Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Toelichting op het SBR ondertekeningsbeleid versie 2.0

Nadere uitleg ten aanzien van het gebruik van elektronische handtekeningen voor het ondertekenen van documenten binnen Standard Business Reporting in Nederland

Documentnaam:	Toelichting op het SBR ondertekeningsbeleid versie 2.0
Status:	Definitief
Datum:	10 oktober 2017

Inhoudsopgave

1 Inleiding

Het SBR ondertekeningsbeleid (in het Engels ook wel de SBR signature policy genoemd) is een in XML-formaat opgestelde normatieve set van regels om elektronische handtekeningen te creëren en te verifiëren. Hiermee wordt de intentie van het zetten van de elektronische handtekening expliciet gemaakt.

Dit document omvat een nadere toelichting op het SBR ondertekeningsbeleid. Het SBR ondertekeningsbeleid duidt de intentie van degene die de elektronische handtekening heeft gezet in de context van Standard Business Reporting in Nederland. Aan dit document kunnen geen rechten worden ontleend.

Het SBR ondertekeningsbeleid definieert de voorwaarden voor het gebruik van een elektronische handtekening in een bepaalde zakelijke context. Deze nadere uitleg gaat nader in op de verschillende technologische, organisatorische en juridische aspecten van het gebruik van elektronische handtekeningen binnen SBR. De regels opgenomen in het SBR ondertekeningsbeleid hebben met name betrekking op de ondertekenende en verifiërende partij en beogen de opstelling, interpretatie en validatie van de elektronische handtekeningen en de hierbij gebruikte PKIoverheid persoonsgebonden certificaten te reguleren.

Het SBR ondertekeningsbeleid vormt een onderdeel van het SBR afsprakenstelsel, zoals vastgesteld in de SBR-governance. Het SBR ondertekeningsbeleid versie 2.0 is door het SBR Beraad bekrachtigd.

1.1 Juridische context

Huidige wetgeving
De Nederlandse wetgever stelt dat een elektronische handtekening dezelfde rechtsgevolgen als een handgeschreven handtekening heeft, indien de methode die daarbij is gebruikt voor authenticatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval[1]. De wetgever geeft een nadere invulling aan wat als voldoende betrouwbaar (gekwalificeerde elektronische handtekening)[2] of onvoldoende betrouwbaar[3] kan worden geacht, maar stelt tevens dat tussen partijen van deze invullingen kan worden afgeweken[4]. Hiermee wordt de ruimte gelaten aan partijen om zelf te bepalen wanneer zij een elektronische handtekening gelijkstellen aan een handgeschreven handtekening[5]. De intentie om dezelfde rechtsgevolgen aan de elektronische handtekening te verbinden als aan de handgeschreven handtekening speelt vooral wanneer de handtekening is bedoeld voor de aanvaarding van verantwoordelijkheid of om het aangaan van een juridische verbintenis te bewijzen.

De techniek voor elektronische handtekeningen maakt het mogelijk om de intentie van het zetten van de elektronische handtekening expliciet zichtbaar te maken. Hierdoor hoeft achteraf geen beoordeling plaats te vinden wat de rechtsgevolgen zijn van een handtekening omdat degene die de elektronische handtekening plaatst al bij voorbaat heeft aangegeven wat zijn intentie hiervan is geweest. De intentie kan bijvoorbeeld zijn om de integriteit en authenticiteit van een document uit te drukken of de wilsuiting van de ondertekenaar aan te geven. Het expliciet maken van de intentie

1 Art. 3:15a lid 1 BW. De MvT Webv geeft aan dat het bestuursrecht aansluit bij deze bepaling. Wel maakt art. 2:16 Awb mogelijk dat bij wettelijk voorschrift aanvullende eisen kunnen worden gesteld.
2 Art. 3:15a lid 2 BW
3 Art. 3:15a lid 3 BW
4 Art. 3:15a lid 6 BW
5 De MvT Wet elektronische handtekeningen geeft dit als volgt weer: "*Het staat partijen vrij om onderling overeen te komen of zij elektronisch ondertekende gegevens zullen aanvaarden en, zo ja, onder welke voorwaarden, in de mate die door het nationale recht wordt toegestaan… uit de partijafspraak, de aard van de transactie, het doel waarvoor de elektronische gegevens werden verzonden of andere omstandigheden van het geval (kan, red.) voortvloeien dat hetgeen elektronisch is verzonden in de gegeven omstandigheden dezelfde rechtsgevolgen heeft als een met de hand ondertekend schriftelijk stuk zou hebben.*" (p. 4)

brengt rechtszekerheid en duidelijkheid met zich mee. De toepassing van een ondertekeningsbeleid speelt een belangrijke rol om de intentie van de verbintenissen te expliciteren.

Europese regelgeving
Sinds 1 juli 2016 is de Europese verordening 910/2014 van kracht. De Europese wetgever stelt in art 25 lid 2 eveneens dat de gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. Daarnaast moeten gekwalificeerde elektronische handtekeningen gebaseerd op een in een lidstaat afgegeven gekwalificeerd certificaat in alle andere lidstaten als gekwalificeerd elektronische handtekening worden erkend.

Uitsluiting
In het SBR ondertekeningsbeleid wordt de term 'elektronische handtekening' gehanteerd. Hieronder wordt verstaan de gekwalificeerde elektronische handtekening die conform art. 3:15a lid 2 BW is opgesteld. Overige elektronische handtekeningen, zoals een gescande handgeschreven handtekening, vallen niet onder de gehanteerde definitie in het SBR ondertekeningsbeleid.

1.2 Doel van het SBR ondertekeningsbeleid

In de praktijk moet de betekenis, of meer specifiek, de precieze intentie van de verantwoordelijkheid die aanvaard wordt door het ondertekenen, vaak worden afgeleid uit de omstandigheden rond de creatie van de handtekening. In veel gevallen wordt dit zo goed begrepen dat de subtiliteiten van de verantwoordelijkheid verkregen door de handeling van het ondertekenen impliciet zijn en zonder verdere analyse afgeleid kunnen worden uit de context. Echter, in enkele gevallen is de intentie niet altijd even duidelijk af te leiden uit de omstandigheden. Dit kan leiden tot problemen omtrent de rechtsgevolgen van een gezette handtekening.
Het doel van het SBR ondertekeningsbeleid is dergelijke situaties te vermijden door de intenties te expliciteren die een ondertekende partij beoogt uit te drukken middels de elektronische handtekening.

1.3 Bron voor het SBR ondertekeningsbeleid

Het SBR ondertekeningsbeleid is opgesteld in XML formaat en is gerealiseerd door het definiëren van de velden uit het schema vermeld in de ETSI TR 102 038 "XML-format for Signature Policies" specificatie. Bij de realisatie van het SBR ondertekeningsbeleid zijn de uitgangspunten van de volgende normen en voorschriften meegenomen:

- ETSI TS 101 733 - Electronic signature formats
- ETSI TR 102 038 - XML-format for Signature Policies
- ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES)
- ETSI TR 102 045 - Signature policy for extended business model
- ETSI TR 102 041 - Signature Policies Report

Aanvullend wordt voldaan aan de minimumvoorschriften voor de grensoverschrijdende verwerking van documenten die door de bevoegde autoriteiten elektronisch zijn ondertekend krachtens Richtlijn 2006/123/EG van het Europees Parlement

2 Algemene informatie

2.1 Uitgangspunten bij het opstellen van het SBR ondertekeningsbeleid

Het SBR ondertekeningsbeleid is opgesteld op basis van de volgende uitgangspunten:

- Een elektronische handtekening moet worden verwerkt door de ondertekenaar en verifiërende partij conform het ondertekeningsbeleid waarnaar wordt verwezen door de ondertekenaar.
- Het ondertekeningsbeleid waarnaar wordt verwezen door de ondertekenaar moet herkend kunnen worden door een identifier.
- Er moet een normatief ondertekeningsbeleid bestaan, bij voorkeur in een gestructureerde vorm vanwege de eenduidigheid.
- De definitieve versie van het normatieve ondertekeningsbeleid moet een unieke binaire codering hebben.

2.2 Identificatie van het SBR ondertekeningsbeleid

Documentnaam:	SBR ondertekeningsbeleid
Versie:	2.0
Object ID:	**urn:sbr:signature-policy:xml:2.0**
Emittent:	SBR programma
Ingangsdatum:	1 november 2017
Einddatum:	-
Beschrijving:	Het SBR ondertekeningsbeleid beschrijft de voorwaarden waaronder elektronische handtekeningen binnen de context van Standard Business Reporting in Nederland worden gebruikt, evenals de voorwaarden wanneer deze handtekeningen als geldig worden beschouwd. In dit kader richt het SBR ondertekeningsbeleid zich op de precieze aard van de verantwoordelijkheid die ondertekenen met zich meebrengt door het expliciteren van de verschillende verplichtingen ('commitments') die elektronische handtekeningen beogen.

2.3 Toepassingsgebied van het SBR ondertekeningsbeleid

Het SBR ondertekeningsbeleid is van toepassing op alle gekwalificeerde elektronische handtekeningen die betrekking hebben op SBR rapportages in Nederland en zijn opgesteld op basis van de XAdES standaard en gezet worden met behulp van een gekwalificeerd persoonsgebonden (beroeps)certificaat vallend onder het stelsel van PKIoverheid.

Het SBR ondertekeningsbeleid is voor onbepaalde tijd geldig en gaat in vanaf de in paragraaf 2.2 vermelde ingangsdatum. De toepasbaarheid van het SBR ondertekeningsbeleid vervalt indien het wordt ingetrokken of een nieuwe versie van kracht wordt.

2.4 Versiebeheer van het SBR ondertekeningsbeleid

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

Versies van de toelichting op het SBR ondertekeningsbeleid worden bewaard op de website van het SBR Programma.

De inhoudelijke wijzigingen ten opzichte van voorgaande versies worden in deze paragraaf uiteengezet:

Versie	Datum	Beschrijving van wijzigingen
1.0	1 juni 2016	Initiële versie
2.0	15 september 2017	- Aanpassing van bestaande typen verplichtingen - Toevoeging van een nieuw type verplichting - Aanpassing in XML bestanden t.b.v. toevoeging van beschrijvingen in het Engels, Frans en Duits.

2.5 Publicatie van het SBR ondertekeningsbeleid

Het normatieve SBR ondertekeningsbeleid is vanwege de eenduidigheid in een gestructureerde vorm opgesteld, te weten in het XML formaat. Deze en het begeleidende XML Schema bestand (XSD) zijn gepubliceerd op www.nltaxonomie.nl/sbr/signature_policy_schema/.

3 Typen verplichtingen ('commitments')

Het SBR ondertekeningsbeleid definieert verschillende typen verplichtingen ('commitments'), waarbij de semantiek van deze verplichtingen op nauwkeurige wijze is beschreven. Door het beschrijven van de verplichtingen kan een ondertekenaar in de elektronische handtekening expliciet verwijzen naar een verplichting. Om dit te realiseren verwijst de ondertekenaar naar de identifier van de verplichting die met de elektronische handtekening wordt beoogd. Bij de aanvaarding van een geverifieerde handtekening impliceert de opname van een expliciete verplichting in de elektronische handtekening dus ook aanvaarding van de semantiek die dit type verplichting met zich meebrengt.
Als een elektronische handtekening is voorzien van een type verplichting die afwijkt van de typen verplichtingen die zijn gedefinieerd in het ondertekeningsbeleid wordt deze verplichting als nietig beschouwd.

Het SBR ondertekeningsbeleid onderkent de volgende typen verplichtingen:

- Ondertekenen verklaring (indien er sprake is van het oorspronkelijke object van onderzoek)
- Ondertekenen verklaring (indien het object waarbij een kopie van de verklaring wordt afgegeven een afgeleide is van het oorspronkelijk object van onderzoek)
- Waarmerken

Deze typen verplichtingen worden in de onderstaande paragrafen nader uiteengezet.

3.1 Ondertekenen verklaring (indien er sprake is van het oorspronkelijk object van onderzoek)

Object ID	**urn:sbr:signature-policy:proof-of-intent-of-practitioner-to-express-an-opinion**
Beschrijving	Dit type verplichting geeft aan dat de ondertekenaar de integriteit, authenticiteit en onweerlegbaarheid van de afgegeven verklaring erkent en in dit kader bevestigt de afgegeven verklaring uit vrije wil te hebben opgesteld en vrijgegeven.
Toepassingsgebied	Dit type verplichting kan worden toegepast op alle situaties in Nederland binnen de reikwijdte van het SBR ondertekeningsbeleid, waar een verklaring in een digitaal formaat wordt afgegeven door de ondertekenaar.
Semantiek	De betekenis van dit type verplichting is dat de ondertekenaar het volgende bevestigt: - een verklaring bij een gerenderd object te hebben afgegeven; - deze verklaring te hebben opgesteld en vrijgegeven; - dit ook nadrukkelijk op deze wijze heeft beoogd te doen om verantwoordelijkheid te nemen voor de gerenderde inhoud van deze verklaring. De rendering, voor de mens leesbaar gemaakt, dient plaats te vinden volgens de voor het domein van toepassing zijnde presentatieafspraken.

3.2 Ondertekenen verklaring (indien het object waarbij een kopie van de verklaring wordt afgegeven een afgeleide is van het oorspronkelijke object van onderzoek)

Object ID	**urn:sbr:signature-policy:proof-of-intent-of-practitioner-to-add-an-copy-of-the-opinion**
Beschrijving	Dit type verplichting geeft aan dat de ondertekenaar heeft bevestigd dat dit een kopie is van de afgegeven verklaring. En in dit kader de integriteit, authenticiteit en onweerlegbaarheid van dit afschrift erkent en deze uit vrije wil te hebben opgesteld en vrijgegeven.
Toepassingsgebied	Dit type verplichting kan worden toegepast op alle situaties in Nederland

	binnen de reikwijdte van het SBR ondertekeningsbeleid, waar een afschrift van een verklaring in een digitaal formaat wordt afgegeven door de ondertekenaar.
Semantiek	De betekenis van dit type verplichting is dat de ondertekenaar het volgende bevestigt: - een kopie van de verklaring bij een gerenderd object van onderzoek te hebben afgegeven; - dit gerenderde object is een afgeleide van het oorspronkelijke object van onderzoek; - deze verklaring te hebben opgesteld en vrijgegeven; - dit ook nadrukkelijk op deze wijze heeft beoogd te doen om verantwoordelijkheid te nemen voor de inhoud van deze verklaring; - dat de gerenderde verklaring ook mag worden bijgevoegd bij een gerenderd object zoals benoemd in de type verplichting voor waarmerken. De rendering, voor de mens leesbaar gemaakt, dient plaats te vinden volgens de voor het domein van toepassing zijnde presentatieafspraken.

3.3 Waarmerken

Object ID	**urn:sbr:signature-policy:proof-of-integrity-of-the-object-for-which-the-practitioner-expresses-an-opinion**
Beschrijving	Dit type verplichting geeft aan dat de ondertekenaar het object waar de verklaring betrekking op heeft waarmerkt om de integriteit van het object te waarborgen.
Toepassingsgebied	Dit type verplichting kan worden toegepast op alle situaties in Nederland binnen de reikwijdte van het SBR ondertekeningsbeleid waar ondertekenaars de integriteit willen of moeten waarborgen van een object waar een door hen afgegeven verklaring betrekking op heeft.
Semantiek	De betekenis van dit type verplichting is dat de ondertekenaar het volgende bevestigt: - dit is het object waarbij de ondertekenaar een verklaring heeft afgegeven zoals benoemd in de type verplichtingen voor het ondertekenen van verklaringen. Door het toepassen van dit type verplichting ontstaat een onweerlegbare relatie tussen het object en de hierbij afgegeven verklaring.

4 Valideren van de elektronische handtekening

Ten behoeve van het valideren van elektronische handtekening definieert het SBR ondertekeningsbeleid de regels die gevolgd moeten worden door zowel de ondertekenaar bij het creëren van de elektronische handtekening en door de verifiërende partij bij de controle van een dergelijke elektronische handtekening. Deze regels hebben betrekking op verschillende verplichtingen ('commitments') die voortvloeien uit het gebruik van de elektronische handtekeningen.

Het SBR ondertekeningsbeleid maakt onderscheid tussen een lijst van voorschriften die van toepassing zijn op alle verschillende typen verplichtingen en een lijst van voorschriften die alleen gelden voor een bepaald type toezegging. In de onderstaande paragrafen worden deze verschillende voorschriften nader uiteengezet.

4.1 Voorschriften voor alle verschillende typen verplichtingen

De volgende voorschriften zijn van toepassing op het creëren en valideren van alle typen toezeggingen op basis van het onderhavige ondertekeningsbeleid:

4.1.1 Voorschriften voor ondertekenaar en verifiërende partij

Door het specificeren van de eisen aan zowel de ondertekenaar als de verifiërende partij worden de verantwoordelijkheden van beide partijen voor het verstrekken van de benodigde informatie duidelijk gedefinieerd.

Ondertekenende partij:
Naast het creëren van een elektronische handtekening dient de ondertekenende partij ook een initiële verificatie uit te voeren van de handtekening en alle validatiegegevens te verstrekken die nodig zijn om daaropvolgend de onweerlegbaarheid van de elektronische handtekening vast te stellen.

Op basis van het SBR ondertekeningsbeleid is de ondertekenende partij verplicht om bij de creatie de volgende gegevens toe te voegen aan de elektronische handtekening (als signed qualifying properties):

- De identifier van het toegepaste ondertekeningsbeleid (SignaturePolicyIdentifier)
- De identifiers van het relevante type toezeggingen (CommitmentTypeIndication)
- Informatie over de externe bestanden waarnaar verwezen wordt (DataObjectFormat)

De ondertekende partij dient de publieke sleutel op te nemen van het certificaat van de eindgebruiker dat gebruikt is voor het ondertekenen.

Verifiërende partij
De mogelijkheid bestaat voor verifiërende partijen om op basis van unsigned qualifying properties, aanvullende kwalificerende eigenschappen op te geven en indien nodig toe te voegen aan de elektronische handtekening. In het SBR ondertekeningsbeleid wordt hiervan geen gebruik gemaakt.

Partijen die de geldigheid van een elektronische handtekening bij een SBR rapportage willen verifiëren kunnen dit doen na het verkrijgen van de relevante documenten. Zij kunnen deze verificatie uitvoeren op basis van de validatie gegevens die onderdeel zijn van de elektronische handtekeningen die daar door de ondertekenaars zijn geplaatst.

4.1.2 Voorwaarden voor het vertrouwen in certificaten

De enige certificaten die geaccepteerd worden voor het creëren van elektronische handtekeningen binnen het SBR ondertekeningsbeleid zijn gekwalificeerde certificaten die onder de persoonlijke controle staan van de betreffende ondertekenaar. Deze gekwalificeerde certificaten zijn X.509 certificaten uit het PKIoverheid (Public Key Infrastructure voor de overheid) stelsel. Het gekwalificeerd certificaat dient te zijn uitgegeven door een PKIoverheid erkende Trust Service Provider (TSP) en minimaal van de tweede generatie te zijn (G2). Het certificaat kent een hoge mate van beveiliging en is maximaal geldig voor een periode van vijf jaar.

Bij het verifiëren van een beroepscertificaat is het van belang dat naast de geldigheidsdatum ook wordt gecontroleerd dat tijdens het ondertekenen het beroepscertificaat niet was ingetrokken. De lijst met ingetrokken certificaten (ook wel: certificate revocation list of CRL genoemd) wordt beschikbaar gesteld door de TSP dat het certificaat heeft verstrekt.

4.1.3 Voorwaarden voor het vertrouwen in tijdstempels ('timestamps')

De huidige versie van het SBR ondertekeningsbeleid maakt geen gebruik van tijdstempels ('timestamps') die worden afgegeven door een externe partij in de rol van Time Stamping Authority (TSA).

4.1.4 Beperkingen op algoritmen

Uitsluitend de volgende algoritmes en bijbehorende minimale sleutellengtes mogen gebruikt worden voor het creëren van elektronische handtekeningen binnen de reikwijdte van het SBR ondertekeningsbeleid.

- http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 / 2048 bits
- http://www.w3.org/2001/04/xmldsig-more#rsa-sha384 / 2048 bits
- http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 / 2048 bits

4.2 Voorschriften die alleen gelden voor een bepaald type verplichting

Er zijn op dit moment geen voorschriften die gelden voor een bepaald type verplichting.