Afsprakenstelsel eHerkenning

Koppelvlakspecificatie HM-AD

Versie 1.7b

INHOUDSOPGAVE

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 HM-AD	1.7b

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
29/03/10	0.8def		T.b.v. proef-impl	Projectbureau
06/09/10	1.0	Vorm wijzigingen en doorvoeren verschillende RFCs	Ter goedkeuring	Projectbureau
17/12/10	1.0a	RFCs verwerkt conform besluit Kernteam 6 dec	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 okt	Definitief	Projectbureau
23/12/11	1.3	RFCs verwerkt conform besluit kernteam 13 dec	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	RFC0186 verwerkt	Definitief	Beheerorganisatie
24/05/13	1.7	RFC0200, RFC0204, RFC0210, RFC0211 verwerkt	Definitief	Beheerorganisatie
27/08/13	1.7a	RFC0225, RFC0226	Definitief	Beheerorganisatie
10/11/13	1.7b	RFC240	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.

1.1 Doel en doelgroep van dit document

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

1.2 Leeswijzer

Het vervolg van dit document ziet er als volgt uit.
Hoofdstuk 2 beschrijft de algemene eisen voor het koppelvlak, de technische informatiebeveiligingseisen en de foutafhandeling.
Hoofdstuk 3 bevat de berichtenspecificaties.
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.
In hoofdstuk 4 wordt daarnaast nog een overzicht gegeven van generieke onderwerpen die in het document “Koppelvlakspecificatie DV-HM” zijn gespecificeerd.
Dit document sluit daarna af met enkele bijlagen waar vanuit de tekst naar verwezen wordt.

1.3 Begrippenlijst, Terminologie en Typologie

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 "gebruiken authenticatiemiddel" en MOET door elke eHerkenningsmakelaar en door elke authenticatiedienst worden geïmplementeerd. De algemene eisen, zoals beschreven in Hoofdstuk 2 van het document "Koppelvlakspecificatie DV-HM" zijn ook op het koppelvlak HM-AD van kracht, met uitzondering van het alternatieve koppelvlak / de alternatieve binding, zoals beschreven in "Koppelvlakspecificatie DV-HM" in paragraaf 2.1 (alternatieve koppelvalk en/of binding) en paragraaf 2.2.2.2 (Alternatieve binding).

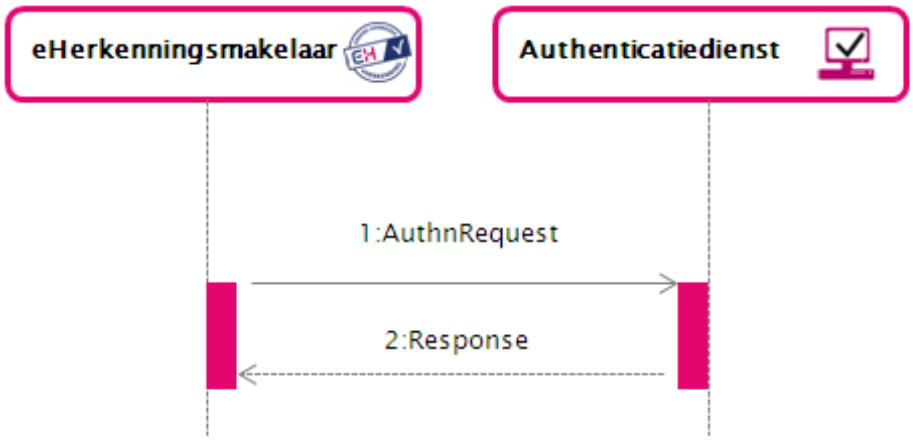
Ook de technisch informatiebeveiligingseisen, zoals geformuleerd in hoofdstuk 3 van het document "Koppelvlakspecificatie DV-HM", zijn van toepassing op het koppelvlak HM-AD.

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

3 Berichtenspecificaties

Dit hoofdstuk beschrijft de berichten van het hier beschreven koppelvlak.

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



Figuur 1: Sequence diagram HM-AD

De specifieke invulling van deze berichten wordt hieronder beschreven. Detailinformatie over de inhoud van velden kan worden gevonden in hoofdstuk 9 van het document “Koppelvlakspecificatie DV-HM”.

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.

3.1 AuthnRequest (1)

Zie paragraaf 5.1 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
@Destination	SAML: URL van de authenticatiedienst waarop het bericht wordt aangeboden. MOET overeenkomen met de metadata van de eHerkenningsmakelaar.
@Consent	eHerkenning: MAG NIET worden opgenomen.

Data element	Invulling
@ForceAuthn	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 ontbreken van de specificatie MAG de authenticatiedienst gebruik maken van een bestaande SSO sessie indien aanwezig.
@IsPassive	eHerkenning: MAG worden opgenomen. Indien IsPassive wordt opgenomen MOET de waarde “false” zijn.
@ProtocolBinding	SAML: MAG NIET worden opgenomen omdat AssertionConsumerServiceIndex binnen eHerkenning is voorgeschreven.
@AssertionConsumerServiceIndex	eHerkenning: Met dit attribuut element laat de afzender weten waar naar welk url het antwoord terug gestuurd moet worden. De waarde van AssertionConsumerServiceIndex MOET overeenkomen met een index van de assertionconsumerservice in de metadata van de eHerkenningsmakelaar.
@AssertionConsumerServiceURL	SAML: MAG NIET worden opgenomen omdat AssertionConsumerServiceIndex binnen eHerkenning is voorgeschreven.
@AttributeConsumingServiceIndex	eHerkenning: De waarde MOET “4” zijn. Dit geeft aan dat het om het in dit document beschreven koppelvlak gaat.
@ProviderName	eHerkenning: MOET overeenkomen met de OrganizationDisplayName van de dienstverlener uit de dienstencatalogus. Zie [eHerkenning – Koppelvlakspecificatie DV-HM 1.2].
Issuer	eHerkenning: MOET de EntityID van de eHerkenningsmakelaar bevatten. Zie paragraaf 9.2.3 van 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 van het document “Koppelvlakspecificatie DV-HM” voor specifieke eisen.
Extensions	eHerkenning: MOET het attribuut ServiceID (met het lange formaat) bevatten. Zie paragraaf 9.2.2 van het document “Koppelvlakspecificatie DV-HM”. 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

Data element	Invulling
	metadata of de vraag aanvullende attributen uitvraagt, dan MOETEN deze hier worden opgenomen. Indien zowel in de vraag als in de metadata aanvullende attributen zijn gedefinieerd, dan MOETEN al deze attributen worden opgenomen. Hiertoe MOET één RequestedAttributes element worden opgenomen met daarin de RequestedAttribute elementen uit de vraag van de dienstverlener. Uitsluitend de attributen die door de betreffende authenticatiedienst 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. 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 9.2.1 van het document “Koppelvlakspecificatie DV-HM”.
Scoping	eHerkenning: MAG NIET worden opgenomen

3.1.1 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. Het koppelvlak voor dit bericht is als onderstaand.

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 Authenticatiedienst waarop het bericht wordt aangeboden.
NameID	eHerkenning: MOET een waarde bevatten, dit MAG NIET het interne pseudoniem of het specifieke pseudoniem zijn. Zie paragraaf 9.2.4 van “Koppelvlakspecificatie DV-HM”.
Issuer	eHerkenning: MOET de EntityID van de eHerkenningsmakelaar bevatten. Zie paragraaf 9.2.3 van “Koppelvlakspecificatie DV-HM”.
Signature	eHerkenning: MOET de elektronische handtekening van de eHerkenningsmakelaar over het hele bericht bevatten. Zie paragraaf 3.2 van “Koppelvlakspecificatie DV-HM” voor specifieke eisen.

3.2 *Response (2)*

Zie paragraaf 5.2 voor een voorbeeld.

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	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 de authenticatiedienst bevatten. Zie paragraaf 9.2.3 van het document “Koppelvlakspecificatie DV-HM”. De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
Signature	eHerkenning: MOET de elektronische handtekening van de authenticatiedienst over het hele bericht bevatten. Zie paragraaf 3.2 van het document “Koppelvlakspecificatie DV-HM” 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 **Error! Reference source not found.**. StatusDetail MAG NIET worden opgenomen.

Data element	Invulling
Assertion	eHerkenning: MOET een verklaring over de authenticatie bevatten (zie de volgende paragraaf).

55 ### *3.2.1 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 authenticatiedienst bevatten. Zie paragraaf9.2.3 van het document "Koppelvlakspecificatie DV-HM". De attributen NameQualifier, SPNameQualifier, Format en SPProviderID MOGEN NIET worden opgenomen.
	Signature	eHerkenning: MAG NIET worden opgenomen
	Subject	eHerkenning: MOET in het geval van vertegenwoordiging een NameID element bevatten met daarin het intern pseudoniem van de uitvoerende natuurlijk persoon. Zie paragraaf 9.2.4.1 van het document "Koppelvlakspecificatie DV-HM". MOET in het geval van handelen door een burger/consument of een beroepsbeoefenaar een NameID element bevatten met daarin het specifiek pseudoniem van de uitvoerende natuurlijk persoon. Zie paragraaf 9.2.4.2 van het document "Koppelvlakspecificatie DV-HM". Het NameID element MOET het attribuut NameQualifier bevatten met daarin het OIN van het KvK nummer van de authenticatiedienst. Zie Zie paragraaf 8.1 van het document "Koppelvlakspecificatie DV-HM". 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

Data element		Invulling
		bevatten. Het AuthnContext element MOET een AuthnContextClassRef element met daarin het betrouwbaarheidsniveau waarop de authenticatie heeft plaatsgevonden en een AuthenticatingAuthority element met daarin het OIN van het KvK nummer van de authenticatiedienst. Zie paragraaf Zie paragraaf 9.2.1 van het document “Koppelvlakspecificatie DV-HM”. respectievelijk paragraaf Zie paragraaf 9.1 van het document “Koppelvlakspecificatie DV-HM”. In het geval van proxying MOET het AuthenticatingAuthority element zijn gevuld met een uniek identificerend kenmerk van de partij die de authenticatie heeft uitgevoerd. Andere attributen en elementen MOGEN NIET worden opgenomen.
	Optioneel Attribute-Statement	eHerkenning: MOET worden opgenomen wanneer de StatusCode 'Success' is. MAG anders NIET worden opgenomen. Wanneer deze wordt opgenomen gelden de volgende eisen: • Representation MOET worden opgenomen. Zie paragraaf 9.3.6 van document “Koppelvlakspecificatie DV-HM” • AuthorizationRegistryID MAG worden opgenomen. Zie paragraaf 9.3.4 van document “Koppelvlakspecificatie DV-HM” • In geval van geen vertegenwoordiging (dus handelen door een burger/consument of een beroepsbeoefenaar) MOET precies één attribuut worden opgenomen dat de dienstafnemer identificeert. Dit attribuut MOET overeenkomen met één van de mogelijke dienstafnemers die dienst kan afnemen. • Wanneer aanvullende attributen door de herkenningsmakelaar zijn gevraagd, deze attributen beschikbaar zijn en voor deze attributen door uitvoerende natuurlijk persoon user consent is verleend (tijdens authenticatie of via eerder gegeven consent) MOGEN deze, uitsluitend wanneer de StatusCode ‘Success’is, hier worden opgenomen. Aanvullende attributen MOETEN worden opgenomen als EncryptedAttribute 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

Data element		Invulling
		ciphervalue bevat de met de key van de DV uit de dienstencatalogus versleutelde waarde van het gevraagde attribuut. Bijvoorbeeld voor een ActingPersonName : <saml:Attribute Name= "urn:nl:eherkenning1.3:AdditionalAttribute: ActingPersonName "> <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> • Andere AttributeStatement elementen MOGEN NIET worden opgenomen.

56

4 Dienstencatalogus, Attribuutcatalogus, Metadata en data-elementen

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
- 9 Data-elementen

5 Bijlage voorbeeld berichten

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

5.1 AuthnRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" " Version="2.0"
IssueInstant=" " Destination=" " ForceAuthn="true" AssertionConsumerServiceIndex=" "
AttributeConsumingServiceIndex="4" 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"
IsRequired=”false”/>
```

```
105             </ehsamlp:RequestedAttributes>
106         </samlp:Extensions>
107         <samlp:RequestedAuthnContext Comparison="minimum">
108                 <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
109     </saml:AuthnContextClassRef>
110         </samlp:RequestedAuthnContext>
111 </samlp:AuthnRequest>
```

112 *5.2 Response*

```
113 <?xml version="1.0" encoding="UTF-8"?>
114 <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" " InResponseTo=" "
115 Version="2.0" Destination=" " IssueInstant=" " Consent=" ">
116         <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
117    </saml:Issuer>
118         <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
119                 <ds:SignedInfo>
120                         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
121 c14n#"/>
122                         <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
123 more#rsa-sha256"/>
124                         <ds:Reference URI=" ">
125                                 <ds:Transforms>
126                                         <ds:Transform
127 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
128                                         <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
129 c14n#"/>
130                                 </ds:Transforms>
131                                 <ds:DigestMethod
132 Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
133                                 <ds:DigestValue>
134             </ds:DigestValue>
135                         </ds:Reference>
136                 </ds:SignedInfo>
137                 <ds:SignatureValue>
138       </ds:SignatureValue>
139                 <ds:KeyInfo>
140                         <ds:KeyName>
141                 </ds:KeyName>
142                 </ds:KeyInfo>
143         </ds:Signature>
144         <samlp:Status>
```

```
145                 <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">
146       </samlp:StatusCode>
147          </samlp:Status>
148          <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID=" "
149 IssueInstant=" ">
150                 <saml:Issuer>
151       </saml:Issuer>
152                 <saml:Subject>
153                       <saml:NameID NameQualifier=" ">
154          </saml:NameID>
155                       <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
156                             <saml:SubjectConfirmationData Recipient=" " NotOnOrAfter=" ">
157             </saml:SubjectConfirmationData>
158                       </saml:SubjectConfirmation>
159                 </saml:Subject>
160                 <saml:Conditions NotBefore=" " NotOnOrAfter=" ">
161                       <saml:AudienceRestriction>
162                             <saml:Audience>
163             </saml:Audience>
164                       </saml:AudienceRestriction>
165                 </saml:Conditions>
166                 <saml:AuthnStatement AuthnInstant=" ">
167                       <saml:AuthnContext>
168                             <saml:AuthnContextClassRef>
169             </saml:AuthnContextClassRef>
170                       </saml:AuthnContext>
171                 </saml:AuthnStatement>
172                 <saml:AttributeStatement>
173
174                       <saml:EncryptedAttribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
175                             <xenc:EncryptedData mlns:xenc=http://www.w3.org/2001/04/xmlenc#
176 Id="Encrypted_DATA_ID" Type="http://www.w3.org/2001/04/xmlenc#Element">
177                                   <xenc:EncryptionMethod Algorithm=
178 "http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
179                                   <ds:KeyInfo>
180                                         <ds:Keyname> </ds:Keyname>
181                                   </ds:KeyInfo>
182                                   <xenc:CipherData>
183                                         <xenc:CipherValue>   </xenc:CipherValue>
184                                   </xenc:CipherData>
185                             </xenc:EncryptedData>
186                       </saml:EncryptedAttribute>
```

```
                    </saml:AttributeStatement>
                </saml:Assertion>
</samlp:Response>
```