

KvK Assurance

TECHNISCHE TOELICHTING OP HET PROCES

Inhoud

Inleiding.....	2
Gerelateerde documenten	2
NBA-beroepscertificaat	3
Waarvoor is het beroepscertificaat?	3
Hoe vraag ik het aan?	3
<i>Het aanvraagproces</i>	3
Hoe controleer ik het certificaat?	3
XAdES en detached signatures	4
Wat is een detached signature?	4
Wat is XAdES?	4
Hoe werkt het?	4
De subset van de jaarrekening	6
De XPATH-query	6
Samenhang van documenten.....	7
Hoofddocument: Jaarrekening.....	7
<i>Bestandsnaam</i>	7
<i>Inhoud</i>	7
Bijlage: De detached signature.....	7
<i>Bestandsnaam</i>	7
<i>Inhoud</i>	7
Bijlage: De accountantsverklaring	8
<i>Bestandsnaam</i>	8
<i>Inhoud</i>	8
Digipoort validaties	9
Bijlage consistentie validatie	9
XBRL validatie	9
Detached signature validatie.....	9
Handtekening validatie.....	9
Certificaat validatie	10
Validatie door Kamer van Koophandel.....	10

Inleiding

Dit document is een verdere toelichting/verdieping op het KvK Assurance proces, maar bevat niet de technische details zoals besproken in de berichtstroomspecificatie Jaarrekening_AV. Het biedt hiermee een middenweg tussen functionaliteit en de techniek (op hoofdlijnen).

Gerelateerde documenten

- Procesbeschrijving
- Berichtstroomspecificatie Jaarrekening_AV
- Voorbeeldberichten
- Servicebeschrijving AanleverService WUS2.0 voor bedrijven v1.2

NBA-beroepscertificaat

Bij het afgeven van een elektronische accountantsverklaring moet deze met een elektronische handtekening worden ondertekend. Hiervoor is het NBA beroepscertificaat ontwikkeld. Dit certificaat is verplicht voor het afgeven van accountantsverklaringen via SBR.

Waarvoor is het beroepscertificaat?

Het NBA-beroepscertificaat betreft een persoonlijk PKI-overheid certificaat, specifiek voor accountants. Bij de aanvraag wordt in het accountantsregister gecontroleerd of de aanvrager accountant is. Met het beroepscertificaat kan de ontvanger onomstotelijk vaststellen welke persoon ondertekend heeft en dat deze persoon een accountant (RA of AA) is.

Hoe vraag ik het aan?

De beroepscertificaten zijn aan te vragen bij Certificate Service Providers (CSP's). De CSP's zijn verplicht ingeschreven bij de OPTA. De NBA heeft de volgende partijen gemachtigd om beroepscertificaten uit te reiken:

- KPN Corporate Market BV
- ESG de elektronische signatuur BV
- QuoVadis Trustlink BV
- Digidentity BV
- CreAim (dealer van KPN certificaten)

Het aanvraagproces

Het proces voor het aanvragen van een NBA-beroepscertificaat kent een aantal extra stappen naast het standaard certificaataanvraag-proces:

- Een Certificate Service Providers (CSP) controleert of de aanvrager accountant is in het accountantsregister van de NBA.
- Bij afgifte van het certificaat geeft de certificaatverlener dit door aan de NBA. Hierbij wordt het publieke certificaat meegegeven.
- Bij uitschrijving uit het accountantsregister gaat er een melding van de NBA naar de certificaatverlener waarna deze het certificaat intrekt.

Hoe controleer ik het certificaat?

- Een certificaat bevat een geldigheidsdatum. Een certificaat is alleen geldig wanneer het gebruikt wordt binnen de opgegeven begin- en einddatum.
- Een certificaat kan om verschillende redenen ingetrokken worden. Dit wordt gedaan door de certificaatverlener. Deze plaatst het certificaat op zijn Certificate Revocation List. De locatie naar deze lijst is opgegeven in certificaat (*CRL Distribution Points*)
- De beroepscertificaten kunnen alleen uitgegeven worden door bovenstaande CSP's. Certificaten van andere CSP's zijn niet bruikbaar.

XAdES en detached signatures

Wat is een detached signature?

Een detached signature is letterlijk een handtekening welke los wordt bewaard van zijn getekende data. Daar waar in het geval van een enveloping of enveloped signature, de handtekening bij de getekende data wordt bewaard. Er zijn een aantal redenen waarom er is gekozen voor een detached signature:

- Een handtekening wordt bewaard in XML. Deze XML zou anders moeten worden toegevoegd aan een XBRL-instance. Weinig software kan hier mee omgaan.
- Achteraf (na deponeren) moet vastgesteld kunnen worden dat een handtekening is gezet of dat een jaarrekening is gewaarmerkt door een accountant. Door het los bewaren van de handtekening is dit mogelijk. Anders zou de handtekening, wegens eerder genoemde softwarematige beperkingen, verwijderd moeten worden en zo verloren gaan.
- De toepassing van de detached signature dient twee doelen: het ondertekenen van een accountantsverklaring en het waarmerken van een jaarrekening.

Wat is XAdES?

XAdES staat voor XML Advanced Electronic Signature. Het definieert een XML formaat voor het toepassen van geavanceerde en gekwalificeerde elektronische handtekeningen, die voldoen aan de Europese richtlijn betreffende elektronische handtekeningen zoals deze in het Burgerlijk Wetboek is verwerkt en die bovendien geldig kunnen zijn over een lange periode. De XAdES is een aanvulling op XML signatures (XML-DSIG, zoals reeds toegepast binnen Digipoort).

XAdES kent zes verschijningsvormen, waardoor kan worden gekozen voor meer of minder informatie die binnen de handtekening wordt opgenomen. Voor KvK Assurance wordt gebruik gemaakt van het basis niveau van een XAdES handtekening, de zogenaamde –BES/EPES variant.

Hoe werkt het?

Een detached signature wordt als volgt opgebouwd:

1. Neem de verwijzingen van de desbetreffende documenten op.
2. Bereken over deze verwijzingen de hashwaarde. Zo wordt de integriteit van deze informatie gewaarborgd.
3. Bereken vervolgens de hashwaarde van de accountsverklaring en voeg deze toe.
4. Bepaal de subset van de jaarrekening met een XPATH-query. Voeg deze XPATH-query ook toe.
5. Bereken vervolgens van deze subset de hashwaarde en voeg deze toe.
6. Zodra alle hashwaardes berekend zijn dient er een XML signature gezet te worden over alle drie de hashwaardes.

De XML structuur van een detached signature, conform de KvK Assurance eisen, ziet er uit als hieronder weergegeven. De volledige structuur en de exacte technische vulling is vastgelegd in de berichtstroomspecificatie Jaarrekening_AV. Hiervan zijn ook voorbeeldberichten beschikbaar.

```

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ds:SignedInfo>
    <ds:Reference URI="#xmldsig-signedproperties">
      <!-- Hash-waarde onderstaand SignedProperties-element -->
    </ds:Reference>
    <ds:Reference Id="xmldsig-ref0" URI="#financialstatementswithdate.xml">
      <!-- XPath en hash-waarde van de subset van de jaarrekening -->
    </ds:Reference>
    <ds:Reference Id="xmldsig-ref1" URI="#av.xml">
      <!-- hash-waarde van de accountantsverklaring -->
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue><!-- De digitale handtekening--></ds:SignatureValue>
  <ds:KeyInfo>
    <!-- Base64-encoded versie van het (publieke) NBA-beroepscertificaat -->
  </ds:KeyInfo>
  <ds:Object>
    <xades:QualifyingProperties Target="#xmldsig-qualifyingproperties">
      <xades:SignedProperties Id="xmldsig-signedproperties">
        <xades:SignedSignatureProperties>
          <xades:SignaturePolicyIdentifier>
            <!-- Verwijzing naar de volgendende policy:
            Het proces (inclusief waarborgen) waarin
            de XAdES tot stand komt. -->
            <xades:SignaturePolicyId>
              <xades:SigPolicyId>
                <xades:Identifier>xyz</xades:Identifier>
              </xades:SigPolicyId>
              <xades:SigPolicyHash>
                <!-- Hash berekent over de Policy -->
              </xades:SigPolicyHash>
            </xades:SignaturePolicyId>
          </xades:SignaturePolicyIdentifier>
        </xades:SignedSignatureProperties>
        <xades:SignedDataObjectProperties>
          <xades:DataObjectFormat ObjectReference="#xmldsig-ref0">
            <!-- Verwijzing naar de jaarrekening -->
          </xades:DataObjectFormat>
          <xades:DataObjectFormat ObjectReference="#xmldsig-ref1">
            <!-- Verwijzing naar de accountantsverklaring-->
          </xades:DataObjectFormat>
          <xades:CommitmentTypeIndication>
            <!-- Koppeling tussen een policy en de
            referentie behorende bij de jaarrekening -->
            <xades:CommitmentTypeId></xades:CommitmentTypeId>
            <xades:ObjectReference>xmldsig-ref0</xades:ObjectReference>
          </xades:CommitmentTypeIndication>
          <xades:CommitmentTypeIndication>
            <!-- Koppeling tussen een policy en de
            referentie behorende bij de verklaring -->
          </xades:CommitmentTypeIndication>
        </xades:SignedDataObjectProperties>
      </xades:SignedProperties>
    </xades:QualifyingProperties>
  </ds:Object>
</ds:Signature>

```

De subset van de jaarrekening

Voor het realiseren van de subset van de jaarrekening bevat XML-DSIG een transform mechanisme dat dit mogelijk maakt. Dit mechanisme faciliteert de toepassing van XPATH, waarmee delen van een XBRL-instance geselecteerd kunnen worden. Het maakt hier gebruik van pad expressies om te navigeren binnen XBRL-instances. Met een XPATH-query is het dan mogelijk om een subset van een XBRL-instances te bepalen.

De subset kan bestaan uit de jaarrekening zonder de elementen die betrekking hebben op de *DocumentAdoption*, maar ook uit een nog kleinere set. Dit wordt bepaald door de accountant. Voor het bepalen van de beide subsets kan gebruik gemaakt worden van verschillende type XPATH-queries. Beide typen worden benoemd.

De XPATH-query

Wanneer we uitgaan van een jaarrekening waarvan de subset uit alle elementen bestaat, behalve de elementen welke betrekking hebben op de datum van vaststelling, zou deze query er als volgt uit zien:

```
/xbrli:xbrl//*[not(local-name()='DocumentAdoptionStatus' or local-name()='DocumentAdoptionDate' and namespace-uri()='http://www.nltaxonomie.nl/8.0/basis/venj/items/bw2-data')]
```

De bovenstaande query ziet er ingewikkeld uit. Als we de query opbreken in delen wordt het echter een stuk eenvoudiger:

Onderdeel	Uitleg
<code>/xbrli:xbrl</code>	Binnen het root-element XBRL
<code>/*[]</code>	Wil ik alle top-level elementen
<code>not(local-name()='DocumentAdoptionStatus' or local-name()='DocumentAdoptionDate')</code>	Welke niet de naam <i>DocumentAdoptionStatus</i> OF <i>DocumentAdoptionDate</i> dragen
<code>and namespace-uri()='http://www.nltaxonomie.nl/8.0/basis/venj/items/bw2-data')</code>	En van de namespace <i>http://www.nltaxonomie.nl/8.0/basis/venj/items/bw2-data</i> zijn

Voor meer informatie over XPath zie: http://www.w3schools.com/xpath/xpath_functions.asp.

Het zelf testen van XPATH-queries kan met één van de vele online XPATH-evaluators.

Samenhang van documenten

Om de accountantsverklaring en de detached signature mee te kunnen sturen met een jaarrekening, wordt binnen Digipoort gebruikt gemaakt van bijlagen. Aan het aanleveren van de verzameling documenten worden echter wel de nodige eisen gesteld. Deze eisen gelden naast de eisen gesteld in de Servicebeschrijving AanleverService WUS2.0 voor bedrijven v1.2. De technische informatie is terug te vinden in de berichtstroomspecificatie Jaarrekening_AV.

Hoofddocument: Jaarrekening

Een KvK Assurance aanlevering (het aanleverRequest) bevat, naast de nodige metadata, een hoofddocument en een tweetal bijlagen. Dit hoofddocument bestaat altijd de base64-encoded jaarrekening aanwezig in het element `//aanleverRequest/berichtInhoud/inhoud`.

Bestandsnaam

Voor dit document wordt er ook een bestandsnaam meegegeven. Deze bestandsnaam is van belang voor de koppeling met de accountantsverklaring, zoals vastgelegd in de detached signature.

Inhoud

De jaarrekening dient van het type XBRL te zijn. Deze XBRL moet een HREF bevatten welke aangeeft op welke versie van de NT-KvK de instance gebaseerd is. Bij de aanlevering zal gecontroleerd worden of de opgegeven versie te gebruiken is met de versie van de NBA-T welke is gebruikt voor de accountantsverklaring. Deze combinatie is vastgelegd in de berichtstroomspecificatie.

Toevoegen ID's

Mocht het zo zijn dat de accountant bepaald meer dan alleen de *DocumentAdoption* elementen uit te willen sluiten van de subset, dan is het nodig om het attribuut *ID* toe te voegen aan alle elementen van de instance. Dit attribuut kan, in combinatie met een custom XPATH-query, gebruikt worden om een beperktere subset te bepalen. Dit attribuut dient dan volgens de volgende conventie gevuld te worden:

```
<prefix[1]><underscore[1]><elementnaam[1]><zero-based sequentie nummer[0-*]>
```

Bijvoorbeeld: `bw2-i_DocumentAdoptionDate`

Bijlage: De detached signature

Eén van de twee bijlagen is de detached signature, zoals opgesteld conform de eisen gesteld in de Jaarrekening_AV berichtstroomspecificaties. In welke bijlage dit document zit, is niet relevant.

Bestandsnaam

In de detached signature worden verwijzingen naar de accountantsverklaring en de jaarrekening opgenomen. Deze verwijzing gaat op basis van de volgende conventie: `#<bestandsnaam>`.

Deze verwijzingen dienen overeen te komen met de waarden opgenomen in beide

`//aanleverRequest/berichtBijlagen/bijlage/bestandsnaam` elementen. In het aanleverRequest dient echter de # niet voor te komen.

Inhoud

Het document, met daarin de detached signature, moet opgebouwd zijn volgens de XAdES specificatie, een XML-DSIG uitbreiding. Om te controleren of het dit document betreft, wordt gecontroleerd of het document het root-element *Signature* bevat met de correcte namespace (opgenomen in de berichtstroomspecificatie Jaarrekening_AV). Vervolgens wordt de syntax gevalideerd tegen het XAdES schema.

Bijlage: De accountantsverklaring

De andere bijlage bestaat uit de accountantsverklaring. De accountantsverklaring beschrijft wie de verklaring heeft afgegeven en over welke onderdelen de verklaring is afgegeven. Dit laatste wordt in tekst opgenomen in de verklaring zelf.

Bestandsnaam

Zoals benoemd dient de bestandsnaam, opgenomen in de aanlevering, gelijk te zijn aan de verwijzing in de detached signature. Wederom dient de bestandsnaam hier zonder de #, zoals meegenomen in de detached signature, opgenomen te worden.

Inhoud

De accountantsverklaring dient van het type XBRL te zijn. Deze XBRL moet een HREF bevatten welke aangeeft aan welke versie van de NBA-T hij voldoet. Bij de aanlevering zal gecontroleerd worden of de opgegeven versie te gebruiken is met de versie van de NT-KvK welke is gebruikt voor de jaarrekening. Deze combinatie is vastgelegd in de berichtstroomspecificatie Jaarrekening_AV.

Digipoort validaties

Een aanlevering t.b.v. KvK Assurance wordt op verschillende niveaus gevalideerd. We kennen de standaard koppelvakvalidaties, zoals deze gelden voor het WUS2.0 voor bedrijven v1.2 koppelvak. Voor KvK Assurance zijn er echter een aantal validaties toegevoegd. Hieronder een beschrijving van deze extra validaties die plaatsvinden op deze aanleveringen.

Voor alle checks zijn foutcodes gedefinieerd welke teruggegeven worden mocht de fout zich voordoen. Deze zijn terug te vinden in de statussen en foutcodes toelichting voor KvK Assurance.

Bijlage consistentie validatie

Deze validatie controleert allereerst of er daadwerkelijk twee bijlagen aanwezig zijn. Vervolgens zal gecontroleerd worden of de bijlagen ook van het juiste typen zijn; één van het type XBRL en één van het type XML met daarin de juiste root en namespace combinatie. Ten slotte wordt ook gekeken of de bijlage van het type XBRL een entripoint bevat welke gecombineerd mag worden met de entripoint van het hoofddocument. Het kan zijn dat bepaalde versies van de NT-KvK niet gecombineerd mogen worden met bepaalde versies van de NBA-T taxonomie. De toegestane combinaties zijn vastgelegd in de berichtstroomspecificatie voor Jaarrekening_AV.

XBRL validatie

De aangeleverde XBRL instances (de jaarrekening en de accountantsverklaring) worden bij het koppelvak van Digipoort al gecontroleerd op XML validiteit. In het proces worden beide echter nogmaals gevalideerd, dit keer echter tegen de versie van de taxonomie welke hoort bij het opgegeven entripoint. In een taxonomie kunnen linkbases relaties worden opgenomen die de relaties tussen verschillende elementen beschrijven. De aangeboden XBRL documenten worden gevalideerd aan de hand van deze relaties.

Mochten er fouten gevonden worden, dan zal Digipoort aangeven in welke document de fout is gevonden.

Detached signature validatie

Wanneer beide XBRL instances gevalideerd zijn, wordt ook de XML instance, de detached signature, gevalideerd. Hiervoor wordt de instance tegen het XAdES schema aangehouden om zo te kijken of het voldoet aan de gestelde eisen. Het gaat hier dus niet om een inhoudelijke validatie, maar om de validatie van de structuur/syntax van de bijlage.

Handtekening validatie

De digitale handtekening, gezet door de aanleverende partij, wordt al standaard gecontroleerd door het koppelvak Digipoort. Voor KvK Assurance is er echter sprake van nog een digitale handtekening, die van de accountant, aanwezig in de detached signature. Deze wordt echter niet door het koppelvak gecontroleerd, maar zit als een aparte stap in het proces.

Deze validatie stap zal een aantal zaken controleren:

- Is er een certificaat meegegeven in de handtekening?
- Is de handtekening gezet met dit certificaat?
- Is de handtekening correct?
- Zijn de berekende hashwaardes correct?
- Zijn alle verwijzingen in de detached signature correct?

Certificaat validatie

Ten slotte wordt ook gevalideerd of het certificaat, gebruikt voor de digitale handtekening in de detached signature, ook echt valide is. Dit wordt gecontroleerd met behulp van drie checks:

- Betreft het een NBA-beroepscertificaat?
- Is het certificaat niet ingetrokken?
- Is het certificaat nog geldig?

Validatie door Kamer van Koophandel

Na verwerking van uw bericht in Digipoort wordt het bericht ook door de Kamer van Koophandel gevalideerd. Via de contactpagina kunt u meer informatie over deze validaties opvragen. Deze validaties worden niet ondersteund in de Aansluit Suite Digipoort. Zelf valideren kan via de *Aansluit Suite* of via www.nlvalidatie.nl.