Afsprakenstelsel eHerkenning

Koppelvlakspecificatie HM-MR

Versie 1.7a

INHOUDSOPGAVE

COLOFON

Auteur	Status
Beheerorganisatie Afsprakenstelsel eHerkenning	Definitief
Project	**Datum**
Afsprakenstelsel eHerkenning	27 augustus 2013
Organisatie	**Classificatie**
Logius	Openbaar
Titel van het document	**Versie**
Afsprakenstelsel eHerkenning – Koppelvlakspecificatie HM-MR	1.7a

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
29/03/10	0.8def	Ten behoeve van proefimplementaties		Projectbureau
06/09/10	1.0	Vorm wijzigingen en doorvoeren verschillende RFCs	Definitief	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
06/02/13	1.5a	Errata uit RFC0197 verwerkt	Definitief	Beheerorganisatie
01/04/13	1.6	RFC0186 verwerkt	Definitief	Beheerorganisatie
24/05/13	1.7	RFC0188, RFC0204, RFC210, RFC0211, RFC0213, RFC0216 verwerkt	Definitief	Beheerorganisatie
27/08/13	1.7a	RFC0225, RFC0227	Definitief	Beheerorganisatie

DISTRIBUTIE

Datum	Distributie	Versie
	Kernteam, Gebruikersraad en publicatie op eherkenning.nl	1.7a

GOEDKEURING

Datum	Naam	Versie
27/08/13	Alle RFCs voor versie 1.7a goedgekeurd door kernteam	1.7a

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.

1.1 Doel en doelgroep van dit document

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

1.2 Leeswijzer

Hoofdstuk 2 beschrijft de algemene eisen voor het koppelvlak, de technische informatiebeveiligingseisen en de foutafhandeling.
Een aantal generieke eHerkenning koppelvlakspecificaties, die geldig zijn voor alle koppelvlakken, zijn centraal beschreven in het document “Koppelvlakspecificatie DV-HM”. Dit document verwijst op diverse plaatsen naar deze generieke specificaties.Hoofdstuk 3 bevat de berichtenspecificaties. In hoofdstuk 4 wordt nog een overzicht gegeven van generieke onderwerpen die in het document “Koppelvlakspecificatie DV-HM” zijn gespecificeerd. In hoofdstuk 5 wordt een overzicht gegeven van de gebruikte data-elementen. Het document sluit af met enkele bijlagen waar vanuit de tekst naar verwezen wordt.

1.3 Begrippenlijst

De begrippenlijst, Terminologie en Typologie zijn consistent toegepast over de verschillende eHErkenning koppelvlakken.
Zie hiervoor de beschrijvingen in Koppelvlakspecificatie DV-HM – Hoofdstuk 1 – paragrafen Begrippenlijst, Terminologie en Typologie.

2 Algemene eisen, technische informatiebeveiligingseisen en foutafhandeling

Het in dit document beschreven koppelvlak wordt gebruikt voor de implementatie van de use case "raadplegen machtigingenregister" en MOET door elke eHerkenningsmakelaar en door elk machtigingenregister worden geïmplementeerd.

De algemene eisen, zoals beschreven in Hoofdstuk 2 van het document "Koppelvlakspecificatie DV-HM" zijn ook op het koppelvlak HM-MR van kracht, met uitzondering van het alternatieve koppelvlak / de alternatieve binding, zoals beschreven in "Koppelvlakspecificatie DV-HM", paragraaf 2.1 (alternatieve koppelvalk en/of binding) en paragraaf 2.2.2.2 (Alternatieve binding)

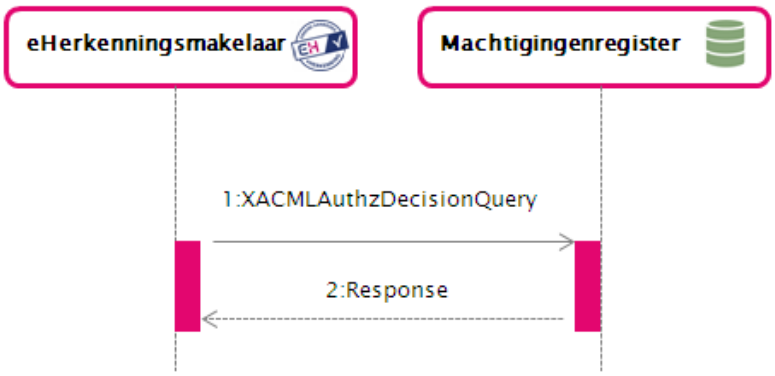
Ook de technisch informatiebeveiligingseisen, zoals geformuleerd in hoofdstuk 3 van het document "Koppelvlakspecificatie DV-HM", zijn van toepassing op het koppelvlak HM-MR.

Ook de foutafhandeling, zoals geformuleerd in hoofdstuk 4 van het document "Koppelvlakspecificatie DV-HM", zijn van toepassing op het koppelvlak HM-MR.

3 Berichtenspecificaties

Dit hoofdstuk beschrijft de berichten van het hier beschreven koppelvlak.

De use case “raadplegen machtigingenregister” wordt in het hier beschreven koppelvlak ingevuld met en SAML 2.0 AuthnRequest en Response.



Figuur 1: Sequence diagram HM-MR

De specifieke invulling van deze berichten wordt hieronder beschreven. Detailinformatie over de inhoud van velden kan worden gevonden in hoofdstuk 5.

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

3.1 XACMLAuthzDecisionQuery (1)

Zie paragraaf 6.1 voor een voorbeeld.

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
@ReturnContext	eHerkenning: De waarde MOET “true” zijn.

Data element		Invulling
@Destination		SAML: URL van de machtigingenregister waarop het bericht wordt aangeboden. MOET overeenkomen met de metadata van het machtigingenregister.
@Consent		eHerkenning: MAG NIET worden opgenomen.
@InputContextOnly		eHerkenning: MAG NIET worden opgenomen
Issuer		eHerkenning: MOET de EntityID van de eHerkenningsmakelaar bevatten. Zie paragraaf 9.2.3 in het document “Koppelvlakspecificatie DV-HM”. 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 in het document “Koppelvlakspecificatie DV-HM”. voor specifieke eisen.
Extensions		eHerkenning: MOET AssertionConsumerServiceIndex bevatten. Zie paragraaf 5.1.3.
Request	Subject	eHerkenning: MOET AuthenticationMeansID bevatten. Zie paragraaf 5.1.4.
	Resource	eHerkenning: MOET twee XACML attributen, ServiceID (in het lange formaat)en LevelOfAssurance bevatten. Indien de verschillende soorten dienstafnemers die toegang kunnen krijgen tot een dienst door de dienstverlener zijn opgenomen in de vraag, of indien de dienstverlener in de metadata of de vraag aanvullende attributen uitvraagt MOETEN deze hier als attribuut worden opgenomen. Indien zowel in de vraag als in de metadata aanvullende attributen zijn gedefinieerd, dan MOETEN al deze attributen worden opgenomen. Uitsluitend de attributen die door het betreffende machtigingenregister kunnen en mogen worden geleverd mogen door de eHerkenningsmakelaar worden opgenomen. De eHerkenningsmakelaar MOET hier op controleren. Zie document [eHerkenning -Attribuutcatalogus] en hoofdstuk 8 Metadata in het document “Koppelvlakspecificatie DV-HM”. Andere XML attributen MOGEN NIET worden opgenomen.

Data element		Invulling
		Andere elementen MOGEN NIET worden opgenomen. Een machtigingenregister MAG vragen om aanvullende attributen negeren, maar MAG het bericht NIET weigeren.
	Action	eHerkenning: MOET het XACML attribuut Action-ID bevatten. Zie paragraaf 5.1.2.
	Environment	eHerkenning: MOET leeg zijn.

48 ### *3.2 Response (2)*

49 Zie paragraaf 6.2 voor een voorbeeld.

Data element	Invulling
@ID	SAML: Uniek kenmerk van het bericht
@InResponseTo	SAML: Uniek kenmerk van de XACMLAuthzDecisionQuery 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	SAML: URL van de eHerkenningsmakelaar waarop het bericht wordt aangeboden. MOET overeenkomen met de metadata van de dienstverlener.
@Consent	eHerkenning: MAG NIET worden opgenomen
Issuer	eHerkenning: MOET de EntityID van het machtigingenregister bevatten. Zie paragraaf 9.2.3 in het document “Koppelvlakspecificatie DV-HM”. De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
Signature	eHerkenning: MOET de elektronische handtekening van het machtigingenregister over het hele bericht bevatten. Zie document “Koppelvlakspecificatie DV-HM”, paragraaf 3.2 voor specifieke eisen.
Extensions	eHerkenning: MAG NIET worden opgenomen

Data element	Invulling
Status	eHerkenning: MOET een element StatusCode bevatten met daarin de status van de authenticatie. In geval van een fout MOET dit element worden gevuld conform de beschrijvingen in hoofdstuk 4 in het document "Koppelvlakspecificatie DV-HM". StatusDetail MAG NIET worden opgenomen.
Assertion	eHerkenning: MOET een verklaring over de bevoegdheid bevatten (zie de volgende paragraaf).

3.2.1 Verklaring over bevoegdheid

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 het machtigingenregister bevatten. Zie paragraaf 9.2.3 in het document "Koppelvlakspecificatie DV-HM". De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
	Signature	eHerkenning: MOET de elektronische handtekening van het machtigingenregister over deze hele assertion bevatten. Zie "Koppelvlakspecificatie HM-DV", paragraaf 3.2 voor specifieke eisen.
	Subject	eHerkenning: MAG 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. Andere Conditions MOGEN NIET worden opgenomen.
	Advice	eHerkenning: MAG NIET worden opgenomen
	XACMLAuthz-Decision Statement	eHerkenning: MOET een SAML Statement van het type XACMLAuthzDecisionStatementType bevatten. Zie hieronder.

51

Data element				Invulling
XACMLAuthz Decision Statement	Response	Result	@ResourceID	eHerkenning: MAG NIET worden opgenomen
			Decision	XACML: Een van de binnen XACML 2.0 toegestane waarden. In geval van annuleren of een fout MOET dit element worden gevuld met de waarde Deny. Zie ook de beschrijvingen in hoofdstuk 4 in het document “Koppelvlakspecificatie DV-HM”.
			Obligations	Obligation urn:nl:eherkenning:1.7:RequireConfirmationFromNextMR FulfillOn=Permit AttributeAssignment urn:nl:eherkenning:1.0:AuthorizationRegistryID = <MR2> (zie paragraaf 9.3.4 van “Koppelvlakspecificatie DV-HM”) eHerkenning: Indien het een ketenmachtiging betreft constateert het eerste machtigingsregister dit en specificeert middels Obligation dat de tweede schakel geverifieerd MOET worden en dat anders de Decision = Permit niet geldt.
			Status	eHerkenning: MOET een element StatusCode bevatten met daarin de status van de authenticatie. In geval van een fout MOET dit element worden gevuld conform de beschrijvingen in hoofdstuk 4 in het document “Koppelvlakspecificatie DV-HM”. StatusDetail MAG NIET worden opgenomen.
	Request		Subject	Eherkenning: Bevat het XACMLAuthzDecisionQuery Subject element met alle in de vraag genoemde attributen. Zie paragraaf 3.1. Het in de vraag opgenomen

Data element			Invulling
			AuthenticationMeansID MOET worden verwijderd. Wanneer de Decision 'Permit' is MOET het attribuut ActingEntityID worden toegevoegd. Zie paragraaf 5.1.1
		Resource	eHerkenning: MOET het Resource element uit de vraag bevatten. Wanneer de Decision 'Permit' is • MOET LevelOfAssuranceUsed worden opgenomen. Zie paragraaf 5.1.8. • MOET precies één attribuut worden opgenomen dat de dienstafnemer identificeert (Zie paragraaf 5.1.6 in dit document en paragraaf 7.1 in "Koppelvlakspecificatie DV-HM"). • Indien het EntityConcernedID een KvK-nummer bevat, dan MAG tevens een tweede EntityConcernedID gevuld met het vestigingsnummer (zie paragraaf 9.3.1 in "Koppelvlakspecificatie DV-HM") worden opgenomen. • Wanneer Obligation is opgenomen MOET hier worden opgenomen: Intermediates (Identifier of intermediate1) zie paragraaf 5.1.10 EncryptedAttributes MOGEN worden opgenomen wanneer aanvullende attributen door de herkenningsmakelaar zijn gevraagd en voor deze attributen door uitvoerende natuurlijk persoon of de machtigingenbeheerder van de vertegenwoordigde dienstafnemen / intermediaire partij user consent is verleend (tijdens de transactie of middels vooraf gegeven consent) en wanneer de Decision 'Permit' is.NextAuthorizationRegistryID MAG worden opgenomen. Zie paragraaf 8.3.1. van het document "Koppelvlakspecificatie HM-AD".

Data element			Invulling
			Andere attributen MOGEN NIET worden opgenomen.
		Action	eHerkenning: MOET gelijk zijn aan het Action element uit de vraag. Zie paragraaf 3.1.
		Environment	eHerkenning: MOET leeg zijn.

3.3 Ketenmachtigingen

Om gebruik te kunnen maken van een ketenmachtiging, MOET de volledige keten van dienstafnemer tot uitvoerend natuurlijk person bekend zijn bij het eerste machtigingenregister (MR), het machtigingenregister waar de user interactie plaatsvindt.

eHerkenning ondersteunt alleen ketens met één tussenschakel:

- Gebruiker G (uitvoerend natuurlijk persoon) · Intermediair A · Dienstafnemer B.

De toestemming dat de gebruiker mag handelen namens Intermediair A is geregistreerd als machtiging bij het eerste MR. De informatie dat er een machtiging van Dienstafnemer B voor Intermediair is, en bij welk MR deze is opgeslagen, MOET ook bekend zijn bij het eerste MR (of opgevraagd worden op moment van de authenticatie).

Het eerste MR antwoordt dan als volgt:

- Het specifiek pseudonym van de gebruiker in attribuut urn:nl:eherkenning:1.0:ActingEntityID
- Het OIN van Intermediair A in attribuut urn:nl:eherkenning:1.7:Intermediates

Ten behoeve van toekomstige uitbreiding is dit een multi-value attribuut. Op dit moment MOET Intermediates maximaal één waarde bevatten.

Het Identificerend kenmerk van Dienstafnemer B staat in attribuut urn:nl:eherkenning:1.7:EntityConcernedID:KvKnr (in het geval van een KvK-nummer, dit kan ook ander type identificerend kenmerk zijn, zie “Koppelvlakspecificatie DV-HM” paragraaf 7.1).

De HM stuurt vervolgens deze informatie (alle hierboven gespecificeerde attributen) naar de MR die is aangegeven in het urn:nl:eHerkenning:1.7:RequireConfirmationFromNextMR element in Obligations, aangezien deze de machtiging geregistreerd heeft van Dienstafnemer B · Intermediair A. De volgende MR herkent dit als een claim confirmation request op basis van de aanwezigheid van het Intermediates attribute

Het mechanisme en protocol voor het uitwisselen van informatie tussen MRs over welke machtigingen waar zijn opgeslagen valt buiten de scope van de eHerkenning specificatie. Hieronder wordt de afhandeling van de vervolgvraag nader uitgelegd.

3.4 Verificatie van de volgende schakel query

Indien de HM een verklaring van een MR ontvangt met een obligation dan MOET deze vervolgvraag gesteld worden. Deze XACMLAuthzDecisionQuery wordt gesteld via een SOAP backchannel met een XACML query in de body van het bericht.

Deze query lijkt op de XACMLAuthzDecisionQuery van de eerste vraag (zie paragraaf 3.1).

Afwijkingen t.o.v. de query zoals beschreven in paragraaf 3.1 :

- @Destination: SAML: URL van de machtigingenregister waarop het bericht wordt aangeboden. MOET overeenkomen met de metadata van het machtigingenregister. Deze URL wordt ontvangen in de response van voorgaand machtigingenregister (of indien deze ontbreekt aan de uitvoerende natuurlijk persoon gevraagd).
- Request -> Subject
    - eHerkenning: MOET ActingEntityID bevatten. Zie paragraaf 5.1.1.
    - MOET EntityConcernedID bevatten. (zie paragraaf 5.1.6)
    - MOET Intermediates attribuut bevatten als ontvangen in de response van voorgaand machtigingenregister

3.5 Verificatie van de volgende schakel response

Betreffende MR geeft hierop een response die lijkt op de response zoals beschreven in paragraaf 3.2.1.

Afwijkingen t.o.v. de response zoals beschreven in paragraaf 3.2 :

- Signature :
  eHerkenning: MOET de elektronische handtekening van het machtigingenregister over deze hele assertion bevatten. Zie “Koppelvlakspecificatie HM-DV”, paragraaf 3.2 voor specifieke eisen.
- XACMLAuthz Decision Statement | Request | Subject
  eHerkenning: Bevat het XACMLAuthzDecisionQuery Subject element met alle in de vraag genoemde Attributen inclusief het ActingEntityID en Intermediates.

4 Dienstencatalogus, Attribuutcatalogus en Metadata

Informatie over het formaat van, het gebruik van en de verspreiding van de dienstencatalogus, de attribuutcatalogus en de metadata is te vinden in het document koppelvlak specificatie DV-HM, in de hoofdstukken:

- 6. Dienstencatalogus
- 7. Attribuutcatalogus
- 8 Metadata

5 Data-elementen

Dit hoofdstuk beschrijft alle voor eHerkenning gedefinieerde XACML data-elementen.
Voor eHerkenning gedefinieerde SAML data-elementen zijn beschreven in het document koppelvlakspecificatie DV-HM.
Gebruikte SAML of XACML elementen die zuiver volgens de SAML of XACML standaard worden gebruikt zijn hier niet opgenomen.

5.1 XACML Attributen

Deze paragraaf beschrijft de data-elementen die als XACML 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.

5.1.1 ActingEntityID

Omschrijving	Een XACML Attribute element met daarin het specifiek pseudoniem van de handelende natuurlijk persoon. Zie paragraaf 9.2.4.2 in het document "Koppelvlakspecificatie DV-HM".. Het element MAG NIET andere attributen (@) bevatten dan hier beschreven.
@AttributeID	urn:nl:eherkenning:1.0:ActingEntityID
@Datatype	http://www.w3.org/2001/XMLSchema#string
AttributeValue	Zie paragraaf 9.2.4.2 in het document "Koppelvlakspecificatie DV-HM".

5.1.2 Action-ID

Omschrijving	Een XACML Attribute element met daarin de action-id. Het element MAG NIET andere attributen (@) bevatten dan hier beschreven.
@AttributeID	urn:oasis:names:tc:xacml:1.0:action:action-id
@Datatype	http://www.w3.org/2001/XMLSchema#string
AttributeValue	MOET de waarde "Authenticate" bevatten

5.1.3 AssertionConsumerServiceIndex

Omschrijving	eHerkenning: Met dit attribuut element laat de afzender weten waar naar welk url het antwoord terug gestuurd moet worden. Een XACML Attribute element gebaseerd op het gelijknamige SAML attribuut met daarin een waarde die MOET overeenkomen met een index van de AssertionConsumerService in de metadata van de eHerkenningsmakelaar. Het element MAG NIET andere attributen (@) bevatten dan hier beschreven.
@AttributeID	urn:nl:eherkenning:1.0:AssertionConsumerServiceIndex
@Datatype	http://www.w3.org/2001/XMLSchema#unsignedShort
@Issuer	EntityID van de eHerkenningsmakelaar. Zie paragraaf 9.2.3 in het document "Koppelvlakspecificatie DV-HM".
AttributeValue	0 t/m 99999

5.1.4 AuthenticationMeansID

Omschrijving	Een XACML Attribute element met daarin het intern pseudoniem van de handelende natuurlijk persoon. Zie paragraaf 9.2.4.1 in het document "Koppelvlakspecificatie DV-HM". Het element MAG NIET andere attributen (@) bevatten dan hier beschreven.
@AttributeID	urn:nl:eherkenning:1.0:AuthenticationMeansID
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID van de authenticatiedienst. Zie paragraaf 9.2.3 in het document "Koppelvlakspecificatie DV-HM".
AttributeValue	Zie paragraaf 9.2.4.1 in het document "Koppelvlakspecificatie DV-HM".

5.1.5 EncryptedAttribute

Omschrijving	Een encrypted aanvullend attribuut waarbij aan ieder encrypted attribuut een uniek Encrypted_DATA_ID wordt toegekend dat gelijk is aan de attribuutbenaming uit de eHerkenning attribuutcatalogus (bijv. urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail). Voor versleuteling MOET gebruik gemaakt worden van het certificaat van de

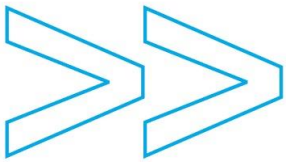
	dienstverlener (ServiceCertificate) dat is opgenomen in de Dienstencatalogus. Per EncryptedAttribute wordt, in het encrypted attribuut, ook een betrouwbaarheidsniveau meegegeven. In het encrypted attribuut wordt een ciphervalue opgenomen. Deze ciphervalue bevat de met de key van de DV uit de dienstencatalogus versleutelde waarde van het gevraagde attribuut.
Voorbeeld	Bijvoorbeeld voor een BusinessName : <saml:Attribute Name= "urn:nl:eherkenning1.3:AdditionalAttribute:BusinessName"> <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:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema- instance" xsi:type="eh:betrouwbaarheidsniveau"> </saml:AttributeValue> </saml:Attribute>

111 ### *5.1.6 EntityConcernedID*

Omschrijving	Een XACML Attribute wat overeenkomt met het SAML attribuut zoals beschreven in het document “Koppelvlakspecificatie DV-HM”, paragraaf 9.3.1

112 ### *5.1.7 LevelOfAssurance*

Omschrijving	Een XACML Attribute element met daarin het minimale betrouwbaarheidsniveau dat door de dienstverlener vereist wordt. Zie paragraaf 9.2.1 in het document “Koppelvlakspecificatie DV-HM”. Het element MAG NIET andere attributen (@) bevatten dan hier beschreven.
@AttributeID	urn:nl:eherkenning:1.0:LevelOfAssurance
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID van de eHerkenningsmakelaar. Zie paragraaf 9.2.3 in het document “Koppelvlakspecificatie DV-HM”.
AttributeValue	Zie paragraaf 9.2.1 in het document “Koppelvlakspecificatie DV-HM”.



113 ### *5.1.8 LevelOfAssuranceUsed*

Omschrijving	Een XACML Attribute element met daarin het betrouwbaarheidsniveau van de geregistreerde bevoegdheid. Wanneer aan de verklaring verschillende registraties ten grondslag liggen en wanneer deze registraties op verschillende betrouwbaarheidsniveaus zijn vastgelegd MOET het hoogste betrouwbaarheidsniveau worden gehanteerd. Zie paragraaf 9.2.1 in het document “Koppelvlakspecificatie DV-HM”. Het element MAG NIET andere attributen (@) bevatten dan hier beschreven.
@AttributeID	urn:nl:eherkenning:1.0:LevelOfAssuranceUsed
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID van het machtigingenregister. Zie paragraaf 9.2.3 in het document “Koppelvlakspecificatie DV-HM”.
AttributeValue	Zie paragraaf 9.2.1 in het document “Koppelvlakspecificatie DV-HM”.

114 ### *5.1.9 ServiceID*

Omschrijving	Een optioneel XACML Attribute element wat overeenkomt met het SAML attribuut zoals beschreven in het document “Koppelvlakspecificatie DV-HM”, paragraaf 9.3.2.

115 ### *5.1.10 Intermediates*

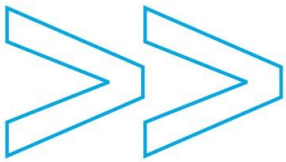
Omschrijving	Een multi valued SAML Attribute element met daarin de Identificerende kenmerken van intermediaire partijen in een ketenmachtiging.
Name	urn:nl:eherkenning:1.7:Intermediates
Type	multi valued, met values van type urn:nl:eherkenning:1.7:IntermediateEntityID:[Name conform document “Koppelvlakspecificatie DV-HM paragraaf 7.1”]
AttributeValue	het identificerend kenmerk van de intermediaire partij conform paragraaf 7.1 van “Koppelvlakspecificatie DV-HM” (het multi valued attribute bevat slechts één waarde).

6 Bijlage voorbeeld berichten

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

6.1 XACMLAuthzDecisionQuery

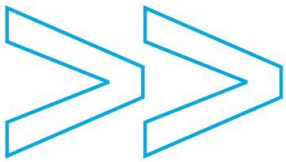
```
<?xml version="1.0" encoding="UTF-8"?>
<xacml-samlp:XACMLAuthzDecisionQuery xmlns:xacml-
samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os" ID=" " Version="2.0" IssueInstant=" "
ReturnContext="true" Destination=" ">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   </saml:Issuer>
        <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>
        <extension base="samlp:RequestAbstractType">
                <attribute name="AssertionConsumerServiceIndex"
DataType="http://www.w3.org/2001/XMLSchema#unsignedShort" Issuer=" ">
                        <AttributeValue>
```



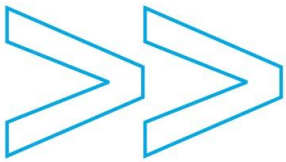
```
        </AttributeValue>
                </attribute>
        </extension>
        <xacml-context:Request xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                <xacml-context:Subject>
                        <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:AuthenticationMeansID"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" ">
                                <xacml-context:AttributeValue>
          </xacml-context:AttributeValue>
                        </xacml-context:Attribute>
                </xacml-context:Subject>
                <xacml-context:Resource>
                        <xacml-context:Attribute AttributeId="urn:nl:eherkenning:1.0:ServiceID"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                <xacml-context:AttributeValue>
          </xacml-context:AttributeValue>
                        </xacml-context:Attribute>
                        <xacml-context:Attribute AttributeId="urn:nl:eherkenning:1.0:LevelOfAssurance"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                <xacml-context:AttributeValue>
          </xacml-context:AttributeValue>
                        </xacml-context:Attribute>
                        <xacml-context:Attribute
AttributeId="urn:nl:eherkenning1.3:AdditionalAttribute:BusinessName"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                <xacml-context:AttributeValue>
                                </xacml-context:AttributeValue>
                        </xacml-context:Attribute>
        </xacml-context:Resource>
                <xacml-context:Action>
                        <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
id" DataType="http://www.w3.org/2001/XMLSchema#string">
                                <xacml-context:AttributeValue>Authenticate</xacml-
context:AttributeValue>
                        </xacml-context:Attribute>
                </xacml-context:Action>
                <xacml-context:Environment>
      </xacml-context:Environment>
        </xacml-context:Request>
</xacml-samlp:XACMLAuthzDecisionQuery>
```

6.2 Response

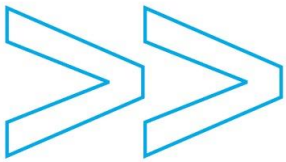
```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" " InResponseTo=" "
Version="2.0" IssueInstant=" " Destination=" ">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   </saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <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>
                <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>
                <saml:Conditions NotBefore=" " NotOnOrAfter=" ">
     </saml:Conditions>
                <saml:Statement xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xacml-
saml:XACMLAuthzDecisionStatementType">
                        <xacml-context:Response xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                                <xacml-context:Result>
                                        <xacml-context:Decision>Permit</xacml-context:Decision>
                                        <xacml-context:Status>
                                                <xacml-context:StatusCode
Value="urn:oasis:names:tc:xacml:1.0:status:ok">
                </xacml-context:StatusCode>
                                        </xacml-context:Status>
                                </xacml-context:Result>
                        </xacml-context:Response>
                        <xacml-context:Request xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
```



```
                                <xacml-context:Subject>
                                        <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:ActingEntityID"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" ">
                                                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
                                        </xacml-context:Attribute>
                                </xacml-context:Subject>
                                <xacml-context:Resource>
                                        <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:ServiceID" DataType="http://www.w3.org/2001/XMLSchema#string">
                                                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
                                        </xacml-context:Attribute>
                                        <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:LevelOfAssurance"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
                                        </xacml-context:Attribute>
                                        <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:LevelOfAssuranceUsed"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
                                        </xacml-context:Attribute>
                                        <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:EntityConcernedID"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
                                        </xacml-context:Attribute>
                                        <xacml-context:ResourceContent>
                                                <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>

                                        <xacml-context:ResourceContent>
                                                </xacml-context:AttributeValue>
                                        </xacml-context:Attribute>
                                    </xacml-context:Resource>
                                    <xacml-context:Action>
                                        <xacml-context:Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
                                                <xacml-context:AttributeValue>Authenticate</xacml-
context:AttributeValue>
                                        </xacml-context:Attribute>
                                    </xacml-context:Action>
                                    <xacml-context:Environment>
                </xacml-context:Environment>
                            </xacml-context:Request>
                        </saml:Statement>
                </saml:Assertion>
</samlp:Response>
```

121