en jaarlijks investerings- en productiestatistieken. De ondernemers die in de steekproef zitten ontvangen een brief van het CBS en zijn verplicht de gegevens binnen de gestelde termijn aan te leveren (anders riskeren zij een boete van het CBS).[47] Ondernemers kunnen de uitgevraagde gegevens in principe schriftelijk of elektronisch bij het CBS indienen. Het CBS verstrekt echter alleen op verzoek vragenlijsten op papier. Ondernemers worden geacht de statistieken online in te vullen bij het CBS aan de hand van inloggegevens die in de brief staan vermeld. Het CBS haalt ook gegevens op bij andere instellingen, zoals de Belastingdienst.

Ook tussen private partijen worden financiële gegevens uitgewisseld. De bank vraagt ondernemers om financiële informatie ten behoeve van de kredietverlening; de kredietrapportage. Veel ondernemers leggen het verzorgen van deze verantwoording bij hun intermediair neer.

Een vormende factor van het speelveld is het kabinetsbeleid. In de jaren negentig is er vanuit het kabinet steeds meer aandacht voor het beperken van administratieve lasten en wordt er ingezet op een meer elektronische overheid. Het Ministerie van Economische Zaken (EZ) is verantwoordelijk voor het bedrijvendomein en zoekt ICT-oplossingen om administratieve lasten te verminderen. In 2002 start EZ een samenwerkingsverband met het bedrijfsleven: het programma ICT en Administratieve Lastenverlichting (ICTAL). Opdracht: met ICT-voorzieningen de administratieve rompslomp bij het bedrijfsleven verminderen.[48]

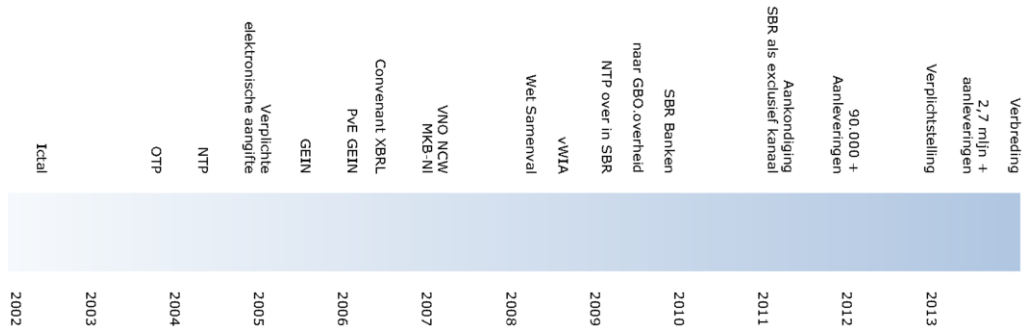
Verschillende voorzieningen worden gelanceerd binnen ICTAL, sommige succesvol, andere minder. Een voorbeeld van een concept dat niet blijkt te werken is het IDEA-concept.[49] Een beleidsexperiment waarbij wordt gekeken of het mogelijk is dat de overheid een gestandaardiseerde set bedrijfsgegevens direct uit de administratie bij het bedrijf ophaalt. Dit blijkt niet de oplossing voor ketenherinrichting. Technisch kan het, maar er zijn juridische barrières: het zou een "*ongewenste en niet noodzakelijke verschuiving van verantwoordelijkheden tussen overheid en bedrijfsleven*" kunnen betekenen, aldus de Staatssecretaris.[50]

---

[47] Artikel 33 jo. 43 Wet op het CBS.
[48] www.e-overheid.nl
[49] IDEA staat voor Interchange of Data between Enterprises and Administrations.
[50] Brief van de Staatssecretaris van EZ aan ACTAL, aangaande het Advies ACTAL ICT-beleid vermindering administratieve lasten, van 30 augustus 2004.

Eén van de meer succesvolle voorzieningen die binnen ICTAL worden ontwikkeld is de Overheidstransactiepoort (OTP) (2004): één adres van de overheid waar de ondernemer zijn gegevens elektronisch naar kan verzenden. De Overheidstransactiepoort zorgt ervoor dat die informatie op een 'intelligente en veilige manier' bij verschillende overheidsinstanties terechtkomt. EZ vergelijkt de OTP met een postkantoor, maar dan elektronisch.[51] Ook is er binnen de ICT aanpak van de Minister van Economische Zaken, naast de technische voorzieningen, toenemende aandacht voor de mogelijkheden t.a.v. het geleidelijk harmoniseren van de informatie die verschillende overheidsinstanties vragen.[52] Uit onderzoek naar ketenherinrichting concludeert men dat er bij de informatie-uitvraag zoveel mogelijk moet worden aangesloten bij de bedrijfsfuncties en gebruik moet worden gemaakt van standaarden.[53]

De eerste stappen richting gestandaardiseerd verantwoorden zijn gezet.



Figuur A1 - Tijdslijn SBR

Bovenstaande tijdslijn geeft een indruk van ontwikkelingen die in het kader van SBR relevant zijn. In het voorgaande is het eerste deel van de tijdslijn, met ICTAL en OTP geschetst. Hierna wordt ingegaan op het vervolg van de tijdslijn: het Nederlands Taxonomieproject en het ontstaan en de ontwikkeling van SBR.

[51] Brief van de Minister van EZ aan de Tweede Kamer van 27 mei 2004; Brief van de Staatssecretaris van EZ aan de Tweede Kamer van 9 juni 2005; beide aangaande het Kabinetsplan aanpak administratieve lasten (29 515).
[52] Brief van de Minister van EZ aan de Tweede Kamer van 27 mei 2004, aangaande het Kabinetsplan aanpak administratieve lasten (29 515).
[53] Brief van de Staatssecretaris van EZ aan ACTAL, aangaande het Advies ACTAL ICT-beleid vermindering administratieve lasten, van 30 augustus 2004.

XBRL en het Nederlandse Taxonomie Project

De visie van de believers
De periode 2004 – 2007 kenmerkt zich door een relatief kleine groep 'believers' die een een gezamenlijke visie voor de toekomst heeft: de verantwoording voor ondernemingen en overheidsinstellingen een stuk goedkoper en beter maken, door gebruik van:

- Een gedeelde taxonomie
- Een generieke (proces)infrastructuur
- Een gedeelde dienstverlener voor het beheer

Technisch: taxonomie en procesinfrastructuur
In 2004 starten het Ministerie van Justitie en het Ministerie van Financiën het Nederlandse Taxonomie Project (NTP). Het project is erop gericht één XBRL-taxonomie te maken voor de jaarrekening en de fiscale opgaven/aangiften waar bedrijven mee te maken hebben. In juni 2005 is de eerste testversie van de Nederlandse Taxonomie gereed. Met proefopstellingen voert een beperkt aan tal betrokkenen ketentesten uit. Het NTP geeft daarmee invulling aan het eerste element van de visie: een gedeelde taxonomie.[54]

In 2005 kondigt de Staatssecretaris van Economische Zaken de implementatie van een nieuw koppelvlak in de OTP aan die webservices mogelijk maakt en daarmee een belangrijke voorwaarde voor elektronisch gegevensverkeer voor financiële verantwoordingsinformatie vervult. De Staatssecretaris geeft aan dat dit zal worden uitgewerkt in een Programma van Eisen voor een Generieke Infrastructuur (GEIN), dat in opdracht van het Ministerie van EZ wordt opgesteld, en waar het NTP gebruik van zal gaan maken.

In mei 2006 deponeert Minister Donner de eerste jaarrekening met behulp van XBRL. In juni van dat jaar wordt de eerste versie van de Nederlandse Taxonomie gepubliceerd. In diezelfde maand wordt het Programma van Eisen GEIN afgerond. Het is de bedoeling dat – met als launching customer het NTP project – er een generieke infrastructuur wordt ontwikkeld om het voor bedrijven makkelijker te maken om te voldoen aan hun verantwoordingsverplichtingen richting de overheid. De generieke infrastructuur is gebaseerd op Service Oriented Architecture (SOA). Het (her)gebruik van losse services zorgt voor de nodige flexibiliteit, zodat de infrastructuur generiek te gebruiken is voor verschillende procesgangen. De bedrijven kunnen hier via één koppelvlak gebruik van maken, zodat ze niet meer te maken hebben met specifieke koppelvlakken voor Belastingdienst, CBS, gemeenten etc. Met het PvE GEIN wordt het tweede element van de visie, de procesinfrastructuur, tot uitvoering gebracht.

---

[54] De taxonomie is een woordenboek van begrippen opgesteld door betrokken overheidspartijen. De begrippen zijn afkomstig uit wet- en regelgeving. Ondernemingen gebruiken de taxonomie om verantwoordingen op te stellen op basis van hun eigen bedrijfsadministratie.

Organisatorisch: convenant en gedeelde dienstverlener
Op 9 juni 2006 tekent een eerste groep organisaties een publiek/privaat convenant. Daarin spreken zij af om door toepassing van de Nederlandse XBRL-taxonomie administratieve lastenverlichting voor ondernemers te realiseren, door vereenvoudiging van het verzamelen, vaststellen en uitwisselen van financiële verantwoordingsinformatie die betrekking heeft op de jaarrekening, fiscale aangiftes en statistiekopgaven.[55] Namens de overheid tekenen de Ministers van EZ, Financiën, Justitie en Binnenlandse Zaken. Dit laatste ministerie tekent vanuit haar verantwoordelijkheid voor GBO.Overheid, de organisatie die in het convenant genoemd staat als beheerder van de voorzieningen (taxonomie en procesinfrastructuur) en die tevens beheerder van de OTP is geworden (een start van de invulling van de gedeelde dienstverlening conform de visie). Met het opnemen van de procesinfrastructuur in het convenant is de verbreding van de scope van het NTP een feit. Het NTP houdt zich niet alleen meer bezig met gegevensstandaardisatie, maar gaat ook een belangrijke rol spelen in de standaardisatie van verantwoordingsprocessen en het realiseren van gedeelde voorzieningen. Het project ontwikkelt zelf een eerste versie van de procesinfrastructuur en blijft de nieuwe versies van de Nederlandse Taxonomie (NT) ontwikkelen en beheren.

Het convenant wordt ook getekend door een aantal intermediairs en softwareleveranciers dat betrokken is bij de ontwikkeling. Zij hebben de taak om in de markt tijdig de nodige infrastructuren en softwarepakketten 'klaar voor XBRL' te ontwikkelen en hun klanten gerelateerde diensten aan te bieden (en de efficiëntie voordelen door te berekenen). Daarnaast tekenen koepelorganisaties van accountants en fiscale adviseurs. De overheid en de uitvragende partijen (Belastingdienst, KvK, CBS) onderhouden en beheren de NT de processtandaarden en de voorzieningen. Het convenant legt de eerste vorm van samenwerking en organisatie in kader van SBR formeel vast. De vele betrokken partijen lijken echter wel een uitdaging te vormen voor het creëren van een duidelijke richting en prioriteiten binnen het SBR-initiatief.

Implementatie blijft achter – nieuwe initiatieven
Voorjaar 2007 sluiten VNO-NCW en MKB Nederland aan bij het convenant uit 2006. Staatssecretaris De Jager geeft op dat moment aan dat hij verwacht dat in 2008 alle belastingaangiftes door ondernemers met behulp van XBRL gedaan kunnen worden. Maar hoewel de verwachtingen dan nog hooggespannen zijn valt het gebruik van de NTP-voorziening tegen. Het project zoekt de oplossing in nieuwe initiatieven. Men hoopt bijvoorbeeld met een wijziging in Boek 2 van het Burgerlijk Wetboek een grote impuls te geven aan het gebruik van de taxonomie. Met deze wijziging wordt de daadwerkelijke samenval van winstaangifte en jaarrekening voor het MKB gerealiseerd.[56] Een vergelijkbare interventie betreft de realisatie van de ver-

[55] Convenant van samenwerking tussen overheid en markt over gebruik van de Nederlandse XBRL-taxonomie, Den Haag, 9 juni 2006.
[56] Artikel 2:396 lid 6 BW, ingevoerd door de Wet samenval fiscale en commerciële jaarrekening (Staatsblad 217, 2008). Daarmee is het voor kleine rechtspersonen mogelijk om jaarrekeningen op te stellen

korte winstaangifte. Een kleine groep (circa acht) intermediairs en de Belastingdienst tekenen eind 2008 convenanten ten behoeve van verkorte winstaangifte vennootschapsbelasting en horizontaal toezicht.[57] Staatssecretaris De Jager tekende namens de Belastingdienst de convenanten die een pilotperiode van twee jaar kennen en die het voor de intermediairs mogelijk maken in XBRL een sterk verkorte winstaangifte aan te leveren.

Het SBR Programma

Transitie in gebruik en in governance
Vanaf 2009 volgt een periode van transitie naar een meer gefocuste opdracht en uitvoering met als doel het geloofwaardig gebruik van SBR door een aantal 'voorlopers' in de keten.

Begin 2009 gaat NTP over in Standard Business Reporting (SBR).Vanuit de Vernieuwing Rijksdienst (VRD) is er geld vrij gemaakt voor het SBR Programma. Met de naamswijziging sluit het programma aan op de internationale naamgeving, zoals onder meer in Australië. Dit land is, geïnspireerd op Nederland, een groot project gestart en maakt dankbaar gebruik van gerealiseerde concepten. Er wordt voor het SBR Programma in Nederland een duidelijk doel vastgesteld: een generieke overheidsoplossing voor system-to-system (S2S) uitwisseling te realiseren en gedeelde verwerking van verantwoordingsinformatie in te richten.
In maart 2009 gaat de procesinfrastructuur over naar GBO.Overheid. Het gebruik van XBRL (de NT) voor verantwoordingen blijft nog steeds ver achter bij de verwachtingen. Op dat moment zijn er nog geen tienduizend berichten aangeleverd. Dit terwijl er meerdere honderdduizenden berichten per jaar nodig zijn om maar in de buurt te komen van de beoogde lastenvermindering. De overheid en betrokkenen zien een overmatige focus op allerlei nieuwe initiatieven – "*onvoldoende geïmplementeerde en uitgewerkte concepten*" - als grootste oorzaak voor het uitblijven van aanlevering. De betrokken ministeries besluiten de focus van SBR te verleggen naar implementatie en gebruik van de NT, en de aansluiting van marktpartijen op de infrastructuur voor berichtuitwisseling met KvK, Belastingdienst en CBS.

De uitvoering van het SBR Programma - inclusief het beheer van de Nederlandse Taxonomie - wordt overgedragen aan GBO.Overheid. Daarmee is deze organisatie ook verantwoordelijk voor de afstemming en governance rondom de infrastructuur en de taxonomie die zij beheert. In het najaar van 2009 wordt er in het kader van de governance een overheidsstuurgroep ingesteld, waarin zowel de uitvragende partijen als de betrokken ministeries op DG-niveau zitting nemen, die de vinger aan de pols houdt voor de nieuwe implementatie. De SG van het Ministerie van EZ is in eerste instantie voorzitter van deze stuurgroep. Met de marktpartijen wordt op hoog niveau

volgens fiscale grondslagen, dus met gebruikmaking van de waarderingsgrondslagen zoals deze worden gebruikt voor de aangifte vennootschapsbelasting.
[57] Convenant betreffende een *pilot* ten aanzien van de verkorte winstaangifte voor de vennootschapsbelasting op basis van de Nederlandse Taxonomie en gebruikmakend van Procesdefinities, 11 december 2008.

afgestemd in het SBR Beraad. De uitvragende partijen en Logius hebben een gezamenlijk implementatieplan opgesteld voor het realiseren van een substantiële toepassing van SBR in het financiële domein en het realiseren van de kaders voor een verantwoorde verbreding van het concept (toepassing in andere ketens). Het projectleidersoverleg (PLO) krijgt de opdracht om dit 'substantieel gebruik' te realiseren, te beginnen bij de op dat moment betrokken marktpartijen (de voorlopers). Het wordt zichtbaar dat de governance nog niet voldoende is toegerust voor opschaling. Er zijn duidelijker afspraken nodig over webservices, service levels etc. Daarnaast ligt er voor het vernieuwde SBR Programma meteen een interessant governance vraagstuk op tafel: Staatssecretaris Heemskerk kondigt in november 2009 aan dat drie grote banken voor hun kredietrapportages over zullen gaan op SBR. Deze banken zijn verenigd in het Financiële Rapportages Coöperatief (FRC). Zij zullen gebruik maken van een eigen bancaire infrastructurele voorziening (BIV) en een eigen extensietaxonomie. De banken geven aan zich te conformeren aan overheidsstandaarden (en ernaar te streven dezelfde koppelvlakken te hanteren als de overheid). Echter, hoe dit operationeel geborgd moet worden is nog niet uitgewerkt.

Naar grootschalig gebruik

In 2010 stelt het programma zichzelf voor 2010-2011 tot doel om naar grootschalig gebruik - een grote stroom XBRL berichten binnen het financiële domein - en stabiele uitvoering en beheer van de voorzieningen toe te werken. Door intensieve samenwerking, publiek-private afstemming en marktbewerking realiseren de SBR partijen een flinke opschaling. In 2011 groeit het aantal aangeleverde OB-aangiften tot circa 87.000 en het aantal jaarrekeningen tot 3.500. De organisatie verandert in deze periode. De opschaling vergt een volwassen beheerorganisatie, focus op shared services en hernieuwde aandacht voor de governance, met name op het raakvlak met de markt.[58] Het programma acht het van belang dat de aangesloten bedrijven in de uitvoering voldoende ondersteund worden, en dat nieuw aansluitende bedrijven passende ondersteuning krijgen. Daarbij zorgen Logius en de uitvragende partijen dat hun servicedesks contact met elkaar hebben, dat externe communicatie onderling wordt afgestemd en dat op voorlichtingsdagen alle aspecten besproken worden. Het PLO vervult een belangrijke rol door voor de opdrachten aan de gedeelde dienstverlener (de uitvoeringsorganisatie Logius, voorheen GBO.Overheid) te zorgen. Er worden antwoorden gezocht voor het vraagstuk over hoe de financiering van de outsourcing en een meerjarenbegroting eruit zouden moeten zien. Ook is er gaandeweg meer aandacht ontstaan voor de organisatorische en juridische randvoorwaarden. Tijdens het NTP diende een juridische bijlage bij PvE GEIN hiertoe. In het SBR Programma is voorzien in een dedicated functie voor compliance aangevuld met een werkgroep compliance voor afstemming met de uitvragende partijen.

[58] Afstemming met de markt gebeurt bijvoorbeeld door aanleveraars te betrekken bij het testen van de taxonomie, voorafgaand aan de bestuurlijke vaststelling en publicatie. De taxonomie krijgt hiermee een bepaalde formele status, een kwaliteit waarop gebruikers kunnen vertrouwen. Dit neemt niet weg dat een gebruiker (vaak een accountant / intermediair) verantwoordelijk is voor het maken van een goede verantwoording, die taak is met de komst van de taxonomie niet veranderd.

Exclusief kanaal
De oplossing die beantwoordt aan de visie (betere en goedkopere verantwoording door gebruik van een gedeelde taxonomie, een generieke procesinfrastructuur en een gedeelde dienstverlener), is nu dus in beheer. In deze vorm kan de organisatie een volgende stap nemen. De overheid realiseert zich, de marktpartijen geven dat ook aan, dat de volledige adoptie door de markt en de stap naar excellent beheer door de dienstverlener achterwege blijft als SBR een optionele oplossing blijft.

In juni 2011 spreken de Minister van Economische Zaken, Landbouw en Innovatie en de Staatssecretaris van Financiën af om van SBR het exclusieve aanleverkanaal te maken voor de aangiftes VPB en IB, per 1 januari 2013. In 2014 zal de OB-aangifte volgen. Dat luidt een periode in van uitfasering van de huidige kanalen, intensieve voorbereiding van de markt en voorbereidingen binnen de Belastingdienst en Logius.

De verplichtstelling geldt alleen voor de aangiften die ondernemingen of hun intermediairs rechtstreeks vanuit softwarepakketten doen (system-to-system). Voor deze groep betekent het de facto een verplichtstelling van SBR. Daarom refereren we in dit boek aan deze stap als de 'verplichtstelling'. Portaal-alternatieven, zoals de website van de Belastingdienst, blijven echter bestaan. Voor de markt betekent de verplichtstelling dat over het gehele domein stabiele en eenduidige koppelvlakken zullen gelden. Een en ander betekent wel dat de overheid niet op korte termijn wijzigingen zal kunnen doorvoeren. Wijzigingen vragen een lange voorbereidings- en voorlichtingstijd; het gaat niet meer om een afgebakende groep 'bekende' aangesloten partijen, zoals in de beginjaren van SBR. De aandacht voor continuïteit bij onderhoud en eventuele incidenten neemt toe.

Een ander punt dat meteen aandacht krijgt is het inrichten van een i-proces voor eMededelen en de herkenningsmiddelen die nodig zijn (met name voor machtigingen). Halverwege 2012 zijn hiervoor oplossingen in gebruik. Daarnaast ondernemen de SBR partijen actie om te voorkomen dat de distributie van de PKIoverheid certificaten[59] een probleem wordt doordat er slechts enkele leveranciers zijn die conform het stelsel certificaten uitgeven.

Voor de governance brengt deze periode een aantal veranderingen met zich mee. Om de randvoorwaarden voor de verplichtstelling in te vullen, zoals eMededelen en certificaatdistributie, geeft het PLO scherpe sturing op projecten. Daarnaast moet de impact van de verplichtstelling op de dienstverlening van Logius in kaart kunnen worden gebracht, en de eisen die daaruit volgen. Om dat te kunnen doen, is er een gedetailleerde beschrijving van de diensten van Logius rondom de taxonomie, de generieke procesinfrastructuur en de afstemming daaromheen nodig: de dienstbe-

[59] De SBR partijen stellen het gebruik van een PKIoverheid certificaat verplicht voor het kunnen aanleveren van een bericht. Deze certificaten worden uitgegeven door een beperkt aantal partijen, die aan de specifieke eisen voor PKIoverheid voldoen (Programma van Eisen van PKIoverheid) en vormen het hoogst betrouwbare authenticatiemechanisme.

schrijving. Het beleidsopdrachtgeverschap wordt door de Belastingdienst en het Ministerie van EZ ingevuld, met de uitvragende partijen als afnemers van verantwoordingsketens. Ook wordt het financiële vraagstuk verdiept. Er wordt een verrekenmodel gevormd voor de kosten van het gebruik van de diensten naar rato van het aantal berichten en/of gebruikers van een verantwoordingsketen.

Ook wordt er intensief gewerkt aan de voorlichting van de markt, in samenwerking met verschillende koepelorganisaties. Zij verspreiden actief informatie over de voortgang van SBR, de status van softwarepakketten en de juiste toepassing van de SBR elementen zoals de taxonomie, de koppelvlakken en de i-processen. Het SBR team bij Logius ondersteunt (toekomstige) aanleveraars en andere betrokkenen.
De SBR overheidspartijen realiseren zich dat transparantie over het SBR Programma en beschikbaarheid van alle relevante voorschriften van belang is voor alle huidige en toekomstige aanleveraars. Bovendien is dit een vereiste van behoorlijk bestuur.

Een en ander betekent ook dat de invulling van organisatorische en juridische randvoorwaarden verder evolueert. Op verschillende domeinen wordt gewerkt aan een basis in wet- en regelgeving voor de toepassing van SBR en formalisering van de rol van de gedeelde dienstverlener (Logius).

De jaarrekeningketen gaat intussen ook werken aan verplichtstelling van SBR voor aanleveringen. Eind 2012 begint de KvK met het voorbereiden van de nodige aanpassingen, te beginnen met een openstellingsbesluit voor SBR en het ontmoedigen van het indienen van de jaarrekening in PDF-formaat.[60] Voor de kleine ondernemingen die niet willen overstappen op SBR ontwikkelt de KvK een selfservice portaal voor handmatige aanlevering. Het portaal zet de ingevoerde jaarrekening om in XBRL en stuurt die naar het Handelsregister.

De banken verwachten positieve effecten van de verplichtstelling voor hun eigen keten, zij voorzien een toename van het aantal aanleveringen van kredietrapportages.[61] Zij stellen zelf SBR (nog) niet verplicht, maar grijpen de impuls van de overheid wel aan om het gebruik te stimuleren. Als laagdrempelig alternatief voor ondernemers die zelf kredietrapportages willen indienen (zonder over software voor system-to-system aanlevering te beschikken), richten de banken een portaal in voor handmatige indiening.

---

[60] Een vraagstuk dat bij die voorbereidingen ook aandacht krijgt is de verantwoordelijkheid voor het jaarrekeningen-deel van de taxonomie. De taxonomie is gebaseerd op de wetgeving. De KvK is echter (anders dan bijvoorbeeld bij de Belastingdienst het geval is), wél degene die de jaarrekeningen ontvangt, maar níet direct verbonden aan de wetgever voor jaarrekeningenrecht, namelijk het Ministerie van Justitie. Gezien de wetgeving zou Justitie een natuurlijke eigenaar zijn voor de jaarrekeningentaxonomie. Justitie is (uit eigen beweging) niet zo nauw betrokken bij SBR als de KvK, ondanks het feit dat de Minister van Justitie in 2006 het Convenant tekende. In 2013 wordt de Raad voor de Jaarverslaggeving verzocht om voortaan een stempel van goedkeuring aan de jaarrekeningentaxonomie te verbinden.
[61] Financiële Rapportages Coöperatief, persbericht van 31 mei 2011, op www.rapportageportaal.nl.

Software en intermediaire diensten
De meeste ondernemers zullen niet direct te maken krijgen met SBR. Uitzondering zijn de zelfaangevers/zelfbouwers. Voor intermediairs en softwareleveranciers, die voor SBR investeringen hebben gedaan of dat nog gaan doen, betekent SBR dat de dienstverlening aan hun klanten deels verandert. Steeds meer intermediairs gaan gebruik maken van online boekhoudsoftware en van portals voor uitwisseling van data met hun klanten. Er zijn intermediairs - accountants, boekhouders, belastingconsulenten, koepels - die vooroplopen bij SBR. Zij draaien al een tijdje mee in de SBR ontwikkelingen, passen SBR toe en stimuleren de verdere toepassing. Daarnaast zijn er intermediairs die het nieuws van de verplichtstelling hebben afgewacht, totdat zij hun processen gingen inrichten op SBR. De koepelorganisaties spelen een rol bij het voorlichten en betrekken van de uiteenlopende groepen intermediairs.

Softwareleveranciers maken hun pakketten geschikt voor SBR. Daarbij zijn er ook voorlopers te onderscheiden; softwareleveranciers die meteen voorbereidingen treffen maar ook een groep die door marktondersteuners vanuit het SBR Programma in beweging wordt gebracht.

Zowel fiscale softwareleveranciers als koepelorganisaties van intermediairs hebben de intentie uitgesproken[62] om de investeringen die zij doen in de overgang naar SBR niet door te rekenen in hogere kosten voor hun klanten.

Verbreding
De volgende periode voor SBR, 2012-2013 en verder, kenmerkt zich door verbreding van SBR naar andere domeinen. De kern van de dienstverlening door Logius vindt vanaf 2012 al op gestructureerde wijze plaats. In 2013 worden de procedures daaromheen en de governance beter uitgewerkt. Onderdeel daarvan is een strategie voor verbreding. De i-processen, opgebouwd uit generieke services, blijken in de praktijk in de verschillende domeinen heel vergelijkbaar: overal gelden dezelfde kaders van wet- en regelgeving voor aanleveren en mededelen. Dit maakt het mogelijk de oplossing breder toe te passen. Toepassing van het SBR concept door een zo groot mogelijk aantal uitvragende partijen is van belang voor het optimaliseren van de voordelen van system-to-system verantwoording en informatieverwerking en de gedeelde dienstverlening. In dat kader richt de organisatie zich in op het verkennen en realiseren van verschillende mogelijkheden voor verbreding van SBR naar andere domeinen. Een domein waar dit succesvol gebeurt is het agrodomein. Het gaat daar om bedrijfseconomische rapportages door intermediairs van agrarische ondernemingen aan het LEI (Landbouw Economisch Instituut). Gegevens die door het LEI weer worden gerapporteerd aan de Europese Commissie. De verbredingsstrategie vanuit SBR richt zich op financiële en maatschappelijke verantwoording in de (semi)publieke sector. In dat kader worden de mogelijkheden verkend of uitgewerkt met de onderwijssector, de zorg en woningcorporaties. Nieuwe toetreders dienen een toetredingsprocedure te doorlopen waarbij wordt gekeken of zij voldoen aan de afspraken die gelden bij SBR.

---

[62] Intentieverklaring SBR-beraad 27 mei 2011

Belangrijke kenmerken van SBR
We eindigen deze achtergrondbeschrijving met een kort overzicht van belangrijke kenmerken van SBR. Kennis van deze kenmerken draagt bij aan een goed begrip van SBR (en van wat SBR níet is).

- SBR is ingericht op het optimaliseren van de voordelen van system-to-system informatieverwerking. System-to-system betekent dat er geautomatiseerde communicatie tussen twee computers plaatsvindt, die in principe zonder menselijke interactie wordt geïnitieerd en afgehandeld.
- SBR is ingericht op professionele verantwoording, met name van ondernemingen (inclusief eenmanszaken). Burgers kunnen er wel gebruik van maken.
- Met SBR kunnen ondernemingen rapporteren aan zowel publieke (bijvoorbeeld CBS) als private (bijvoorbeeld banken) uitvragende partijen.
- In beide gevallen gaat het om verantwoordingsinformatie: financiële gegevens over het bedrijf op basis van de bedrijfsadministratie.
- Het 'eenduidig verantwoorden' binnen SBR ziet op de generieke stappen die voor elk van de verschillende verantwoordingsstromen doorlopen moeten worden, zoals ontvangen, valideren, routeren, bevestigen. De inhoudelijke verwerking en de rechtsgevolgen die daaraan verbonden worden, zijn geen onderdeel van SBR. Er wordt wel gewerkt aan normalisatie en harmonisatie van begrippen, maar de betekenis daarvan blijft zaak van het domein en de betreffende wet- en regelgeving.
- De onderneming 'brengt'. Het aanleveren van een SBR verantwoording gebeurt vaak op basis van plicht, maar wel op eigen initiatief. Er is geen sprake van een centrale database, waarin ondernemers hun bedrijfsadministratie hebben geüpload en waar uitvragers op een gegeven moment uit halen wat ze nodig hebben (oftewel 'eenmalig aanleveren'). Voor elke uitvraag (bijvoorbeeld aangifte 2011, jaarrekening 2010 etc.) levert de onderneming apart een specifieke set gegevens aan. Dit doet overigens niet af aan het feit dat uitvragende partijen onderling bepaalde aangeleverde gegevens delen (zoals het CBS en de Belastingdienst).
- Er is wel sprake van eenmalig inrichten, het '*store once, report to many*' principe: na het eenmalig goed inrichten van hun gegevens kunnen ondernemers verantwoordingsinformatie via één kanaal doorsturen naar de verschillende uitvragende partijen binnen de overheid.

Geraadpleegde bronnen
Voor deze achtergrondbeschrijving is naast interne bronnen van het SBR Programma gebruik gemaakt van de volgende bronnen:

Persberichten

- SBR in 2010-2011, In samenwerking naar grootschalig gebruik en stabiel beheer, SBR Programma, 2010, www.sbr-nl.nl
- *Banken positief over besluit overheid inzet SBR als exclusief rapportagekanaal*, Financiële Rapportages Coöperatief, 31 mei 2011, www.rapportageportaal.nl

Documenten

- Brief van de Minister van Economische Zaken aan de Tweede Kamer, aangaande het Kabinetsplan aanpak administratieve lasten (29 515), 27 mei 2004.
- Brief van de Staatssecretaris van Economische Zaken aan ACTAL, aangaande het Advies ACTAL ICT-beleid vermindering administratieve lasten, 30 augustus 2004.
- Brief van de Staatssecretaris van Economische Zaken aan de Tweede Kamer, aangaande het Kabinetsplan aanpak administratieve lasten (29 515), 9 juni 2005.
- Definitief Programma van Eisen van de generieke infrastructuur, Ministerie van Economische Zaken, maart 2006.
- Convenant van samenwerking tussen overheid en markt over gebruik van de Nederlandse XBRL-taxonomie, 9 juni 2006.
- Convenant betreffende een *pilot* ten aanzien van de verkorte winstaangifte voor de vennootschapsbelasting op basis van de Nederlandse Taxonomie en gebruikmakend van Procesdefinities, 11 december 2008.
- Intentieverklaring SBR-beraad, 27 mei 2011.

Bijlage B – Verantwoording

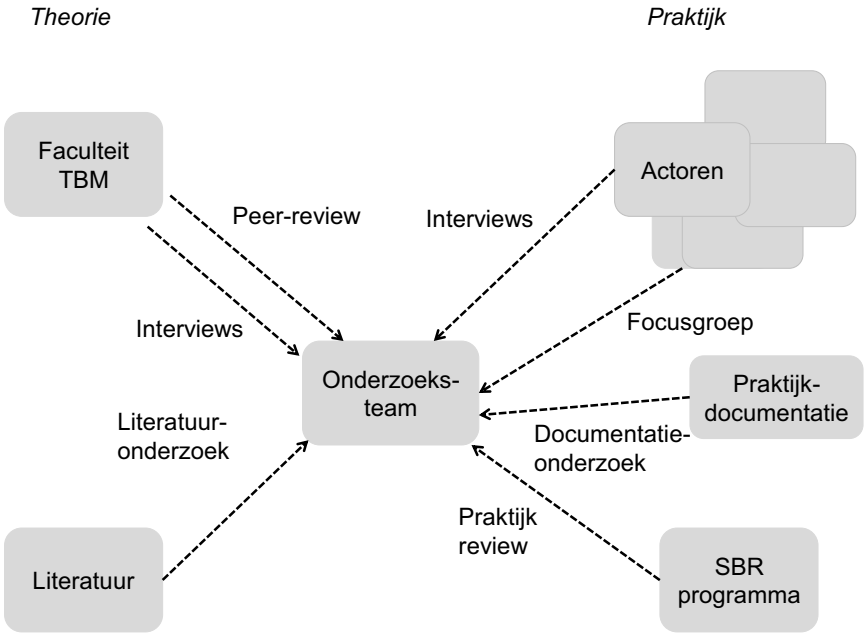
Het SBR kennisborgingsproject had in principe een tweeledige opdracht:

1. Ontsluit de revelante kennis met de betrokken specialisten.
2. Beschrijf – gebruikmakend van de relevante concepten en theorieën – de belangrijkste aspecten van SBR als opgave en oplossing.

Anders gesteld moesten de uitvoerders praktijk en theorie bij elkaar brengen in de vorm van een boek. Hiervoor zijn er binnen de kaders van de opdracht de volgende stappen gezet:

1. Er is samen met de opdrachtgever (Logius) een redactie geformeerd bestaande uit academische en SBR-functionarissen.
2. De redactie heeft een hoofdstukindeling en een eerste totaalopzet voor het boek gemaakt, verfijnd en voorgelegd aan de opdrachtgever.
3. De redactie heeft voor de verschillende hoofdstukken co-auteurs gevraagd die vanuit de praktijk direct betrokken waren bij complexe thema's zoals processen, gegevens, techniek, informatiebeveiliging en beheer.

De redactie – aangevuld met de (co)auteurs – vormden samen het onderzoeksprojectteam. Dit team heeft diverse onderzoeksinstrumenten toegepast om tot dit boek te komen. Onderstaand figuur geeft een overzicht van de onderzoeksinstrumenten.



Figuur B.1 - Overzicht van toegepaste onderzoeksinstrumenten

We belichten hieronder de verschillende onderdelen van het figuur.

Peer-review. Voorlopige gedachten en denklijnen voor dit boek zijn via voordrachten voorgelegd aan en besproken met een breder publiek van betrokkenen, bijvoorbeeld in onderzoeksbijeenkomsten en internationale conferenties. Van de daarbij ontvangen reacties is dankbaar gebruikgemaakt bij de voorbereiding van het boek.

Interviews. Aan de praktijkkant werden er voor ontsluiting van de tacit knowledge diepte-interviews gehouden. Het betreft semi-gestructureerde (half gesloten) interviews van tussen de half en anderhalf uur. Sommige specialisten zijn meermaals gesproken.

Literatuuronderzoek. Dit boek steunt op een groot aantal bronnen welke uit literatuuronderzoek zijn voortgekomen. Hierbij is de beschikbare nationale
en internationale wetenschappelijke literatuur op de diverse hoofdstukthema's ontsloten en bestudeerd[63].

Documentatieonderzoek. Naast de wetenschappelijke literatuur heeft het onderzoeksteam gebruik gemaakt van officiële praktijkdocumentatie en, indien nodig, mogelijk en met toestemming, van werkgroepverslagen.

Praktijk review. Het onderzoeksteam heeft haar tussentijdse rapportages (lees hoofdstukken) middels review-rondes voorgelegd aan specialisten. Hiervoor zijn specialisten geselecteerd die deskundigheid op een specifiek gebied hebben en ver genoeg van het SBR Programma af staan om een onafhankelijk oordeel te geven over de kwaliteit (van een hoofdstuk). Een overzicht van de reviewers treft u in het Dankwoord.

Focusgroep. Voor het evalueren van de resultaten werd een focusgroepsessie gehouden met een grotere en diverse groep van actoren. Een focusgroepsessie heeft als doel evaluatie van de resultaten, verdere verfijning, het creëren van draagvlak en het uitdragen van (tussen)resultaten. De group decision support faciliteiten van de faculteit Techniek, Bestuur en Management werden gebruikt om een focusgroepsessie te ondersteunen. Aan deze sessie hebben vanuit alle disciplines van het SBR Programma functionarissen deelgenomen. De TU Delft had eerder al een groepssessie georganiseerd met publieke en private partijen rond de invoering van XBRL in een project voor Actal. Deze resultaten zijn meegenomen.

---

[63] De digitale bibliotheek van de TU Delft biedt de mogelijkheid om systematisch de (internationale) literatuur te doorzoeken. Zij biedt toegang o.a. tot de databases van IEEE, ACM, SCOPUS, ISI en haar eigen catalogus en de bibliotheken van gerenommeerde uitgevers (zoals Elsevier, Wiley, Springer etc.). Zie www.library.tudelft.nl.

Bijlage C – Begrippen en afkortingen

Begrippen

(e)mededelen	verstrekken van een inhoudelijk bericht door de uitvragende partij aan de belanghebbende
aanleveraar	(semi-) publieke of private partij die met SBR verantwoordingsinformatie aanlevert. De aanleveraar is de belanghebbende of de intermediair
afnemer	publieke organisatie of publieke rechtspersoon die voor het elektronisch verkeer met andere organisaties gebruik maakt van door Logius beheerde generieke voorzieningen en/of diensten
afsprakenstelsel	de gemeenschappelijke kaders en standaarden die de publieke en private partijen in SBR hanteren binnen het domein
authenticatie	vaststellen van de identiteit van de aanleveraar van een verzoek, met een bepaald betrouwbaarheidsniveau
autorisatie	controle of de aanleveraar bevoegd is om gebruik te maken van een bepaalde dienst
belanghebbende	private of (semi-)publieke partij waarop een verantwoordingsplicht rust
bericht	een digitale verzameling elementen met een bepaalde betekenis afkomstig van een verzender (systeem, organisatie of persoon) gericht aan een ontvanger (systeem, organisatie of persoon)
Digipoort	de generieke procesinfrastructuur van de overheid
eXtensible Business Reporting Language (XBRL)	een open standaard voor het definiëren van gestructureerde gegevens in de vorm van platte tekst
geautomatiseerde afhandeling	door informatietechnologie ondersteunde, niet-handmatige uitvoering van taken
gebruiker	publieke of private partij (aanleveraar, intermediair, ondernemer/bedrijf, uitvragende partij) die gebruik maakt van SBR voorzieningen
gegevens	de feiten of begrippen weergegeven in de vorm die geschikt is voor het communiceren, interpreteren en verwerken tot informatie, hetzij door de mens, hetzij door automatische middelen, of door beide
generieke procesinfrastructuur	voor meerdere toepassingen te gebruiken procesinfrastructuur
informatieketen	een aaneenschakeling van organisaties die informatie delen
informatie-uitwisseling	het elektronisch verzenden en ontvangen van gegevens en/of berichten tussen twee of meer partijen
informatieverwerking (gegevensverwerking)	handelingen met betrekking tot informatie en/of berichten, waaronder het vastleggen, bewaren, wijzigen, gebruiken, doorzenden, verspreiden, met elkaar in verband brengen, afschermen en vernietigen van informatie
instance document	een lijst van XBRL tags die elk een bepaalde waarden hebben en verwijzen naar specifieke begrippen in de taxonomie
intermediair	een tussenpersoon die gemachtigd is om te handelen namens de belanghebbende

interoperabiliteit	de mate waarin verschillende in een keten gebruikte technologieën met elkaar kunnen communiceren of gezamenlijk kunnen worden ingezet voor een bepaald doel
koppelvlak	de daadwerkelijke invulling van een set van afspraken en standaarden die de uitwisseling van gegevens tussen informatiesystemen verzorgt
koppelvlakspecificatie	set van afspraken en standaarden die de uitwisseling van gegevens tussen informatiesystemen verzorgt
loose coupling	ontkoppeling tussen de business-functionaliteit en de technische implementatie.
machtiging	bevoegdheid van een intermediair om namens een belanghebbende informatie aan te leveren of te ontvangen
metadata	data die de karakteristieken van gegevens beschrijven: data over data
Nederlandse Taxonomie (NT)	een gedeelde taxonomie die de uitvragende partijen gebruiken in het kader van SBR
Nederlandse Taxonomie Architectuur (NTA)	een set van afspraken die bepaaldt welke onderdelen van de XBRL standaard op welke wijze in een taxonomie worden opgenomen
onderneming	private partij of (semi-)publieke waarop een verantwoordingsplicht rust
open standaard	een standaard die vrij te gebruiken is
proces	een geordende set van taken met een vastgesteld doel
procesinfrastructuur	een stelsel van functionaliteiten dat nodig is voor het geautomatiseerd afhandelen van berichten
SBR Programma	initiatief van de overheid gericht op het realiseren van SBR in verantwoordingsketens in samenwerking tussen overheidspartijen en marktpartijen
Standard Business Reporting (SBR)	oplossing voor de geautomatiseerde uitwisseling en verwerking van informatie in verantwoordingsketens
system-to-system (S2S)	wijze van communicatie of verbinding tussen twee of meer informatiesystemen zonder handmatige tussenkomst
system-to-system-keteningtegratie	koppeling van de informatiesystemen van organisaties zonder menselijke tussenkomst
taxonomie	een verzameling van gecontroleerde woordenboekbegrippen die georganiseerd zijn in een hiërarchische structuur
uitvragende partij	publiek of private partij die verantwoordingsinformatie van belanghebbende vraagt en eisen stelt aan de aanlevering hiervan in het kader van SBR
verantwoordingsinformatie	informatie aangaande de prestatie van of situatie in een organisatie ten behoeve van bepaalde derde
verantwoordingsketen	keten die is ingericht ten behoeve van het genereren en verwerken van verantwoordingsinformatie die hun grondslag vinden in wet-en regelgeving
verantwoordingsproces	proces gericht op het uitwisselen en verwerken van verantwoordingsinformatie
verbreding	Toepassing van SBR in publieke verantwoordingsketens waar het eerder nog niet werd toegepast

Afkortingen

Afkorting	Betekenis
.NET	Microsoft .NET Framework
A	
ACM	Autoriteit Consument & Markt
ADN	Assurantie Data Net
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASL	Application Services Library
ASx	Applicability Statements versie x
AuSP	Autorisatie Service Provider
Awb	Algemene wet bestuursrecht
B	
b2b	business-to-business
b2bi	business-to-business integration
b2g	business-to-government
BAPI	Business Application Programming Interface
BD	Belastingdienst
BISL	Business Information Services Library
BPEL	Business Process Execution Language, afkorting van BPEL4WS
BPEL4WS	Business Process Execution Language for Webservices
BPMN	Business Process Modeling Notation
BPR	Business Process Re-engineering
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
C	
CA	Certificate Authority
CBP	College Bescherming Persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
COBOL	Common Business-Oriented Language
CP	Certificate Policy
CPA	Collaboration Protocol Agreement
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Service Provider
D	
Digipoort	Digipoort Overheidstransactiepoort
OTP	

Digipoort PI	Digipoort Procesinfrastructuur
DSR	Digikoppeling Service Register
DTS	Discoverable Taxonomy Set

E

ebMS	Electronic business XML Message Service
ebXML	electronic business using eXtensible Markup Language
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EDIINT	EDI over the internet
ESB	Enterprise Service Bus
ETSI	European Telecommunications Standards Institute
EZ	Ministerie van Economische Zaken

F

Fi-nummer	Fiscaal nummer
FRC	Financiële Rapportages Coöperatief
FRIS	Financial Reporting Instance Standards
FRTA	Financial Reporting Taxonomy Architecture
FTP	File Transfer Protocol

G

GEIN	Generieke Infrastructuur

H

h2h	human-to-human
h2s	human-to-system
HR	Handelsregister
HRN	HandelsRegisterNummer
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure

I

IASB	International Accounting Standards Board
IB	InkomstenBelasting
ICT	Informatie- en CommunicatieTechnologie
ICTAL	ICT voor Administratieve Lastenverlichting
IDABC	Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens
IEFT	Internet Engineering Task Force
IFRS	International Financial Reporting Standards
i-proces	informatieverwerkingsproces

ISO	International Organization for Standardization
IT	Informatie Technologie
ITIL	Information Technology Infrastructure Library

J

JIT	Just-in-time

K

KPI	Key Performance Indicators
KvK	Kamer van Koophandel

L

LSS	Lean Six Sigma

M

MIME	Multipurpose Internet Mail Extensions
MKB-Nederland	Midden-en KleinBedrijf Nederland
MSA	Mail Submission Agent
MSP	Multi-Sided Platform
MTA	Mail Transfer Agent

N

NBA	Nederlandse Beroepsorganisatie van Accountants
NIST	National Institute for Standards and Technology
NIVRA (thans NBA)	Koninklijk Nederlands Instituut van Registeraccountants
NORA	Nederlandse Overheidsarchitectuur
NT	Nederlandse Taxonomie
NTA	Nederlandse Taxonomie Architectuur
NTP	Nederlands Taxonomie Project

O

OASIS	Organization for the Advancement of Structured Information Standards
OB	Omzetbelasting
OBM	Object Management Group
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OIN	Overheidsidentificatienummer
OSI	Open Systems Interconnection
OSWO	Unit Ondersteuning SoftWare Ontwikkelaars

P

P&T	Processen en Techniek

PA	Policy Authority
PDF	Portable Document Format
PI	Procesinfrastructuur
PKI	Public Key Infrastructure
PKI overheid	Public Key Infrastructure voor de overheid
PMBoK	Project Management Body of Knowledge
POP3	Post Office Protocol versie 3
PRINCE2	PRojects IN Controlled Environments
PvE	Programma van Eisen
PvE GEIN	Programma van Eisen Generieke Infrastructuur

R

RA	Registration Authority
REST	Representational State Transfer
RSA	algoritme voor public key cryptografie ontworpen voor Rivest, Shamir en Adleman
RSIN	Rechtspersonen en Samenwerkingsverbanden Informatie Nummer

S

S2S	system-to-system
SaaS	Software as a Service
SBA	Service Bericht Aanslag
SBR	Standard Business Reporting
SDM	System Development Methodology
SHA	Secure Hash Algoritme
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNO	Serviceniveau overeenkomst
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSC	Shared Service Center
SSL	Secure Socket Layer
STP	Straight Through Processing
SVBR	Semantics of Business Vocabulary and Business Rules
SVR	Simplified Validation Rules

T

TCP/IP	Transmission Control Protocol/Internetprotocol
TLS	Transport Layer Security
ToC	Theory of Constraints
TQM	Total Quality Management
TTP	Trusted Third Party

U

UBL	Universal Business Language
UDDI	Universal Description, Discovery and Integration
UML	Unified Modeling Language
URL	Uniform Resource Locator
US-GAAP	United States Generally Accepted Accounting principles

V

VNO-NCW	fusie tussen het Verbond van Nederlandse Ondernemingen (VNO) en het Nederlands Christelijk Werkgeversverbond (NCW)
VPB	Vennootschapsbelasting
VPB/IB	Vennootschapsbelasting/ Inkomstenbelasting
VPN	Virtual Private Network
VSA	Value Stream Analysis

W

W3C	World Wide Web Consortium
Wbp	Wet bescherming persoonsgegevens
WfMC	Workflow Management Coalition
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
WSDL	Web Services Description Language
WUS	acroniem voor WSDL, UDDI en SOAP

X

XBRL	eXtensible Business Reporting Language
XHTML4	eXtensible HyperText Markup Language, versie 4
Xlink	XML Linking Language
XML	eXtensible Markup Language
XPDL	XML Process Definition Language

Z

ZZP	Zelfstandigen Zonder Personeel

Over de betrokkenen

Bas Avis
De heer drs. Bas Avis is vele jaren werkzaam als Business Consultant, Projectmanager en Accountmanager op het gebied van gegevensuitwisseling tussen bedrijven en overheid. Momenteel is hij Delivery Manager Aansluitondersteuning bij Logius en onder andere verantwoordelijk voor de ondersteuning van SBR partijen tijdens het aansluittraject. Bas werkt vanuit zijn eigen bedrijf BA Management Consultancy en kan bereikt worden via: bas@ba-consultancy.nl.

Bijdrage van Bas: algemeen.

Victor den Bak
De heer ir. Victor den Bak is sinds 2012 werkzaam als Procesanalist bij EBPI en ziet erop toe dat de SBR-informatieprocessen op de juiste wijze landen in de techniek. In deze rol draagt Victor er mede zorg voor dat nieuwe en aangepaste processen voldoen aan de gestelde generieke eisen en kaders op gebied van compliance, informatiebeveiliging en optimaal hergebruik van gestandaardiseerde componenten. Victor kan bereikt worden via: victor@ebpi.nl.

Bijdrage van Victor: mede-auteur van hoofdstuk 7 (Technische inrichting SBR).

Sebastiaan Bal
De heer mr. drs. Sebastiaan Bal RA is sinds 2010 binnen het SBR Programma bij Logius actief als Manager Gegevens en in dit kader verantwoordelijk voor de realisatie van de Nederlandse XBRL Taxonomie. Sebastiaan is expert op het gebied van gegevensdefiniëring, -uitwisseling, -verwerking en -analyse en autoriteit op het gebied van XBRL. Sebastiaan is thans werkzaam bij Thauris en kan bereikt worden via: s.bal@thauris.nl.

Bijdrage van Sebastiaan: hoofd-auteur hoofdstuk 6 (Gegevens), deelname aan kennisborgingssessie.

Nitesh Bharosa
De heer dr.ir Nitesh Bharosa heeft vanuit de Technische Universiteit Delft bijgedragen aan dit boek. De sectie 'Over de redactie' beschrijft meer over zijn rol.

Mark Bisschop
De heer Mark Bisschop heeft een accountancy achtergrond en is als Consultant en Docent verbonden aan XBRL voor Accountants en DOCCO. Op dit moment adviseert hij accountantskantoren op het gebied van IT en werkprocessen. Daarnaast is hij mede-auteur van het XBRL Handboek voor intermediairs. In de periode 2010 – 2013 was Mark actief binnen het SBR Programma bij Logius. Mark kan bereikt worden via: mark@xbrlvooraccountants.nl.

Bijdrage van Mark: algemeen.

Nanko Boerma
De heer drs. Nanko Boerma was van begin 2010 tot begin 2013 binnen het SBR Programma als Bestuurlijk Programmamanager verantwoordelijk voor de vormgeving van de strategische en bestuurlijke kaders, waarbinnen de medewerkers van het SBR programmateam hun expertise konden inzetten en uitbouwen. Nanko is werkzaam bij het Management Centrum en kan worden bereikt via: boerma@management-centrum.com.

Bijdrage van Nanko: algemeen.

Ella Broos
Mevrouw Ella Broos was van begin 2010 tot eind 2013 actief bij het SBR Programma in de rol van Manager Marktondersteuning en Communicatie. Zij is Interim Communicatiemanager, met als expertises crisiscommunicatie en woordvoering en werkt veelal in de ICT- en securitybranche. Zij is bereikbaar via: info@brooscommunicatie.nl.

Bijdrage van Ella: review van ten geleide, hoofdstukken 2 (Ketens en ketencoördinatie), 3 (Verandermanagement in informatieketens) en bijlage A (Achtergrond SBR).

Rob Dortland
De heer dr. ir. Rob Dortland heeft diverse (management-)functies vervuld bij de Rijksoverheid. Meest recente functie was die van plv. Inspecteur-generaal van de Voedsel en Warenautoriteit. In die functie is hij ook betrokken geweest bij de ontwikkeling van innovatief toezicht op basis van Continuous Control Monitoring (CCMT). Sinds 2011 is hij in deeltijd aan Logius verbonden als Regisseur SBR Agrodomein. Rob is momenteel werkzaam als zelfstandig adviseur op het snijvlak overheid-bedrijfsleven en is bereikbaar via: rob.dortland@gmail.com.

Bijdrage van Rob: algemeen, deelname aan de kennisborgingssessie.

Welmoed Fokkema
Mevrouw Welmoed Fokkema LL.M is van 2009 tot 2013 actief geweest binnen het SBR Programma bij Logius als Compliance adviseur, verantwoordelijk voor het waarborgen van compliance en het adviseren over de juridische aspecten van SBR. Welmoed is specialist op het gebied van compliance van business processen, gegevensuitwisseling, informatiebeveiliging en bestuur. Sinds eind 2013 is zij werkzaam als Compliance Manager in de farmaceutische sector. Welmoed kan bereikt worden via: welmoed.fokkema@gmail.com.

Bijdrage van Welmoed: mede-auteur van hoofdstukken 4 (Het besturingsvraagstuk keteninformatiesystemen) en 8 (Beveiliging van informatieketens) en auteur van bijlage A (Achtergrond SBR). Deelname aan de kennisborgingssessie. Redactie over het hele boek.

Bart Hendriksen
De heer ir. Bart Hendriksen is in de rol van Procesanalist en Architect bij Logius sinds 2011 betrokken bij het SBR Programma. In deze rol heeft hij actief bijgedragen aan de realisatie van verschillende voorzieningen van Digipoort, waaronder eMede-

delen en eMachtigen. Bart is specialist op het gebied van service-georiënteerde architectuur, informatiebeveiliging en i-processen. Bart kan bereikt worden via: b.hendriksen@thauris.nl.

Bijdrage van Bart: mede-auteur hoofdstuk 8 (Beveiliging van informatieketens) en review van hoofdstuk 7 (Technische inrichting SBR).

Jan Hidders

De heer dr. ir. Jan Hidders werkt sinds 2008 in de groep Web Informatie Systemen aan de Technische Universiteit Delft als Universitair Docent. Daar doet hij onderzoek naar tools voor Ontology Management en het publiceren van bestaande data als Linked Open Data. Andere onderzoeksonderwerpen waar hij zich mee bezig houdt zijn het optimaliseren van Big Data Processing voor bijvoorbeeld Graph Analytics en specifiek het ontwikkelen van indexen voor graafdatabases. Hij kan bereikt worden via: a.j.h.hidders@tudelft.nl.

Bijdrage van Jan: review van hoofdstuk 6 (Gegevens).

Alexander Hielkema

De heer Alexander Hielkema is sinds 2008 werkzaam bij Logius in verschillende functies en daarin steeds betrokken geweest bij het beheer van de Digipoort. Alexander is van 2010 tot 2013 verantwoordelijk geweest voor het beheer en de exploitatie van onder andere de Digipoort Proces Infrastructuur. Alexander is een ervaren IT manager en expert op het gebied van het beheer van in gegevensuitwisseling toegepaste IT middelen. Alexander kan bereikt worden via: Alexander.hielkema@logius.nl.

Bijdrage van Alexander: algemeen, deelname aan de kennisborgingssessie.

Frans Hietbrink

De heer Frans Hietbrink RE RA is sinds 2009 binnen de Belastingdienst verantwoordelijk voor de implementatie van het SBR gedachtegoed. Frans is 30 jaar werkzaam bij de Belastingdienst, afwisselend in functies met directe contacten met het bedrijfsleven, als Manager en als Intern Accountant. Maar altijd met een focus op de inrichting van administratieve processen en de kwaliteit van gegevens. Momenteel is hij strategisch adviseur SBR/XBRL bij de Belastingdienst. Frans kan bereikt worden via: f_hietbrink@belastingdienst.nl.

Bijdrage van Frans: review van het hele boek, deelname aan de kennisborgingssessie.

Marc van Hilvoorde

De heer Marc van Hilvoorde stond mede aan de wieg van SBR en is de vader van de Nederlandse Taxonomie. Hij schreef diverse artikelen over de XBRL standaard en XBRL assurance en droeg tevens bij aan de totstandkoming van de internationale uitgave van 'XBRL for Dummies'. Marc werkt bij Logius en kan bereikt worden via marc.van.hilvoorde@logius.nl.

Bijdrage van Marc: review van hoofdstuk 6 (Gegevens).

Roland Hommes
De heer Roland Hommes is sinds 2009 als Architect verbonden aan het SBR Programma. Daarvoor heeft hij de Belastingdienst als XBRL specialist vertegenwoordigd in het NTP. Roland heeft aan diverse XBRL specificaties gewerkt en is als zelfstandig consultant actief op het terrein van digitale gestructureerde gegevensuitwisseling en kan bereikt worden via: info@rhocon.nl

Bijdrage van Roland: review van hoofdstuk 6 (Gegevens), deelname aan de kennisborgingssessie.

Niek van Huizen
De heer Niek van Huizen is sinds 2011 bij Logius actief als Change Coördinator en in dit kader verantwoordelijk voor het proces van gestructureerd doorvoeren van wijzigingen via releases op Digipoort ten behoeve van SBR. Niek heeft veel ervaring op het gebied van projectleiding, procesimplementatie, -uitvoering en -evaluatie binnen ICT organisaties. Niek is thans werkzaam bij Logius en kan bereikt worden via: niek.van.huizen@logius.nl.

Bijdrage van Niek: review van hoofdstuk 7 (Technische inrichting SBR).

Jeroen van Hulten
De heer drs. ing. Jeroen van Hulten CSPM is vanaf 2008 als Senior Projectmanager verantwoordelijk voor de invoering van SBR binnen de Belastingdienst. De afgelopen jaren is hij verantwoordelijk geweest voor de invoering diverse e-overheidsontwikkelingen zoals de verplichtstelling elektronische aangifte ondernemers, basisregistraties, DigiD en de vooringevulde aangifte. Daarnaast heeft Jeroen enkele artikelen geschreven en over business cases en projectrisicomanagement. Jeroen kan bereikt worden via: jamjb.van.hulten@belastingdienst.nl.

Bijdrage van Jeroen: algemeen, deelname aan de kennisborgingssessie.

Marijn Janssen
De heer prof.dr.ir Marijn Janssen heeft vanuit de Technische Universiteit Delft bijgedragen aan dit boek. De sectie 'Over de redactie' beschrijft meer over zijn rol.

Mark Janssen
De heer drs. Mark Janssen CISSP CISA is sinds 2007 betrokken bij het Logius product PKIoverheid. Hij is bij Logius werkzaam als Coördinerend Specialistisch Adviseur Bedrijfsvoering waarbij hij ook de rol van Policy Authority PKIoverheid heeft. Mark heeft veel kennis van informatieveiligheid in het algemeen en Public Key Infrastructure (PKI) in het bijzonder. Mark kan bereikt worden via: mark.janssen@logius.nl.

Bijdrage van Mark: review van hoofdstuk 8 (Beveiliging van informatieketens).

Joris Joosten
De heer Joris Joosten is al in 2007 geweest bij het ontwerp van de koppelvlakken voor Digipoort. Na verschillende klussen binnen de e-overheid is Joris nu Architect bij Logius op het gebied van authenticatie en autorisatie. Joris kan bereikt worden via: joris.joosten@logius.nl.

Bijdrage van Joris: review van hoofdstuk 7 (Technische inrichting SBR).

Bram Klievink
De heer dr. ing. Bram Klievink werkt als universitair docent bij de faculteit Techniek, Bestuur en Management van de Technische Universiteit Delft. Hij was betrokken bij diverse projecten op het gebied van de elektronische overheid, grootschalige ICT innovaties in internationale goederenstromen en het toezicht daarop. Momenteel werkt hij aan zijn NWO Veni onderzoek naar bestuursmodellen voor publiek-private informatie-infrastructuren. Bram is te bereiken via: A.J.Klievink@tudelft.nl.

Bijdrage van Bram: review van hoofdstuk 4 (Het besturingsvraagstuk van keteninformatieystemen).

Stephan Kockelkoren
De heer drs. Stephan Kockelkoren is sinds 2010 binnen het SBR Programma bij Logius actief als Coördinator Processen. In dit kader is hij verantwoordelijk voor de afstemming van functionele wensen van betrokken partijen op ketenniveau en de vertaling hiervan in specificaties voor procesafhandeling in Digipoort. Stephan is expert op het gebied van ketenorkestratie, procesmodelering (BPMN) en -implementaties in Digipoort. Stephan is werkzaam bij Cojito en te bereiken via: stephan@cojito.nl.

Bijdrage van Stephan: review van hoofdstuk 5 (I-Processen), deelname aan de kennisborgingssessie.

Baldwin de Kruijf
De heer Baldwin de Kruijf is sinds 2011 binnen het SBR Programma bij Logius actief als Transitiemanager en in dit kader verantwoordelijk voor de transitie van het SBR programma naar de Logius lijnorganisatie. Baldwin is specialist op het gebied van management van beheer. Baldwin is thans werkzaam bij Logius en kan bereikt worden via: baldwin.de.kruijf@logius.nl.

Bijdrage van Baldwin: algemeen.

Stefan van der Kwaak
De heer Drs. S.W. van der Kwaak MMC is sinds 2009 betrokken bij het SBR Programma. Aanvankelijk maakte hij deel uit van het regieteam van het Ministerie van Economische Zaken. Vanaf 2011 is hij verbonden aan het SBR team binnen Logius. In dit verband heeft hij mogelijkheden voor een bredere toepassing van SBR geïnventariseerd, in het bijzonder binnen de agrarische sector. Stefan is werkzaam als zelfstandig professional en bereikbaar via: stefanvanderkwaak@inter-esse.nl.

Bijdrage van Stefan: algemeen, deelname aan de kennisborgingssessie.

Peter Leijnse
De heer ir. Peter Leijnse, Master in Compliance Design & Management, is Senior Architect bij Logius. Hij is actief betrokken bij de vormgeving van bruikbare, betrouwbare en veilige oplossingen voor informatie-uitwisseling in ketens, zowel tussen overheid en bedrijven (Digipoort, SBR, eFactureren), tussen overheid en burgers (MijnOverheid) als binnen de overheid (Digikoppeling). Peter is te bereiken via: peter.leijnse@logius.nl.

Bijdrage van Peter: mede-auteur van hoofdstuk 7 (Technische inrichting SBR), deelname aan de kennisborgingssessie.

Johan Mastenbroek
De heer Johan Mastenbroek is sinds 2004 in diverse rollen betrokken geweest bij SBR initiatieven. Zo was hij betrokken bij het Programma van Eisen Generieke Infrastructuur (GEIN) dat resulteerde in de service georiënteerde architectuur voor elektronische communicatie tussen bedrijfsleven en overheden (het fundament voor de huidige Digipoort). Johan is algemeen directeur EBPI/Inology (de huidige leverancier van keteninformatiediensten voor SBR). Hij is gespecialiseerd in service georiënteerde architecturen (SOA) en IBM producten zoals WebSphere DataPower. Hij is te bereiken via: johan.mastenbroek@ebpi.nl.

Bijdrage van Johan: review van hoofdstuk 7 (Technische inrichting SBR).

Gabriëlle van Mourik
Mevrouw Gabriëlle van Mourik is sinds januari 2007 als Senior Projectmanager werkzaam bij het Centraal Bureau voor de Statistiek (CBS). Van juli 2010 tot en met december 2012 was zij binnen het CBS verantwoordelijk voor de implementatie van XBRL / SBR in de statistische processen en was in die hoedanigheid namens het CBS betrokken bij het SBR Programma. Gabriëlle is IPMA B gecertificeerd, heeft een Masterclass Verandermanagement gevolgd en kan bereikt worden via: g.vanmourik@cbs.nl.

Bijdrage van Gabriëlle: review van hoofdstukken 2 (Ketens en ketencoördinatie) en 3 (Verandermanagement in informatieketens).

Geert Nederhorst
De heer mr. Geert Nederhorst is sinds 1 januari 2013 betrokken binnen het SBR Programma bij Logius, sinds de tweede helft van 2013 in de rol van Manager Vraag. In deze hoedanigheid is hij intensief bezig met het inrichten van afdeling Keteninformatie en hij is vanuit Logius verantwoordelijk voor de verbreding van SBR. Geert is voor 2013 adviseur geweest van de minister en secretaris-generaal van het ministerie van BZK, met Logius in portefeuille. Hij is te bereiken via: geert.nederhorst@logius.nl.

Bijdrage van Geert: review algemeen, review van hoofdstuk 9 (Governance en Beheer) en hoofdstuk 10 (De SBR-verbredingsmethodiek).

Jan Pasmooij
De heer Jan Pasmooij RE RA RO is sinds begin 2011 binnen het SBR Programma bij Logius actief als Adviseur Kennisontwikkeling en -deling, in welke hoedanigheid hij direct betrokken was bij communicatie en voorlichting op het terrein van XBRL/SBR, de ontwikkeling van het SBR Online kennisplatform voor XBRL/SBR en het SBR Boek. Voor 2011 was Jan als voorzitter van XBRL Nederland / EU en als medewerker van het NIVRA (nu NBA) actief betrokken bij de XBRL/SBR ontwikkelingen in Nederland en internationaal. Jan Pasmooij is sedert 2011 zelfstandig gevestigd en kan worden bereikt via: jan@pasmooijce.com

Bijdrage van Jan: review van ten geleide, hoofdstukken 2 (Ketens en ketencoördinatie), 3 (Verandermanagement in informatieketens) en bijlage A (Achtergrond SBR).

Gertjan Peerenboom
De heer ir. Gertjan Peereboom is Strategisch Architect bij de Belastingdienst. Hij was in 2011 actief betrokken bij het SBR Programma. Hij heeft zich met name bezig gehouden met het ontwerp van de machtigingenservice en de aanleverprocessen en het aansluiten van de aangiftestromen van de Belastingdienst. Gertjan heeft als business consultant veel ervaring op gebied van procesarchitectuur en BPM in het publieke domein. Hij kan bereikt worden via: gj.peereboom@belastingdienst.nl.

Bijdrage van Gert Jan: review van hoofdstuk 5 (I-Processen).

Erwin Rigter
De heer Erwin Rigter MSc. is werkzaam als Consultant bij Thauris. Als Procesanalist is Erwin betrokken bij de inrichting van de business line binnen Logius. Daarnaast heeft Erwin een bijdrage geleverd binnen verbredingstrajecten en in de ontwikkeling van de verbredingsmethodiek. Erwin is te bereiken via: e.rigter@thauris.nl.

Bijdrage van Erwin: mede-auteur van hoofdstuk 4 (Het besturingsvraagstuk van keteninformatiesystemen), hoofd-auteur van hoofdstuk 10 (De SBR-verbredingsmethodiek) en review van het hele boek.

Marko Roos
De heer Marko Roos is werkzaam bij de methodologieafdeling van het Centraal bureau voor de Statistiek. Hij houdt zich vooral bezig met het ontwikkelen van methoden om digitaal gegevens te verzamelen. Marko leverde een actieve bijdrage in de totstandkoming van eerste versies van de Nederlandse Taxonomie. Marko kan bereikt worden via: m.roos@cbs.nl.

Bijdrage van Marko: review van hoofdstuk 6 (Gegevens).

Ian Saturday
De heer drs. Ian Saturday is sinds 2013 betrokken bij SBR. Hij faciliteert momenteel de Belastingdienst en de Kamer van Koophandel bij de aansluiting op de Digipoort met nieuwe/gewijzigde i-processen en services (o.a. de toepassing van geavanceerde digitale handtekeningen) en is betrokken bij de formulering van beleidsadviesnota's in het kader van het Single Window Handel en Transport. Ian is werkzaam bij Thauris en kan bereikt worden via: i.saturday@thauris.nl.

Bijdrage van Ian: review van hoofdstukken 1 (Inleiding), 9 (Governance & Beheer) en 10 (De SBR-verbredingsmethodiek).

John Sloof
De heer John Sloof is Beleidsadviseur bij de Kamer van Koophandel Nederland. Hij is sinds 2012 betrokken bij het SBR Programma. John is te bereiken via: john.sloof@kvk.nl.

Bijdrage van John: review van hoofdstukken 2 (Ketens en ketencoördinatie) en 3 (Verandermanagement in informatieketens).

Jacques Urlus
De heer Jacques Urlus RE CISA BBA is al ruim 8 jaar fulltime werkzaam op het gebied van XBRL en SBR. Zijn specialisme ligt voornamelijk aan de gebruikerskant van XBRL. Binnen zijn eigen organisatie Ordina is Jacques verantwoordelijk voor de volledige propositie rondom XBRL. Buiten Ordina is hij de eigenaar en de beheerder

van de grootste website over XBRL (www.dexbrlsite.nl). Jacques kan worden bereikt via: jacques.urlus@ordina.nl.

Bijdrage van Jacques: review van hoofdstuk 8 (Beveiliging van informatieketens), deelname aan kennisborgingssessie.

Roel Vaessen
De heer ing. Roel Vaessen is sinds eind 2010 binnen het SBR Programma bij Logius actief als Implementatiemanager Markt. Vanuit die rol ondersteunt hij marktpartijen zoals softwareontwikkelaars en intermediairs bij de implementatie van SBR. Roel is werkzaam bij Sogeti en kan bereikt worden via: roel.vaessen@sogeti.nl.

Bijdrage van Roel: algemeen.

Ralph Verhelst
De heer ir. Ralph Verhelst heeft als projectleider verschillende scrum teams geleid bij de implementatie van Digipoort in het kader van SBR. Daarnaast is Ralph betrokken geweest bij de realisatie van verschillende generieke overheidsvoorzieningen zoals Digilevering, Digimelding, Digikoppeling en Diginetwerk. Hij is gespecialiseerd in service georiënteerde architecturen (SOA) en IBM producten zoals WebSphere DataPower. Ralph is projectleider bij EBPI/Inology (de huidige leverancier van keteninformatiediensten voor SBR) en is te bereiken via: ralph.verhelst@ebpi.nl.

Bijdrage van Ralph: review van hoofdstuk 7 (Technische inrichting SBR) en review van hoofdstuk 8 (Beveiliging van informatieketens).

Haiko van der Voort
De heer dr. Haiko van der Voort is universitair docent bij de faculteit Techniek, Bestuur en Management van de Technische Universiteit Delft. Hij geeft onderwijs over organisatiekunde en besluitvormingstheorie, voor bachelorstudenten, masterstudenten en professionals. Hij doet bestuurskundig onderzoek naar besluitvorming over normen. Gerelateerde onderwerpen zijn toezicht, kwaliteitsmanagement, certificering en (zelf)regulering. Hij is te benaderen via: h.g.vandervoort@tudelft.nl.

Bijdrage van Haiko: mede-auteur van hoofdstukken 2 (Ketens en ketencoördinatie) en 3 (Verandermanagement in informatieketens) en review van hoofdstuk 4 (Het besturingsvraagstuk van keteninformatiesystemen). Deelname aan de kennisborgingssessie.

Remco van Wijk
De heer Remco van Wijk MSc. heeft als hoofd-auteur en redacteur bijgedragen aan dit boek. De sectie 'Over de redactie' beschrijft meer over zijn rol.

Niels de Winne
De heer ir. Niels de Winne RE heeft als redacteur en auteur bijgedragen aan dit boek. De sectie 'Over de redactie' beschrijft meer over zijn rol.

Tot slot gaat speciale dank uit naar **Iris Koetsenruijter, Maaike Kaasenbrood, Koen Hoijtink, Frans en Henri Guillaume** en **Mark van der Linde** voor de review op inconsistenties, grammatica en spelling. **Annemarie van der Linde** en **Jochem Oosterlee** hebben bijgedragen aan de illustraties. Allen, bedankt!

Literatuuroverzicht

A

Ackoff, R. L. (1989). From Data to Wisdom. *Journal of Applies Systems Analysis, 16*, 3-9.

Adams, C., & Lloyd, S. (2002). *Understanding PKI: Concepts, Standards, and Deployment Considerations* (2 ed.): Addison-Wesley Professional.

Agterhorst, J., & Thaens, M. (2000). Veranderkundige aspecten van uitvoeringsketens. Casus uitvoering van de Huursubsidiewet. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Algemene Rekenkamer. (2007). *Lessen uit ICT-projecten bij de overheid. Deel A*. Den Haag: Tweede kamer van de Staten Generaal.

Algemene Rekenkamer. (2008). *Lessen uit ICT-projecten bij de overheid - Deel B*. Den Haag: Tweede kamer van de Staten Generaal.

Amelsvoort, P. (1996). *Het programmeren en regisseren van veranderingsprocessen: vormgeven aan complexe veranderingsprocessen en organisatievernieuwing*. Vlijmen: ST-Groep.

Arendsen, R. (2008). *Geen bericht, goed bericht: een onderzoek naar de effecten van de introductie van elektronisch berichtenverkeer met de overheid op de administratieve lasten van bedrijven*. (Doctoral), Amsterdam University Press.

Armistead, C., Pritchard, J.-P., & Machin, S. (1999). Strategic business process management for organizational effectiveness. *Long Range Planning, 32*(1), 96-106.

Arsanjani, A. (2002). Developing and Integrating Enterprise Components and Services. *Communications of the ACM, 45*(10), 31-34.

B

Baldwin, C., & Clark, K. (2000). *Design Rules: The Power of Modularity*. MIT Press: Cambridge, MA.

Ballad, B., Ballad, T., & Banks, E. (2010). *Access Control, Authentication, and Public Key Infrastructure*. Sudbury, MA: Jones & Bartlett Learning.

Bauer, J. M., & Herder, P. M. (2009). Designing Socio-Technical Systems. In A. Meijers, D. M. Gabbay, P. Thagard & J. Woods (red.), *Handbook of the Philosophy of Science* (Vol. 9: Philosophy of Technology and Engineering Sciences): Elsevier.

Bekkers, V. (2000). Keteninformatisering en het management van organisatiegrenzen: organisatorische en institutionele implicaties. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Berg, M. (1998). The Politics of Technology: On Bringing Social Theory into Technological Design. *Science, Technology & Human Values, 23*(4), 456-490.
Bergeron, B. (2003). *Essentials of XBRL Financial Reporting in the 21st Century*. New Jersey: John Wiley & Sons.
Berkelaar, T. (2007). Strategieën voor de ontwikkeling van een ICT infrastructuur voor de overheid. In J. Grijpink (Ed.), *Geboeid door ketens*: Platform Keteninformatisering.
Bertino, E., Martino, L. D., Paci, F., & Squicciarini, A. C. (2010). *Security for Web Services and Service-Oriented Architectures*. Heidelberg: Springer.
Besselink, C. (2010). Gegevenskwaliteit in overheidsnetwerken. *Bestuurlijke informatieverzorging, 84*(3), 209-221.
Bharosa, N., van der Voort, H., Hulstijn, J., Janssen, M., van Wijk, R., & de Winne, N. (2011). *Impose With Leeway: Combining an Egineering and Learning Approach in the Management of Public-Private Collaboration*. Paper presented at the IFIP EGOV, Delft, The Netherlands.
Boehm, B. (2002). Get ready for agile methods, with care. *Computer, 35*(1), 64-69.
Bonaccorsi, A., Carmignani, G., & Zammori, F. (2011). Service Value Stream Management (SVSM): Developing Lean Thinking in the Service Industry. *Journal of Service Science and Management*(4), 428-439.
Bonsón, E., Cortijo, V., & Escobar, T. (2009). Towards the global adoption of XBRL using International Financial Reporting Standards (IFRS) *International Journal of Accounting Information Systems, 10*, 46-60.
Boudreau, K., & Hagiu, A. (2010). Platform Rules: Multi-sided Platforms as Regulators. In A. Gawer (Ed.), *Platforms, Markets en Innovation*. Cheltenham, UK: Edward Elgar Publishing.
Brooks, F. P., Jr. (2006). *The mythical man-month* (Anniversary ed.). Indiana, USA: Addison-Wesly.
Brooks, L. (1997). Structuration Theory and New Technology: Analysing Organisationally Situated Computer-Aided Design (CAD). *Information Systems Journal, 7*, 133-151.
Brookshear, G. (2012). *Computer Science - An overview* (11 ed.). Boston: Addison-Wesley.
Brown, A. E., & Grant, G. G. (2005). Framing the Frameworks: A Review of IT Governance Research. *Communications of the Association for Information Systems, 15*, 696-712.
Bruijn, J. A., de. (2011). *Framing*. Amsterdam: Atlas-Contact.
Bruijn, J. A., de, & Herder, P. M. (2009). Systems and Actor Pespectives on Sociotechnical Systems. *IEEE Transactions on Systems, Man and Cybernetics, 39*(5), 981-992.
Bruijn, J. A., de, & ten Heuvelhof, E. F. (1994). *Over complexe netwerken en een tweede generatie sturingsinstrumenten*. Houten: Stenferd Kroese.
Bruijn, J. A., de, & ten Heuvelhof, E. F. (1995). *Netwerkmanagement* (1 ed.). Utrecht: Lemma.
Bruijn, J. A., de, & ten Heuvelhof, E. F. (2007). *Management in Netwerken* (3 ed.). Utrecht: Lemma.
Bruijn, J. A., de, ten Heuvelhof, E. F. & in 't Veld, R. J. (2008). *Procesmanagement - Over procesontwerp en besluitvorming* (3 ed.): Academic Service.

Bruijn, J. A., de, Wagenaar, R. W., van der Voort, H. & van Wendel de Joode, R. (2004). Shared Services in de overheid; Samenwerking tussen beleidspartners. TU Delft.
Buijs, J., van Doorn, V. & Noordam, P. (2004). *Shared Service Centers: Een kwestie van doen*: Kluwer.
Burr, W. E. (2006). Cryptographic hash standards: where do we go from here? *IEEE Security & Privacy, 4*(2), 88-91

C

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy, 7*(1), 78-81
Cameron, K. S., & Quinn, R. E. (2006). *Diagnosing and changing organizational culture: based on the competing values framework*. San Francisco, CA: Jossey-Bass (Wiley imprint).
Carr, D., & Johansson, H. (1995). *Best Practices in Re-engineering: What Works & What Doesn't in the Re-engineering Process*. NY: McGraw-Hill.
Carter, S. (2007). *The New Language of Business: SOA & Web 2.0*. Upper Saddle River, NJ: IBM Press.
Chaffy, D. (2004). *E-business en e-commerce: een managementperspectief*. Edinburg, Harlow: Pearson Education.
Chappell, D. (2004). *Enterprise Service Bus*. Sebastopol, CA: O'Reilly Media.
Chinosi, M., & Trombetta, A. (2012). BPMN: An introduction to the standard. *Computer Standards & Interfaces, 34*, 124-134.
Churchman, C. (1967). Wicked problems. *Management Science, 4*(14), 141-142.
Claassens, R. (2007). Semantische interoperabiliteit met behulp van een bedrijfsbrede taxonomie *Via Nova Architectura*.
Clark, C., Cavanaugh, N., Brown, C., & Sambamurthy, V. (1997). Building Change-Readiness Capabilities in the IS Organization: Insights From the Bell Atlantic Experience. *MIS Quarterly, 21*(4), 425-455.
Clegg, C. W. (2000). Sociotechnical principles for system design. *Applied Ergonomics, 31*, 463-477.
Cohen, M. D., March, J. G., & Olsen, J. P. (1972). A Garbage Can Model of Organizational Choice. *Administrative Science Quarterly, 17*(1), 1-25.
Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly, 35*(1), 128-152.
Curbera, F., Duftler, M., Khalaf, R., Nagy, W., Mukhi, N., & Weerawarana, S. (2002). Unraveling the Web services web: an introduction to SOAP, WSDL, and UDDI *Internet computing, 6*(2), 86 - 93
Cusumano, M. A. (2005). Google: what it is and what it is not. *Communications of the ACM, 48*(2), 15-17.

D

Dalen, J., van. (2000). Ketens en condities. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.
Dannemiller, K., & Jacobs, R. (1992). Changing the Way Organizations Change: A Revolution of Common Sense. *Journal of Applied Behavioral Science, 28*(4), 480-498.

Das, T. K., & Teng, B.-S. (1998). Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances. *The Academy of Management Review, 23*(3), 491–512.
Davenport, T. H. (1993). *Process Innovation: Re-engineering Work through Information Technology*: Harvard Business School Press.
Davenport, T. H., & Short, J. E. (1990). The New Industrial Engineering: Information Technology and Business Process Redesign. *Sloan Management Review, 31*(4), 11-27.
de Wit, B., Rademakers, M., & Brouwer, M. (2000). Ketenstrategie: van virtuele naar reële ketens. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.
Dervitsiotis, K. N. (1998). The challenge of managing organizational change: Exploring the relationship of re-engineering, developing learning organizations and total quality management. *Total Quality Management, 9*(1), 109-122.
Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654.
Donaldson, L. (2001). *The Contingency theory of organizations*. Thousands Oaks: Sage.
Drejer, A. (2002). *Strategic Management and Core Competencies: Theory and Application*. London.
Duivenboden, H., van, van Twist, M., & Veldhuizen, M. (2000). Ketenmanagement in de publieke sector: introductie. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.
Duivenboden, H., van, Veldhuizen, M., & van Twist, M. (2000). Kantelende ketens: naar publiek ketenmanagement. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

E

Earl, M. J. (1994). The New and Old of Business Process Redesign. *Journal of Strategic Information Systems, 3*(1), 5-22.
Eeten, M., van, Bruijn, J. A., de, Voort, H., van der, & Bueren, E., van. (2000). *Koppelen met water*. Delft: Eburon.
Erl, T. (2008). *SOA: Principles of Service Design*. Upper Saddle River, NJ: Prentice Hall.

F

Feenstra, R. W. (2011). *Service Composition: A Method for Developing Compositions in a Multi-actor Context*. Dissertation. Delft, Delft University of Technology
Feo, J. d., & Bar-El, Z. (2002). Creating strategic change more efficiently with a new design for six sigma process. *Journal of Change Management, 3*(1), 60-80.
Fleck, J., & Howells, J. (2001). Technology, the Technology Complex and the Paradox of Technological Determinism. *Technology Analysis & Strategic Management, 13*(4), 523-531.

Floridi, L. (2011). *Semantic Conceptions of Information* E. N. Zalta (Ed.). Geraadpleegd in mei 2013 via http://plato.stanford.edu.

Folmer, E., & Punter, M. (2010). *Beheer- en ontwikkelmodel voor open standaarden. (BOMOS) versie 2*. Enschede: Programmabureau NOiV.

Fremantle, P., Weerawarana, S., & Khalaf, R. (2002). Enterprise services. Examine the emerging files of web services and how it is integrated into existing enterprise infrastructures. *Communications of the ACM, 45*(20), 77-82.

G

Galbraith, J. R. (1973). *Designing complex organizations*: Addisson-Wesley Publishing Company.

GEIN. (2006). Definitief Programma van Eisen van de Generieke Infrastructuur. Geraadpleegd in juni 2012 via www.gein-project.nl.

Goldratt, E. M. (1997). *Critical Chain*. Great Barrington, MA: North River Press.

Goldratt, E. M., & Cox, J. (1984). *The Goal: A Process of Ongoing Improvement*. Great Barrington, MA: North River Press.

Gong, Y., Janssen, M., Overbeek, S., & Zuurmond, A. (2009). *Enabling flexible processes by ECA orchestration architecture*. Paper presented at the the 3rd International Conference on Theory and Practice of Electronic Governance (ICEGOV), Bogota, Columbia.

Gortmaker, J., Janssen, M., & Wagenaar, R. W. (2004). *The Advantages of Web Service Orchestration in Perspective*. Paper presented at the 6th International Conference of Electronic Commerce, ICEC 2004, Delft, The Netherlands.

Gresov, C. (1989). Exploring Fit and Misfit with Multiple Contingencies. *Administrative Sciences Quarterly, 34*(3), 431-453.

Grijpink, J. (2000). Een dynamisch ketenbegrip voor informatisering van externe samenwerking. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Grijpink, J. (2010). *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling*. Den Haag: Boom Lemma uitgevers.

Gruber, T. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition, 5*, 199-220.

Gulati, R., & Singh, H. (1998). The architecture of cooperation: Managing coordination costs and appropriation concerns in strategic alliances. *Administrative Science Quarterly, 43*(4), 781-814.

H

Hagiu, A., & Yoffie, D. B. (2009). What's Your Google Strategy? *Harvard Business Review, 87*(4), 74-81.

Hajer, M. (2003). Policy without polity? Policy analysis and the institutional void. *Policy Sciences, 36*, 175-195.

Hammer, M., & Champy, J. (1993). *Reengineering the Corporation: A Manifesto for Business Revolution,* : Harper Business

Hansen, J. V., & Hill, N. C. (1989). Control and Audit of Electronic Data Interchange. *MIS Quarterly, 13*(4), 403-414.

Hedeman, B., Vis van Heems, G., & Fredriksz, H. (2009). *Best Practice Projectmanagement, op basis van PRINCE2*. Zatbommel: Van Haren Publishing.
Hedeman, B., & Vis van Heemst, G. (2011). *Programmamanagement op basis van MSP* (2 ed.). Zatbommel: Van Haren Publishing.
Heller, J. (1961). *Catch-22*. New York: Simon & Schuster.
Henderson, J., & Venkatraman, N. (1993). Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal, 32*(1), 4-16.
Hines, P., Holweg, M., & Rich, N. (2004). Learning to evolve A review of contemporary lean thinking. *International Journal of Operations & Production Management, 24*(10), 994-1011.
Hoffman, C., & Watson, L. (2010). *XBRL for Dummies*. Hoboken, NJ: Wiley Pusblishing Inc.
Hofman, W. (2003). *EDI, webservices & ebXML, interacties in organisatienetwerken*. 's Hertogenbosch: Uitgeverij Tutein Nolthenius.
Hoppe, R. (2010). *The governance of problems. Puzzling, powering, participation*. Bristol: Policy Press.
Huizing, A., & de Vries, E. J. (red.). (1997). *Business reengineering op doorreis: tussenstation of eindstation?* Alphen aan den Rijn: Samsom.

I

IDABC. (2004). European Interoperability Framework for pan-European eGovernment Services, Interchange of Data between Administrations, Businesses and Citizens. Luxembourg: European Commission, 2004/2094.

J

Janis, I. L. (1972). *Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes*. Oxford, England: Houghton Mifflin.
Jans, E. O. (1991). *Grondslagen administratieve organisatie - Deel B: processen en systemen* (19 ed.). Groningen/Houten: Wolters-Noordhoff.
Janssen, M., Gortmaker, J., & Wagenaar, R. W. (2006). Web service orchestration in public administration: Challenges, roles and growth stages. *Information Systems Management, 23*(2), 44-55.
Janssen, M., Veenstra, A. F. v., Groenleer, M., Voort, H. v. d., Bruijn, H. d., & Bastiaansen, C. (2010). Uit het Zicht: Beleidsmaatregelen voor het versnellen van het gebruik van ICT-toepassingen voor administratieve latenverlichting Delft: ACTAL.
Janssen, M. F. W. H. A., & Gortmaker, J. (2005). Orchestreren van ketenprocessen. *Informatie*, 18-22.
Janssen, M. F. W. H. A., van Veenstra, A., Groenleer, M., van der Voort, H., Bruijn, J. A., de, & Bastiaansen, C. (2010). Uit het Zicht: Beleidsmaatregelen voor het versnellen van het gebruik van ICT-toepassingen voor administratieve latenverlichting. Geraadpleegd in april 2012 via www.actal.nl.
Janssen, M. F. W. H. A., & Wagenaar, R. (2004). *An Analysis of a Shared Services Centre in E-government*. Paper presented at the Proceedings of the 37th Hawaii International Conference on System Sciences.
Juran, J. (1992). *Juran on quality by design*. New York: The Free Press.

Juric, M., Mathew, B., & Sarang. (2006). *Business Process Execution Language for Web Services* Birmingham, UK: Packt Publishing.

K

Kauremaa, J., Kärkkäinen, M., & Ala-Risku, T. (2009). Customer initiated interorganizational information systems: The operational impacts and obstacles for small and medium sized suppliers. *International Journal of Production Economics, 119*(2), 228-239.

Kettinger, W. J., & Grover, V. (1995). Toward a theory of business process change management. *Journal of Management Information Systems, 12*(1), 9-30.

Kettinger, W. J., Teng, J. T. C., & Guha, S. (1997). Business Process Change: A study of methodologies, techniques, and tools. *MIS Quarterly, 21*(1), 55-79.

Khalaf, R., Keller, A., & Leymann, F. (2006). Business processes for Web Services: Principles and applications. *IBM Systems Journal, 45*(2), 425-446.

Kim, H., Pan, G., & Pan, S. (2007). Managing IT-enabled transformation in the public sector: A case study on e-government in South Korea. *Government Information Quarterly, 24*, 338-352.

Kizza, J. M. (2009). *A Guide to Computer Network Security*. New York: Springer-Verlag.

Kleve, P. (2004). *Juridische iconen in het informatietijdperk*. (Proefschrift), Erasmus Universiteit Rotterdam, Kluwer – Deventer.

Klingenberg, A. M. (2011). *Bestuursrecht, e-mail en internet. Bestuursrechtelijke aspecten voor elektronische overheidscommunicatie*. (Proefschrift), De Rijksuniversiteit Groningen, Groningen.

Kloppmann, M., Koenig, D., Leymann, F., Pfau, G., & Roller, D. (2004). Business process Choreography in WebSphere: Combining the Power of BPEL and J2EE. *IBM Systems Journal, 43*(2), 270-296.

Koffijberg, J. (2005). *Getijden van beleid: omslagpunten in de volkshuisvesting. Over de rol van hiërarchie en netwerken bij grote veranderingen*. (Dissertation), Delft University of Technology.

Korsten, A. F. A. (1988). *Bestuurskunde als avontuur*. Deventer: Kluwer.

L

Lamb, R., & Kling, R. (2003). Reconceptualizing Users as Social Actors in Information Systems Research. *MIS Quarterly, 27*(2), 197-236.

Laudon, K., & Laudon, J. (2010). *Bedrijfsinformatiesystemen* (11 ed.). Amsterdam: Pearson Education.

Lee, J.-N., Huyn, M., Kwok, R., & Pi, S.-H. (2003). IT outsourcing evolution: past, present, and future. *Communications of the ACM, 46*(5), 84-89.

Lee, M. (2003). *Conceptualizing the New Governance: A New Institution of Social Coordination*. Paper presented at the Institutional Analysis and Development Mini-Conference, Indiana University, USA.

Lee, Y. W., Strong, D., Kahn, B., & Wang, R. (2002). AIMQ: a methodology for information quality assessment. *Information and Management, 40*, 133-146.

Lewin, K. (1951). *Field Theory in Social Science*. New York: Harper & Row.

Linthicum, D. S. (2003). *Next Generation Application Integration: From Simple Information to Web Services*: Addison Wesley.

Logius. (2011). *Programma van Eisen PKIoverheid*.
Looijen, M. (2004). *Beheer van informatiesystemen* (6 ed.). Den Haag: ten Hagen & Stam.

M

Maes, R. (2003). Informatiemanagement in kaart gebracht. *PrimaVera Working Paper Series*.
Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Computing Surveys (CSUR), 26*(1), 87-119.
Malone, T. W., Yates, J., & Benjamin, R. I. (1987). Electronic Markets and Electronic Hierarchies. *Communications of the ACM, 30*(6), 484-497.
Markus, L., & Bui, Q. (2012). Going Concerns: The Governance of Interorganizational Coordination Hubs. *Journal of Management Information Systems, 28*(4), 163-197.
McComb, D. (2003). *Semantics in Business Systems*: Morgan Kaufmann.
McGilvray, D. (2008). *Executing data quality projects, Ten steps to quality data and trusted information*: Morgan Kaufmann Publishers.
McGovern, J., Sims, O., Jain, A., & Little, M. (2006). *Enterprise service oriented architectures: concepts, challenges, recommendations*. Dordrecht: Springer.
Meijer, S. (2009). *The organisation of transactions; Studying supply networks using gaming simulation*. Wageningen Academic Publishers.
Metselaar, E. E., & Cozijnsen, A. J. (2005). *Van weerstand naar veranderingsbereidheid. Over willen, moeten en kunnen veranderen*. Heemstede: Holland Business Publications.
Mintzberg, H. (1992). *Structure In Fives: Designing Effective Organizations*: Prentice Hall.
Monczka, R. M., Petersen, K. J., Handfield, R. B., & Ragatz, G. L. (1998). Succes Factors in Strategic Supplier Alliances: The Buying Company Perspective. *Decision Sciences, 29*(3), 553–577.
Morgan, T. (2002). *Business Rules and Information Systems: Aligning IT with Business Goals*: Addison Wesley.

N

Nadler, D., & Tushman, M. (1980). A model for diagnosing organizational behavior. *Organizational Dynamics, 9*(2), 35-51.
National Computing Centre. (2005). IT Governance. Developing a successful governance strategy. A Best Practice guide for decision makers in IT. Oxford Road, Manchester: The National Computing Centre.
Newcomer, E., & Lomow, G. (2005). *Understanding SOA with Web services*. NJ: Pearson Education.
Nijsen, A. (2003). *Dansen met de Octopus, Een bestuurskundige visie op informatieverplichtingen van het bedrijfsleven in de sociale rechtsstaat*. Erasmus Universiteit Rotterdam, Uitgeverij Eburon, Delft.

O

O'Neill, P., & Sohal, A. S. (1999). Business Process Reengineering A review of recent literature *Technovation, 19*(9), 571-581.

O'Donnell, O., B., R., & Timonen, V. (2003). Transformational aspects of e-Government in Ireland: Issues to be addressed. *Electronic Journal of e-Government, 1*, 23-32.
Ohno, T. (1988). *Toyota production system: beyond large-scale production*. New York: Productivity Press.
Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science, 3*(3), 398-427.
OSOSS. (2005). *Berichtenverkeer, Dossier Open Standaarden, Programma Open Standaarden en Open Source Software*. Den Haag.
Osterwalder, A., & Pigneur, Y. (red.). (2010). *Business Model Generation*. Hoboken, New Jersey: John Wiley & Sons, Inc.
Ouksel, A. M., & Sheth, A. (1999). Semantic Interoperability in Global Information Systems. *Special Issue of ACM Sigmod Record, 28*(1), 5-12.

P

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners* (2 ed.). Berlin: Springer.
Papazoglou, M. P., & Georgakopoulos, D. (2003). Service-oriented computing. *Communications of the ACM, 46*(10), 24-25.
Pardo, T. A., Gil-Garcia, J. R., & Burke, G. B. (2008). *Governance structures in cross-boundary information sharing: Lessons from state and local criminal justice initiatives*. Paper presented at the 41st Annual Hawaii International Conference on System Sciences.
Parnas, D. L. (1972). On the Criteria To Be Used in Decomposing Systems into Modules. *Communications of the ACM, 15*(12), 1053-1058.
Pidcock, W. (2002). What are the differences between a vocabulary, a taxonomy, a thesaurus, an ontology, and a meta-model? Geraadpleegd in maart 2012, www.infogrid.org/trac/wiki/Reference/PidcockArticle
Piechocki, M., & Felden, C. (2007). *XBRL taxonomy engineering. Definition of XBRL taxonomy development process model*. Paper presented at the Fifteenth European Conference on Information Systems, Technische Universität Bergakademie Freiberg.
Pinsker, R. (2003). XBRL awareness in auditing: a sleeping giant? *Managerial Auditing Journal, 18*(9), 732-736.
Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall.
Provan, K. G., & Kenis, P. (2007). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory, 18*(2), 229-252.

Q

Quinn, R. (1998). *Persoonlijk meesterschap in management; Voorbij rationeel management*. Den Haag: Academic Service.

R

Redman, T. C. (1995). Improve Data Quality for Competitive Advantage. *Sloan Management Review, 36*(2), 99-107.

Reimer, U. (2001). *Tutorial on Organizational Memories for Capturing, Sharing and Utilizing Knowledge*. Paper presented at the International Conference on Enterprise Information Systems, ICEIS 2001, Setubal, Portugal.
Reynolds, G., & Stair, R. (2013). *Fundamentals of Information Systems* (7 ed.): Cengage Learning.
Rhodes, R. (1996). The New Governance: Governing without Government. *Political Studies, 44*(4), 652-667.
Richards, K. (2007). *Agile Project Management: Running PRINCE2 projects with DSDM*. UK: The Stationery Office.
Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120-126.
Roebuck, K. (2011). *Public Key Infrastructure: High-Impact Strategies - What You Need to Know*: Emereo Pty Limited.
Rogers, E. M. (2003). *Diffusion Of Innovations* (5 ed.). New York: Free Press.
Royce, W. (1970). *Managing the Development of Large Software Systems*. Paper presented at the IEEE WESCON. Reprinted in Proceedings of the 9th International Conference on Software Engineering (1987).
Rutgers, M. (2011). Het torentje van de overheid. In COAP (Ed.), *Het eigene van de overheid, input voor het debat over de rol van de overheid*.

S

Sambamurthy, V., & Zmud, R. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies *MIS Quarterly, 23*(2), 261-290.
Schekkerman, J. (2000). Ketenintegratie en architecturen. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.
Schellekens, M. H. M. (2004). *Electronic Signatures, Authentication Technology from a Legal Perspective* Den Haag: T.M.C. Asser Press.
Scholl, H. J., & Klischewski, R. (2007). E-Government Integration and Interoperability: Framing the Research Agenda. *International Journal of Public Administration, 30*(8), 889-920.
Simatupang, T. M., & Sridharan, R. (2002). The Collaborative Supply Chain. *International Journal of Logistics Management, 13*(1), 15-30.
Simsion, G. C., & Witt, G. C. (2005). *Data Modeling Essentials* (3 ed.): Morgan Kaufmann Publishers.
Stallings, W. (2007). *Data and Computer Communications* (8 ed.): Prentice Hall.
Stallings, W. (2009). *Business Data Communications*. Upper Saddle River, New Jersey: Prentice Hall.
Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice* (5 ed.). Boston: Pearson Education, Inc.
Sutanto, J., Kankanhalli, A., Tay, J., Raman, K., & Tan, B. (2009). Change Management in Interorganizational Systems for the Public. *Journal of Management Information Systems, 25*(3), 133-175.

T

Teece, D. J. (1998). Capturing value from knowledge assets: the new economy, markets for know-how and intangible assets. *California Management Review, 40*, 55-79.

Tel, G. (2002). *Cryptografie: beveiliging van de digitale maatschappij*. Amsterdam: Pearson Education.

ten Berge, J. B. J. M., & Michiels, F. C. M. A. (2001). *Besturen door de overheid* (4 ed.). Deventer: W.E.J. Tjeenk Willink.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge; Improving Decisions about Health, Wealth and Hapiness*. New Haven: Yale University Press.

The Royal Academy of Engineering. (2004). The Challenges of Complex IT Projects. London: The Royal Academy of Engineering and The British Computer Society.

Thiadens, T. (2008). *Sturing en organisatie van ICT-voorzieningen* (2 ed.). Zaltbommel: Van Haren Publishing.

Thomas, S. A. (2000). *SSL & TLS Essentials - Securing the Web*. New York: Wiley Computer Publishing.

Tiwana, A., Konsynski, B., & Bush, A. (2010). Research Commentary: Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Information Systems Research, 21*(4), 675-687.

Turner, M. (2003). Turning software into a service. *Computer, 36*(10), 38 - 44.

Tushman, M. (1977). A Political Approach to Organizations: A Review and Rationale. *Academy of Management Review, 2*(2), 206-216.

Tuunainen, V. K. (1999). Opportunities of effective integration of EDI for small businesses in the automotive industry. *Information & Management, 34*, 361-375.

Twist, M., van, Edelenbos, J., & Broek, M., van den. (1998). In dilemma's durven denken. *M&O, 5*, 7-23.

U

Uschold, M. (2003). Where Are the Semantics in the Semantic Web? *AI Magazine, 24*(3), 25-36.

Uzzi, B. (1997). Social structure and competition in interfirm networks: The paradox of embededness. *Administrative Science Quarterly, 42*, 35-67.

V

van der Aa, A. (2009). *Regie en ICT in dienstbare ketens. Samen (net)werken aan maatschappelijke oplossingen*. Den Haag: Boom Lemma.

Van der Laan, A. (2006). Ontwerpen van een enterprise service bus. *Software Release Magazine, 3*(10), 11-17.

van Oost, E., Alberts, G., van den Ende, J., & Lintsen, H. (1998). *De opkomst van de informatietechnologie in Nederland*. Den Haag: Ten Hagen Stam.

van Wessel, R. M. (2008). *Realizing Business Benefits from Company IT Standardization*. (Proefschrift), Tilburg.

Ven, A., van de, & Walker, G. (1984). The Dynamics of Interorganizational Coordination. *Administrative Science Quarterly, 29*(4), 598-621.

Vidgen, R., Avison, D., Wood, B., & Wood-Harper, T. (2002). *Developing web information systems*. Cornwall, UK: Butterworth-Heinemann.

W

W3C (2004). Web Services Glossary. Geraadpleegd in augustus 2013 via www.w3.org/TR/2004/NOTE-ws-gloss-20040211

Wastell, D. G., White, P., & Kawalek, P. (1994). A methodology for business process redesign: experiences and issues. *Journal of Strategic Information Systems, 3*(1), 23-40.

Weening, H. (2006). *Smart Cities; Omgaan met onzekerheid*. Delft: Eburon.

Weerakkody, V., & Dhillon, G. (2008). Moving from E-Government to T-Government: A Study of Process Re-engineering Challenges in a UK Local Authority Perspective. *International Journal of Electronic Government Research, 4*(4), 1-16.

Weerawarana, S., Curbera, F., Leyman, F., Storey, T., & Ferguson, D. (2005). *Web Services Platform Architecture*. Upper Saddle River, NJ: Prentice Hall.

Weill, P. (2004). Don't Just Lead, Govern: How Top-Performing Firms Govern IT. *MIS Quarterly Executive, 3*(1), 1-17.

Weill, P., & Ross, J. W. (2005). A matrixed approach to designing IT governance. *MIT Sloan Management Review, 46*(2), 26-34.

Weske, M. (2007). *Business Process Management. Concepts, Languages, Architecturees*. Berlin Heidelberg: Springer.

West, J. (2007). he Economic Realities of Open Standards: Black, White and Many Shades of Gray *Standards and Public Policy* (pp. 87-122). Cambridge: Cambridge University Press.

White, S., & Miers, D. (2008). BPMN Modeling and Reference Guide: Understanding and Using BPMN. Lighthouse Point, FL, USA: Future Strategies Inc.

Wit, B., de, Rademakers, M., & Brouwer, M. (2000). Ketenstrategie: van virtuele naar reële ketens. In: H. van Duivenboden, M. van Twist, M. Veldhuizen, R. in 't Veld (red.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Womack, J., Roos, D., & Jones, D. (1990). *The Machine That Changed the World*. New York, NY: Rawson and Associates.

Womack, J. P., & Jones, D. T. (1996). *Lean Thinking: Banish waste and create wealth in your organization*. New York: Simon & Schuster.

Wortmann, H., & Kremer, D. (2011). Het belang van goed opdrachtgeverschap. *Management Executive* (juli).

WRR (2006). *Lerende overheid - een pleidooi voor probleemgerichte politiek*. Amsterdam: Amsterdam University Press.

WRR (2011). *iOverheid*. Amsterdam: Amsterdam University Press.

Wu, Y. C. (2003). Lean Manufacturing: A Perspective of Lean Suppliers. *International Journal of Operations & Production Management, 23*(11), 1349-1376.

Z

Zuurmond, A. (1994). De Infocratie - een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk. Rotterdam: Erasmus Universiteit.