Afsprakenstelsel eHerkenning

Koppelvlakspecificatie DV-HM

Versie 1.7b

INHOUDSOPGAVE

Afsprakenstelsel eHerkenning 1

Koppelvlakspecificatie DV-HM 1

1 Inleiding 6

1.1 Doel en doelgroep van dit document 6

1.2 Intellectuele Eigendom 6

1.3 Leeswijzer 6

1.4 Begrippenlijst 6

1.5 Terminologie 6

1.6 Typografie 7

2 Algemene eisen 8

2.1 Gebruik van SAML 2.0 8

2.1.1 SAML Web Browser SSO Profile 8

2.1.2 Bindings 8

2.1.3 Relay State 9

2.1.4 Namespace aliases 9

2.2 HTTP Headers 9

2.3 Optionele elementen en attributen 9

2.4 Sessies bij deelnemers 9

2.5 Sessies bij dienstverleners 10

2.6 Verzonden formulieren moeten verwijderd worden (zodat opnieuw insturen van hetzelfde formulier vanuit browser leidt tot een foutmelding)Versionering 10

2.7 Taalvoorkeur 10

2.8 Cookies 11

2.9 Character set en encoding 11

3 Technische informatiebeveiligingseisen 12

3.1 Beveiliging verbinding 12

3.2 Signing berichten 12

3.3 Gebruik PKIoverheid gegevens 13

3.4 Synchronisatie systeemklokken 14
4 Foutafhandeling 15
4.1 Annuleren 15
4.2 Foutief opgemaakte berichten 15
4.3 Functioneel ontoereikende berichten 15
5 Berichtenspecificaties 17
5.1 AuthnRequest (1) 17
5.1.1 LogoutRequest 20
5.2 Response (2) 21
5.2.1 Verklaring over authenticatie 22
5.2.2 AttributeStatement 24
5.3 Alternatieve binding 24
5.3.1 HTTP Redirect binding 25
5.3.2 HTTP Artifact binding 25
6 Dienstencatalogus 28
6.1 Formaat 28
6.2 Publicatie 29
7 Attribuutcatalogus 30
7.1 Identificerende kenmerken van dienstafnemers 31
8 Metadata 33
8.1 Formaat metadata 33
8.2 Aanleveren metadata door beheerorganisatie 40
9 Data-elementen 42
9.1 OIN formaat 42
9.1.1 FI-nummer 42
9.1.2 KvK nummer 42
9.1.3 Vestigingsnummer 42
9.1.4 DigiKoppeling registry 42
9.1.5 Buitenlandse registers 43
9.2 Identificerende kenmerken 44
9.2.1 Betrouwbaarheidsniveau 44

9.2.2 ServiceID 44
9.2.3 EntityID 45
9.2.4 Pseudoniemen 45
9.3 SAML Attributen 47
9.3.1 Entity ConcernedID 47
9.3.2 ServiceID 47
9.3.3 AuthorizationRegistryID 48
9.3.4 IntermediateEntityID 48
9.3.5 Representation 49
9.4 URL of POST variabele: EherkenningPreferredLanguage 49
10 Bijlage XML Schema dienstencatalogus 50
11 Bijlage voorbeeld berichten 53
11.1 AuthnRequest 53
11.2 Response 54
12 eHerkenning XML Schema extensions 57
12.1 XML schema metadata extension 57
12.2 XML schema attribute extension 57

COLOFON

Auteur	Status
Beheerorganisatie Afsprakenstelsel eHerkenning	Definitief
Project	**Datum**
Afsprakenstelsel eHerkenning	10 november 2013
Organisatie	**Classificatie**
Logius	Openbaar
Titel van het document	**Versie**
Afsprakenstelsel eHerkenning – Koppelvlakspecificatie DV-HM	1.7a

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
29/03/10	0.8def		Proef-impl.	Projectbureau
06/09/10	1.0	Vorm wijzigingen en doorvoeren verschillende RFCs	Ter goedk.	Projectbureau
17/12/10	1.0a	RFCs verwerkt conform besluit Kernteam 6 december	Definitief	Projectbureau
17/06/11	1.1	RFCs verwerkt conform besluit kernteam 31 mei	Definitief	Projectbureau
12/11/11	1.2	RFCs verwerkt conform besluit kernteam 11 oktober	Definitief	Projectbureau
23/12/11	1.3	RFCs verwerkt conform besluit kernteam 13 december	Definitief	Projectbureau
05/01/12	1.3a	Correcties op RFC102, RFC105 en RFC124 doorgevoerd	Definitief	Projectbureau
28/04/12	1.4	RFCs verwerkt conform besluit kernteam 20 maart	Definitief	Beheerorganisatie
12/07/12	1.5	RFCs verwerkt conform besluit kernteam 26 juni	Definitief	Beheerorganisatie
01/04/13	1.6	RFC0182, RFC0186, RFC0197, RFC0199, RFC0202, RFC0207 verwerkt	Definitief	Beheerorganisatie
24/05/13	1.7	RFC0188, RFC0200, RFC0204, RFC0208, RFC0210, RFC0211, RFC0213, RFC0216 verwerkt	Definitief	Beheerorganisatie
27/08/13	1.7a	RFC0220, RFC0225, RFC0226, RFC0227 verwerkt	Definitief	Beheerorganisatie
10/11/13	1.7b	RFC0245 verwerkt	Definitief	Beheerorganisatie

DISTRIBUTIE

Datum	Distributie	Versie
	Tactisch overleg, Gebruikersraad en publicatie op eherkenning.nl	1.7b

GOEDKEURING

Datum	Naam	Versie
30/10/13	Alle RFCs voor versie 1.7b goedgekeurd door Tactisch overleg	1.7b

1 Inleiding

Dit document maakt deel uit van het afsprakenstelsel eHerkenning. Het kan niet los worden gezien van de andere documenten van het afsprakenstelsel.
Voor een algemene introductie op, en een overzicht van alle documenten binnen eHerkenning wordt de lezer van dit document aangeraden eerst het document [eHerkenning – Algemene introductie] te lezen.
Generieke specificaties betreffende de eHerkenning koppelvlakken (DV-HM, HM-AD en HM-MR) zijn opgenomen in dit document. De koppelvlak specificaties HM-AD en HM MR verwijzen op verschillende plaatsen naar de specificaties in dit document.

1.1 Doel en doelgroep van dit document

Dit document beschrijft het koppelvlak tussen de dienstverlener en de eHerkenningsmakelaar. Het is bedoeld voor iedereen die behoefte aan de meest gedetailleerde technische specificaties.

1.2 Intellectuele Eigendom

eHerkenning stelt de Koppelvlakspecificatie DV-HM onherroepelijk en royalty free voor eenieder beschikbaar. Dit houdt in dat de Koppelvlakspecificatie DV-HM ook buiten het Afsprakenstelsel eHerkenning toepasbaar is en/of hierin wijzigingen kunnen worden aangebracht. Bij het gebruik van het koppelvlak DV-HM buiten het Afsprakenstelsel eHerkenning is het echter niet toegestaan het Merk eHerkenning te gebruiken in verband met de uitvoering en of aanbieding van elektronische (web)diensten.

1.3 Leeswijzer

Het vervolg van dit document ziet er als volgt uit. Hoofdstuk 2 beschrijft de algemene eisen voor het koppelvlak. Hoofdstuk 3 beschrijft de technische informatiebeveiligingseisen. In hoofdstuk 4 wordt de foutafhandeling beschreven. Hoofdstuk 5 bevat de berichtenspecificaties. Hoofdstuk 6 beschrijft de dienstencatalogus en hoofdstuk 8 de metadata. In hoofdstuk 9 wordt een overzicht gegeven van de gebruikte data-elementen. Het document sluit af met enkele bijlagen waar vanuit de tekst naar verwezen wordt.

1.4 Begrippenlijst

Binnen eHerkenning wordt één begrippenlijst gehanteerd. Zie de bijlage in document [eHerkenning – Algemene introductie]. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden. Dat zelfde geldt ook andersom: waar in dit document de zelfstandige-naamwoords-vorm van een werkwoord wordt gehanteerd, heeft deze dezelfde betekenis als het gedefinieerde werkwoord.

1.5 Terminologie

Ter wille van de leesbaarheid van de tekst is overal ‘hij’ geschreven waar ‘hij of zij’ bedoeld wordt.

De woorden “MOET”, “MAG NIET”, “ZOU MOETEN”, “ZOU NIET MOETEN”, en “MAG” in dit document moeten worden geïnterpreteerd gelijk aan hun Engelstalige equivalenten (“MUST", "MUST NOT / SHALL NOT", "SHOULD", "SHOULD NOT" en "MAY") als beschreven in RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt). Waar deze exacte termen bedoeld zijn worden ze in hoofdletters weergegeven. De betekenis van deze woorden is:

- MOET: een absolute vereiste
- MAG NIET: een absoluut verbod
- ZOU MOETEN: sterke wens, tenzij er valide reden is in specifiek geval af te wijken
- ZOU NIET MOETEN: ongewenst, tenzij er valide reden is om het in specifiek geval toe te laten
- MAG: een vrije keuze, een optie

1.6 Typografie

In de meer technische delen van de documentatieset worden de woorden “MOET”, “MAG NIET”, “ZOU MOETEN”, “ZOU NIET MOETEN” en “MAG” altijd in hoofdletters genoteerd.

2 Algemene eisen

Het in dit document beschreven koppelvlak wordt gebruikt voor de implementatie van de use case "Gebruiken eHerkenning als dienstafnemer" en MOET (m.u.v. paragraaf 0 en 5.3) door elke eHerkenningsmakelaar worden geïmplementeerd en worden aangeboden aan haar gebruikers, de dienstverleners[1].

2.1 Gebruik van SAML 2.0

Dit koppelvlak maakt gebruik van SAML 2.0. Een dienstverlener wordt gezien als een service provider. Een eHerkenningsmakelaar wordt gezien als een identity provider.

2.1.1 SAML Web Browser SSO Profile

Voor het in dit document beschreven koppelvlak MOET het SAML Web Browser SSO Profile worden gebruikt. Voor het uitvragen van attributen wordt optioneel gebruik gemaakt van een extensie.

2.1.2 Bindings

Binnen SAML kunnen verschillende bindings worden toegepast om berichten te transporteren tussen partijen.

2.1.2.1 HTTP Post Binding

Voor het in dit document beschreven koppelvlak MOET elke eHerkenningsmakelaar de HTTP POST binding[2] implementeren en aanbieden aan haar klanten, de dienstverleners. Een eHerkenningsmakelaar MAG ook de alternatieve binding implementeren en aanbieden zoals in de vorige paragraaf beschreven.

2.1.2.2 Alternatieve binding

Om dienstverleners tegemoet te komen wordt in dit document ook een alternatieve, optionele binding beschreven. Dit is de binding die gedurende proefimplementaties is gebruikt voor het koppelvlak tussen dienstverlener en eHerkenningsmakelaar. eHerkenningsmakelaars MOGEN deze binding implementeren en aanbieden.

De beschreven alternatieve binding is een combinatie van de HTTP Redirect[3] en HTTP Artifact[4] binding gebruiken, waarbij de vraag wordt gesteld met een HTTP Redirect binding en het antwoord wordt gegeven met een HTTP Artifact binding.

---

1 Dit gaat lock-in tegen en stelt zgn. middleware leveranciers in staat generieke stukken software te bouwen die bij alle eHerkenningsmakelaars te gebruiken zijn.

2 urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
3 urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
4 urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact

De recommendations met betrekking tot het samenstellen van een artifact (paragraaf 3.6.4 van de SAML 2.0 binding specificatie[5]) MOETEN zijn geïmplementeerd.

2.1.3 Relay State

Elk SAML request bericht MAG RelayState data bevatten. De response op een SAML request met RelayState data MOET deze RelayState data ook bevatten. De inhoud van de RelayState MAG NIET groter zijn dan 80 byte en MOET door de partij die de RelayState creëert worden beschermd tegen wijzigingen.

2.1.4 Namespace aliases

Wellicht ten overvloede wordt opgemerkt dat het partijen vrij staat te kiezen welke aliases worden gebruikt voor de afkorting van namespaces in tags.

2.2 HTTP Headers

Voor alle content die naar een browser van een handelende natuurlijk persoon wordt gestuurd MOETEN de volgende HTTP headers worden gebruikt:

- Cache-Control met waarde "no-cache, no-store"
- Pragma met waarde "no-cache"

2.3 Optionele elementen en attributen

Optionele elementen en attributen MOGEN worden opgenomen in berichten. Deze elementen MOETEN dan worden gevuld conform specificaties en MOGEN dus NIET leeg zijn.

2.4 Sessies bij deelnemers

Deelnemers MOGEN ten behoeve van Single Sign-On een sessie bijhouden indien de gebruiker dit heeft aangegeven. In deze sessie MOGEN de volgende gegevens worden bijgehouden:

- een eHerkenningsmakelaar houdt gebruikersvoorkeuren (gekozen authenticatiedienst en gekozen machtigingenregister) bij.
- een authenticatiedienst houdt de identiteit van de handelende natuurlijk persoon bij. Op basis van deze sessie MAG de authenticatiedienst direct een nieuwe verklaring over de authenticatie afgeven aan dienstverleners die een vraag stellen waarbij Single Sign On is gespecificeerd. Daarbij dienen de eisen aangaande maximale levensduur gevolgd te worden.
- een machtigingenregister houdt gebruikersvoorkeuren (gekozen te vertegenwoordige partij) bij.

. De maximale levensduur van een sessie bij de AD bedraagt 2 uur, tenzij tussentijds een nieuwe

5 http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

authenticatieverklaring wordt afgegeven, waarbij de sessie met maximaal 2 uur MAG worden verlengd.
Deelnemers MOGEN een handelende natuurlijk persoon de mogelijkheid geven uit te loggen.
Deze mogelijkheid heeft dezelfde functionaliteit als logout vanuit een dienstverlener (zie § 2.5). Deelnemers moeten evenals dienstverleners zorgen dat na uitloggen of verlopen van een authenticatie sessie cookies verwijderd zijn en dat eerder ontvangen formulieren bij opnieuw insturen tot een foutmelding leiden.
Een eHerkenningsmakelaar MOET gebruikersvoorkeuren bijhouden door gebruik te maken van een separate cookieserver. Deze moet bij de beheerorganisatie worden aangemeld zodanig dat deze via een DNS server het domein .sso.eherkenning.nl verkrijgt. Dit zorgt ervoor dat alle eHerkenningsmakelaars de betreffende cookies kunnen benutten.

2.5 Sessies bij dienstverleners

De dienstverlener die SSO toepast is zelf verantwoordelijk voor het lokaal bijhouden van de sessie.

De dienstverlener MOET tijdens de sessie permanent een uitlogmogelijkheid bieden en tonen.

Een dienstverlener moet logout als volgt implementeren:

- Sessiecookies moeten verwijderd worden en de sessie moet worden vernietigd
- Verzonden formulieren moeten verwijderd worden (zodat opnieuw insturen van hetzelfde formulier vanuit browser leidt tot een foutmelding)
- Vervolgens wordt geredirect naar de eHerkenningsmakelaar en daarbij wordt een logoutbericht verzonden conform 5.1.1 LogoutRequest

2.6 Verzonden formulieren moeten verwijderd worden (zodat opnieuw insturen van hetzelfde formulier vanuit browser leidt tot een foutmelding)Versionering

Omdat verschillende versies van het afsprakenstelsel op koppelvlakniveau van elkaar moeten kunnen worden onderscheiden MOET gebruik gemaakt worden van versionering van de berichten in het geïmplementeerde koppelvlak. Omdat in de SAML 2.0 berichten hiervoor geen veld beschikbaar is en het niet wenselijk is hiervoor een extensie in de berichten te gebruiken MOETEN deelnemers de URL waarop SAML berichten kunnen worden aangeboden in de gepubliceerde metadata koppelen aan een versie van het afsprakenstelsel. Voor twee verschillende versies van het afsprakenstelsel MAG dus NIET dezelfde URL worden gebruikt. Bijv.

http://www.deelnemer.nl/SAML-endpoint/v1.0/

Zie ook hoofdstuk 8.

2.7 Taalvoorkeur

Binnen eHerkenning is het mogelijk om de taal voorkeur van de handelende natuurlijk persoon door te geven zodat de dialoog in deze taal kan worden gevoerd. Omdat in de SAML 2.0 berichten hiervoor geen veld beschikbaar is en het niet wenselijk is hiervoor een extensie in de berichten te gebruiken MAG EherkenningPreferredLanguage als query variabele in de URL of als POST variabele worden meegegeven. Zie ook paragraaf 9.3.3.

2.8 Cookies

Deelnemers hanteren cookies voor verschillende functies. Voor de afspraken over deze functies wordt het SAML 2.0 Web Browser SSO Profile toegepast.
Voor cookies waarin authenticatiedienstselectie wordt vastgelegd wordt het Identity Provider Discovery Profile toegepast en wel als volgt:

- Het common domain is "`*.sso.eherkenning.nl`"
- De naam van de cookie MOET zijn "`_saml_idp`"
- De cookie MOET een pad prefix van "`/`" hebben.
- Het betreft een secure cookie.
- De cookie is persistent.
- De inhoud van de cookie bestaat uit één of meer door een enkele spatie gescheiden Base-64 gecodeerde URI waarden.
- Iedere URI waarde is een uniek identificerend nummer van een authenticatiedienst als gedefinieerd in § 9.2.3 EntityID

Om te zorgen dat de common domain cookies voor alle eHerkenningsmakelaars beschikbaar komen worden ze via de browser van. de handelend natuurlijk persoon verzonden naar een cookieserver behorende bij betreffende eHerkenningsmakelaar maar op het common domain geplaatst. Dit kan op basis van redirects en / of op basis van een script opgenomen in de aan de handelende natuurlijk persoon verzonden HTML pagina.

Indien gebruik gemaakt wordt van een script dan dient dit foutafhandeling te omvatten zodanig dat bij niet reageren van de cookieserver het proces vervolgd wordt alsof er geen cookie waarde gelezen of geschreven hoeft te worden. Indien gebruik gemaakt wordt van redirects of scripts uit staan ZOU de eHerkenningsmakelaar MOETEN detecteren wanneer een verzonden request niet beantwoord wordt en daarna dezelfde vraag opnieuw gesteld wordt. In dat geval moet bij herhaalde vraag een alternatief pad gevolgd worden zonder cookies. Doel hiervan is te voorkomen dat voortgang van het proces belemmerd wordt bij disfunctioneren van de cookies.

2.9 Character set en encoding

Voor alle berichten MOET gebruik worden gemaakt van de Unicode character set in UTF-8 encoding.

3 Technische informatiebeveiligingseisen

Dit hoofdstuk beschrijft de eisen waarmee de maatregelen die in het kader van informatiebeveiliging zijn getroffen worden geïmplementeerd.

3.1 Beveiliging verbinding

Voor alle verbindingen tussen twee systemen gelden de volgende eisen:

- Alle verbindingen MOETEN gebruik maken van SSL 3.0 of TLS.
- In het WS-I basic security profile[6] worden enkele cipher suites afgeraden. Deze MOGEN NIET voor SSL of TLS worden gebruikt.
- Voor SSL of TLS ZOU een deelnemer een PKIoverheid G2 SSL certificaat MOETEN gebruiken. Wanneer geen PKIoverheid G2 SSL certificaat wordt gebruikt MOET een deelnemer een EV SSL certificaat met een sleutellengte van ten minste 2048 bits gebruiken. Het (extended) key usage van het gebruikte certificaat MOET gebruik voor SSL/TLS toestaan.
- Voor SSL of TLS ZOU een dienstverlener een EV SSL certificaat met een sleutellengte van ten minste 2048 bits MOETEN gebruiken. Een dienstverlener MOET een SSL certificaat met een sleutellengte van ten minste 1024 bits gebruiken.

N.B. Het gebruik van andere SSL certificaten dan PKIoverheid G2 certifcaten zal op termijn niet meer worden toegestaan.

3.2 Signing berichten

Om authenticiteit, integriteit en onweerlegbaarheid te garanderen MOET elk bericht dat is beschreven in dit document worden voorzien van een elektronische handtekening van de verzender van het bericht. De ontvanger van een bericht MOET alle elektronische handtekeningen in het bericht valideren alvorens het bericht verder te verwerken.

- De ontvanger MOET controleren dat het bericht ondertekend is met een valide elektronische handtekening, die gezet is over de gehele inhoud van het bericht met de Enveloped Signature Transform[7].
- De ontvanger MAG NIET het bericht verder verwerken als het bericht delen bevat die niet ondertekend zijn met een valide elektronische handtekening.

Voor het genereren van een elektronische handtekening gelden de volgende eisen:

- De elektronische handtekening MOET worden gezet over het hele bericht met de Enveloped Signature Transform[7].

6 http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html

- Canonicalization MOET gebeuren volgens de exclusive c14n methode[8].
- Digests MOETEN worden berekend met het SHA-256 algoritme.
- De SignatureValue MOET worden berekend met het RSA-SHA256 algoritme.
- Voor het ondertekenen van berichten MOET een deelnemer een PKIoverheid G2 certificaat met een sleutellengte van ten minste 2048 bits gebruiken. Het (extended) key usage van het gebruikte certificaat MOET gebruik voor signing toestaan.
- Voor het ondertekenen van berichten MOET een dienstverlener een PKIoverheid G1 certificaat met een sleutellengte van ten minste 1024 bits of een PKIoverheid G2 certificaat met een sleutellengte van ten minste 2048 bits gebruiken.
- De handtekening MAG een keyinfo element bevatten, met daarin een KeyName. De KeyName MOET overeenkomen met een KeyName genoemd in de metadata van de verzender voor de betreffende rol. De handtekening MAG NIET andere keyinfo bevatten (zoals X509Data).

  Als in het bericht geen KeyInfo element wordt opgenomen dan MOET er minimaal een (1) geldig certificaat in de metadata staan waartegen het bericht gevalideerd kan worden. Indien er meer dan 1 certificaat in de metadata staat dan MOET de deelnemer het bericht valideren tegen ieder geldig certificaat. De deelnemer MAG met haar dienstafnemers afspreken om de periode waarin er meer dan een certificaat in de metadata staat te beperken. Op deze wijze kan een hoge belasting van het systeem beperkt worden.

3.3 Gebruik PKIoverheid gegevens

Om goed gebruik te kunnen maken van PKIoverheid MOETEN ontvangers van berichten voldoen aan de eisen voor de ontvangende partij zoals beschreven in het PKIoverheid Programma van Eisen. Hierbij zijn de volgende aspecten van belang:

- Het Stamcertificaat “Staat der Nederlanden Root CA - G2”[9] vertrouwen.
- Alle Domeincertificaten en alle CSP-certificaten[10] kennen en vertrouwen.
- De PKIoverheid CRL[11] met regelmaat raadplegen.

---

7 http://www.w3.org/2000/09/xmldsig#enveloped-signature
8 http://www.w3.org/TR/xml-exc-c14n/

9 Zie http://www.pkioverheid.nl
10 Zie http://www.pkioverheid.nl
11 Zie http://crl.pkioverheid.nl

3.4 Synchronisatie systeemklokken

In het netwerk wordt gewerkt met Coordinated Universal Time, UTC genaamd. Alle tijdsaanduidingen in de berichten worden opgemaakt in de vorm yyyy-mm-ddThh:mm:ssZ. (De T(time) en Z(zulu) zijn vaste waarden).

Elke deelnemer en dienstverlener MOET door middel van synchronisatie met een betrouwbare nauwkeurige tijdbron de afwijking van de systeemtijd minder of gelijk aan 2 seconden laten zijn.

4 Foutafhandeling

Deze paragraaf beschrijft de wijze waarop fouten MOETEN worden afgehandeld in het netwerk, opdat de gebruikers en de deelnemers naar voldoening worden geïnformeerd en bediend. Bij foutafhandeling wordt het principe gehanteerd dat fouten worden afgehandeld daar waar de fout binnen het netwerk optreedt.

4.1 Annuleren

In de normale berichtenflow kan de handelende natuurlijk persoon het proces afbreken door te klikken op de “annuleren” knop. In het hoofdstuk Use Cases worden de scenario's geëxpliciteerd waarbij een eindgebruiker op de “annuleren” knop kan drukken.

Als de gebruiker annuleert MOET de deelnemer de gebruiker automatisch terugsturen naar de verzender, met een geldig SAML bericht, met een StatusCode Value = AuthnFailed. Een verzender MAG een StatusMessage opnemen (bijvoorbeeld “Authentication Cancelled”).

4.2 Foutief opgemaakte berichten

Wanneer een partij een foutief opgemaakt bericht ontvangt dan MOET de deelnemer het proces direct afbreken. Onder een foutief opgemaakt bericht wordt (onder andere) verstaan: ongeldige XML, geen SAML, niet valide handtekening, ongeldige digest en verkeerde versie SAML.

De ontvanger MOET de handelende natuurlijk persoon melden dat een onherstelbare fout is opgetreden.

De ontvangende partij MOET de fout in onderzoek nemen en MOET de verzender op hoogte stellen dat er een fout is opgetreden. De verzender MOET de fout in onderzoek nemen.

4.3 Functioneel ontoereikende berichten

Er kan een vraag aan een deelnemer worden gesteld, die functioneel ongeldig is. Bijvoorbeeld omdat een verkeerde issuer wordt opgevoerd. Wanneer een partij een bericht ontvangt dat functioneel niet volgens specificaties is dan MOET de ontvangende partij het proces afbreken. De ontvangende partij MOET de gebruiker automatisch terugsturen naar de verzender, met een geldig SAML bericht, met een SAML status code Requester, en een firstlevel status code RequestDenied. De ontvanger MOET in de SAML status message aangeven wat het probleem is (bijvoorbeeld “missing or unknow issuer”).

Er kan een vraag aan een deelnemer worden gesteld, waar een deelnemer geen antwoord op heeft. Bijvoorbeeld omdat een betrouwbaarheidsniveau wordt gevraagd waar een AD niet aan kan voldoen. Wanneer een partij een bericht ontvangt dat functioneel niet door de partij kan worden afgehandeld dan MOET de ontvangende partij het proces afbreken. De ontvangende partij MOET de gebruiker automatisch terugsturen naar de verzender, met een geldig SAML bericht, met een SAML status code Responder, en een firstlevel status code RequestUnsupported. De ontvanger MOET in de SAML status message aangeven wat het probleem is (bijvoorbeeld “level not supported”).

Wanneer een partij een bericht ontvangt dat te oud is (issueinstant), of dit bericht niet verwacht op dat moment (onbekend inresponseto) in het proces, dan MOET de ontvangende partij het proces afbreken. De ontvangende partij MOET de gebruiker automatisch terugsturen naar de verzender, met een geldig SAML

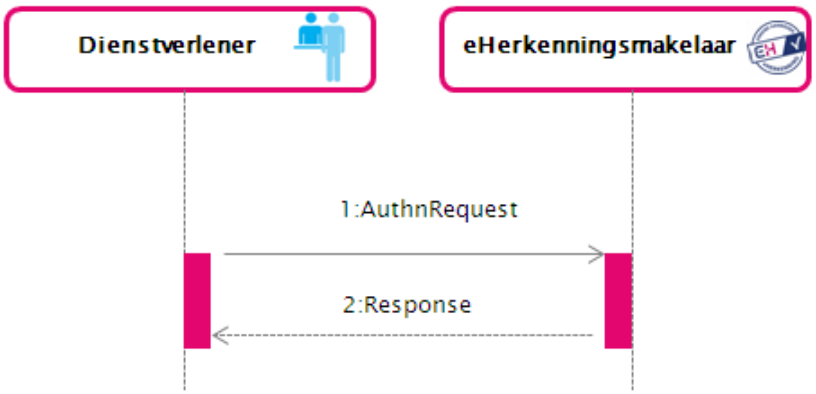
268 bericht, met een SAML status code Responder, en een firstlevel status code RequestDenied. De ontvanger
269 MOET in de SAML status message aangeven wat het probleem is (bijvoorbeeld “message invalid”).

270 De verzender MOET deze fouten in onderzoek nemen. De verzender stelt de gebruiker op de hoogte van de
271 reden van het mislukken. De verzender MAG de gebruiker een alternatief bieden.

5 Berichtenspecificaties

Dit hoofdstuk beschrijft de berichten van het hier beschreven koppelvlak.

De use case “authenticatie handelende dienstafnemer” wordt in het hier beschreven koppelvlak ingevuld met en SAML 2.0 AuthnRequest en Response.



Figuur 1: Sequence diagram DV-HM

De specifieke invulling van deze berichten wordt hieronder beschreven. Detailinformatie over de inhoud van velden kan worden gevonden in hoofdstuk 9.

Wanneer in de beschrijving van een bericht de kolom invulling begint met “SAML:” betekent dit dat dit een standaard invulling is. Als de invulling begint met “eHerkenning:” betekent dit dat het om een eHerkenning specifieke invulling gaat.

5.1 AuthnRequest (1)

Deze paragraaf beschrijft reguliere Authentication Requests.

Data element	Invulling
@ID	SAML: Uniek kenmerk van het bericht
@Version	SAML: Versie van het SAML protocol. De waarde MOET “2.0” zijn.
@IssueInstant	SAML: Tijd waarop het bericht is aangemaakt
@Destination	SAML: URL van de eHerkenningsmakelaar waarop het bericht wordt

Data element	Invulling
	aangeboden. MOET overeenkomen met de metadata van de eHerkenningsmakelaar.
@Consent	eHerkenning: MAG worden opgenomen. Als Consent wordt opgenomen, dan MOET deze de default waarde urn:oasis:names:tc:SAML:2.0:consent:unspecified bevatten.
@ForceAuthn	eHerkenning: Met de waarde “true” wordt gespecificeerd dat een bestaande Single Sign-On sessie voor die betreffende vraag NIET gebruikt MAG worden. Bij waarde “false” of leeg of bij ontbreken van de specificatie MAG de authenticatiedienst gebruik maken van een bestaande SSO sessie indien aanwezig.
@IsPassive	eHerkenning: MAG worden opgenomen. Als IsPassive wordt opgenomen dan MOET de waarde “false” zijn.
@ProtocolBinding	SAML: MAG NIET worden opgenomen indien AssertionConsumerServiceIndex wordt gebruikt. Als deze is opgenomen dan MOET de waarde gelijk zijn aan de urn:oasis:names:tc:SAML:2.0:bindings:http-POST binding.
@AssertionConsumerServiceIndex	eHerkenning: Dit attribuut element geeft aan naar welke url de HM het antwoord voor de DV stuurt. Dit index verwijst naar een url in de dienstverlenermetadata. De HM en DV moeten, voor het gebruik van dit veld, indices met urls specificeren. De waarde van AssertionConsumerServiceIndex MOET overeenkomen met een index van de assertionconsumerservice in de metadata van de dienstverlener. Als de AsserionConsumerServiceIndex en de AssertionConsumerServiceUrl beiden niet zijn opgenomen, dan MOET de makelaar het retourbericht sturen naar het met “isDefault=true” gemarkeerde endpoint in de metadata.
@AssertionConsumerServiceURL	SAML: AssertionConsumerServiceUrl MAG worden opgenomen als er geen AssertionConsumerServiceIndex is opgenomen. Als de AssertionConsumerServiceUrl is opgenomen dan MOET de deelnemer controleren of de AssertionConsumerServiceUrl is opgenomen in de metadata van de dienstverlener.Als deze niet is opgenomen in de metadata dan MOET de deelnemer het bericht weigeren met een statuscode RequestDenied.

Data element	Invulling
@AttributeConsumingServiceIndex	SAML: MAG een index bevatten die overeenkomt met een AttributeConsumingService in de metadata van dienstverlener. Als de AttributeConsumingServiceIndex niet is opgenomen dan MOET de deelnemer de AttributeConsumingService gebruiken die is gemarkeerd met “isDefault=true”. De AttributeConsumingService MOET exact één (1) attribuut bevatten waarvan de naam gelijk is aan een ServiceID in het lange formaat. Zie paragraaf 9.2.2. **Nota bene:** Een applicatie die geen AttributeConsumingServiceIndex kan doorgeven kan nu verschillende diensten en/of attribuut contracten uitvragen door op verschillende EntityID's metadata uit te wisselen. Bestaande applicaties op het 1.5 koppelvlak en eerder kunnen in de metadata voor de verschillende diensten een AttributeConsumingService opnemen waarvan de Index gelijk is aan het korte formaat van de service ID. Deze bestaande systemen blijven zo onverminderd werken.
@ProviderName	eHerkenning: MAG worden opgenomen, maar MOET worden genegeerd door de eHerkenningsmakelaar[12].
Issuer	eHerkenning: MOET de EntityID van de dienstverlener bevatten. Zie paragraaf 9.2.3. De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
Signature	eHerkenning: MOET de elektronische handtekening van de dienstverlener over het hele bericht bevatten. Zie paragraaf 3.2 voor specifieke eisen.
Extensions	eHerkenning: Optioneel element. Indien de verschillende soorten dienstafnemers die toegang kunnen krijgen tot een dienst worden opgenomen in de vraag (dit MOET een

12 De eHerkenningsmakelaar gebruikt ook het element ProviderName, maar vult dit op andere wijze.

Data element	Invulling
	subset zijn van de soorten die in de dienstencatalogus staan), of indien aanvullende attributen worden uitgevraagd (deze MOGEN een superset zijn van wat in de DV metadata is opgenomen) MOET hier één RequestedAttributes element worden opgenomen. In het RequestedAttributes element MOETEN uitsluitend attributen worden opgenomen die zijn opgenomen in de attribuutcatalogus (zie hoofdstuk 7). Deze attributen MOETEN worden opgenomen als Name van een RequestedAttribute. Andere XML attributen MOGEN NIET worden opgenomen. Andere elementen MOGEN NIET worden opgenomen. Een authenticatiedienst MAG vragen om aanvullende attributen negeren, maar MAG NIET het hele bericht weigeren.
Subject	eHerkenning: MAG NIET worden opgenomen
NameIDPolicy	eHerkenning: MAG NIET worden opgenomen.
Conditions	eHerkenning: MAG NIET worden opgenomen.
RequestedAuthnContext	eHerkenning: MOET een attribuut Comparison=”minimum” en een element AuthnContextClassRef met daarin opgenomen het door de dienstverlener vereiste minimale betrouwbaarheidsniveau bevatten. Zie paragraaf 9.2.1.
Scoping	eHerkenning: MAG NIET worden opgenomen

5.1.1 LogoutRequest

Voor Single Logout wordt het Single Logout Profile dat onderdeel is van SAML 2.0 Web Browser SSO Profile toegepast met dien verstande dat rekening gehouden wordt met het doorgeven van het logoutbericht via de eHerkenningsmakelaar naar de authenticatiedienst. Alleen de LogoutRequest van de dienstverlener waar de handelend natuurlijk persoon uitloggen kiest naar de authenticatiedienst wordt ondersteund.

Het koppelvlak voor dit bericht is als onderstaand.

Data element	Invulling
@ID	SAML: Uniek kenmerk van het bericht

Data element	Invulling
@Version	SAML: Versie van het SAML protocol. De waarde MOET “2.0” zijn.
@IssueInstant	SAML: Tijd waarop het bericht is aangemaakt
@Destination	SAML: URL van de eHerkenningsmakelaar waarop het bericht wordt aangeboden.
NameID	eHerkenning: MOET een NameID element bevatten met daarin het specifiek pseudoniem van de handelende natuurlijk persoon. Zie paragraaf 9.2.4.2.
Issuer	eHerkenning: MOET de EntityID van de dienstverlener bevatten. Zie paragraaf 9.2.3.
Signature	eHerkenning: MOET de elektronische handtekening van de dienstverlener over het hele bericht bevatten. Zie paragraaf 3.2 voor specifieke eisen.

5.2 Response (2)

Zie paragraaf 11.2 voor een voorbeeld.

Het identificerende nummer van de vertegenwoordigde dienstafnemer en het specifiek pseudoniem van de uitvoerende natuurlijk persoon worden bij ketenmachtigingen op dezelfde wijze in de verklaring van de HM opgenomen als bij een enkelvoudige machtigingen. De aanvullende informatie over de keten wordt in een apart attribuut opgenomen.

Nota bene: De HM zal niet aanduiden van welke MRs de achterliggende verklaringen afkomstig zijn. Aanvullende attributen hebben betrekking op de vertegenwoordigde dienstafnemer of op de uitvoerende natuurlijk persoon. Er is geen mechanisme ingericht om een aanvullend attribuut dat specifiek op een intermediaire partij betrekking heeft op te nemen.

Data element	Invulling
@ID	SAML: Uniek kenmerk van het bericht.
@InResponseTo	SAML: Uniek kenmerk van het AuthnRequest waarop dit Response bericht het antwoord is.
@Version	SAML: Versie van het SAML protocol. De waarde MOET “2.0” zijn.
@IssueInstant	SAML: Tijd waarop het bericht is aangemaakt.

Data element	Invulling
@Destination	SAML: URL van de dienstverlener waarop het bericht wordt aangeboden. MOET overeenkomen met de metadata van de dienstverlener.
@Consent	eHerkenning: MAG worden opgenomen. Als Consent wordt opgenomen, dan MOET deze de default waarde urn:oasis:names:tc:SAML:2.0:consent:unspecified bevatten.
Issuer	eHerkenning: MOET de EntityID van de eHerkenningsmakelaar bevatten. Zie paragraaf 9.2.3. De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
Signature	eHerkenning: MOET de elektronische handtekening van de eHerkenningsmakelaar over het hele bericht bevatten. Zie paragraaf 3.2 voor specifieke eisen.
Extensions	eHerkenning: MAG NIET worden opgenomen.
Status	eHerkenning: MOET een element StatusCode bevatten met daarin de status van de authenticatie. In geval van annuleren of een fout MOET dit element worden gevuld met de waarde AuthnFailed. Zie ook de beschrijvingen in hoofdstuk 4. StatusDetail MAG NIET worden opgenomen.
Assertion	eHerkenning: MOET een verklaring over de authenticatie met daarin een verklaring over de bevoegdheid bevatten (zie de volgende paragraaf).

303 ### *5.2.1 Verklaring over authenticatie*

Data element		Invulling
Assertion	@Version	SAML: Versie van het SAML protocol. De waarde MOET “2.0” zijn.
	@ID	SAML: Unieke referentie naar de assertion
	@IssueInstant	SAML: Tijd waarop de assertion is aangemaakt
	Issuer	eHerkenning: MOET de EntityID van de eHerkenningsmakelaar bevatten. Zie paragraaf 9.2.3. De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
	Signature	eHerkenning: MAG NIET worden opgenomen

Data element		Invulling
	Subject	eHerkenning: MOET een NameID element bevatten met daarin het specifiek pseudoniem van de handelende natuurlijk persoon. Zie paragraaf 9.2.4.2. Het NameID element MOET een NameQualifier attribuut hebben, dat is gevuld met het EntityID van het machtigingenregister. Een SubjectConfirmation element dat voldoet aan het Web Browser SSO profile MOET zijn opgenomen. Andere SubjectConfirmation of SubjectConfirmationData elementen MOGEN NIET worden opgenomen.
	Conditions	eHerkenning: MOET worden opgenomen. De attributen NotBefore en NotOnOrAfter MOETEN worden gevuld met respectievelijk het tijdstip van uitgifte van de assertion en 120 seconden na de uitgifte van de assertion. Een Audience element in het AudienceRestriction element dat voldoet aan het Web Browser SSO profile MOET zijn opgenomen. Andere Audience elementen MOGEN NIET worden opgenomen. Andere Conditions MOGEN NIET worden opgenomen.
	Advice	eHerkenning: MAG NIET worden opgenomen
	AuthnStatement	eHerkenning: Het attribuut AuthnInstant MOET het tijdstip van authenticatie bevatten. Het AuthnContext element MOET een AuthnContextClassRef element met daarin het betrouwbaarheidsniveau dat is gebruikt* bevatten. Zie paragraaf 9.2.1 respectievelijk paragraaf 9.1. Het AuthenticatingAuthority element MOET zijn gevuld met het EntityID van de authenticatiedienst die de authenticatie heef uitgevoerd. Andere attributen en elementen MOGEN NIET worden opgenomen. * Het betrouwbaarheidsniveau dat is gebruikt MOET het laagste zijn van de betrouwbaarheidsniveaus van de verklaring over de authenticatie van de authenticatiedienst en de verklaring over de bevoegdheid van het machtigingenregister.
	AttributeStatement	eHerkenning: MOET een AttributeStatement conform de volgende

Data element		Invulling
		paragraaf bevatten. Andere AttributeStatement elementen MOGEN NIET worden opgenomen.

304 ### *5.2.2 AttributeStatement*

Data element		Invulling
Onderdeel van verklaring over authenticatie	AttributeStatement	eHerkenning: MOET het attribuut ServiceID (in het lange formaat) bevatten en bevat precies één EntityConcernedID dat de dienstafnemer identificeert (bevat een name die het type identificerend nummer identificeert, zie paragraaf 9.3.1) MAG het attribuut IntermediateEntityID (bevat een name die het type identificerend nummer specificeert, zie ook paragraaf 9.3.4) bevatten. Indien het EntityConcernedID een KvK-nummer bevat dan MAG tevens een tweede EntityConcernedID gevuld met het vestigingsnummer (zie 9.3.1) worden opgenomen. Indien een EntityConcernedID met het Vestigingsnummer is opgenomen MOET er ook een EntityConcernedID worden opgenomen met het subdossiernummer[13]. Wanneer aanvullende attributen door de dienstverlener zijn gevraagd en deze attributen door authenticatiedienst en/of machtigingenregister als EncryptedAttribute zijn geleverd dan MOETEN deze hier worden opgenomen. Andere attributen MOGEN NIET worden opgenomen.

305 ## *5.3 Alternatieve binding*

306 Wanneer de beschreven berichten over de in paragraaf 2.1.2.2 beschreven alternatieve binding worden
307 uitgewisseld gelden de volgende eisen.

[13] Alleen **tot 1 april 2014**. Na 1 april 2014 vervalt de verplichting om het subdossiernummer op te nemen in berichten.

5.3.1 HTTP Redirect binding

Voor de implementatie voor de HTTP Redirect binding gelden de volgende eisen:

- Het AuthnRequest bericht is gelijk aan het bericht beschreven in paragraaf 5.1, maar MAG NIET een <ds:Signature> element bevatten.
- Het bericht MOET worden gecomprimeerd met de DEFLATE methode waarna Base64 encoding MOET worden toegepast.
- Het gecomprimeerde en gecodeerde bericht MOET aan het URL toegevoegd worden als een query string parameter en MOET worden aangeduid als SAMLRequest.
- Als RelayState data wordt meegegeven in het HTTP Redirect bericht moet deze apart geencodeerd aan de URL toegevoegd worden als een query string parameter en MOET deze worden aangeduid als RelaySate. Als er geen RelayState wordt meegegeven MOET de hele parameter ontbreken in de URL.
- Over het deel van de URL SAMLRequest=value&RelayState=value MOET een elektronische handtekening worden berekend. Deze elektronische handtekening MOET gegenereerd worden zoals beschreven in paragraaf 3.2. De elektronische handtekening MOET worden opgenomen als een query string parameter. Deze parameter wordt aangeduid als Signature.

5.3.2 HTTP Artifact binding

Voor de implementatie van de HTTP Artifact binding worden alleen eisen gesteld aan de ArtifactResolve en ArtifactResponse berichten.

5.3.2.1 ArtifactResolve

Data element	Invulling
@ID	SAML: Uniek kenmerk van het bericht
@Version	SAML: Versie van het SAML protocol. De waarde MOET “2.0” zijn.
@IssueInstant	SAML: Tijd waarop het bericht is aangemaakt
@Destination	eHerkenning: MAG NIET worden opgenomen
@Consent	eHerkenning: MAG worden opgenomen. Als Consent wordt opgenomen, dan MOET deze de default waarde urn:oasis:names:tc:SAML:2.0:consent:unspecified bevatten.
Issuer	eHerkenning: MOET de EntityID van de dienstverlener bevatten. Zie paragraaf 9.2.3. De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
Signature	eHerkenning: MOET de elektronische handtekening van de dienstverlener over het

Data element	Invulling
	hele bericht bevatten. Zie paragraaf 3.2 voor specifieke eisen.
Extensions	eHerkenning: MAG NIET worden opgenomen
Artifact	SAML: Bevat het Artifact dat als query parameter is ontvangen.

327 *5.3.2.2 ArtifactResponse*

Data element	Invulling
@ID	SAML: Uniek kenmerk van het bericht.
@InResponseTo	SAML: Uniek kenmerk van het AuthnRequest waarop dit Response bericht het antwoord is.
@Version	SAML: Versie van het SAML protocol. De waarde MOET “2.0” zijn.
@IssueInstant	SAML: Tijd waarop het bericht is aangemaakt.
@Destination	eHerkenning: MAG NIET worden opgenomen
@Consent	eHerkenning: MAG worden opgenomen. Als Consent wordt opgenomen, dan MOET deze de default waarde urn:oasis:names:tc:SAML:2.0:consent:unspecified bevatten.
Issuer	eHerkenning: MOET de EntityID van de eHerkenningsmakelaar bevatten. Zie paragraaf 9.2.3. De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
Signature	eHerkenning: MOET de elektronische handtekening van de eHerkenningsmakelaar over het hele bericht bevatten. Zie paragraaf 3.2 voor specifieke eisen.
Extensions	eHerkenning: MAG NIET worden opgenomen
Status	eHerkenning: MOET een element StatusCode bevatten met daarin de status van de authenticatie. In geval van annuleren of een fout MOET dit element worden gevuld met de waarde AuthnFailed. Zie ook de beschrijvingen in hoofdstuk 4. StatusDetail MAG NIET worden opgenomen.
any ##any	eHerkenning: MOET een Response bericht bevatten (zie paragraaf 5.1.1). Dit

Data element	Invulling
	bericht MAG NIET een <ds:Signature> element bevatten.

6 Dienstencatalogus

In dit hoofdstuk wordt het formaat en de publicatie van de dienstencatalogus beschreven.

6.1 Formaat

De dienstencatalogus MOET voldoen aan het volgende formaat:

- IssueInstant (Tijdstip waarop de dienstencatalogus is aangemaakt)
- NotOnOrAfter (Tijdstip waarop de dienstencatalogus niet meer geldig is)
- Version (Versie van de dienstencatalogus in het formaat nl:eherkenning:<versie afsprakenstelsel>:<volgnummer dienstencatalogus>. Bijv. nl:eherkenning:0.8def:1)
- Signature (Ondertekening door beheerorganisatie, eHerkenningsmakelaar of dienstverlener, ten behoeve van authenticiteit, integriteit en onweerlegbaarheid).
- Per dienstverlener:
  - IsPublic (attribuut dat aangeeft of de dienstverlener eHerkenning publiekelijk in gebruik heeft)
  - ServiceProviderID (Het OIN van de dienstverlener)
  - OrganizationDisplayName (De naam van de dienstverlener zoals deze door deelnemers MOET worden afgebeeld, max 64 tekens). Dit element MAG voor verschillende talen worden opgenomen.
  - Per dienst:
    - IsPublic (attribuut dat aangeeft of de dienst eHerkenning publiekelijk in gebruik heeft)
    - ServiceID (Een door de dienstverlener toegekend en aangeleverd uniek nummer van 1 tot 64000 in het formaat urn:nl:eherkenning:DV:<OIN>:services:<uniek service nummer>
    - ServiceName (Naam van de dienst, bepaald door de dienstverlener, max 64 tekens) Dit element MAG voor verschillende talen worden opgenomen.
    - ServiceDescription (Korte omschrijving van dienst, max 1024 tekens, bepaald door dienstverlener. Machtigingenregisters MOGEN deze tekst gebruiken om beheerders te helpen bij het vastleggen van bevoegdheden). Dit element MAG voor verschillende talen worden opgenomen.
    - ServiceDescriptionURL (Een url van max. 512 tekens waar een uitgebreide omschrijving van dienst is te vinden, bepaald door dienstverlener. Machtigingenregisters MOGEN deze link opnemen om beheerders te helpen bij het vastleggen van machtigingen).Dit element MAG voor verschillende talen worden opgenomen.
    - AuthnContextClassRef (Betrouwbaarheidsniveau dat vereist is voor de dienst, bepaald door dienstverlener)
    - HerkenningsmakelaarId (Het OIN van de Herkenningsmakelaar die de dienstcatalogus entry van deze dienst aanlevert)
    - AdditionalHerkenningsmakelaarId (multivalue entry met de OIN's van overige Herkenningsmakelaars die deze dienst leveren)

- EntityConcernedTypesAllowed (optionele multivalue entry met de verschillende soorten dienstafnemers die toegang kunnen krijgen tot de dienst)
- ServiceCertificate: PKI certificaat van dienstverlener met daarin de publieke sleutel die gebruikt kan worden om opgevraagde attributen te versleutelen.

Het formaat van de dienstencatalogus is de vorm van een XML Schema opgenomen in hoofdstuk 10.

6.2 Publicatie

De beheerorganisatie publiceert de dienstencatalogus op een vaste locatie. De dienstencatalogus wordt voorafgaand aan publicatie gesorteerd op respectievelijk HerkenningsmakelaarId en ServiceId.

Een deelnemer MOET periodiek op een vooraf door de beheerorganisatie gekozen tijdstip, de dienstencatalogus verwerken. Gegevens over de URL en de periodiciteit staan beschreven in [Operationeel handboek].

Een deelnemer ZOU de metadata MOETEN verwerken met een automatisch proces. Een deelnemer MOET in verband met rollback, of andere wijzigingen, dit automatische proces ook op tussentijdse momenten kunnen uitvoeren.

7 Attribuutcatalogus

Dit hoofdstuk definieert de in eHerkenning maximaal beschikbare aanvullende attributen die kunnen worden opgevraagd. Het betreft hier uitsluitend ongevalideerde attributen. Het leveren van deze attributen is niet verplicht.

Per attribuut wordt een naam en formaat gespecificeerd. Ook wordt aangegeven of het attribuut door een authenticatiedienst of machtigingenregister kan worden geleverd.

Alle attribuut strings zijn opgemaakt in de Unicode character set in UTF-8, net zoals de rest van het bericht. Het RequestedAttributes heeft de namespace:

“urn:nl:eherkenning:1.3a:attributeextension:RequestedAttributes”. Geleverde attributen hebben een attributenaam die begint met "urn:nl:eherkenning:1.3:AdditionalAttribute".

Voor de leesbaarheid is dat niet opgenomen in onderstaande tabel.
(zie eHerkenning XML schema extensions, hoofdstuk 12).

Attribuutnaam	Format	Omschrijving	AD/MR
BusinessAddress	String max 256	Adres van de handelende natuurlijk persoon, in de context van de gebruikte bevoegdheid	MR
BusinessEmail	String max 256	E-Mailadres van de handelende natuurlijk persoon, in de context van de gebruikte bevoegdheid	MR
BusinessPhone	String max 128	Telefoonnummer van de handelende natuurlijk persoon, in de context van de gebruikte bevoegdheid	MR
ActingPersonName	String max 128	Naam van de handelende natuurlijk persoon	AD
PersonalEmail	String max 256	E-Mailadres van de handelende natuurlijk persoon, geregistreerd bij middelenuitgifte (zou dus privé kunnen zijn)	AD
PersonalPhone	String max 128	Telefoonnummer van de handelende natuurlijk persoon, geregistreerd bij middelenuitgifte (zou dus privé kunnen zijn)	AD
BusinessName	String max 128	Naam van het handelde bedrijf.	MR

Userdefined	String max 256	Een gebruikersgedefinieerd attribuut is een tekstveld dat bij de registratie door degene die opgave doet wordt vastgelegd.	MR
BusinessAddressCity	String max 128	Plaatsnaam van de handelende natuurlijk persoon, in de context van de bevoegdheid.	MR
BusinessAddressPostalCode	String max 128	Postcode van de handelende natuurlijk persoon, in de context van de bevoegdheid.	MR
BusinessAddressHouseNumber	String max 128	Huisnummer van de handelende natuurlijk persoon, in de context van de bevoegdheid.	MR

De attributen BusinessAddressCity, BusinessAddressPostalCode en BusinessAddressHouseNumber worden naast het attribuut BusinessAddress redundant toegestaan.

De attributen in bovenstaande tabel mogen voor handelende natuurlijk personen waarvan de bevoegdheid beperkt is tot een bepaalde vestiging eveneens per vestiging worden vastgelegd.

7.1 Identificerende kenmerken van dienstafnemers

Een speciaal categorie attributen, die verder ook aan bovenstaande eisen voldoen, zijn de identificerende kenmerken van de verschillende soorten dienstafnemers of intermediairs.
Geleverde identificerende kenmerken van dienstafnemers hebben een attribuutnaam die begint met "urn:nl:eherkenning:1.7:EntityConcernedID:".
Geleverde identificerende kenmerken van intermediairs hebben een attribuutnaam die begint met "urn:nl:eherkenning:1.7:IntermediateEntityID:".
De volgende typen identificerende kenmerken van dienstafnemers en intermediairs worden onderscheiden:

Naam	Omschrijving	Waarde	Toegestaan voor ketenmachtiging?
Pseudo	Een specifiek pseudoniem dat wordt gebruikt om een burger/consument te identificeren.	Zie paragraaf 9.2.4.2	Nee
KvKnr	Het KvKnummer van de vertegenwoordigde dienstafnemer/intermediair of vergelijkbaar nummer	OIN van het KvKnummer, het FI-nummer, de Digikoppeling registry of nummer uit buitenlands register. Zie paragraaf 9.1 en verder	Ja

Vestigings nr	Het vestigingsnummer van de vertegenwoordigde dienstafnemer	OIN van het vestigingsnummer. Zie paragraaf 9.1.3	Nee voor intermediair, Ja voor dienstafnemer
RSIN	Het RSIN van de vertegenwoordigde dienstafnemer/intermediair	OIN van het RSIN	Ja
Subdossier Nr[14]	Het subdossiernummer van de vertegenwoordigde dienstafnemer	Het OIN van het subdossiernummer	Nee voor intermediair, Ja voor dienstafnemer

Indien 'Toegestaan voor ketenmachtiging?' de optie 'Nee' bevat, dan mag dit type identificerend kenmerk niet worden gebruikt voor dienstafnemers of intermediairs in een keten van machtigingen
Op verzoek van deelnemers en/of hun klanten kunnen speciale identificerende kenmerken van beroepsbeoefenaren als type dienstafnemer en/of intermediair worden opgenomen. Dergelijke identificerende kenmerken mogen alleen door deelnemers worden verstrekt als aan alle voor het betreffende kenmerk beschreven criteria (nader uit te werken door beheerorganisatie) wordt voldaan.
Voor het toevoegen en/of wijzigen van identificerende kenmerken zal de beheerorganisatie een proces inrichten buiten het huidige wijzigingsproces om.

[14] Uitsluitend te gebruiken op koppelvlak HM-MR, tot 1 april 2014. MAG NIET gebruikt worden op koppelvlak DV-HM.

8 Metadata

In het eHerkenning netwerk is het gebruik van SAML metadata tussen deelnemers verplicht voor het beschrijven van de URLs en certificaten die worden gebruikt op de verschillende koppelvlakken. Het uitwisselproces is iteratief: Deelnemers leveren metadata van hun eigen SAML systeem aan. De beheerorganisatie controleert deze metadata, en aggregeert de metadata van de verschillende deelnemers, en verspreidt de geaggregeerde metadata onder de deelnemers. In dit hoofdstuk wordt beschreven welke metadata door deelnemers moet worden aangeleverd, hoe de beheerorganisatie de geaggregeerde metadata publiceert, en hoe de deelnemers die moeten interpreteren.

Tussen dienstverleners en eHerkenningsmakelaars is het niet verplicht gebruik te maken van SAML metadata. Wanneer wel gebruik wordt gemaakt van SAML metadata kan gebruik gemaakt worden van het in dit hoofdstuk beschreven niet normatieve formaat.

8.1 Formaat metadata

Een deelnemer in de rol van eHerkenningsmakelaar, authenticatiedienst, of machtigingenregister MOET metadata aanleveren aan de beheerorganisatie, over een systeem dat de rol van de deelnemer in het netwerk implementeert. In dat geval gelden de volgende regels:

Een deelnemer MAG GEEN metadata aanleveren voor een rol of functionaliteit waarvoor zij (nog) niet is toegetreden[15]. Een deelnemer die meerdere rollen speelt in het netwerk MOET voor ieder rol afzonderlijk metadata aanleveren.

De deelnemer MOET metadata aan de beheerorganisatie aanleveren als valide SAML bestand, volgens urn:oasis:names:tc:SAML:2.0:metadata met daarin één ondertekend EntitiesDescriptor element. De ondertekening MOET worden uitgevoerd conform hetgeen is beschreven in hoofdstuk 3.

Het element EntityDescriptor bevat één of meer EntityDescriptor elementen.

Elk EntityDescriptor element MOET het entityID en een aanvullend version attribuut bevatten en MAG GEEN andere SAML attributen bevatten. Het entityID MOET de vorm urn:nl:eherkenning:ROL:OIN:INDEX hebben, waarbij ROL één van DV, HM, AD, of MR is afhankelijk van de rol, OIN het OIN is van de dienstverlener of deelnemer, en INDEX een zelfgekozen index is van vier cijfers. Het version attribuut wordt gedefinieerd in de bijlage, zie paragraaf 12.1en bevat de versie van de koppelvlakspecificaties waarop de entity communiceert.Voorbeeld:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor
```

15 Deze eis geldt voor metadata voor het productienetwerk. Voor metadata voor het acceptatienetwerk geldt deze eis niet omdat daar ook systemen moeten kunnen getest van partijen die nog niet zijn toegetreden.

```
ID="[reference for dsig]"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="urn:nl:eherkenning:HM:99999900000010000:0001" >
   <ds:Signature>...</ds:Signature>
...
</md:EntityDescriptor>
```

In de EntityDescriptor MOETEN één of meerdere elementen van het type ContactPerson opgenomen waarin naam, emailadres, en telefoonnummer staan beschreven van personen met wie, in geval van problemen, contact kan worden opgenomen door deelnemers of de beheerorganisatie.

In de metadata MOETEN gegevens opgenomen worden over de eigen organisatie, door het opnemen van één element van het type Organization, waarin naam (OrganizationName), de leesbare naam voor gebruikers (OrganizationDisplayName), en website (OrganizationURL) staan beschreven.

Één rol MAG met meerdere systemen worden vervult. Voor ieder systeem afzonderlijk wordt dan metadata aangeleverd. De metadata MOET dan een verschillend EntityID's bevatten, waar het element Organization hetzelfde is.

Wanneer een systeem berichten gebaseerd op verschillende versies van het afsprakenstelsel kan versturen dan MOET voor elke versie afzonderlijk metadata worden aangeleverd. Dus als een entity op meerdere versies van het koppelvlak kan communiceren (bijv. op eh:version=1.5 en eh:version=1.7) dan worden beiden binnen de EntitiesDescriptor als aparte EntityDescriptor opgenomen.

Deze EntityDescriptors MOGEN dezelfde EntityID's hebben of verschillende EntityID's.Een herkenningsmakelaar MOET voor de verschillende logische systemen, die elk verschillende versies van de eHerkenning koppelvlakken ondersteunen, aparte EntityDescriptor elementen opnemen in de metadata. Dus een herkenningsmakelaar die op meerdere versies van het koppelvlak kan communiceren (bijv. op eh:version=1.5 en eh:version=1.7) neemt binnen de EntitiesDescriptor beide versies als aparte EntityDescriptor op in de metadata. Deze EntityDescriptors MOGEN dezelfde EntityID's hebben of verschillende EntityID's.

Een AD/MR MOET de waardes van eh:version in de metadata gebruiken om te bepalen welke EntityDescriptor gebruikt moet worden voor communicatie met een herkenningsmakelaar. EntityDescriptors met een versienummer dat anders is dan de versie van de AD/MR ZOUDEN genegeerd MOETEN worden door de AD/MR.Een authenticatiedienst heeft op een moment in de tijd maar één geldige EntityDescriptor. Om overgang naar een nieuwe versie te faciliteren MAG een authenticatiedienst precies twee verschillende EntityDescriptor elementen opvoeren. Eén EntityDescriptor element MOET dan het SAML attribuut validUntil bevatten. Het andere EntityDescriptor element MOET dan het eHerkenning validFrom attribuut bevatten (zie bijlage, paragraaf 12.1). De dateTime waarde van beide velden MOET gelijk zijn. Deze twee EntityDescriptors MOGEN dezelfde EntityID's hebben of verschillende EntityID's.

Een HM MOET de waardes ValidFrom en ValidUntil in de metadata gebruiken indien aanwezig om te bepalen welke EntityDescriptor geldig is voor communicatie met een authenticatiedienst.Een machtigingenregister heeft op een moment in de tijd maar één geldige EntityDescriptor. Om overgang naar een nieuwe versie te faciliteren MAG een machtigingenregister precies twee verschillende EntityDescriptor elementen opvoeren. Eén EntityDescriptor element MOET dan het SAML attribuut validUntil bevatten. Het andere EntityDescriptor element MOET dan het eHerkenning validFrom attribuut bevatten (zie bijlage, paragraaf 12.1). De dateTime waarde van beide velden MOET gelijk zijn.

Deze twee EntityDescriptors MOGEN dezelfde EntityID's hebben of verschillende EntityID's.

Een HM MOET de waardes ValidFrom en ValidUntil in de metadata gebruiken indien aanwezig om te bepalen welke EntityDescriptor geldig is voor communicatie met een machtigingenregister.Een authenticatiedienst of machtigingenregister MOET in de EntityDescriptor het betrouwbaarheidsniveau opnemen waarop herkenningsvragen kunnen worden afgehandeld, middels een extensie van EntityDescriptor element, zoals beschreven in het document SAML V2.0 Identity Assurance Profiles.

Voorbeeld:

```
...
<md:Extensions>
      <attr:EntityAttributes>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
Name="urn:oasis:names:tc:SAML:attribute:assurancecertification">
            <saml:AttributeValue>
 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
            </saml:AttributeValue>
         </saml:Attribute>
      </attr:EntityAttributes>
   </md:Extensions>
...
```

Verschillende EntityDescriptor elementen MOETEN altijd gevat zijn in een EntitiesDescriptor element.

Voorbeeld:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor
   ID="[reference for dsig]"
   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
   xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:Signature>...</ds:Signature>

      <md:EntityDescriptor
         entityID="urn:nl:eherkenning:AD:9999990000010000:0001"
         eh:version="1.1a" validUntil="2011-03-15T00:00:00Z">
```

```
        ...
    </md:EntityDescriptor>

    <md:EntityDescriptor
        entityID="urn:nl:eherkenning:AD:9999990000010000:0001"
        eh:version="1.3" eh:validFrom="2011-03-15T00:00:00Z">
        ...
    </md:EntityDescriptor>

</md:EntitiesDescriptor>
```

Een eHerkenningsmakelaar neemt één IDPSSODescriptor element op met daarin één SingleSignOnService element en geen andere elementen.

Voorbeeld:

```
...
<md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://...."/>
</md:IDPSSODescriptor>

...
```

Een dienstverlener MOET één SPSSODescriptor opnemen.
Deze minimaal één (1) AssertionConsumingService bevatten. Als er meerdere AssertionConsumingService entries worden opgenomen dan MOET één (1) van deze entries gemarkeerd zijn als de default door middel van de indicatie “isDefault=true”
Daarnaast MAG een dienstverlener optioneel per aangeboden service één AttributeConsumingService element opnemen waarin de dienstverlener aangeeft welke additionele attributen hij voor de betreffende service wil ontvangen.
Iedere AttributeConsumingService MOETexact één (1) attribuut bevatten waarvan de naam gelijk is aan een ServiceID in het lange formaat. (Zie paragraaf 9.2.2.).
Daarnaast MAG iedere AttributeConsumingService één of meer RequestedAttributes bevatten die voorkomen in de eHerkenning attribuutcatalogus.
Bij ieder gevraagd attribuut dat wordt opgenomen MAG de dienstverlener door middel van de indicatie isRequired aangeven of het attribuut noodzakelijk is om de DV applicatie goed te laten functioneren. Als deze indicatie niet wordt meegegeven dan wordt als default isRequired=”false” verondersteld.
Een AD/MR MAG op basis van ‘isRequired=true’ tijdens de transactie de attribuutwaarde aan de gebruiker vragen, maar dit hoeft niet. De dienstverlener zal hier rekening mee moeten houden bij de afhandeling.
Andere elementen MOGEN NIET worden opgenomen.

506 Voorbeeld dienstverlener:

```
...
<md:SPSSODescriptor AuthnRequestsSigned="true"
WantAssertionsSigned ="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
...
   <md:AssertionConsumerService  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://..." index="1" isDefault='true'/>
   <md:AttributeConsumingService isDefault="true" index="1">
         <md:ServiceName xml:lang="en">Voorbeeld Dienst 1</md:ServiceName>
         <md:RequestedAttribute Name="urn:nl:eherkenning:DV:0000000312345678000:services:0001">
                  </md:RequestedAttribute>
         <md:RequestedAttribute isRequired="false"
               Name="urn:nl:eherkenning1.3:AdditionalAttribute:ActingPersonName"/>
         <md:RequestedAttribute isRequired="true"
               Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail"/>
        <md:RequestedAttribute isRequired="false"
               Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalPhone"/>
   </md:AttributeConsumingService>
   <md:AttributeConsumingService isDefault="false" index="2">
        <md:ServiceName xml:lang="en">Voorbeeld Dienst 50</md:ServiceName>
       <md:RequestedAttribute     Name="urn:nl:eherkenning:DV:0000000312345678000:services:0050">
                  </md:RequestedAttribute>
       <md:RequestedAttribute isRequired="false"
                Name="urn:nl:eherkenning1.3:AdditionalAttribute:ActingPersonName"/>
       <md:RequestedAttribute isRequired="true"
                Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail"/>
   </md:AttributeConsumingService>
</md:SPSSODescriptor>

...
```

507 Een authenticatiedienst of machtigingenregister MOET één IDPSSODescriptor element opnemen met daarin
508 één SingleSignOnService element, en MAG GEEN geen andere elementen opnemen. Het SingleSignOnService
509 element MOET als attribuut SAML POST binding bevatten en MAG GEEN andere attributen bevatten.

510 Voorbeeld:

```
...
<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAuthnRequestsSigned="true">
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://...."/>
</md:IDPSSODescriptor>
```

...

511
512

513 Een eHerkenningsmakelaar MOET één IDPSSODescriptor en één SPSSODescriptor opnemen en MAG GEEN
514 andere elementen opnemen. De IDPSSODescriptor van de eHerkenningsmakelaar MAG meerdere
515 SingleSignOnService elementen bevatten en MOET tenminste één SingleSignOnService element bevatten met
516 de SAML POST binding. De SPSSODescriptor van de eHerkenningsmakelaar MOET twee
517 AssertionConsumerService elementen bevatten met de SAML POST binding, met indices 1 en 2 voor
518 antwoorden van respectievelijk authenticatiediensten en machtigingenregisters en mag geen andere
519 elementen bevatten.

520 Voorbeeld eHerkenningsmakelaar:

```
...
<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAuthnRequestsSigned="true">
...
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://...."/>
</md:IDPSSODescriptor>
<md:SPSSODescriptor AuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
...
   <md:AssertionConsumerService  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://..." index="1"/>
     <md:AssertionConsumerService  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://..." index="2"/>
</md:SPSSODescriptor>

...
```

521

522 Een IDPSSODescriptor bevat als attribuut WantAuthnRequestsSigned=true en MAG GEEN andere optionele
523 attributen bevatten. Een SPSSODescriptor element MOET als attribuut AuthnRequestsSigned=true en
524 WantAssertionsSigned=true en MAG GEEN andere optionele attributen bevatten.

525 Een IDPSSODesriptor of SPSSODescriptor MOET één of meerdere KeyDescriptor elementen bevatten met het
526 attribuut use="signing". Ieder KeyDescriptor element MOET een KeyName én een geldig G2 PKIoverheid
527 certificaat bevatten, waarmee de SAML berichten van de deelnemer kunnen worden geauthenticeerd. Nota
528 bene: Dienstverleners en deelnemers moeten alle genoemde KeyDescriptors verwerken. In de
529 handtekeningen in de protocolberichten wordt door middel van de KeyName aangeduid welk certificaat uit
530 de metadata is gebruikt voor de ondertekening.

531 Voorbeeld:

```
...
<md:KeyDescriptor use="signing">
      <ds:KeyInfo>
          <ds:KeyName>
```

```
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
          </ds:KeyName>
          <ds:X509Data>
            <ds:X509Certificate>
...
             </ds:X509Certificate>
           </ds:X509Data>
       </ds:KeyInfo>
</md:KeyDescriptor>

...
```

8.2 Aanleveren metadata door beheerorganisatie

De beheerorganisatie controleert de metadata van de deelnemers op conformiteit, verwijdert de handtekeningen en aggregeert de metadata tot een enkel bestand. De geaggregeerde metadata bestaat uit een ondertekend EntitiesDecriptor element met een attribuut cacheduration=”P7D”, en een attribuut Name van het formaat urn:nl:eherkenning:VERSIEAS:metadata:OMGEVING:VOLGNUMMER, waarbij VERSIEAS de versie van het afsprakenstelsel aanduidt, OMGEVING de betreffende omgeving (P of A) aanduidt, en VOLGNUMMER een oplopend nummer is wat de verschillende metadata versies onderscheidt. De ondertekening MOET worden uitgevoerd conform hetgeen is beschreven in hoofdstuk 3.

Het EntitiesDescriptor element bevat 3 EntitiesDescriptor elementen met de namen Authenticatiediensten, Machtingenregisters, eHerkenningsmakelaars en daarin de metadata van de verschillende deelnemers in de verschillende rollen.

Het EntitiesDescriptor element kan daarnaast ook een element Dienstverleners bevatten met daarin fictieve dienstverleners. Iedere eHerkenningsmakelaar MOET de dienstverleners hierin genoemd verwerken. Deze dienstverleners staan genoemd in de dienstencatalogus en kunnen worden gebruikt door de beheerorganisatie en voor testen.

Voorbeeld:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor
ID="[reference for dsig]"
Name="urn:nl:eherkenning:1.0:metadata:P:36" cacheduration="P7D"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:Signature>...</ds:Signature>
   <md:EntitiesDescriptor Name="Authenticatiediensten">
...
   </md:EntitiesDescriptor>
```

```
   <md:EntitiesDescriptor Name="Machtigingenregisters">
...
   </md:EntitiesDescriptor>
   <md:EntitiesDescriptor Name="Herkenningsmakelaars">
...
   </md:EntitiesDescriptor>
   <md:EntitiesDescriptor Name="Dienstverleners">
...

   </md:EntitiesDescriptor>
```

De beheerorganisatie publiceert de metadata op een vaste locatie. Omwille van de privacy van de gegevens van de contactpersonen in de metadata is de locatie een niet geïndexeerde URL met server-side SSL die alleen wordt gedeeld met de deelnemers.

Een deelnemer MOET periodiek op een vooraf door de beheerorganisatie gekozen tijdstip, de metadata verwerken. Gegevens over de URL en de periodiciteit staan beschreven in het document [eHerkenning - Operationeel handboek].

Een deelnemer MOET de metadata verwerken met een automatisch proces, wat in ieder geval binnen een kwartier is voltooid. Een deelnemer MOET in verband met rollback, of andere wijzigingen, dit automatische proces ook op tussentijdse momenten, in overleg met de beheerorganisatie, kunnen starten (bijvoorbeeld handmatig).

9 Data-elementen

Dit hoofdstuk beschrijft alle voor eHerkenning gedefinieerde data-elementen. Gebruikte SAML elementen die zuiver volgens de SAML standaard worden gebruikt zijn hier niet opgenomen.

9.1 OIN formaat

Binnen eHerkenning wordt het OIN formaat gebruikt om deelnemers, dienstverleners en bepaalde soorten dienstafnemers en intermediairs aan te duiden. Het OIN formaat is gedefinieerd binnen DigiKoppeling. Een OIN bestaat uit de volgende geconcateneerde elementen:

- Een prefix van 8 cijfers die het register aanduidt waar het nummer is gedefinieerd
- Een nummer waarvan de invulling afhangt van het register

Binnen eHerkenning worden FI-nummers, KvK nummers, vestigingsnummers en nummers uit de DigiKoppeling registry gebruikt. Nummers uit buitenlandse handelsregisters of vergelijkbare openbare registers kunnen worden toegevoegd nadat daarvoor een specifieke prefix is uitgegeven.

9.1.1 FI-nummer

Het FI-nummer heeft als prefix 00000001 of 00000002. Het nummer bestaat uit het 9-cijferige nummer met een suffix van 3 cijfers. Voor prefix 00000001 is deze suffix altijd 000.

Voorbeeld: 00000001123456789000 of 00000002123456789001

9.1.2 KvK nummer

Het KvK nummer heeft als prefix 00000003.
Het nummer bestaat uit het 8-cijferige KvK nummer met een suffix van 0000, bijvoorbeeld:

00000003123456780000

9.1.3 Vestigingsnummer

Het vestigingsnummer heeft als prefix 00000006. Het nummer bestaat uit het 12-cijferige vestigingsnummer, bijvoorbeeld:

000000061234567890 12

9.1.4 DigiKoppeling registry

Dit nummer wordt door Logius uitgegeven aan dienstverleners die geen (eigen) KvK nummer hebben.

Het nummer uit de DigiKoppeling registry heeft als prefix 00000004.
Het nummer bestaat uit een 9-cijferig nummer gevolgd door 000, bijvoorbeeld:

00000004123456789000

9.1.5 Buitenlandse registers

Voor het gebruik van eHerkenning door buitenlandse dienstafnemers uit andere EU lidstaten kunnen specifieke prefixen worden vastgesteld in samenwerking met Logius en het Nederlandse dienstenloket (Antwoord voor Bedrijven). Daarbij wordt per register van betreffend land een prefix uitgegeven. Indien van toepassing wordt er zowel een prefix voor het bedrijfsniveau (onderneming en rechtspersoon) als een prefix voor het vestigingsniveau uitgegeven. Per land moet op de website van eHerkenning worden gecommuniceerd dat dienstafnemers van het betreffende land hiervan gebruik kunnen maken, onder verwijzing naar het Nederlandse dienstenloket en de specifieke voorschriften van het betreffende land.

Daarbij geldt de regel dat indien er een KvK nummer is uitgegeven aan de betreffende dienstafnemer dat altijd dat nummer gebruikt moet worden. Dat wil zeggen dat in het Nederlandse handelsregister ingeschreven dienstafnemers en vestigingen van buitenlandse dienstafnemers niet het nummer waarin zij in een buitenlands register zijn ingeschreven mogen gebruiken binnen eHerkenning. Indien enig onderdeel van de dienstafnemer in het Nederlandse handelsregister is geregistreerd dan moet het KvK nummer gebruikt worden.

9.2 Identificerende kenmerken

Binnen eHerkenning worden de volgende identificerende kenmerken gedefinieerd.

9.2.1 Betrouwbaarheidsniveau

Om de betrouwbaarheidsniveaus van eHerkenning in de berichten te onderscheiden wordt onderstaande subset van de in de SAML 2.0 specificaties voor het AuthnContextClassRef element gebruikte waarden toegestaan. Andere waarden MOGEN NIET worden gebruikt.

eHerkenning niveau	SAML2 AuthnContextClassRef element
1	urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
2	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
2+[16]	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
3	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
4	urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

Zie ook document [eHerkenning - Betrouwbaarheidsniveaus].

9.2.2 ServiceID

Binnen eHerkenning worden alle diensten aangeduid met een binnen de context van de dienstverlener uniek nummer, de ServiceID. Elk ServiceID is in de dienstencatalogus opgenomen als onderdeel van een urn van het formaat

urn:nl:eherkenning:DV:<OIN>:services:<ServiceID>

waarbij <OIN> staat voor het OIN van de dienstverlener die de dienst verleent. Door middel van de urn worden diensten uniek binnen eHerkenning gedefinieerd.

Geregistreerde diensten MOETEN een ServiceID van 1 of hoger hebben. Een loket- of portalfunctie wordt in berichten aangeduid met het gereserveerde ServiceID met waarde '0'. Deze wordt niet opgenomen in de dienstencatalogus.

De ServiceID wordt in berichten in twee formaten gebruikt:

1. Het korte formaat. Hier wordt alleen de ServiceID opgenomen.

16 Niveau werd tijdens de proefimplementaties aangeduid met de benaming “niveau NL”.

2. Het lange formaat. Hier wordt de volledige urn opgenomen.

9.2.3 EntityID

Binnen eHerkenning worden alle systemen van deelnemers en dienstverleners aangeduid met een EntityID die is opgenomen in de metadata. De EntityID is van het formaat

urn:nl:eherkenning:<ROL>:<OIN>:entities:<index>

waarbij <ROL> de waarden DV, HM, AD of MR kan hebben, <OIN> staat voor het het KvK nummer of DigiKoppeling nummer van de deelnemer of het FI-nummer,KvK nummer of DigiKoppeling nummer dienstverlener. De <index> is een vrij door deelnemer of dienstverlener te kiezen nummer van 0 t/m 8999 om verschillende endpoints mee te definiëren. Nummers van 9000 t/m 9999 zijn gereserveerd voor testsystemen.

Bij veranderingen aan een systeem van een deelnemer (bijvoorbeeld bij overgang naar een nieuwe versie van eHerkenning) MAG de deelnemer het entityID van een systeem wijzigen.

9.2.4 Pseudoniemen

Binnen eHerkenning wordt een uitvoerende persoon op de volgende manieren aangeduid:

- In geval van vertegenwoordiging:
  a. binnen het netwerk met een intern pseudoniem door de authenticatiedienst; en
  b. binnen en buiten het netwerk met een specifiek pseudoniem door het machtigingenregister
- In geval van geen vertegenwoordiging:
  a. Binnen en buiten het netwerk met een specifiek pseudoniem door de authenticatiedienst

9.2.4.1 Intern pseudoniem

Het intern pseudoniem wordt bepaald en vastgelegd door de authenticatiedienst en MOET uniek zijn binnen de authenticatiedienst. Elke keer dat hetzelfde authenticatiemiddel wordt gebruikt ZOU ook hetzelfde intern pseudoniem MOETEN worden teruggegeven. Op verzoek van de handelende natuurlijk persoon MAG echter altijd nieuw pseudoniem worden gegenereerd. Een eenmaal gebruikt intern pseudoniem MAG NIET worden hergebruikt. De enige uitzondering hierop bestaat wanneer een authenticatiemiddel wordt vervangen en de authenticatiedienst met voldoende zekerheid kan vaststellen dat het daadwerkelijk om vervanging gaat. In dat geval MAG voor het nieuwe authenticatiemiddel hetzelfde intern pseudoniem worden gebruikt.

Het formaat van het intern pseudoniem MOET hexadecimale waarde van 32 byte zijn. Bijv.

ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890

9.2.4.2 Specifiek pseudoniem

Het specifiek pseudoniem kan op twee manieren worden gecreëerd:

1. In geval van vertegenwoordiging door een machtigingenregister. Het is dan uniek voor elke verschillende combinatie van uitvoerende natuurlijk persoon, vertegenwoordigde dienstafnemer en dienstverlener.
    a. In het geval van een ketenmachtiging is het pseudoniem uniek voor elke verschillende combinatie van uitvoerende natuurlijk persoon, intermediair en dienstverlener
2. In geval van geen vertegenwoordiging door een authenticatiedienst. Het is dan uniek voor elke verschillende combinatie van dienstafnemer en dienstverlener.

Een specifiek pseudoniem wordt bij voorkeur eenmalig gegenereerd en vervolgens opgeslagen, maar mag ook per verzoek worden gegenereerd, zolang dit maar op een vaste manier gebeurt en dus voor elk verzoek dezelfde waarde oplevert.

Verschillen in specifieke pseudoniemen kunnen gebruikt worden door dienstverleners om vast te stellen dat er sprake is van verschillende uitvoerend natuurlijk personen (vier-ogen principe). Om die reden MOET een MR voor het genereren van een nieuw pseudoniem voor een bestaande combinatie van dienstverlener, uitvoerend natuurlijk persoon en dienstafnemer (of intermediair in het geval van ketenmachtigingen) toestemming hebben van de machtigingenbeheerder of wettelijk vertegenwoordiger van de dienstafnemer (resp. de intermediair). Redenen voor het genereren van een nieuw pseudoniem kunnen zijn:

- Natuurlijk persoon heeft een andere functie gekregen binnen hetzelfde bedrijf en mag daarom niet meerop basis van het oude pseudoniem toegang krijgen tot dossiers bij dienstverleners gekoppeld aan de oude rol;
- Identiteit van natuurlijk persoon is ongewild bekend geraakt bij dienstverlener(s) en nieuw pseudoniem is gewenst om de identiteit weer af te schermen/te pseudonimiseren;
- Vanwege een fusie/splitsing van dienstverleners is migratie naar een nieuw pseudoniem gewenst.

Het formaat van het specifiek pseudoniem MOET een hexadecimale waarde van 32 byte zijn.
Bijv. ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890

In geval van vertegenwoordiging wordt deze waarde gevolgd door een @ en een hexadecimale waarde van 16 byte. Bijv.
ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890@ABCDEF1234567890ABCDEF1234567890

De waarde van 32 byte MOET een random waarde zijn. Dit kan bijvoorbeeld worden bereikt d.m.v. een SHA256 hash over de volgende elementen (in deze volgorde en gescheiden door een scheidingsteken) te berekenen:

1. Het OIN van de dienstverlener
2. Een in de context van de vertegenwoordigde dienstafnemer uniek (doch niet per se exclusief) identificerend kenmerk van de uitvoerende natuurlijk persoon.

Dit kenmerk MAG door de beheerder of door de maker van het pseudoniem bepaald worden, maar MAG ook het interne pseudoniem zijn.

3. Het identificerend kenmerk van de vertegenwoordigde dienstafnemer (alleen in geval van vertegenwoordiging zonder ketenmachtiging) of van de intermediair (in geval van ketenmachtiging).

Andere methodes om tot een 32 byte random waarde te komen zijn dus ook toegestaan.

De waarde van 16 byte MOET een MD5 hash over het identificerend kenmerk van de vertegenwoordigde dienstafnemer (of intermediair in het geval van een ketenmachtiging) zijn.

N.B. Er kunnen nog andere formaten van specifieke pseudoniemen in omloop zijn. Gebruikers van het specifiek pseudoniem wordt dan ook afgeraden (delen van) het pseudoniem te gebruiken voor andere doeleinden dan het identificeren van de uitvoerende natuurlijk persoon.

9.3 SAML Attributen

Deze paragraaf beschrijft de data-elementen die als SAML Attribute element in berichten voorkomen.

De voor eHerkenning specifieke attributen worden aangeduid met een urn. Deze urn bevat het versienummer van het afsprakenstelsel waarin (die versie) van het betreffende attribuut voor het eerst is opgenomen.

9.3.1 Entity ConcernedID

Omschrijving	Een SAML Attribute element met daarin het Identificerende kenmerk van de handelende dienstafnemer die door de handelende natuurlijk persoon vertegenwoordigd wordt (of zelf is).
Name	urn:nl:eherkenning:1.7:EntityConcernedID:[Naam identificerend kenmerk] Zie 7.1 Identificerende kenmerken van dienstafnemers voor een lijst met alle toegestane elementnamen en hun invulling
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	Zie paragraaf 7.1.
Opmerkingen	

9.3.2 ServiceID

Omschrijving	Een SAML Attribute element met daarin de ServiceID van de dienst waarvoor de toegang wordt gevraagd of de bevoegdheid

	voor is vastgesteld. Zie paragraaf 9.2.2.
Name	urn:nl:eherkenning:1.0:ServiceID
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	Zie paragraaf 9.2.2. De waarde MOET overeenkomen met de waarde van @AttributeConsumingServiceID uit het AuthnRequest. Zie paragraaf 5.1.

707 ### *9.3.3 AuthorizationRegistryID*

Omschrijving	Een SAML Attribute element met daarin een EntityID van het machtigingenregister dat moet worden bevraagd in de use case "raadplegen machtigingenregister". Deze EntityID MOET voorkomen in de metadata. Zie paragraaf **9.2.3**.
Name	urn:nl:eherkenning:1.0:AuthorizationRegistryID
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	Zie paragraaf 9.1
Opmerkingen	Als een AuthorizationRegistryID door een AD wordt teruggegeven dan MOET de waarde van het attribuut Representation TRUE zijn.

708 ### *9.3.4 IntermediateEntityID*

Omschrijving	Een SAML Attribute element met daarin het identificerende nummer van de intermediaire partij die voorkomt in de ketenmachtiging
Name	urn:nl:eherkenning:1.7:IntermediateEntityID:[Naam identificerend kenmerk] Zie 7.1 Identificerende kenmerken van dienstafnemers voor een lijst met toegestane elementnamen en hun invulling. Let op dat niet alle vormen van identificerence kenmerken zijn toegestaan voor intermediairs.
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	Zie paragraaf 7.1

Opmerkingen	Als een AuthorizationRegistryID door een AD wordt teruggegeven dan MOET de waarde van het attribuut Representation TRUE zijn.

709 ### *9.3.5 Representation*

Omschrijving	Een SAML Attribute element met daarin een indicatie of sprake is van vertegenwoordiging
Name	urn:nl:eherkenning:1.7:Representation
Type	http://www.w3.org/2001/XMLSchema#boolean
AttributeValue	True of false

710

711 ## *9.4 URL of POST variabele: EherkenningPreferredLanguage*

Omschrijving	Taalvoorkeur van handelende natuurlijk persoon
Naam	EherkenningPreferredLanguage
Formaat	Volgens ISO 639-1:2002

10 Bijlage XML Schema dienstencatalogus

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:eh="urn:nl:eherkenning:dc:1.7"
targetNamespace="urn:nl:eherkenning:dc:1.7" elementFormDefault="qualified"
attributeFormDefault="unqualified">
	<xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="xmldsig-
core-schema.xsd"/>
	<xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion" schemaLocation="saml-schema-
assertion-2.0.xsd"/>
	<xs:import namespace="urn:oasis:names:tc:SAML:2.0:metadata" schemaLocation="saml-schema-
metadata-2.0.xsd"/>
	<!--Elements-->
	<xs:element name="Service">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="eh:ServiceID"/>
				<xs:element ref="eh:ServiceName" maxOccurs="unbounded"/>
				<xs:element ref="eh:ServiceDescription" maxOccurs="unbounded"/>
				<xs:element ref="eh:ServiceDescriptionURL" minOccurs="0"
maxOccurs="unbounded"/>
				<xs:element ref="saml2:AuthnContextClassRef"/>
				<xs:element ref="eh:HerkenningsmakelaarId"/>
				<xs:element ref="eh:AdditionalHerkenningsmakelaarId" minOccurs="0"
maxOccurs="unbounded"/>
				<xs:element name="SSOSupport" type="xs:boolean" minOccurs="0"
maxOccurs="1"/>
				<xs:element ref="eh:EntityConcernedTypesAllowed" minOccurs="0"
maxOccurs="unbounded"/>
				<xs:element ref="eh:ServiceCertificate" minOccurs="0"
maxOccurs="unbounded"/>
			</xs:sequence>
			<xs:attribute ref="eh:IsPublic" use="required"/>
		</xs:complexType>
	</xs:element>
	<xs:element name="ServiceCatalogue">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="ds:Signature"/>
```

```
                        <xs:element ref="eh:ServiceProvider" maxOccurs="unbounded"/>
                </xs:sequence>
                <xs:attribute ref="eh:IssueInstant" use="required"/>
                <xs:attribute ref="eh:NotOnOrAfter" use="required"/>
                <xs:attribute ref="eh:Version" use="required"/>
                <xs:attribute name="ID" type="xs:string"/>
        </xs:complexType>
</xs:element>
<xs:element name="EntityConcernedTypesAllowed">
        <xs:complexType>
                <xs:simpleContent>
                        <xs:extension base="xs:string"/>
                </xs:simpleContent>
        </xs:complexType>
</xs:element>
<xs:element name="ServiceDescription">
        <xs:complexType>
                <xs:simpleContent>
                        <xs:restriction base="md:localizedNameType">
                                <xs:maxLength value="512"/>
                        </xs:restriction>
                </xs:simpleContent>
        </xs:complexType>
</xs:element>
<xs:element name="ServiceDescriptionURL">
        <xs:complexType>
                <xs:simpleContent>
                        <xs:restriction base="md:localizedURIType">
                                <xs:maxLength value="512"/>
                        </xs:restriction>
                </xs:simpleContent>
        </xs:complexType>
</xs:element>
<xs:element name="ServiceID" type="xs:anyURI"/>
<xs:element name="ServiceName">
        <xs:complexType>
                <xs:simpleContent>
                        <xs:restriction base="md:localizedNameType">
                                <xs:maxLength value="64"/>
                        </xs:restriction>
                </xs:simpleContent>
        </xs:complexType>
```

```
        </xs:element>
        <xs:element name="ServiceProvider">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element ref="eh:ServiceProviderID"/>
                                <xs:element ref="eh:OrganizationDisplayName"
maxOccurs="unbounded"/>
                                <xs:element ref="eh:Service" maxOccurs="unbounded"/>
                        </xs:sequence>
                        <xs:attribute ref="eh:IsPublic" use="required"/>
                </xs:complexType>
        </xs:element>
        <xs:element name="ServiceProviderID" type="xs:anyURI"/>
        <xs:element name="ServiceCertificate">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element ref="md:KeyDescriptor"/>
                        </xs:sequence>
                </xs:complexType>
        </xs:element>
        <xs:element name="HerkenningsmakelaarId" type="xs:anyURI"/>
        <xs:element name="AdditionalHerkenningsmakelaarId" type="xs:anyURI"/>
        <xs:element name="OrganizationDisplayName">
                <xs:complexType>
                        <xs:simpleContent>
                                <xs:restriction base="md:localizedNameType">
                                        <xs:maxLength value="64"/>
                                </xs:restriction>
                        </xs:simpleContent>
                </xs:complexType>
        </xs:element>
        <!--Attributes-->
        <xs:attribute name="IssueInstant" type="xs:dateTime"/>
        <xs:attribute name="IsPublic" type="xs:boolean"/>
        <xs:attribute name="NotOnOrAfter" type="xs:dateTime"/>
        <xs:attribute name="Version" type="xs:anyURI"/>
</xs:schema>
```

11 Bijlage voorbeeld berichten

In deze bijlage worden twee voorbeeldberichten gegeven. Er zijn geen voorbeeldwaarden voor elementen en attributen ingevuld.

11.1 AuthnRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ForceAuthn="true"
Destination=" " AssertionConsumerServiceIndex=" " AttributeConsumingServiceIndex="2" ID=" "
IssueInstant=" " Version="2.0" ProviderName=" ">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 </saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256"/>
                        <ds:Reference URI=" ">
                                <ds:Transforms>
                                        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
                                </ds:Transforms>
                                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                                <ds:DigestValue>
            </ds:DigestValue>
                        </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>
        </ds:SignatureValue>
                <ds:KeyInfo>
                        <ds:KeyName>
                </ds:KeyName>
                </ds:KeyInfo>
        </ds:Signature>
        <samlp:Extensions>
          <ehsamlp:RequestedAttributes>
                <md:RequestedAttribute
```

```
Name="urn:nl:eherkenning1.3:AdditionalAttribute:ActingPersonName"/>
            <md:RequestedAttribute Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail"/>
            <md:RequestedAttribute Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalPhone"/>
          </ehsamlp:RequestedAttributes>
        </samlp:Extensions>
        <samlp:RequestedAuthnContext Comparison="minimum">
                <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     </saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

11.2 Response

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" " InResponseTo=" "
Version="2.0" Destination=" " IssueInstant=" ">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   </saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256"/>
                        <ds:Reference URI=" ">
                                <ds:Transforms>
                                        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
                                </ds:Transforms>
                                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                                <ds:DigestValue>
           </ds:DigestValue>
                        </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>
     </ds:SignatureValue>
                <ds:KeyInfo>
                        <ds:KeyName>
                </ds:KeyName>
```

```
                </ds:KeyInfo>
        </ds:Signature>
        <samlp:Status>
                <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">
      </samlp:StatusCode>
        </samlp:Status>
        <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID=" "
IssueInstant=" ">
                <saml:Issuer>
      </saml:Issuer>
                <saml:Subject>
                        <saml:NameID>
          </saml:NameID>
                        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                                <saml:SubjectConfirmationData Recipient=" " NotOnOrAfter=" ">
            </saml:SubjectConfirmationData>
                        </saml:SubjectConfirmation>
                </saml:Subject>
                <saml:Conditions NotBefore=" " NotOnOrAfter=" ">
                        <saml:AudienceRestriction>
                                <saml:Audience>
            </saml:Audience>
                        </saml:AudienceRestriction>
                </saml:Conditions>
                <saml:AuthnStatement AuthnInstant=" ">
                        <saml:AuthnContext>
                                <saml:AuthnContextClassRef>
            </saml:AuthnContextClassRef>
                                <saml:AuthenticatingAuthority>
            </saml:AuthenticatingAuthority>
                        </saml:AuthnContext>
                </saml:AuthnStatement>
                <saml:AttributeStatement>
                        <saml:Attribute Name="urn:nl:eherkenning:1.0:ServiceID">
                                <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
            </saml:AttributeValue>
                        </saml:Attribute>
                        <saml:Attribute Name="urn:nl:eherkenning:1.0:EntityConcernedID">
                                <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
            </saml:AttributeValue>
```

```
                    </saml:Attribute>

                    <saml:EncryptedAttribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                        <xenc:EncryptedData mlns:xenc=http://www.w3.org/2001/04/xmlenc#
Id="Encrypted_DATA_ID" Type="http://www.w3.org/2001/04/xmlenc#Element">
                            <xenc:EncryptionMethod Algorithm=
"http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                            <ds:KeyInfo>
                                <ds:Keyname> </ds:Keyname>
                            </ds:KeyInfo>
                            <xenc:CipherData>
                                <xenc:CipherValue>   </xenc:CipherValue>
                            </xenc:CipherData>
                        </xenc:EncryptedData>
                    </saml:EncryptedAttribute>
                </saml:AttributeStatement>
            </saml:Assertion>
</samlp:Response>
```

12 eHerkenning XML Schema extensions

12.1 XML schema metadata extension

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:eh="urn:nl:eherkenning:1.3:metadataextensions"
   targetNamespace="urn:nl:eherkenning:1.3:metadataextensions"
   elementFormDefault="qualified" attributeFormDefault="unqualified">
         <xs:attribute name="validFrom" type="xs:dateTime"/>
         <xs:attribute name="version" type="xs:string"/>
</xs:schema>
```

12.2 XML schema attribute extension

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:ehsamlp="urn:nl:eherkenning:1.3a:attributeextension"
                targetNamespace="urn:nl:eherkenning:1.3a:attributeextension"
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                elementFormDefault="qualified" attributeFormDefault="unqualified">
   <xs:element name="RequestedAttributes">
      <xs:complexType>
         <xs:sequence>
            <xs:element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
         </xs:sequence>
      </xs:complexType>
   </xs:element>

</xs:schema>
```