Ondertekeningsbeleid van het SBR domein handelsregister

Openbare consultatie
Dit document is gepubliceerd voor consultatiedoeleinden. Wij nodigen u uit op de inhoud van dit document te reageren. Uw reactie zien wij graag voor 31 januari 2025 tegemoet. Mail uw reactie naar sbr@logius.nl o.v.v. “ondertekeningsbeleid domein handelsregister”.

Alle reacties zijn openbaar en worden op de SBR website gepubliceerd, tenzij u bij de indiening expliciet aangeeft dat u hier geen prijs op stelt.

Op basis van de reacties stelt de domeingovenance de definitieve versie vast. Deze zullen vervolgens op de SBR website worden gepubliceerd.

Datum: 9 december 2024
Versie: 0.9

Inhoudsopgave

1. Inleiding

Dit document beschrijft het ondertekeningsbeleid voor gekwalificeerde elektronische handtekening(en) en zegel(s) op documenten binnen de reikwijdte van het SBR domein Handelsregister. Dit zijn documenten die op basis van Standard Business Reporting (SBR) in Nederland worden gedeponeerd bij het handelsregister van de Kamer van Koophanden (KVK). Hierbij moet onder meer gedacht worden aan het elektronisch ondertekenen van de opgemaakte jaarrekening door bestuurder(s) en commissaris(sen) van een rechtspersoon. SBR is de Nederlandse methode voor het elektronisch uitwisselen van bedrijfsrapportages of andere zakelijke documenten tussen organisaties.

Een ondertekeningsbeleid is een set van regels voor het aanmaken, augmenteren, valideren en het voor lange termijn bewaren van één of meer onderling verbonden elektronische handtekeningen en zegels. Het bepaalt de technische en procedurele eisen aan elektronische handtekeningen en zegels, zodat de geldigheid van de handtekeningen en zegels kan worden vastgesteld. Een ondertekeningsbeleid maakt de aspecten van het proces van ondertekening transparant voor alle betrokkenen, zoals ondertekenaars, ontvangers en arbiters. Dit verhoogt het vertrouwen in en de acceptatie van de elektronische handtekeningen en zegels die aan het ondertekeningsbeleid voldoen.

Dit ondertekeningsbeleid volgt de structuur zoals vastgelegd in ETSI TS 119 172-1[1]. In deze technische specificatie worden de verschillende onderdelen van een ondertekeningsbeleid nader uiteengezet.

1.1. Situatieschets

De situatieschets formaliseert de belangrijkste technologische, organisatorische en juridische aspecten omtrent het aanmaken, augmenteren, valideren en het voor lange termijn bewaren van gekwalificeerde elektronische handtekeningen en zegels. Bovendien maakt het expliciet wat de intentie is van de gekwalificeerde elektronische handtekening respectievelijk de gekwalificeerde elektronische zegel.

1.1.1. Processchets

Jaarrapportage
Bestuurders van rechtspersonen zijn jaarlijks verplicht om een jaarrekening op te (laten) maken volgens BW2[2]. De jaarrekening moet vervolgens worden ondertekend door bestuurders en commissarissen en in het geval van stichtingen door bestuurders en zij die deel uitmaken van het toezichthoudende orgaan (hierna: bestuurders en commissarissen). Deze handtekening kan op vrijwillige basis ook worden gezet met behulp van een gekwalificeerde elektronische handtekening.

Artikel in BW2[2] voor ondertekening	**Type rechtspersoon**	**Tekenplichtigen**
49 lid 2	Vereniging	Bestuurders en commissarissen
58 lid 2	Coöperaties en onderlinge waarborgmaatschappijen	Bestuurders en commissarissen
101 lid 2	Naamloze Vennootschap	Bestuurders en commissarissen
210 lid 2	Besloten Vennootschap	Bestuurders en commissarissen

300 lid 2	Stichtingen	Bestuurders en hen die deel uitmaken van het toezichthoudende orgaan

Tabel 1: Tekenplichtigen van rechtspersonen volgens BW2

Zodra bestuurders en commissarissen akkoord gaan met de inhoud van de jaarrekening, start het proces van ondertekening. Tijdens dit proces verifieert elke bestuurder en commissaris de jaarrekening. Zij stellen vast dat er geen duidelijke fouten zijn geïntroduceerd als gevolg van de verschillende aanpassingen tijdens het opmaken van de jaarrekening, zodat deze aan de wettelijke vereisten voldoet. In geval van het vrijwillig zetten van een gekwalificeerde elektronische handtekening, maken de bestuurders en commissarissen die de inhoud verifiëren gebruik van gecertificeerde XBRL-software die bij voorkeur onderdeel uitmaakt van een 'signature creation application' (SCA) die de inhoud van de jaarrekening visualiseert. Na succesvolle verificatie wordt de jaarrekening elektronisch ondertekend door de bestuurders en de commissarissen. Met het ondertekenen bevestigen bestuurders en commissarissen dat zij achter de inhoud van de jaarrekening staan.

Een jaarrekening wordt in principe ondertekend door alle bestuurders en commissarissen van de rechtspersoon. Wanneer een bestuurder of commissaris de jaarrekening niet ondertekent, moet dit met opgave van reden op de jaarrekening vermeld worden. Bestuurders en commissarissen kunnen de jaarrekening vrijwillig ondertekenen met een gekwalificeerde elektronische handtekening (ook wel 'Qualified Electronic Signature'). De gekwalificeerde elektronische handtekening wordt in dat geval gezet met behulp van een gekwalificeerd persoonsgebonden certificaat.

In aanvulling op de ondertekening van de jaarrekening door bestuurders en commissarissen, kan een jaarrapportage, waar de jaarrekening samen met het bestuursverslag en overige gegevens onderdeel van uitmaakt, ook vrijwillig gewaarmerkt worden om de integriteit, authenticiteit en onweerlegbaarheid van de jaarrapportage te garanderen. Dit gebeurt met behulp van een gekwalificeerde elektronische zegel (Qualified Electronic Seal) op naam van de rechtspersoon. De zegel wordt door een geautoriseerd persoon geplaatst met behulp van het gekwalificeerd certificaat voor elektronische zegels van de rechtspersoon.

De gekwalificeerde elektronische handtekening van de bestuurder of commissaris:
- garandeert juridisch de integriteit en authenticiteit van de inhoud van de jaarrekening;
- koppelt de jaarrekening aan de ondertekenaar;
- legt de onweerlegbaarheid van de jaarrekening vast, waarmee de bestuurder of commissaris aangeeft dat dit het document is waar zij akkoord mee gaan;
- koppelt de jaarrekening aan de datum en het tijdstip waarop deze is ondertekend met een vertrouwde tijdstempel die onmiddellijk na ondertekening van de jaarrekening is aangemaakt;
- wordt vervolgens uitgebreid tot een zelfvoorzienende vorm om het behoud van de geldigheid ervan op lange termijn te garanderen.

De gekwalificeerde elektronische zegel van de rechtspersoon:
- waarmerkt de integriteit en authenticiteit van de inhoud van de jaarrapportage;
- koppelt de jaarrapportage aan de rechtspersoon;
- legt de onweerlegbaarheid van de jaarrapportage vast, waarmee de rechtspersoon aangeeft dat dit het document is wat zij hebben opgesteld.

1.1.2. Vormvereisten

In deze paragraaf worden de vormvereisten uiteengezet waaraan zowel de gekwalificeerde elektronische handtekening en/of zegel als de te ondertekenen documenten moeten voldoen volgens dit ondertekeningsbeleid.

Deze vormvereisten gebruiken de sleutelwoorden zoals gedefinieerd in RFC 2119 (zie Appendix A voor de interpretatie hiervan).

Vereisten aan de te ondertekenen documenten:

- De te ondertekenen documenten MOETEN zijn opgesteld in iXBRL formaat.
- De te ondertekenen documenten MOETEN technisch valide zijn.
- De te ondertekenen documenten MOETEN refereren naar een toegestane versie van de KVK taxonomie.

Vereisten aan de gekwalificeerde elektronische handtekening en/of zegel:

- Elektronische handtekeningen en zegels MOETEN gekwalificeerde elektronische handtekeningen en zegels zijn.
- Gekwalificeerde elektronische handtekeningen MOETEN worden gegenereerd op basis van een gekwalificeerd certificaat voor elektronische handtekeningen conform de eIDAS-verordening[3].
- Gekwalificeerde elektronische zegels MOETEN worden gegenereerd op basis van een gekwalificeerd certificaat voor elektronische zegels conform de eIDAS-verordening[3].
- De gekwalificeerde elektronische handtekening MAG beschikken over een valide gekwalificeerde elektronische attestatie conform de eIDAS-2.0-verordening[4] met de bevestiging dat de certificaathouder is ingeschreven in het Handelsregister als bestuurder of commissaris voor de betreffende rechtspersoon.
- Elke gekwalificeerde elektronische handtekening of gekwalificeerd elektronisch zegel MOET worden opgesteld op basis van de XAdES specificatie conform ETSI EN 319 132-1[5].
- Elke gekwalificeerde elektronische handtekening of gekwalificeerd elektronisch zegel MOET afzonderlijk worden vastgelegd in een apart bestand (‘detached’).
- Een gekwalificeerde elektronische handtekening of gekwalificeerd elektronisch zegel MOET het niveau B-LTA gebruiken. Het B-LTA niveau maakt het mogelijk om een handtekening en zegel lange tijd na de generatie ervan te valideren. Dit is van belang omdat een jaarrapportage na deponering voor een langere periode beschikbaar is in het Handelsregister. Het is hierbij van belang dat naderhand objectief vastgesteld kan worden wanneer de handtekening of zegel is gezet, dat het gekwalificeerde certificaat waarmee het is gezet geldig was op het moment van ondertekenen en dat de gekwalificeerde elektronische handtekening of zegel sindsdien niet is gewijzigd, ongeacht de recente ontwikkelingen in cryptografische technologieën.
- In de gekwalificeerde elektronische handtekening of het gekwalificeerd elektronisch zegel MOET worden verwezen naar dit ondertekeningsbeleid door het opnemen van een unieke identifier (zie paragraaf 1.3.2).
- In de gekwalificeerde elektronische handtekening of het gekwalificeerd elektronisch zegel MOET NIET een signature policy qualifier gebruikt worden.
- In de gekwalificeerde elektronische handtekening of het gekwalificeerd elektronisch zegel MOET NIET het SignaturePolicyStore qualifying property gebruikt worden.
- In de gekwalificeerde elektronische handtekening of het gekwalificeerd elektronisch zegel MOETEN één of meer commitment types worden opgenomen die aansluiten bij de generieke commitment types zoals beschreven in Annex B van ETSI TS 119 172-1[1].
- De gekwalificeerde elektronische handtekening of het gekwalificeerd elektronisch zegel MOET kunnen worden geverifieerd door vertrouwende partijen, en MOET NIET vertrouwen van de verificateur in de betreffende SCA vereisen.

- Het is AANBEVOLEN dat de ondertekenaars de bestanden bewaren op een wijze die voldoet aan de eisen voor augmentatie en archivering uit dit ondertekeningsbeleid.

Vereisten aan de gekwalificeerde certificaten:
- Het is AANBEVOLEN dat gekwalificeerde certificaten voor elektronische handtekeningen en zegels worden gehanteerd die vallen onder de root- en intermediaire Certification Authority (CA)-certificaten die zijn uitgegeven onder de Public Key Infrastructure (PKI) voor de Nederlandse overheid, ook wel bekend als PKIoverheid (PKIo).

1.2. Toepassingsdomein

1.2.1. Reikwijdte van het ondertekeningsbeleid

Dit ondertekeningsbeleid is van toepassing op gekwalificeerde elektronische handtekeningen en zegels die worden gebruikt binnen het SBR domein Handelsregister in Nederland.

De reikwijdte van het ondertekeningsbeleid van het SBR domein Handelsregister ziet toe op:
- gekwalificeerde elektronische handtekeningen die door een bestuurder of commissaris worden gegenereerd voor het ondertekenen van een jaarrekening; en
- gekwalificeerde elektronische zegels die door een rechtspersoon worden gegenereerd voor het waarmerken van een jaarrapportage.

De generatie van een gekwalificeerde elektronische handtekening en/of zegel vindt plaats na succesvolle validatie van elk te ondertekenen bestand.

De toepassing van gekwalificeerde elektronische handtekeningen en zegels bij accountantsverklaringen in iXBRL formaat valt buiten de reikwijdte van dit ondertekeningsbeleid. Hiervoor wordt verwezen naar het NBA ondertekeningsbeleid met object ID urn:nba:ondertekeningsbeleid:pdf:1.0 op https://digital.nba.nl.

De toepassing van gekwalificeerde elektronische handtekeningen bij documenten in XBRL formaat valt voorlopig buiten de reikwijdte van dit ondertekeningsbeleid. Hiervoor wordt verwezen naar het (verouderde) SBR ondertekeningsbeleid met object ID urn:sbr:signature-policy:xml:2.0 op https://nltaxonomie.nl/sbr/signature_policy_schema/v2.0/SBR-signature-policy-v2.0.xml.

1.2.2. Toepassingsdomein

De elektronische handtekeningen en zegels die onder dit ondertekeningsbeleid vallen, zijn alleen de handtekeningen en zegels die in paragraaf 1.1 worden beschreven.

1.2.3. Transactiecontext

Niet van toepassing.

1.3. Naamgeving, identificatie en conformiteitsregels

1.3.1. Naam van het ondertekeningsbeleid

Ondertekeningsbeleid van het SBR domein Handelsregister

1.3.2. Identificatie van ondertekeningsbeleid

Documentnaam:	Ondertekeningsbeleid van het SBR domein Handelsregister
Versie:	1.0
Object ID:	urn:sbr:handelsregister:ondertekeningsbeleid:pdf:1.0
Emittent:	Domeingovernance SBR domein Handelsregister
Ingangsdatum:	1 januari 2025
Einddatum:	Onbepaald
Beschrijving:	Het ondertekeningsbeleid beschrijft de regels voor het aanmaken, augmenteren en valideren van gekwalificeerde elektronische handtekeningen en zegels in het kader van het SBR domein Handelsregister in Nederland.

1.3.3. Conformiteitsregels

Dit ondertekeningsbeleid claimt geen enkele conformiteit met enig ander ondertekeningsbeleid.

1.3.4. Distributiepunten

Het beleid wordt gepubliceerd op de SBR website via de volgende link:<nader te bepalen>.

1.4. Beheer van ondertekeningsbeleid

1.4.1. Autoriteit van ondertekeningsbeleid

Organisatienaam:	Domeingovernance SBR domein Handelsregister
KVK-nummer:	Niet van toepassing
Bezoekadres:	Niet van toepassing
Postadres:	Niet van toepassing
E-mailadres:	sbr@logius.nl

1.4.2. Contactpersonen

Vragen over het ondertekeningsbeleid kunnen worden geadresseerd aan de domeingovernance SBR domein Handelsregister via het vermelde postadres of e-mailadres in paragraaf 1.4.1.

1.4.3. Goedkeuringsprocedures

De domeingovernance SBR domein Handelsregister kan het ondertekeningsbeleid, binnen de kaders van haar governance, op elk moment wijzigen of uitbreiden zonder voorafgaande kennisgeving. De domeingovernance SBR domein Handelsregister zal het gewijzigde beleid ten minste een week voor inwerkingtreding publiceren en gebruikers hiervan op de hoogte stellen.

1.5. Acroniemen en definities

1.5.1. Afkortingen

DA	:	Driving Application
DTBS	:	Data to be signed
JSON	:	JavaScript Object Notation
PKI	:	Public Key Infrastructure
QES	:	Qualified Electronic Signature
QTSP	:	Qualified Trust Service Provider
SCA	:	Signature Creation Application

SVA	:	Signature Validation Application
TSA	:	Time-Stamp Authority
TSP	:	Trust Service Provider
XBRL	:	eXtensible Business Reporting Language
XML	:	eXtensible Markup Language
XAdES	:	XML Advanced Electronic Signature

1.5.2. Definities

Dit ondertekeningsbeleid hanteert de inhoudelijke definities zoals opgesteld hieronder.

Data to be signed zijn de gegevens die worden ondertekend. Dit zijn de documenten die ondertekend of gewaarmerkt worden alsook de gegevens die de ondertekening en interpretatie hiervan ondersteunen.

Driving Application is een applicatie die het proces van ondertekenen, augmenteren en/of valideren van elektronische ondertekeningen automatiseert. Het levert de input voor verwerking door de Signature Creation Application en ontvangt de ondertekende data. In de context van augmenteren en valideren levert de Driving Application de ondertekening en eventueel andere gegevens aan de Signature Augmentation Application en de Signature Validation Application en ontvangt de resultaten.

JSON is een gestandaardiseerd gegevensformaat. JSON maakt gebruik van voor de mens leesbare tekst in de vorm van data-objecten die bestaan uit een of meer attributen met bijbehorende waarden.

Signature Augmentation Application is een applicatie die het augmenteren van handtekeningen implementeert wat betekent dat bepaalde toepassingen, zoals tijdstempels of validatiegegevens aan de ondertekening worden toegevoegd om deze beter bestand te maken tegen veranderingen of om de levensduur van de ondertekening te verlengen.

Signature Creation Application is een applicatie die de gebruiker helpt om de data aan te bieden zodat deze ondertekend kunnen worden en stelt de ondertekende data beschikbaar voor verdere verwerking.

Signature Validation Application is een applicatie die de ondertekening valideert aan de hand van een reeks validatieregels en stelt een validatierapport op.

2. Toepassingsbeleid van de ondertekeningen

2.1. Gerelateerde wettelijke vereisten

Waar van toepassing MOETEN elektronische handtekeningen en zegels, alsmede de dienstverleners en gebruikte applicaties die vallen onder dit ondertekeningsbeleid voldoen aan de volgende bepalingen:

- eIDAS-verordening[3]
- eIDAS-2.0-verordening[4]
- Algemene Verordening Gegevensbescherming[6]
- Besluit vertrouwensdiensten[7]

2.2. Vereisten aan informatiebeveiliging

De creatie, validatie en augmentatie van ondertekeningen MOETEN voldoen aan de eisen zoals uiteengezet in de eIDAS-verordening[3]. Het is AANBEVOLEN dat de applicaties voldoen aan de beveiligingseisen zoals benoemd in ETSI TS 119 101[8] of vergelijkbare normen en standaarden.

2.3. Vereisten voor het aanmaken, valideren en augmenteren van ondertekeningen

Het is AANBEVOLEN dat de SCA, SVA en SAA voldoen aan de vereisten zoals beschreven in ETSI TS 119-101[8].

Het is AANBEVOLEN dat de SVA een melding geeft indien een document na ondertekenen nog gewijzigd is.

2.4. Vereisten voor de ontwikkeling van de applicaties

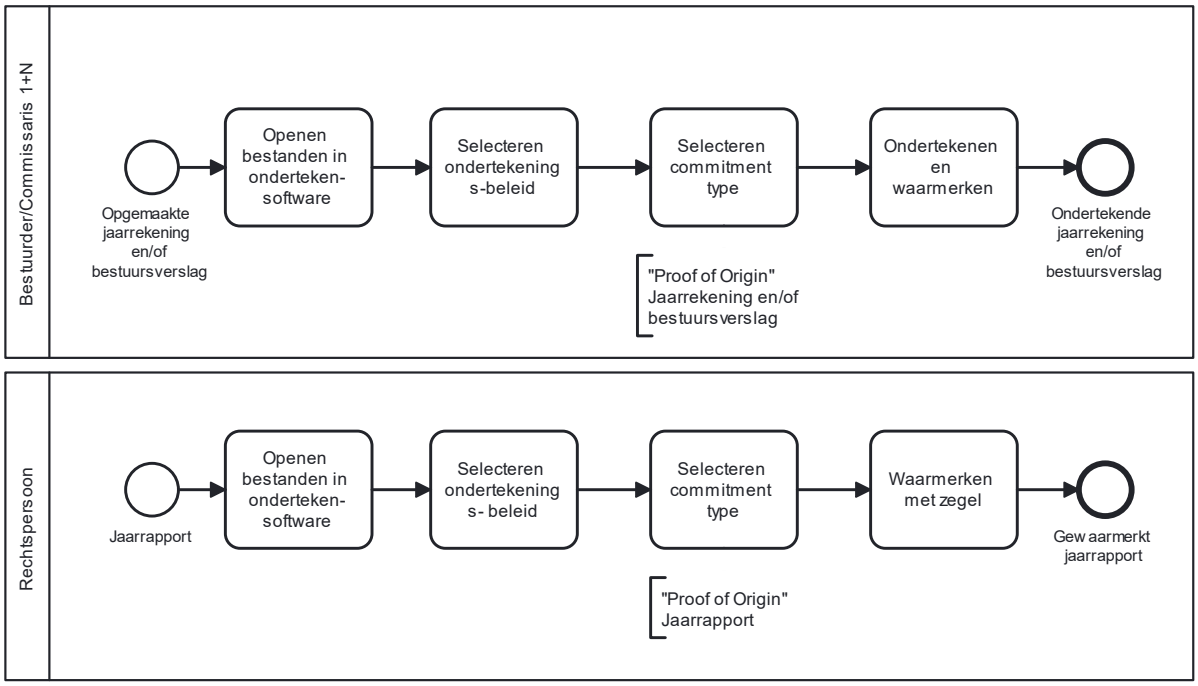
Het is AANBEVOLEN dat de SCA, SVA, SAA en DA voldoen aan de vereisten en regels zoals uiteengezet in ETSI TS 119 101[8].

3. Business scoping parameters

3.1. BSPs die verband houden met de betreffende toepassing/het betreffende bedrijfsproces

3.1.1. BSP(a): Volgorde van de ondertekening(en)

Jaarrapportage
De elektronische handtekening en/of zegel waarop dit ondertekeningsbeleid van toepassing is komt tot stand gedurende het proces dat is gevisualiseerd in Figuur 1.



Figuur 1: Ondertekenproces van de jaarrekening en/of bestuursverslag en waarmerkproces van de jaarrapportage

Om bovenstaand proces voor ondertekening van de jaarrekening en/of het bestuursverslag te starten dient iedere bestuurder of commissaris de opgemaakte jaarrekening en/of het bestuursverslag in iXBRL formaat te hebben ontvangen. Ook beschikt de bestuurder of commissaris over een gekwalificeerd persoonsgebonden certificaat om de jaarrekening en/of het bestuursverslag te ondertekenen. Optioneel beschikt de rechtspersoon over een gekwalificeerd certificaat voor elektronische zegels om de jaarrapportage separaat te waarmerken. De bestuurder of commissaris heeft vastgesteld dat de bovengenoemde documenten en middelen voldoen aan de vormvereisten van paragraaf 1.1.2.

Het plaatsen van een gekwalificeerde elektronische handtekening en/of zegel zoals beschreven in Figuur 1 start nadat de inhoud van de opgemaakte jaarrekening en/of het bestuursverslag niet meer wordt gewijzigd. Als een bestuurder of commissaris besluit de jaarrekening niet te ondertekenen moet dit worden vermeld op de jaarrekening. Hierdoor wijzigt de jaarrekening en start het ondertekenproces opnieuw, waarbij de bestuurders of commissarissen die de jaarrekening reeds ondertekend hebben opnieuw moeten tekenen.

De bestuurder of commissaris moet de jaarrekening en/of het bestuursverslag ondertekenen met een gekwalificeerde elektronische handtekening op basis van het gekwalificeerde

persoonsgebonden certificaat van de bestuurder of commissaris. Dit proces verloopt op hoofdlijnen als volgt:

- De bestuurder of commissaris opent de jaarrekening en/of het bestuursverslag in de ondertekensoftware.
- De bestuurder of commissaris selecteert de gewenste versie van het betreffende ondertekeningsbeleid.
- De bestuurder of commissaris selecteert het commitment type “Proof of Origin” voor de jaarrekening en/of het bestuursverslag (zie paragraaf 3.3.2 BSP (g)).
- De bestuurder of commissaris ondertekent de jaarrekening met behulp van het gekwalificeerde persoonsgebonden certificaat en creëert met de ondertekensoftware een gekwalificeerde elektronische handtekening.

Een geautoriseerde persoon van de rechtspersoon kan de jaarrapportage (waar de jaarrekening samen met het bestuursverslag en overige gegevens onderdeel van uitmaakt) waarmerken met een gekwalificeerde elektronische zegel. Dit *optionele* waarmerkproces, dat aanvullend is op het bovenstaande ondertekenproces, verloopt op hoofdlijnen als volgt:

- De geautoriseerde persoon van de rechtspersoon opent de jaarrapportage in de ondertekensoftware.
- De geautoriseerde persoon van de rechtspersoon selecteert de gewenste versie van het betreffende ondertekeningsbeleid.
- De geautoriseerde persoon van de rechtspersoon selecteert het commitment type “Proof of Creation” (zie paragraaf 3.3.2 BSP (g)).
- De geautoriseerde persoon van de rechtspersoon waarmerkt de jaarrapportage met behulp van het gekwalificeerde organisatie certificaat en creëert met de ondertekensoftware een gekwalificeerde elektronische zegel.

3.1.2. BSP (b): De te ondertekenen data

De DTBS bestaat uit de informatie die de ondertekening en interpretatie en context van de ondertekening ondersteunen (‘signature attributes’).

Document	Data to be signed (DTBS)	Type handtekening	Wie tekent?
1	De signature attributes, bestaande uit onder meer de referentie naar het ondertekencertificaat, commitment types, tijdstip van ondertekenen en identiteitsattributen van de ondertekenaar.	XAdES B-LTA	Bestuurders en commissarissen van de rechtspersoon

Tabel 2: beschrijving van handtekening(en) behorend tot DTBS

3.1.3. BSP (c): Het verband tussen ondertekende gegevens en handtekening(en) en zegel(s)

De relatie tussen de ondertekende gegevens en de handtekening(en) en zegel(s) is beschreven in Tabel 2 in termen van de data die wordt ondertekend en het formaat en het baseline level van de ondertekening.

Het XAdES B-LTA formaat ondersteunt zowel het plaatsen van handtekeningen als zegels. De handtekeningen en zegels hebben een vrijstaande positie ten opzichte van de ondertekende data (‘detached’).

3.1.4. BSP (d): Doelgroep

Er zijn diverse belanghebbenden bij het verwerken van de jaarrapportage (zie Tabel 3). Dit zijn actoren die vanuit een specifieke rol deze bestanden verwerken en zodoende zekerheid willen hebben over de authenticiteit en integriteit van de documenten en de wijze van ondertekening.

Actor	Omschrijving en rol	Altijd betrokken?
Bestuurder(s) en commissaris(sen)	Bestuurders en commissarissen, en in het geval van stichtingen door bestuurders en hen die deel uitmaken van het toezichthoudende orgaan, moeten de opgemaakte jaarrekening ondertekenen.	Ja
Aandeelhouders	Aandeelhouders moeten de ondertekende jaarrekening vaststellen. Zij vertrouwen op de inhoud van de ondertekende jaarrekening. Als alle aandeelhouders ook (statutair) bestuurder zijn, geldt het ondertekenen ook als vaststelling van de jaarrekening.	Ja (indien van toepassing)
Derde partijen	Andere derde partijen die vertrouwen op de inhoud van de jaarrekening.	Nee
Geautoriseerd persoon namens de rechtspersoon	Geautoriseerd persoon namens de rechtspersoon kan de jaarrapportage waarmerken met een gekwalificeerde elektronische zegel	Nee (optioneel)

Tabel 3: Beschrijving van betrokken actoren

3.1.5. BSP (e): Verantwoordelijkheid voor het valideren en augmenteren van ondertekeningen

Het uitgangspunt voor de regels met betrekking tot het valideren en augmenteren van gekwalificeerde elektronische handtekeningen en zegels, is dat de bestuurder of commissaris MOET zorgen dat de bestanden voldoen aan de volgende eisen alvorens de bestanden te verspreiden.

- De te ondertekenen documenten voldoen aan de vormvereisten van paragraaf 1.1.2 en zijn geschikt voor ondertekening met gekwalificeerde elektronische handtekeningen of zegels op basis van het B-LTA niveau.
- De validiteit van de ondertekening is geverifieerd door de bestuurder of commissaris met een Signature Validation Application op basis van ETSI EN 319 102-1[10].
- De ondertekening voldoet aan de vormvereisten van paragraaf 1.1.2.
- De verantwoordelijkheid voor het controleren of de bestuurders en commissarissen tekenbevoegd zijn, ligt bij de aandeelhouders of andere derde partijen zelf. Zij kunnen in het Handelsregister controleren of de personen die hebben ondertekend zijn ingeschreven als bestuurder of commissaris bij de betreffende rechtspersoon.

Alle belanghebbenden die op de documenten vertrouwen zijn zelf verantwoordelijk voor het augmenteren van de handtekeningen zodat de validiteit ervan over een langere periode gewaarborgd kan worden.

3.2. BSPs Invloed van wettelijke / regelgevende bepalingen

3.2.1. BSP (f): Wettelijke type digitale ondertekeningen

De ondertekeningen en zegels in dit beleid MOETEN een gekwalificeerde elektronische handtekening en gekwalificeerd elektronisch zegel zijn in overeenstemming met de eIDAS-verordening[3].

De gekwalificeerde elektronische handtekening en gekwalificeerd elektronisch zegel MOETEN worden opgesteld op basis van de XAdES specificatie conform ETSI EN 319 132-1[5].

De gekwalificeerde elektronische handtekening en zegel MOETEN van B-LTA niveau zijn.

3.2.2. BSP (g): Verplichtingen aangegaan door de ondertekenaar

De handtekeningen en zegels beschreven in paragraaf 3.1.1 kennen het generieke commitment type 'Proof of Creation' en/of 'Proof of Origin' zoals beschreven in Annex B van ETSI TS 119 172-1[1].

- De referentie naar de jaarrapportage in de gekwalificeerde elektronische zegel bevat het Commitment type "Proof of Creation" waarmee de geautoriseerde persoon van de rechtspersoon aangeeft dat de jaarrapportage is opgesteld door de rechtspersoon.
- De referentie naar de jaarrekening en/of het bestuursverslag in de gekwalificeerde elektronische handtekening bevat het Commitment type "Proof of Origin" waarmee de commissaris of bestuurder bevestigt de jaarrekening en/of het bestuursverslag te hebben opgesteld, goedgekeurd en afgegeven.

3.2.3. BSP (h): Niveau van zekerheid aangaande tijd

In lijn met paragrafen 3.1.2 en 3.2.1 wordt voor al het bewijs aangaande tijd een gekwalificeerde elektronische tijdstempel die in overeenstemming is met de eIDAS-verordening[3] toegevoegd aan de handtekening of zegel.

De SCA MOET borgen dat alle XAdES B-LTA ondertekeningen, die worden gegenereerd in overeenstemming met dit ondertekeningsbeleid, aan deze eis voldoen.

3.2.4. BSP(i): Formaliteiten van ondertekenen

Om te borgen dat de gevolgen van de implicaties en betekenis van de handtekening en zegel duidelijk gecommuniceerd worden aan de ondertekenaar, moet voldaan worden aan de volgende eisen:

- Voor elke ondertekening MOET met voldoende mate van zekerheid gewaarborgd kunnen worden dat de ondertekenaars begrijpen wat de implicaties zijn van de handeling (i.e. ondertekenen en verzegelen) die zij gaan verrichten.
- Er MOET met voldoende mate van zekerheid gewaarborgd kunnen worden dat de juiste actor tekent bij het desbetreffende tekenmoment.
- Het is AANBEVOLEN dat met voldoende mate van zekerheid bewezen kan worden dat de DTBS van de juiste partij afkomstig is.

3.2.5. BSP(j): Houdbaarheid van handtekeningen en zegels

Alle handtekeningen en zegels geïdentificeerd in paragraaf 3.1.1 hebben een lange levensduur en MOETEN voor een periode van minimaal 10 jaar na ondertekening te verifiëren zijn. Deze periode is gebaseerd op de wettelijke bewaartermijn van administratieve gegevens voor bedrijven.

3.2.6. BSP(k): Archivering

Voor elke handtekening en zegel waarop dit ondertekeningsbeleid van toepassing is, wordt AANBEVOLEN dat deze gearchiveerd worden op een manier die validiteit op lange termijn garandeert. Hier kan gebruik worden gemaakt van archiveringsdiensten zoals beschreven in artikel 34 van de eIDAS-verordening[3].

3.3. BSPs Gerelateerde processen voor de actoren met betrekking tot aanmaken, augmenteren en valideren van ondertekeningen

3.3.1. BSP (l): Identiteit (en rollen/attributen) van de ondertekenaars

De identiteitscontrole MOET door middel van een TSP in overeenstemming met de eIDAS-verordening[3] worden uitgevoerd. Hierbij worden de identiteitsattributen onweerlegbaar vastgelegd in een gekwalificeerd certificaat die onder controle staat van de bijbehorende natuurlijke persoon.

De ondertekenaar die een gekwalificeerde elektronische handtekening zet MOET zijn ingeschreven in het Handelsregister als bestuurder of commissaris van de betreffende rechtspersoon.

3.3.2. BSP (m): Niveau van zekerheid vereist voor de authenticatie van de ondertekenaar

Zoals gespecificeerd in paragraaf 3.2.1 zijn alle handtekeningen en zegels waarop dit beleid van toepassing is gekwalificeerd. Dit houdt in dat de authenticatie van de ondertekenaars plaatsvindt op basis van een gekwalificeerd elektronisch certificaat. Het niveau van zekerheid vereist voor de authenticatie van de ondertekenaar bij de uitgifte van het gekwalificeerd elektronisch certificaat MOET 'hoog' zijn conform artikel 24 in samenhang met artikel 8 van de eIDAS-verordening[3].

3.3.3. BSP (n): Aanmaken van ondertekeningen

Zoals gespecificeerd in 3.2.1 zijn alle handtekeningen en zegels waarop dit beleid van toepassing is gekwalificeerd. Dit houdt in dat alle handtekeningen en zegels MOETEN worden aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en zegels in overeenstemming met de eIDAS-verordening[3].

3.4. Overige BSPs

3.4.1. BSP (o): Overige informatie die met de handtekening of zegel moet worden geassocieerd

Alle handtekeningen en zegels binnen de reikwijdte van dit ondertekeningsbeleid bevatten een verwijzing naar dit ondertekeningsbeleid, gebruikmakend van de in paragraaf 1.3.2 gespecificeerde identifier.

3.4.2. BSP (p): Cryptografische suites

Elke handtekening of zegel gespecificeerd in 3.1.1 wordt verzekerd met een berekende hash op basis van ETSI TS 119 312[9]. Deze robuustheid is afdoende voor een gekwalificeerde elektronische handtekening of zegel.

3.4.3. BSP (q): Technologische omgeving

Niet van toepassing.

4. Verklaringen over het technische proces en implementatie

Voor de handtekeningen en zegels binnen dit ondertekeningsbeleid is een overzichtstabel opgesteld die de business scoping parameters samenvat en aangeeft welke technische vereisten hieruit voortkomen. Alle handtekeningen en zegels in dit beleid zijn gebaseerd op gekwalificeerde elektronische XAdES B-LTA handtekeningen of zegels waarvoor één overzichtstabel is opgesteld.

Naam van autoriteit van ondertekeningsbeleid: domeingovernance SBR domein Handelsregister **Naam en identifier van het ondertekeningsbeleid:** ondertekeningsbeleid van het SBR domein Handelsregister **Identifier van ondertekeningsbeleid:** urn:sbr:handelsregister:pdf:1.0			
BSP	**BSP naam**	**Samenvatting BSP**	**Technische verklaring**
A	Volgorde van de ondertekening(en)	Het ondertekenen van de jaarrekening gebeurt met één handtekening van ieder van de bestuurders en commissarissen. Bestuurders en commissarissen kunnen in parallel tekenen. Het (optioneel) waarmerken van de jaarrapportage middels een zegel is een proces dat naast het ondertekenproces van de jaarrekening uitgevoerd kan worden door een geautoriseerd persoon van de rechtspersoon.	Bij sequentieel ondertekenen wordt de opvolgende elektronische handtekening over de DTBS heen gezet inclusief de reeds aanwezige handtekeningen. Bestuurders en commissarissen kunnen in parallel tekenen, dit hoeft dus niet sequentieel te zijn. Dit houdt in dat zij separaat de jaarrekening kunnen ondertekenen. De handtekening van een bestuurder of commissaris is dan geen onderdeel van de DTBS van de bestuurder of commissaris die daarna tekent.
B	De te ondertekenen data	De signature attributes die de handtekening en interpretatie hiervan ondersteunen.	Conform ETSI EN 319 102-1[10] paragraaf 4.2.6 bestaat de DTBS uit het document van de ondertekenaar of een representatie daarvan, en alle signature attributes, waaronder: ● Referentie naar gekwalificeerd ondertekencertificaat ● Referentie naar dit ondertekeningsbeleid ● Commitment type met betrekking tot de jaarrekening ● Optioneel commitment type met betrekking tot de jaarrapportage ● Tijdstip van ondertekenen ● Locatie van ondertekenen ● Attributen van ondertekenaar ● Attestaties (optioneel)
C	Het verband tussen de ondertekende gegevens en handtekening(en) of zegel(s)	De DTBS wordt ondertekend of verzegeld met een detached ondertekening in het XAdES B-LTA formaat.	De DTBS wordt tijdens het aanmaken van de handtekening of zegel gehasht en versleuteld conform toepasbare norm en standaard zoals beschreven in hoofdstuk 7 van ETSI TS 119 312[9]. De DTBS wordt ondertekend of verzegeld met een XAdES B-LTA ondertekening conform ETSI EN 319 132-1[5].
D	Doelgroep	De doelgroep bestaat uit de bestuurders en commissarissen van de rechtspersoon, de	De betrokken bestuurders en commissarissen ondertekenen de documenten met behulp van hun gekwalificeerde certificaten. In dit

		rechtspersoon, aandeelhouders en andere derde partijen die vertrouwen op de jaarrapportage.	certificaat zijn attributen vastgelegd die gekoppeld zijn aan hun identiteit. Deze attributen zijn vastgesteld met een gekwalificeerd middel en zijn daarom valide gekwalificeerde elektronische handtekeningen.
E	Verantwoordelijkheid voor het valideren en augmenteren van ondertekeningen	De bestuurders en commissarissen stellen vast dat de documenten voldoen aan de eisen uit dit ondertekeningsbeleid alvorens zij de ondertekende documenten verspreiden. Zij verifiëren de handtekening en verstrekken alle benodigde validatiegegevens. Derde partijen die op de documenten vertrouwen, zijn zelf verantwoordelijk voor het augmenteren van de handtekeningen waarbij validiteit op lange termijn geborgd wordt.	Validatie van de ondertekening wordt uitgevoerd door de DA. De SVA controleert de hash en ondertekening en stelt een validatierapport op welke gevalideerd kan worden.
F	Wettelijke type digitale ondertekeningen	De handtekeningen zijn gekwalificeerde elektronische handtekeningen en de zegels zijn gekwalificeerde elektronische zegels in overeenstemming met de eIDAS-verordening[3].	De gekwalificeerde elektronische handtekening en zegel moet worden opgesteld op basis van de XAdES specificatie conform ETSI EN 319 132-1[5].
G	Verplichting aangegaan door de ondertekenaar	De ondertekeningen zijn geassocieerd met het commitment type 'Proof of Origin', wat aangeeft dat de ondertekenaar de DTBS heeft opgesteld, goedgekeurd en afgegeven, of 'Proof of Creation', wat aangeeft dat de ondertekenaar de ondertekende gegevens heeft aangemaakt (maar niet per se akkoord gaat)	Het commitment type wordt vastgelegd door het als attribuut op te nemen in de DTBS conform ETSI EN 319 102-1[10]. Dit gebeurt in de vorm van een identifier die meer informatie bevat over de exacte inhoud van het commitment type. Deze staan beschreven in Annex B van ETSI TS 119 172-1[1].
H	Niveau van zekerheid aangaande tijd	Voor al het bewijs aangaande tijd wordt gebruikgemaakt van een gekwalificeerde elektronische tijdstempel in overeenstemming met de eIDAS-verordening[3].	Voor het zetten van een XAdES ondertekening op B-LTA niveau, worden er verschillende tijdstempels toegevoegd. Niet-gekwalificeerde tijdstempels worden als signed attributes toegevoegd conform ETSI EN 319 102-1[10]. De gekwalificeerde tijdstempel wordt gezet door een qualified TSA over de ondertekening en alle andere data objecten. Dit geeft zekerheid over het tijdstip waarop de ondertekening wordt gezet. De SCA moet borgen dat alle B-LTA ondertekeningen aan deze eis voldoen.
I	Formaliteiten van ondertekenen	Door eisen aan de logica wordt geborgd dat de gevolgen en implicaties van de te zetten ondertekeningen duidelijk zijn voor de ondertekenaar.	De implicaties van het zetten van de ondertekening volgen uit de inhoud van de DTBS. De DA en SCA waarborgen de integriteit hiervan door implementatie van het 'what you see is what you sign' principe

			en passende waarborgen die ervoor zorgen dat de DTBS van juiste partij afkomstig is en dat de juiste partij tekent.
J	Houdbaarheid van digitale ondertekeningen	De ondertekeningen binnen dit ondertekeningsbeleid moeten nog ten minste 10 jaar na ondertekening te verifiëren zijn.	Een tijdstempel inclusief validatiemateriaal wordt gezet door een TSA conform ETSI EN 319 132-1[5], indien de kans aanwezig is dat de cryptografie verloopt binnen 10 jaar na ondertekening wordt er een nieuwe tijdstempel gezet door de TSA over de informatie van de voorgaande tijdstempel inclusief het validatiemateriaal dat aanwezig is.
K	Archivering	Voor de handtekeningen en zegels in dit ondertekeningsbeleid wordt aanbevolen dat deze gearchiveerd worden op een manier die de lange termijn validiteit garandeert.	Implementatie van B-LTA niveau bij handtekeningen van XAdES formaat faciliteert lange termijn archivering, mede door de aanwezigheid van een gekwalificeerde elektronische tijdstempel. Hieruit volgend moeten de handtekeningen en zegels binnen dit ondertekeningsbeleid voldoen aan de eisen aan handtekeningen van B-LTA niveau in de XAdES specificatie conform ETSI EN 319 132-1[5]. Indien de cryptografie van de gezette handtekeningen dreigt te verlopen dient deze te worden geactualiseerd volgens algemeen geldende archiveringsnormen.
L	Identiteit (en rollen/attributen) van de ondertekenaars	De identificatie en vastlegging van de identiteitsattributen worden door middel van een TSP in overeenstemming met de eIDAS-verordening[3] uitgevoerd. De bestuurder of commissaris die tekent, moet als zodanig zijn ingeschreven voor de rechtspersoon in het Handelsregister.	De attributen van de ondertekenaar worden als “signed attributes” toegevoegd aan de inhoud van de handtekening die beschreven zijn in het certificaat van de ondertekenaar (zie BSP(b)).
M	Niveau van zekerheid vereist voor de authenticatie van de ondertekenaar	Authenticatie vindt plaats op basis van een gekwalificeerd elektronisch certificaat dat wordt uitgegeven door een QTSP in overeenstemming met de eIDAS-verordening[3]. Het niveau van zekerheid vereist voor de authenticatie van de ondertekenaar bij de uitgifte van het certificaat is 'hoog' conform artikel 24 in samenhang met artikel 8 van de eIDAS-verordening[3].	Het niveau van authenticatie vereist voor gekwalificeerde elektronische handtekeningen is Sole Controle Assurance Level 2 (SCAL2). Hierbij zijn de sleutels voor het ondertekenen met hoge betrouwbaarheid in het bezit van de ondertekenaar.
N	Aanmaken van ondertekeningen	Ondertekeningen worden aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische ondertekeningen in overeenstemming met de eIDAS-verordening[3].	De SCA moet voldoen aan de eIDAS-verordening[3].

O	Overige informatie die met de handtekening moet worden geassocieerd	Alle handtekeningen en zegels in dit ondertekeningsbeleid bevatten een verwijzing naar dit ondertekeningsbeleid, gebruikmakend van de in paragraaf 1.3.2 gespecificeerde identifier.	Voor alle handtekeningen en zegels geldt dat een verwijzing naar dit ondertekeningsbeleid onderdeel is van de DTBS. Deze dient opgenomen te worden conform 4.2.5.3 van ETSI EN 319 102-1[10].
P	Cryptografische suites	Elke handtekening en zegel wordt verzekerd met een hash volgens de meest recente normen.	Bij het zetten van gekwalificeerde elektronische handtekeningen en zegels moeten passende cryptografische technieken worden gebruikt zoals genoemd in hoofdstuk 7 van ETSI EN 119 312[10].
Q	Technologische omgeving	Niet van toepassing.	Niet van toepassing.

5. Overige zakelijke en juridische zaken

Niet van toepassing.

6. Compliance audit en overige toetsingen

Niet van toepassing.

Bijlage A - Interpretatie sleutelwoorden zoals gedefinieerd in RFC 2119 [Bradner 1997]

RFC 2119	RFC 2119 definitie	NL vertaling	Definitie
MUST	This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.	**MOET**	Deze term betekent dat de beschreven specificatie een absolute vereiste is.
MUST NOT	This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.	**MOET NIET**	Deze term betekent dat de beschreven specificatie een absoluut verbod is.
SHOULD	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.	**AANBEVOLEN**	Deze term betekent dat er in bepaalde omstandigheden geldige redenen kunnen zijn om een bepaald punt te negeren, maar dat de volledige implicaties moeten worden begrepen en zorgvuldig afgewogen alvorens een andere koers te kiezen.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.	**NIET AANBEVOLEN**	Deze term betekent dat er in bepaalde omstandigheden geldige redenen kunnen bestaan waarom het gedrag aanvaardbaar of zelfs nuttig is, maar dat de volledige implicaties ervan moeten worden begrepen en de zaak zorgvuldig moet worden afgewogen alvorens het toe te passen.
MAY	This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.	**MAG**	Deze term of het adjectief "OPTIONEEL" betekent dat een item echt optioneel is. Een implementatie die een bepaalde optie niet opneemt MOET bereid zijn samen te werken met een andere implementatie die de optie wel opneemt, zij het misschien met verminderde functionaliteit. Op dezelfde manier MOET een implementatie die een bepaalde optie wel opneemt, bereid zijn om samen te werken met een andere implementatie die de optie niet opneemt (behalve natuurlijk voor de functie die de optie biedt).

Tabel 7: Interpretatie sleutelwoorden zoals gedefinieerd in RFC 2119 [Bradner 1997]

Bijlage B - Referenties

Verwijzing		Bron
1	ETSI TS 119 172-1	ETSI TS 119 172-1 V1.1.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents https://www.etsi.org/deliver/etsi_ts/119100_119199/11917201/01.01.01_60/ts_11917201v010101p.pdf
2	BW2	Burgerlijk Wetboek 2: Rechtspersonen. https://wetten.overheid.nl/BWBR0003045/
3	eIDAS-verordening	Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG https://eur-lex.europa.eu/eli/reg/2024/1183/oj
4	eIDAS-2.0-verordening	Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit https://eur-lex.europa.eu/eli/reg/2014/910/oj
5	ETSI EN 319 132-1	ETSI EN 319 132-1 V1.3.0 (2024-04) Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.03.00_20/en_31913201v010300a.pdf
6	Algemene Verordening Gegevensbescherming	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming)
7	Besluit vertrouwensdiensten	Besluit van 22 februari 2017, houdende vaststelling van eisen inzake verlening van vertrouwensdiensten, tot intrekking van het Besluit elektronische handtekeningen en tot aanpassing van enige andere besluiten (Besluit vertrouwensdiensten)
8	ETSI TS 119 101	ETSI TS 119 101 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation https://www.etsi.org/deliver/etsi_ts/119100_119199/119101/01.01.01_60/ts_119101v010101p.pdf
9	ETSI TS 119 312	ETSI TS 119 312 V1.4.3 (2023-08) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.03_60/ts_119312v010403p.pdf
10	ETSI EN 319 102-1	ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf