

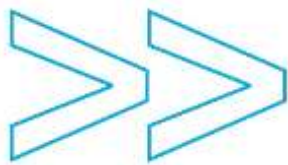


Afsprakenstelsel eHerkenning

Testen voor deelnemers

Versie 1.7b





INHOUDSOPGAVE

Afsprakenstelsel eHerkenning	1
Testen voor deelnemers	1
1 Inleiding	4
1.1 Doel en doelgroep van dit document.....	4
1.2 Leeswijzer	4
1.3 Begrippenlijst	4
1.4 Terminologie	4
2 Testen voor deelnemers	5
2.1 Metadata, authenticatiemiddelen en machtigingen voor testen	5
3 Monitoren	6
4 Simulatortest – Conformiteit	6
4.1 Simulatortest testcases Algemeen	6
4.2 Simulatortest testcases eHerkenningmakelaar	8
4.3 Simulatortest testcases Authenticatiedienst.....	19
4.4 Simulatortest testcases Machtigingenregister	26
5 Simulatortest Checklist.....	32
6 Ketentest – Interoperabiliteit	39
6.1 Randvoorwaardes ketentest testcases	39
6.2 Ketentest testcases eHerkenningmakelaar	39
6.3 Ketentest testcases Authenticatiedienst.....	45
6.4 Ketentest testcase Machtigingenregister	49
7 Ketentest Checklist.....	53



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 – Testen voor deelnemers	1.7b

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
09/06/10	1.0		Definitief	Projectbureau
17/12/10	1.0a	Geen wijzigingen	Definitief	Projectbureau
17/06/11	1.1	Aangepast in lijn met besluit kernteam 31 mei	Definitief	Projectbureau
12/11/11	1.2	Geen wijzigingen	Definitief	Projectbureau
02/02/12	1.3	RFCs 101 t/m 145 verwerkt	Definitief	Projectbureau
28/04/12	1.4	Geen wijzigingen	Definitief	Beheerorganisatie
04/07/12	1.4a	RFC's 146 t/m 163 (release 1.4) verwerkt	Definitief	Beheerorganisatie
12/07/12	1.5	RFCs verwerkt conform besluit kernteam 26 juni	Definitief	Beheerorganisatie
01/04/13	1.6	RFC0197 verwerkt	Definitief	Beheerorganisatie
31/05/13	1.7	RFC0188, RFC0200, RFC0204, RFC0210, RFC0211 verwerkt	Definitief	Beheerorganisatie
27/08/13	1.7a	RFC0225, RFC0226 verwerkt	Definitief	Beheerorganisatie
10/11/13	1.7b	RFC0245 verwerkt	Definitief	Beheerorganisatie

DISTRIBUTIE

Datum	Distributie	Versie
	Kernteam, 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 testen en monitoren binnen het net werk van eHerkenning, voor deelnemers. Dienstverleners vallen buiten de scope van dit document, zij worden doorverwezen naar het document [eHerkenning – Testen voor dienstverleners] en het testonderdeel in het document [eHerkenning – Operationeel handboek].

Dit document is een dynamisch onderdeel van het afsprakenstelsel, dat wil zeggen dat dit document door de tijd zal blijven groeien. Zodra er nieuwe testcases, issues enzovoorts zijn zullen zij worden toegevoegd aan dit document.

1.2 Leeswijzer

Het document begint met een algemene beschrijving van het hoe en waarom van testen. Vervolgens wordt in het kort de optie tot monitoren van de staat van het netwerk beschreven. Tenslotte worden de concrete toetredingstesten, checklists en testcases beschreven.

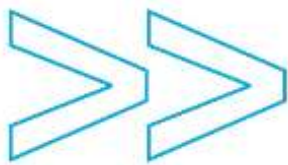
Bij iedere testcase is in de “Notities/Opmmerkingen” een referentie naar RFC nummers en eventueel een korte toelichting opgenomen waarin wordt ingegaan op specifieke aandachtspunten voor de betreffende testcase in verband met impact vanuit in deze release doorgevoerde RFC's.

1.3 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.

1.4 Terminologie

Ter wille van de leesbaarheid van de tekst is overal ‘hij’ geschreven waar ‘hij of zij’ bedoeld wordt. Overal waar in dit document nieuw of nieuwe wordt gebruikt om een toetredend systeem aan te duiden, worden ook nieuwe releases van een bestaand systeem bedoeld.



2 Testen voor deelnemers

Om te zorgen dat nieuwe releases en nieuwe toetredingen van deelnemers zo goed mogelijk verlopen, is het vereist dat de functionaliteit hiervan wordt getest. Er zijn in deze versie van het afsprakenstelsel twee soorten testen te onderscheiden, te weten: een set simulatortesten, en een set ketentesten.

De simulatortesten wordt uitgevoerd met de eHerkenning simulator, een instrument dat berichten verzendt en de antwoorden beoordeelt op validiteit volgens het afsprakenstelsel. De focus van deze test is conformiteit aan het afsprakenstelsel.

De ketentesten vindt plaats in een apart netwerk van systemen, ieder in een eigen OTAP A-omgeving (A-systemen in het vervolg). In de ketentest worden ketens van HM, AD en MR getest door elke mogelijke combinatie van systemen te testen. De focus van de ketentesten is interoperabiliteit van de verschillende systemen van de deelnemers.

Er wordt van de deelnemers verwacht dat zij, voordat ze hun systemen in productie nemen, deze uitgebreid testen. Voor de bovengenoemde testen zijn testcases opgesteld en is een checklist beschikbaar waarop de deelnemers het resultaat van de testen kunnen noteren. De beheerorganisatie ontvangt voor toetreding van de deelnemers de ingevulde checklists. Aan de hand van de checklists zal de beheerorganisatie adviseren over de toelating en/of de duur van het verdere traject.

Zijn alle testen volgens de deelnemer naar behoren verlopen dan zal de beheerorganisatie over gaan tot het uitvoeren van toetredingstesten. De testen zijn feitelijk een, door de beheerorganisatie uit te voeren, controle op de zelfverklaring van de toetredende partij. De beheerorganisatie gebruikt de zelfde testcases, het zelfde test netwerk en de zelfde test-tooling. Aan de hand van de uitkomst van de toetredingstesten wordt bepaald of er nog technische issues openstaan die voor de toetreding moeten worden opgelost.

De beheerorganisatie zal in samenspraak met de deelnemers periodiek penetratietesten uit laten voeren door een gespecialiseerde partij. De scope van deze testen zal per keer worden bepaald. Voor het uitvoeren van een penetratietest is altijd toestemming nodig van de deelnemers die getest gaan worden. Deze tests hebben dus een status aparte ten opzichte van de overige testen.

2.1 Metadata, authenticatiemiddelen en machtigingen voor testen

Om het testen mogelijk te maken moet de toetreder de metadata van de te testen systemen doorgeven aan de beheerorganisatie. De beheerorganisatie zal de metadata toevoegen aan de metadata van de bestaande A-systemen, en de verzamelde metadata publiceren. Toetreders én deelnemers verwerken deze metadata periodiek volgens standaard procedures voor de A-systemen.

Om de ketentesten mogelijk te maken is het noodzakelijk dat alle partijen in het netwerk authenticatiemiddelen en machtigingen van elkaar hebben. Een nieuwe toetredende partij moet dus bij de andere partijen middelen en machtigingen aanvragen en de toetredende partij moet (indien van toepassing) middelen en machtigingen uitgeven aan de andere deelnemers.

De procedure rond metadata wordt verder beschreven in het document [Operationeel Handboek].



3 Monitoren

Het is mogelijk om de status van het netwerk te monitoren door periodiek automatisch testcases af te werken. Hiervoor kunnen deelnemers zelf tooling ontwerpen of aanschaffen.

De beheerorganisatie monitort zelf de staat van het netwerk (nog) niet actief. Mochten deelnemers het netwerk actief willen monitoren, dan moeten zij in ieder geval het in de dienstencatalogus vermelde monitoring OIN hiervoor gebruiken (99999900000002).

4 Simulatortest – Conformiteit

In deze test wordt conformiteit aan het afsprakenstelsel getest door de systemen van deelnemers te koppelen aan de simulator.

De deelnemer dient, voor de relevante rollen en niveaus, de alle testcases te doorlopen. De ervaringen en resultaten dienen te worden genoteerd in de checklist uit hoofdstuk 5. Hierbij moet de deelnemer het relevante buildnummer van het geteste systeem te noteren. Pas als de beheerorganisatie de simulatorchecks als voldoende beoordeelt (mede op basis van aangeleverde ervaringen en resultaten), zal de verklaring in overweging worden genomen en worden op basis van deze checklist de testen gecontroleerd.

Mocht de beheerorganisatie toch nog discrepanties tegenkomen zal de deelnemer verzocht worden deze op te lossen en de relevante testcases opnieuw uit te voeren. Hierna moet een deelnemer de checklist opnieuw indienen, waarna het proces opnieuw start.

De beheerorganisatie zal naast de hier beschreven tests ook de vrijheid behouden meer te testen dan is beschreven. Deze tests zullen gaan over conformiteit aan de SAML / XACML / WS standaarden en best practices op het gebied van it-security. Mocht hieruit blijken dat er nog fouten in de systemen zitten zal de beheerorganisatie direct contact met de deelnemer zoeken en een traject afspreken waarin de deelnemer de fouten kan herstellen.

4.1 Simulatortest testcases Algemeen

Deze testcases zijn voor alle rollen gelijk. Sommigen gaan automatisch en zelfs random. Anderen zullen moeten worden aangevinkt om getest te worden. De algemene testen zijn op te delen in drie soorten, te weten:

Random value swaps, gebeuren automatisch.

Deze tests zijn onderdeel van het normale gedrag van de simulator, bij elk bericht bepaalt de simulator (random) welke type waarde te gebruiken. Alle door de simulator gebruikte waarden moeten worden geaccepteerd. Alle weigeringen van de te testen systemen zijn een fail.

- Boolean values worden random gegenereerd als 0/false en 1/true.
De simulator kiest voor elke boolean wat voor value soort te gebruiken. Alle verschillende soorten values moeten worden geaccepteerd.



- 100 • Simulator signingcertificaten worden random gewisseld.
101 De simulator heeft meerdere certificaten in de metadata zitten. De simulator kiest bij elk bericht zelf een
102 certificaat. Alle certificaten van de simulator die in de metadata staan moeten worden geaccepteerd.
- 103 • Twee simulator oin's, worden random gewisseld.
104 De gesimuleerde HM/AD en MR hebben twee oins in de metadata. De simulator kiest bij elk bericht een
105 oin om te gebruiken. Alle oins van de simulator die in de metadata staan moeten worden geaccepteerd.
- 106 • Meerdere dienstverlener ServiceID, worden random gewisseld.
107 De gesimuleerde DV heeft meerdere ServiceIDs. De simulator kiest bij elk bericht van de gesimuleerde
108 dienstverlener een te gebruiken ServiceID, alle ServiceIDs uit de dienstencatalogus moeten worden
109 geaccepteerd.
- 110 **Error parsing checks, moeten geforceerd worden.**
- 111 Systemen moeten berichten valideren op een aantal vlakken. Om te controleren of de afhankelijkheden ook
112 gevalideerd worden, zijn er geforceerde errors in de simulator gebouwd. Wordt het bericht als valide
113 aangemerkt is dit een fail.
- 114 • Genereren van een verkeerde digest.
115 Maak een goed bericht op de simulator, voor de te testen rol, en druk op generate message. In plaats
116 van meteen post request te drukken, voeg je een karakter toe aan het bericht. Zorg ervoor dat dit op een
117 plek gebeurt waar geen andere functies mee breken. Hierdoor klopt de digest van het bericht niet meer.
118 Klik nu op "postg request" om het bericht te versturen.
119 ○ Als het bericht geaccepteerd wordt is dit een fail.
120 ○ Als de ontvanger het proces niet direct afbreekt is dit een fail.
- 121 • Genereren van een keyname-key mismatch.
122 ○ Vink het bijbehorende vakje aan om een misvormd bericht met een keyname-key mismatch te
123 sturen.
124 ○ Als het bericht geaccepteerd wordt is dit een fail.
125 ○ Als de ontvanger het proces niet direct afbreekt is dit een fail.
- 126 **Missing fields checks, handmatig 1 voor 1 de elementen uitvinken/leeg laten**
- 127 Essentiële elementen mogen niet ontbreken, als een verplicht element ontbreekt moet het bericht geweigerd
128 worden. Als een optioneel element ontbreekt moet het bericht geaccepteerd worden. Alle andere
129 gedragingen zijn een fail. De checks afvinken op de checklists.
- 130 • Voor elk te testen rol, berichten genereren waar 1 voor 1 een essentieel element (eventueel attribuut)
131 ontbreekt. Systemen moeten berichten waar een essentieel element in ontbreekt verwerpen en berichten
132 waar een optioneel element ontbreekt accepteren.
- 133 • Voor elk te testen rol, berichten genereren waar 1 voor 1 een essentieel element leeg gelaten word.
134 Systemen moeten berichten waar een element leeg is verwerpen.



4.2 Simulatortest testcases eHerkenningmakelaar

Deze testcases zijn bedoeld om de conformiteit van een toetredende eHerkenningmakelaar, of een nieuwe release van een bestaande HM te testen. De simulator genereert berichten voor de HM die aan de test onderworpen wordt.

Doel:	Het testen van conformiteit aan het afsprakenstelsel van een eHerkenningmakelaar (HM).
Samenvatting:	De simulatortesten controleren de conformiteit aan het afsprakenstelsel, allereerst volgens de normale flow en ten slotte aan de abnormale flow.

Testcase naam:	01 – HM – Normale flow – Toont de HM het juiste lijstje AD's bij een authenticatievraag.
Beschrijving:	De normale flow afhandeling voor een HM. Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van de berichten van en naar een HM.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV.2. Controleer de lijst met AD's die door de HM wordt getoond. Noteer de bevindingen in de checklist.
Succes:	De test is een succes als alle AD's die opgenomen zijn in de acceptatie metadata worden getoond.
Requirements:	<ul style="list-style-type: none">• De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

Testcase naam:	02 – HM – Verstuurt de HM na keuze AD de juiste vraag aan de AD
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van de berichten van en naar een HM.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV.2. Kies uit de keuze lijst voor de AD's de simulator AD.3. Controleer of de simulator het bericht als correct valideert. Noteer de



	bevindingen in de checklist.
Succes:	De test is een succes als de simulator het bericht van de HM als correct valideert en aangeeft dat er geen fouten zijn.
Requirements:	<ul style="list-style-type: none"> De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

141

Testcase naam:	03 – HM – AD geeft een MR door aan de HM
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van de berichten van en naar een HM.
Stappen:	<ol style="list-style-type: none"> Genereer een bericht vanuit de gesimuleerde AD voor de HM. Zorg dat het bericht naar de gesimuleerde (of andere) MR verwijst door de correcte AttributeValue bij AuthorizationRegistryID in te vullen. (99999900000001 in het geval van de simulator) De AD geeft door aan de HM welke MR gebruikt dient te worden en de HM stuurt de tester meteen door naar de bijbehorende MR. Noteer de bevindingen in de checklist.
Succes:	De test is een succes als de HM het bericht van de AD juist verwerkt en de tester naar de bijbehorende MR stuurt.
Requirements:	<ul style="list-style-type: none"> De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

142

Testcase naam:	04 – HM – AD geeft geen MR door aan de HM
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van de berichten van en naar een HM.



Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht vanuit de gesimuleerde DV voor de HM. 2. Kies de gesimuleerde AD uit de lijst met AD's 3. Verwijder (op de gesimuleerde AD) het vinkje achter saml:AttributeStatement en verstuur een "status:Success" bericht terug naar de HM. 4. Controleer of de HM vraagt om een MR te selecteren. Noteer de bevindingen in de checklist.
Succes:	De test is een succes als de HM het bericht van de AD correct verwerkt, de melding geeft dat de MR niet bekend is en de lijst met MR's presenteert.
Requirements:	<ul style="list-style-type: none"> • De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

143

Testcase naam:	05 – HM – Berichten tussen HM en MR en correcte afhandeling van de machtiging.
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van de berichten van en naar een HM.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht vanuit de gesimuleerde DV voor de HM. 2. Kies de gesimuleerde AD uit de lijst. 3. Verwijder (op de gesimuleerde AD) het vinkje voor saml:AttributeStatement en verstuur een "status:Success" bericht terug naar de HM. 4. De HM meldt dat er geen MR bekend is en presenteert de lijst met MR's. 5. Selecteer uit de lijst met MR's de simulator MR. 6. Stuur van de simulator MR een correct "xacml-context:Decision Permit" bericht naar de HM terug. 7. Controleer of de simulator het van de HM ontvangen bericht als correct valideert. Noteer de bevindingen in de checklist.
Succes:	De test is een succes als de gesimuleerde MR het bericht van de HM correct valideert.



Requirements:	<ul style="list-style-type: none">• De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

144

Testcase naam:	06 – HM – Mislukte authenticatie
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van de berichten van en naar een HM.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht vanuit de gesimuleerde DV voor de HM.2. Kies de gesimuleerde AD uit de lijst3. Forceer een mislukte authenticatie door het vakje voor “fail” aan te vinken en op refresh te klikken. Stuur het bericht naar de HM.4. Controleer op de HM of het annuleren correct wordt afgehandeld en de gebruiker de keuze krijgt om opnieuw een AD te kiezen. Noteer de bevindingen in de checklist.
Succes:	<p>De test is een succes als de HM correct reageert op het “AuthnFailed” bericht en de HM de gebruiker in stap 4 op de hoogte stelt van het feit dat er een fout is opgetreden (zonder in te gaan op de aard van de fout).</p> <p>De HM vraagt de gebruiker vervolgens om een nieuwe keuze voor een AD te maken.</p>
Requirements:	<ul style="list-style-type: none">• De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	
RFC0102/RFC0136: controle toegevoegd dat de eindgebruiker correct wordt geïnformeerd over de opgetreden fout.	

145

Testcase naam:	07 – HM – Mislukte controle van de machtiging
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van



	de berichten van een DV naar een HM.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht vanuit de gesimuleerde DV voor de HM. 2. Kies de simulator AD uit de lijst. 3. Laat de simulator AD een "status:Success" bericht terugsturen naar de HM (met daarin voer de locatie van de simulator MR in bij "@Destination"). 4. Ga door naar de gesimuleerde MR en zorg dat deze reageert met een "xacml-context:Decision Deny" bericht, door bij "xacml-context:Decision" Permit te vervangen door Deny.
Succes:	De test is een succes als de HM correct reageert op het bericht dat de controle van de machtiging niet gelukt is. En de gesimuleerde DV een correct "AuthnFailed" bericht ontvangt.
Requirements:	<ul style="list-style-type: none"> • De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

146

Testcase naam:	08 – HM – Annuleren replay
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van een HM.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht vanuit de gesimuleerde DV voor de HM. 2. Kies een (niet gesimuleerde) AD (met annuleer functie) uit de lijst. 3. Annuleer de authenticatie op de AD, je keert terug naar de HM 4. Selecteer een nieuwe / dezelfde AD
Succes:	De test is een succes als de HM correct reageert op het annuleren van de authenticatie en de gebruiker een andere AD laat kiezen (en dan ook daadwerkelijk doorstuurt).
Requirements:	<ul style="list-style-type: none"> • De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	



147

Testcase naam:	09 – HM – ForceAuthn=false
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van een HM.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht vanuit de gesimuleerde DV voor de HM. Zet het attribuut ForceAuthn (@ForceAuthn) op false/0.2. Selecteer de gesimuleerde AD.3. Controleer of in het door de gesimuleerde AD ontvangen bericht het attribuut ForceAuthn op false/0 staat.
Succes:	De test is een succes als de HM de waarde van het attribuut ForceAuthn correct doorgeeft.
Requirements:	<ul style="list-style-type: none">• De te testen HM en de simulator moeten de meest recente acceptatie metadata verwerkt hebben.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

148

Testcase naam:	10 – HM – Correcte naamsvermelding dienstencatalogus
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van een HM.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht vanuit de gesimuleerde DV voor de HM.2. De HM dient als dienst te vermelden: “eHerkenning Testdienst wil u herkennen voor Testdienst niveau X”. waarbij X het nummer van het gevraagde betrouwbaarheidsniveau is (bijv. 2 voor Eh2).
Succes:	<p>De test is een succes als de HM de informatie uit de dienstencatalogus correct doorgeeft in het formaat “<OrganizationDisplayName> wil u herkennen voor <ServiceName> (1) Kies de aanbieder van uw eHerkenningsmiddel Let op! U heeft een eHerkenningsmiddel van minimaal betrouwbaarheidsniveau <eH niveau gebaseerd op AuthnContextClassRef> nodig.”</p>



Requirements:	<ul style="list-style-type: none">• De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

149

Testcase naam:	11 – HM – Niet bestaande ServiceID
Beschrijving:	Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van een HM.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht vanuit de gesimuleerde DV voor de HM. Vervang hierbij het ServiceID door een niet bestaand ServiceID (het attribuut AttributeConsumingServiceIndex)2. Een niet bestaand ServiceID wordt beschouwd als een foutief opgemaakt bericht en moet worden afgehandeld conform paragraaf 4.2 van [Koppelvlakspecificatie DV-HM]:<ul style="list-style-type: none">• Proces direct afbreken• Handelend natuurlijk persoon melden dat een onherstelbare fout is opgetreden• Fout in onderzoek nemen en verzender op de hoogte stellen dat een fout is opgetreden. Verzender moet de fout in onderzoek nemen.
Succes:	De test is een succes als de HM de niet bestaande ServiceID correct afhandelt.
Requirements:	<ul style="list-style-type: none">• De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	
RFC0102/RFC0136: controle toegevoegd dat de eindgebruiker correct wordt geïnformeerd over de opgetreden fout.	

150

Testcase naam:	12 – HM – Ondersteunen meerdere koppelvlakken
----------------	---



Beschrijving:	Controleert correcte ondersteuning van meerdere koppelvlakken door een HM.
Stappen:	1. Herhaal de hierboven beschreven testcases 01 t/m 11 en 13 maar gebruik hierbij een andere, door de HM gepubliceerde, versie van het koppelvlak door een andere versie van de Simulator te gebruiken. (gebruik bijv. simulator 1.5 in plaats van simulator 1.7)
Succes:	De test is een succes als de testcases succesvol worden afgerond.
Requirements:	<ul style="list-style-type: none"> De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. De HM moet in de metadata gepubliceerd hebben dat meerdere koppelvlakken ondersteund worden. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0113, RFC0130: Deze testcase is geïntroduceerd om het testen van de ondersteuning van meerdere koppelvlakken door HM's mogelijk te maken.	

151

Testcase naam:	13 – HM – Controle van de betrouwbaarheidsniveaus
Beschrijving:	HM controleert dat bij verschillend betrouwbaarheidsniveau van authenticate en machtiging het laagste niveau beide wordt gebruikt in het antwoord aan de DV (zwakste schakel principe) en dat het betrouwbaarheidsniveau voldoet aan de vraag van de DV.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht vanuit de gesimuleerde DV voor de testen HM. Vervang hierbij het AuthnContextClassRef met betrouwbaarheidsniveau 2. 2. Kies de simulator AD uit de lijst bij de HM 3. Genereer een antwoord vanuit de simulator AD. Gebruik het betrouwbaarheidsniveau 1 in AuthnContextClassRef. 4. HM moet het proces afbreken en een AuthnFailed bericht aan de DV terugsturen. 5. Genereer een bericht vanuit de gesimuleerde DV voor de testen HM. Vervang hierbij het AuthnContextClassRef met betrouwbaarheidsniveau 2. 6. Kies de simulator AD uit de lijst bij de HM 7. Genereer een antwoord vanuit de simulator AD. Gebruik het betrouwbaarheidsniveau 2 in AuthnContextClassRef. 8. HM stuurt een bericht naar de simulator MR 9. Genereer een antwoord vanuit de gesimuleerde MR . Gebruik het



	betrouwbaarheidsniveau 1 10. HM moet het proces afbreken en een AuthnFailed bericht aan de DV terugsturen. 11. Genereer een bericht vanuit de gesimuleerde DV voor de testen HM. Vervang hierbij het AuthnContextClassRef met betrouwbaarheidsniveau 2. 12. Genereer een antwoord vanuit de simulator AD. Gebruik het betrouwbaarheidsniveau 3 in AuthnContextClassRef. 13. HM stuurt een bericht naar de simulator MR 14. Genereer een antwoord vanuit de gesimuleerde MR . Gebruik het betrouwbaarheidsniveau 4 bij de LevelOfAssuranceUsed 15. HM stuurt een antwoord naar de gesimuleerde DV. Controleer dat de AuthnContextClassRef betrouwbaarheidsniveau 3 bevat
Succes:	De test is een succes als de alle stappen en controles zijn succesvol afgerond.
Requirements:	<ul style="list-style-type: none"> De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

152

Testcase naam:	14 – HM – Additionele attributen
Beschrijving:	testen van de functionaliteit Attribuutverstrekking.
Stappen:	1. Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV waarbij zowel door de AD als de MR verstrekte additionele attributen worden opgevraagd. 2. Kies uit de keuze lijst voor de AD's de simulator AD. 3. Selecteer uit de lijst met MR's de simulator MR. 4. Controleer in de lijst "decoded attributes" bij "DV / Response Received" of voor de gevraagde additionele attributen een Attribute Value wordt terug gegeven.
Succes:	De test is een succes als de gevraagde additionele attributen worden teruggegeven.



Requirements:	<ul style="list-style-type: none"> De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0114, RFC0124, RFC0155, RFC0211: Deze testcase is geïntroduceerd om het testen van de functionaliteit attribuutverstrekking mogelijk te maken.	

153

Testcase naam:	15 – HM – Ondersteuning ketenmachtiging
Beschrijving:	Controleert correcte ondersteuning van ketenmachtiging
Stappen:	1 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV 2 Kies uit de keuze lijst voor de AD's de simulator AD. 3 Ga door naar de simulator MR 4 Vink het vakje ketenmachtiging aan 5 HM rondt de machtiging proces af een stuurt een antwoord aan de gesimuleerde DV
Succes:	De test is een succes als de gesimuleerde DV geen fouten heeft gemeld
Requirements:	<ul style="list-style-type: none"> De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities/opmerkingen: RFC0188	

154

Testcase naam:	16 – HM – Ondersteunen B2C
Beschrijving:	Controleert correcte ondersteuning van B2C
Stappen:	1 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV, vervang het attribuut AttributeConsumingServiceIndex met waarde "20". In



	<p>de dienstencatalogus staat bij deze service "Pseudo" bij EntityConcernedTypesAllowed</p> <p>2 Kies de simulator AD van de keuze lijst bij de HM</p> <p>3 Vink het vakje "no representation" bij de simulator AD en verstuur een antwoord naar de HM. Het antwoord van de simulator AD bevat een specifieke pseudoniem in plaats van de interne pseudoniem, het attribuut Representation met waarde false en het identificerende attribuut "urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo".</p> <p>4 De HM moet een antwoord met geslaagde autorisatie direct naar de simulator DV te versturen (mag geen bericht naar een MR versturen)</p> <p>5 Controleer dat de simulator DV geen fouten geeft gemeld</p> <p>6 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV, vervang het attribuut AttributeConsumingServiceIndex met waarde "12". In de dienstencatalogus staat bij deze service "KvK" bij EntityConcernedTypesAllowed</p> <p>7 Kies de simulator AD van de keuze lijst bij de HM</p> <p>8 Vink het vakje "no representation" bij de simulator AD en verstuur een antwoord naar de HM. Het antwoord van de simulator AD bevat een specifieke pseudoniem in plaats van de interne pseudoniem, het attribuut Representation met waarde false en het identificerende attribuut "urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo".</p> <p>9 De HM moet een antwoord met authn failed direct naar de simulator DV te versturen (mag geen bericht naar een MR versturen)</p> <p>10 Controleer dat de simulator DV geen fouten geeft gemeld</p>
Succes:	De test is een succes als alle stappen correct zijn afgehandeld
Requirements:	<ul style="list-style-type: none"> De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. De HM moet in de metadata gepubliceerd hebben dat meerdere koppelvlakken ondersteund worden. Tester moet toegang hebben tot de eHerkenning simulator.
<p>Notities/opmerkingen:</p> <p>RFC0204</p>	



Testcase naam:	17 – HM – Ondersteunen SSO
Beschrijving:	Controleert correcte ondersteuning van SSO
Stappen:	<ol style="list-style-type: none"> 1 Verwijder alle cookies van het .sso.eherkenning.nl domain 2 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV 3 De HM moet een keuzelijst van alle ADs en een vakje “Bewaar selectie authenticatiedienst” tonen 4 Kies vervolgens de simulator AD en vink het vakje “Bewaar selectie authenticatiedienst” 5 Controleer dat een cookie met naam _saml_idp en domain .sso.eherkenning.nl wordt gemaakt. Controleer dat de cookie base64 encoded waarde van de EntityID van de simulator AD bewaart, een pad prefix van “/” heeft een secure is. 6 Voltooi de login bij de gekozen AD en kies voor ‘houd mij ingelogd’. Breek na terugkeer bij de DV het proces af en genereer opnieuw een bericht voor de te testen HM vanuit de gesimuleerde DV. 7 Controleer dat de HM direct naar de simulator AD gaat, zonder AD keuze scherm te tonen. 8 Bij de simulator AD, genereer een authn failed bericht. 9 HM moet het AD keuze scherm opnieuw tonen
Succes:	De test is een succes als alle stappen correct zijn afgehandeld
Requirements:	<ul style="list-style-type: none"> • De te testen HM en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities/opmerkingen: RFC0200	

156 4.3 Simulatortest testcases Authenticatiedienst

157 Deze testcases zijn bedoeld om de conformiteit van een toetredende authenticatiedienst, of een nieuwe
 158 release van een bestaande AD te testen. De simulator genereert berichten voor de AD die aan de test
 159 onderworpen wordt.

Doel:	Het testen van de functionaliteit en het voldoen aan het afsprakenstelsel van
-------	---



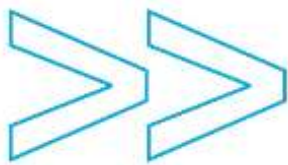
	een authenticatiedienst (AD).
Samenvatting:	Deze testcases beschrijven het testen van een authenticatiedienst. Allereerst wordt de normale flow afhandeling getest, waarna vervolgens uitzonderingen op de normale flow en hun afhandeling getest worden.

160

Testcase naam:	01 – AD – Normale flow
Beschrijving:	De normale flow afhandeling voor een AD. Controleert correcte afhandeling en het voldoen aan het afsprakenstelsel van de berichten van en naar een AD.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht op de gesimuleerde HM voor de AD. Zorg dat dit bericht het betrouwbaarheidsniveau heeft van het test middel dat wordt gebruikt. 2. Doorloop de authenticatie bij de AD. 3. Bij terugkeer op de simulator geeft de simulator aan of het ontvangen bericht correct gevalideerd wordt. Noteer de bevindingen in de checklist. 4. Herhaal indien mogelijk de stappen 1 t/m 3 voor lagere betrouwbaarheidsniveaus. Deze niveaus moeten hetzelfde resultaat opleveren.
Succes:	Bij een geslaagde authenticatie valideert de simulator de respons van de AD correct.
Requirements:	<ul style="list-style-type: none"> • De te testen AD en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet in bezit zijn van een middel voor de te testen AD. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

161

Testcase naam:	02 – AD – Replay normale flow
Beschrijving:	Deze test controleert correcte afhandeling door de AD bij twee opeenvolgende authenticatie vragen van de zelfde gebruiker. De AD moet, bij ForceAuthn=true, elke authenticatie vraag als een nieuwe behandelen.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht op de gesimuleerde HM voor de AD. Zorg dat dit bericht het betrouwbaarheidsniveau heeft van het test middel dat wordt



	<p>gebruikt en dat ForceAuthn op true/1 staat.</p> <ol style="list-style-type: none"> Doorloop de authenticatie bij de AD. Bij het terug komen op de simulator worden stap 1 en 2 (voor een tweede keer) meteen opnieuw doorlopen. Noteer de bevindingen in de checklist.
Succes:	De AD dient hetzelfde te reageren op de tweede authenticatievraag als op de eerste authenticatievraag.
Requirements:	<ul style="list-style-type: none"> De te testen AD en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. Tester moet in bezit zijn van een middel voor de te testen AD. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

162

Testcase naam:	03 – AD – Te hoog authenticatie niveau ten opzichte van het testmiddel
Beschrijving:	Controleert correcte afhandeling door de AD van een authenticatievraag op een hoger niveau dan het gebruikte middel.
Stappen:	<ol style="list-style-type: none"> Genereer een bericht op de gesimuleerde HM voor de AD. Zorg dat dit bericht een hoger betrouwbaarheidsniveau heeft dan het test middel dat wordt gebruikt. Doorloop de authenticatie bij de AD. De AD hoort te melden dat het gevraagde niveau niet voldaan kan worden met het gebruikte middel. Noteer de bevindingen in de checklist. Indien na de melding niet alsnog een geslaagde authenticatie op het juiste niveau plaatsvindt, moet de AD de gebruiker met AuthnFailed terugsturen naar de HM. Noteer de bevindingen in de checklist.
Succes:	Bij een geslaagde authenticatie meldt de AD dat het gebruikte middel niet aan het gevraagde authenticatie niveau voldoet en geeft aan de gebruiker een suggestie voor de vervolghandeling die de persoon naar aanleiding van de fout uit zou kunnen voeren.
Requirements:	<ul style="list-style-type: none"> De te testen AD en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. Tester moet in bezit zijn van een middel, minimaal één niveau lager dan het hoogst mogelijke betrouwbaarheidsniveau van de te testen AD. Tester moet toegang hebben tot de eHerkenning simulator.



Notities / opmerkingen:

RFC0102/RFC0136: controle toegevoegd dat de eindgebruiker correct wordt geïnformeerd over de opgetreden fout.

163

Testcase naam:	04 – AD – Mislukte authenticatie
Beschrijving:	Controleert correcte afhandeling van een mislukte authenticatie door de AD.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht op de gesimuleerde HM voor de AD. Dit bericht moet het niveau hebben van het test middel dat wordt gebruikt.2. Forceer een mislukte authenticatie door:<ol style="list-style-type: none">a. een verkeerde gebruikersnaam te gebruikenb. een verkeerd wachtwoord te gebruikenc. een verkeerd token mee te geven (een verkeerde sms code, een verkeerde token code)3. Herhaal tot alle van toepassing zijnde mogelijkheden bij 2 zijn geprobeerd. Noteer de bevindingen in de checklist.4. Herhaal indien van toepassing 1 t/m 3 ook voor de niveaus lager dan het gebruikte middel.
Succes:	De AD dient in alle gevallen de authenticatie te weigeren. De AD dient in alle gevallen een generieke foutmelding (zoals “uw gebruikersnaam of wachtwoord is verkeerd”) te genereren en moet aan de gebruiker een suggestie geven voor de vervolghandeling die de persoon naar aanleiding van de fout uit zou kunnen voeren.
Requirements:	<ul style="list-style-type: none">• De te testen AD en de simulator moeten de meest recente acceptatie metadata verwerkt hebben.• Tester moet in bezit zijn van een middel voor de te testen AD.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	
RFC0102/RFC0136: controle toegevoegd dat de eindgebruiker correct wordt geïnformeerd over de opgetreden fout.	

164

Testcase naam:	05 – AD – Afgebroken authenticatie
----------------	------------------------------------



Beschrijving:	Controleert correcte afhandeling van een afgebroken authenticatie op de AD.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht op de gesimuleerde HM voor de AD. 2. Klik op de pagina van de AD op annuleren. 3. Controleer of het annuleren succesvol verloopt. Noteer de bevindingen in de checklist.
Succes:	De AD stuurt na het klikken op annuleren terug naar de simulator. De simulator valideert het ontvangen bericht correct. En het bericht bevat de Statuscode: "urn:oasis:names:tc:SAML:2.0:status:AuthnFailed".
Requirements:	<ul style="list-style-type: none"> • De te testen AD en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet in bezit zijn van een middel voor de te testen AD. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

165

Testcase naam:	06 - AD - ForceAuthn=false
Beschrijving:	Controleert correcte afhandeling van een ForceAuthn=false bericht op de AD.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht op de gesimuleerde HM voor de AD. Zet het attribuut ForceAuthn (@ForceAuthn) op false/0. 2. De AD vraagt de gebruiker te authenticeren, of als er nog sessie is: geeft direct een geldig authenticatie bericht terug. 3. Als er bij stap 2 moest geauthenticeerd worden, herhaal stap 1 en 2. Hierna moet een geldig authenticatiebericht teruggestuurd worden.
Succes:	De AD stuurt bij ForceAuthn=false direct een geldig authenticatiebericht terug, mits er een geldige sessie op de AD is.
Requirements:	<ul style="list-style-type: none"> • De te testen AD en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet in bezit zijn van een middel voor de te testen AD. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	



166

Testcase naam:	06 – AD –afhandeling van de “Keep alive” berichten
Beschrijving:	Controleert correcte afhandeling van de “Keep alive” berichten
Stappen:	<ol style="list-style-type: none">1 Verwijder alle cookies van de AD domain2 Genereer een bericht op de gesimuleerde HM voor de AD. Zet het attribuut IsPassive op true/1 en ForceAuthn op false/0.3 De AD geeft een AuthnFailed bericht terug, of als AD geen SSO ondersteuning aanbiedt dan laat de AD de gebruiker zichzelf authenticeren een stuurt een geldige Sucess Response naar de HM4 Genereer een bericht op de gesimuleerde HM voor de AD, binnen 5 minuten. Zet het attribuut isPasive op false/0 en ForceAuthn op true/15 AD laat de gebruiker zichzelf authenticeren en stuurt en Sucess Response naar de HM. Als AD de SSO ondersteunt, wordt ook een cookie op de browser van de gebruiker gezet6 Genereer een bericht op de gesimuleerde HM voor de AD. Zet het attribuut isPasive op true/1 en ForceAuthn op false/07 De AD geeft een Success Response terug, of als AD geen SSO ondersteuning aanbiedt dan laat de AD de gebruiker zichzelf authenticeren een stuurt een geldige Sucess Response naar de HM
Succes:	De test is een succes als alle stappen zonder fouten zijn doorgelopen (noteer als de AD wel/niet SSO ondersteunt)
Requirements:	<ul style="list-style-type: none">• De te testen AD en de simulator moeten de meest recente acceptatie metadata verwerkt hebben.• Tester moet in bezit zijn van een middel voor de te testen AD.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0200	

167

Testcase naam:	08 – AD – Additionele attributen (Optionele test)
Beschrijving:	Optionele test t.b.v. het testen van de functionaliteit Attribuutverstrekking.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht vanuit de simulator DV voor de simulator HM2. Kies de te testen AD uit de keuzelijst bij de simulator HM3. Doorlop de authenticatie bij de AD4. Conroleer dat de simulator HM geen foutmeldingen geeft.



	5. Controleer of alle attributen van de AD worden correct getoond in de "Decrypted attributes lijst bij de simulator HM.
Succes:	De test is een succes als de gevraagde additionele attributen worden teruggegeven.
Requirements:	<ul style="list-style-type: none"> • De te testen AD en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator. • Tester moet een test middel hebben en een lijst van attribuut waarden met de bijhorende consent status dat bij de AD geregistreerd is.
Notities / opmerkingen: RFC0114, RFC0124, RFC0155, RFC 0211: Deze testcase is geïntroduceerd om het testen van de functionaliteit attribuutverstrekking mogelijk te maken.	

168

Testcase naam:	09 – AD – Support B2C (Optionele test)
Beschrijving:	Optionele test t.b.v. het testen van de B2C functionaliteit
Stappen:	<ol style="list-style-type: none"> 1) Genereer een bericht voor de simulator HM vanuit de gesimuleerde DV, vervang het attribuut AttributeConsumingServiceIndex met waarde "20". In de dienstencatalogus staat bij deze service "Pseudo" bij EntityConcernedTypesAllowed 2) Genereer een bericht voor de te testen AD vanuit de gesimuleerde HM 3) Er zijn twee mogelijkheden, AD ondersteunt een Pseudo identificerend kenmerk of niet <ol style="list-style-type: none"> a) Als de AD een Pseudo identificerend kenmerk ondersteunt: <ol style="list-style-type: none"> i) Loop de authenticatie proces bij AD door ii) AD stuurt een Response terug naar de HM iii) Controleer dat de simulator HM geen fouten meldt iv) Controleer in de Response dat de status code Success is, dat de AttributeStatement element aanwezig is met een attribuut urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo en met een attribuut Representation met waarde "false" b) Als de AD geen Pseudo identificerend kenmerk ondersteunt: <ol style="list-style-type: none"> i) Loop de authenticatie proces bij AD door ii) AD stuurt een Response terug naar de HM iii) Controleer dat de simulator HM geen fouten meldt iv) Controleer in de Response dat de status code Success is, dat geen attribuut urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo



	aanwezig is en dat het attribuut Representation waarde "true" heeft
Succes:	De test is een succes als alle stappen zijn zonder fouten doorgelopen (noteer welke variant bij stap 3 getest is, a of b)
Requirements:	<ul style="list-style-type: none"> De te testen AD en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	
RFC0204	

169

170 4.4 Simulatortest testcases Machtigingenregister

171 Deze testcases zijn bedoeld om de conformiteit van een toetredend machtigingenregister, of een nieuwe
 172 release van een bestaande MR te testen. De simulator genereert berichten voor de MR die aan de test
 173 onderworpen wordt.

Doel:	Het testen van de functionaliteit en het voldoen aan het afsprakenstelsel van een machtigingenregister (MR).
Samenvatting:	Deze testcases beschrijven het testen van een machtigingenregister. Allereerst wordt de normale flow afhandeling getest, waarna vervolgens uitzonderingen op de normale flow en hun afhandeling getest worden.

174

Testcase naam:	01 – MR – Normale flow
Beschrijving:	De normale flow afhandeling voor een MR. Controleert correcte afhandeling en het voldoen van de berichten van en naar een MR.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht op de gesimuleerde HM voor de MR. Dit bericht moet het interne pseudoniem bevatten van het testmiddel. 2. Voltooi eventueel de handelingen op de MR voor een correcte machtiging. 3. Controleer het door de simulator ontvangen bericht. Noteer de bevindingen in de checklist.
Succes:	De simulator valideert het ontvangen bericht als correct. Het bericht heeft een "xacml-context:Decision Permit".



Requirements:	<ul style="list-style-type: none"> • De te testen MR en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet in bezit zijn van een testmachtiging bij de MR. • Tester moet het bij de machtiging behorende interne pseudoniem hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
<p>Notities / opmerkingen:</p> <p>RFC0105/RFC0245: bij uitvoeren van stap 3 dient specifiek gecontroleerd te worden dat een EntityConcernedID gevuld wordt met het KvKNr, het vestigingsnummer en het SubdossierNr (die laatste verplicht tot 1/1/2014).</p> <p>Voor het maken van het bericht:</p> <p>@Issuer (ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Subject1_xacml-context:Attribute1-Issuer) vullen met entityID van de eigen AD. Bijvoorbeeld voor KPN AD 1.5 ACC: CONTENT=urn:nl:eherkenning:AD:00000003341158450000:entities:0001</p> <p>AuthenticationMeansID (ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Subject1_xacml-context:Attribute1_xacml-context:AttributeValue1) vullen met InternalPseudonym van de eigen test user. Bijvoorbeeld: CONTENT=a020cf994a5babdddaa7854f715a68c0730b9ec795e94958d2f077ccd566caca</p> <p>ServiceID (ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Resource3_xacml-context:Attribute1_xacml-context:AttributeValue1) vullen met Service overeenkomstig de machtiging. Bijvoorbeeld Simulator Dienstverlener 1, Testdienst niveau 1: CONTENT=urn:nl:eherkenning:DV:99999900000001:services:1</p> <p>LevelOfAssurance (ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Resource3_xacml-context:Attribute3_xacml-context:AttributeValue1) vullen met niveau behorend bij de machtiging. Bijvoorbeeld voor testdienst niveau 1: CONTENT=urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</p>	

175

Testcase naam:	02 – MR – Machtigingsvraag van een te hoog betrouwbaarheidsniveau
Beschrijving:	Controleert op de correcte afhandeling van een machtigingsvraag op een te hoog niveau.
Stappen:	1. Genereer een bericht op de gesimuleerde HM voor de MR. Dit bericht moet het persistent pseudoniem bevatten van het testmiddel. Dit bericht moet



	<p>om een hoger betrouwbaarheidsniveau vragen dan waar het testmiddel op geregistreerd is. (xacml-context:AttributeValue)</p> <ol style="list-style-type: none"> 2. Voltooi eventueel de handelingen op de MR voor een correcte machtiging. 3. Controleer het door de simulator ontvangen bericht. Noteer de bevindingen in de checklist.
Succes:	De simulator valideert het ontvangen bericht als correct. Het door de simulator ontvangen bericht bevat "xacml-context:Decision Deny". De MR brengt de tester op de hoogte van de discrepantie tussen het authenticatieniveau en het machtigingsniveau.
Requirements:	<ul style="list-style-type: none"> • De te testen MR en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet in bezit zijn van een testmachtiging bij de MR. • Tester moet het bij de machtiging behorende persistent pseudoniem hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

176

Testcase naam:	03 – MR – Mislukte controle van de machtiging
Beschrijving:	Controleert op de correcte afhandeling van een mislukte (niet bestaand persistent pseudoniem) controle van de machtiging.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht op de gesimuleerde HM voor de MR. Dit bericht moet een niet bestaand persistent pseudoniem bevatten. 2. De MR dient te melden dat de machtiging niet bestaat. 3. Controleer het door de simulator ontvangen bericht. Noteer de bevindingen in de checklist.
Succes:	De simulator valideert het ontvangen bericht als correct. Het door de simulator ontvangen bericht bevat "xacml-context:Decision Deny".



Requirements:	<ul style="list-style-type: none"> De te testen MR en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. Tester moet in bezit zijn van een testmachtiging bij de MR. Tester moet het bij de machtiging behorende persistent pseudoniem hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

177

Testcase naam:	04 – MR – Niet bestaand ServiceID
Beschrijving:	Controleert op de correcte afhandeling van een niet bestaand ServiceID.
Stappen:	<ol style="list-style-type: none"> Genereer een bericht op de gesimuleerde HM voor de MR. Dit bericht moet een niet bestaand ServiceID en een bestaand persistent pseudoniem bevatten. De MR dient te melden dat de dienst en/of machtiging niet bestaat.
Succes:	De MR weigert berichten met een niet bestaand ServiceID en geeft een bijbehorende foutmelding in het bericht naar de HM.
Requirements:	<ul style="list-style-type: none"> De te testen MR en de simulator moeten de meest recente acceptatie metadata verwerkt hebben. Tester moet in bezit zijn van een testmachtiging bij de MR. Tester moet het bij de machtiging behorende persistent pseudoniem hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0130: Deze RFC kan getest worden door in deze testcase als “niet bestaand ServiceID” een ServiceID te kiezen wat niet meer voorkomt in de, op het moment van testen gepubliceerde, dienstencatalogus maar wat wel bestaan heeft in een eerdere versie van de betreffende dienstencatalogus.	

178

Testcase naam:	05 – MR – Additionele attributen (Optionele test)
----------------	---



Beschrijving:	Optionele test t.b.v. het testen van de functionaliteit Attribuutverstrekking.
Stappen:	<ol style="list-style-type: none"> 1 Genereer een bericht voor de te testen MR vanuit de gesimuleerde HM waarbij door de MR verstrekte additionele attributen worden opgevraagd. 2 Stuur een Response bij de MR 3 Controleer dat de simulator HM geen foutmelding geeft. 4 Controleer of alle attributen van de MR correct worden getoond in de "Decrypted attributes lijst bij de simulator HM.
Succes:	De test is een succes als de gevraagde additionele attributen worden teruggegeven en alle stappen zonder fouten zijn doorgelopen.
Requirements:	<ul style="list-style-type: none"> • De te testen MR en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator. • Tester moet een interne pseudoniem hebben met een machtiging voor één van de simulator diensten bij de MR
Notities / opmerkingen:	
RFC0211	

179

Testcase naam:	06 – MR –Ketenmachtiging (Optionele test)
Beschrijving:	Optionele test t.b.v. het testen van de functionaliteit ketenmachtiging.
Stappen:	<ol style="list-style-type: none"> 1 Genereer een bericht voor de te testen MR vanuit de gesimuleerde HM waarbij een interne pseudoniem van de simulator wordt gebruikt. 2 Kies een ketenmachtiging bij de MR, waar de tweede schakel bij de simulator MR is opgenomen. 3 Controleer dat de gesimuleerde HM geen fouten heeft gemeld een dat een melding geeft dat dit een ketelmachtiging is waar de tweede schakel wordt opgehaald bij de simulator MR. 4 Genereer een bericht voor de simulator MR vanuit de gesimuleerde HM waarbij een interne pseudoniem van de simulator wordt gebruikt. 5 Kies de te testen MR vanuit de "second MR in the chain" keuze lijst een vervolgens druk op de "Refresh"knop 6 Verstuur de bericht naar de simulator HM, en controleer dat de simulator geen fouten heeft gemeld
Succes:	De test is een succes als alle stappen boven zonder fouten zijn uitgevoerd.



Requirements:	<ul style="list-style-type: none">• De te testen MR en de simulator moeten de meest recente acceptatie metadata en dienstencatalogus verwerkt hebben.• Tester moet toegang hebben tot de eHerkenning simulator.• MR moet de benodigde machtigingen registreren.
Notities / opmerkingen:	
RFC0188	

180



5 Simulatortest Checklist

Deze checklist hoort bij de ketentest uit hoofdstuk 4. De deelnemer dient, voor de relevante rollen en niveaus, de alle testcases te doorlopen. De ervaringen en resultaten dienen te worden genoteerd in onderstaande tabel. Hierbij moet de deelnemer het relevante buildnummer van het geteste systeem te noteren. Pas als de beheerorganisatie de simulatorchecks als voldoende beoordeelt (mede op basis van aangeleverde ervaringen en resultaten), zal de verklaring in overweging worden genomen en zal op basis van deze checklist de testen controleren.

Mocht de beheerorganisatie toch nog discrepanties tegenkomen zal de deelnemer verzocht worden dezen op te lossen de volledige testcases opnieuw uit te voeren. Hierna mag een deelnemer de checklist opnieuw indienen, waarna het proces opnieuw start.

Bij resultaat kunnen de waardes S (succes), F (fail), of N (niet getest) en een toelichting worden ingevuld.

Simulatortest Testcases HM	Resultaat	Toelichting
HM – Keyname–Key Mismatch A	S / F / N	
HM – Keyname–Key Mismatch B	S / F / N	
HM – Verkeerde digest	S / F / N	
HM – Missing fields		In deze kolom de uitkomst van de missing fields tests.
@IssueInstant	S / F / N	
@ID	S / F / N	
@AssertionConsumerServiceIndex	S / F / N	
@AttributeConsumingServiceIndex	S / F / N	
@IsPassive	S/F/N	
@ProtocolBinding	S/F/N	
@Consent	S/F/N	
– Issuer	S / F / N	
– RequestedAuthnContext	S / F / N	



- AuthnContextClassRef	S / F / N	
HM – Empty fields		In deze kolom de uitkomst van de empty fields tests.
@IssueInstant	S / F / N	
@ID	S / F / N	
@AssertionConsumerServiceIndex	S / F / N	
@AttributeConsumingServiceIndex	S / F / N	
- Issuer	S / F / N	
@Comparison	S / F / N	
- AuthnContextClassRef	S / F / N	
HM – Specifieke testcases		
01 – HM	S / F / N	
02 – HM	S / F / N	
03 – HM	S / F / N	
04 – HM	S / F / N	
05 – HM	S / F / N	
06 – HM	S / F / N	
07 – HM	S / F / N	
08 – HM	S / F / N	
09 – HM	S / F / N	
10 – HM	S / F / N	
11 – HM	S / F / N	



12 – HM	S / F / N	
13 – HM	S / F / N	
14 – HM	S/F/N	
15 – HM	S/F/N	
16 – HM	S/F/N	
17 – HM	S/F/N	
HM – Random value swaps		
Simulatortest Testcases AD	Resultaat	Toelichting
AD – Keyname–Key Mismatch A	S / F / N	
AD – Keyname–Key Mismatch B	S / F / N	
AD – Verkeerde digest	S / F / N	
AD – Specifieke testcases		
01 – AD	S / F / N	
02 – AD	S / F / N	
03 – AD	S / F / N	
04 – AD	S / F / N	
05 – AD	S / F / N	
06 – AD	S / F / N	
07 – AD	S / F / N	
08 – AD (optioneel)	S / F / N	
09 – AD (optioneel)	S / F / N	



AD – Missing fields		In deze kolom de uitkomst van de missing fields tests.
@ProviderName	S / F / N	
@IssueInstant	S / F / N	
@ID	S / F / N	
@AssertionConsumerServiceIndex	S / F / N	
@AttributeConsumingServiceIndex	S / F / N	
– Issuer	S / F / N	
– RequestedAuthnContext	S / F / N	
– AuthnContextClassRef	S / F / N	
AD – Empty fields		In deze kolom de uitkomst van de empty fields tests.
@ProviderName	S / F / N	
@IssueInstant	S / F / N	
@ID	S / F / N	
@AssertionConsumerServiceIndex	S / F / N	
@AttributeConsumingServiceIndex	S / F / N	
– Issuer	S / F / N	
@Comparison	S / F / N	
– AuthnContextClassRef	S / F / N	
AD – Random value swaps	S / F / N	
Simulatortest Testcases MR	Resultaat	Toelichting



MR – Keyname–Key Mismatch A	S / F / N	
MR – Keyname–Key Mismatch B	S / F / N	
MR – Verkeerde digest	S / F / N	
MR – Specifieke testcases		
01 – MR	S / F / N	
02 – MR	S / F / N	
03 – MR	S / F / N	
04 – MR	S / F / N	
05 – MR (optioneel)	S / F / N	
06 – MR (optioneel)	S / F / N	
MR – Missing fields		In deze kolom de uitkomst van de missing fields tests.
@IssueInstant	S / F / N	
@ID	S / F / N	
– Issuer	S / F / N	
– Extensions	S / F / N	
– xacml–context:Attribute (1)	S / F / N	
– xacml–context:AttributeValue	S / F / N	
– xacml–context:Request	S / F / N	
– xacml–context:Subject	S / F / N	
– xacml–context:Attribute (2)	S / F / N	
– xacml–context:AttributeValue	S / F / N	



- xacml-context:Resource	S / F / N	
- xacml-context:Attribute (3)	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Attribute (4)	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Action	S / F / N	
- xacml-context:Attribute	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Environment	S / F / N	
MR – Empty fields		In deze kolom de uitkomst van de empty fields tests.
@IssueInstant	S / F / N	
@ID	S / F / N	
- Issuer	S / F / N	
- Extensions	S / F / N	
- xacml-context:Attribute (1)	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Request	S / F / N	
- xacml-context:Subject	S / F / N	
- xacml-context:Attribute (2)	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Resource	S / F / N	



- xacml-context:Attribute (3)	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Attribute (4)	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Action	S / F / N	
- xacml-context:Attribute	S / F / N	
- xacml-context:AttributeValue	S / F / N	
- xacml-context:Environment	S / F / N	
MR – Random value swaps	S / F / N	



6 Ketentest – Interoperabiliteit

Deze testset volgt na de geslaagde simulator testen. In deze test wordt interoperabiliteit getest van de nieuwe implementatie, met bestaande (andere nieuwe) implementaties in de acceptatieomgevingen.

Wat geldt voor de simulatortesten geldt ook voor de ketentesten (zie hoofdstuk 4). Pas na goedkeuring van zowel de simulatortesten als de ketentesten kan een deelnemer pas toetreden.

Voor deze tests is het essentieel dat elke deelnemer testmiddelen heeft van de andere deelnemers, op elk toegetreten of nog toe te treden betrouwbaarheidsniveau. Hiervoor moet de deelnemer de bijbehorende persistente pseudoniemen kennen.

De testcases starten steeds met een herkenningsvraag van de Simulator DV (de gesimuleerde dienstverlener) gesteld via de POST-binding aan een HM. De testcases zijn als volgt:

6.1 Randvoorwaardes ketentest testcases

Binnen het afsprakenstelsel kunnen van zowel de metadata als van de dienstencatalogus van deelnemers gelijktijdig meerdere versies gepubliceerd zijn. Om de juiste werking van de combinatie van ondersteuning van meerdere koppelvlak versies te kunnen testen moeten in de testomgeving meerdere versies gepubliceerd zijn en moet bekend zijn welke versies door welke deelnemers worden ondersteund.

6.2 Ketentest testcases eHerkenningsmakelaar

In dit geval gebruikt de toetreder (of een deelnemer met een nieuwe release) authenticatiemiddelen en machtigingen, die door deelnemers zijn verstrekt. Elke deelnemer wordt geacht aan een nieuwe eHerkenningsmakelaar een testmiddel voor zijn authenticatiedienst en/of machtigingenregister te verstrekken. Voor ieder testmiddel (combinatie) in het A-netwerk worden de volgende testen uitgevoerd:

Doel:	Het testen van interoperabiliteit tussen de systemen in het netwerk en een nieuwe eHerkenningsmakelaar (HM).
Samenvatting:	De ketentesten controleren de interoperabiliteit binnen het afsprakenstelsel, door het doorlopen van de flow tussen de verschillende systemen.

Testcase naam:	01 – HM – Normale flow – Handelt de HM de berichten van de verschillende AD's en MR's correct af.
Beschrijving:	De normale flow afhandeling voor een HM. Controleert correcte afhandeling en interoperabiliteit tussen de HM en andere systemen in het netwerk.
Stappen:	1. Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV, begin met het hoogste betrouwbaarheidsniveau van het bijbehorende



	<p>middel.</p> <ol style="list-style-type: none"> 2. Kies een AD uit de lijst die door de HM wordt getoond, als alleen een MR moet worden getest, kies dan de simulator AD. 3. Authenticiteer bij de gekozen AD met het verstrekte testmiddel, in het geval van de simulator AD, voer de locatie van de MR in bij "@Destination". 4. Vervolg naar de bij het testmiddel horende MR. 5. Rond indien nodig de stappen bij de MR af voor correcte machtiging. 6. Controleer in de gesimuleerde DV de correctheid van het ontvangen bericht en noteer de bevindingen in de checklist. 7. Herhaal de stappen 1 t/m 6 indien van toepassing ook op lagere betrouwbaarheidsniveaus 8. Herhaal de stappen 1 t/m 7 voor elke AD en/of MR.
Succes:	De test is een succes als alle AD en MR (eventueel als testmiddel combinatie) het verwachte resultaat oplevert.
Requirements:	<ul style="list-style-type: none"> • De tester moet in het bezit zijn van testmiddelen voor elke AD in het netwerk. • De tester moet in het bezit zijn van machtigingen bij elke MR in het netwerk. • De testmiddelen mogen onafhankelijk van elkaar zijn, maar ook in AD – MR combinatie verstrekt worden, in het laatste geval hoeven deze niet verder onafhankelijk van elkaar getest worden. • De te testen HM moet de meest recente acceptatie metadata verwerkt hebben. • De AD's en MR's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

213

Testcase naam:	02 – HM – Afbreken normale flow – Handelt de HM de AuthnFailed berichten van de verschillende AD's correct af.
Beschrijving:	De normale flow afhandeling voor een HM, in het geval van het annuleren van authenticeren door de gebruiker. Controleert correcte afhandeling en interoperabiliteit tussen de HM en AD's in het netwerk.



Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV. 2. Kies een AD uit de lijst die door de HM wordt getoond. 3. Annuleer het authenticeren door op de annuleer knop van de AD te klikken. 4. Controleer op de HM of het annuleren correct wordt afgehandeld en de gebruiker de keuze krijgt om opnieuw een AD te kiezen. Noteer de bevindingen in de checklist. 5. Herhaal de stappen 1 t/m 4 voor elke AD.
Succes:	De test is een succes als alle AD's bij de HM het verwachte resultaat opleveren.
Requirements:	<ul style="list-style-type: none"> • De te testen HM moet de meest recente acceptatie metadata verwerkt hebben. • De AD's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

214

Testcase naam:	03 – HM – Afbreken normale flow, met replay – Handelt de HM de user replays correct af.
Beschrijving:	De normale flow afhandeling voor een HM, in het geval van het annuleren van authenticeren door de gebruiker. Controleert correcte afhandeling en interoperabiliteit tussen de HM en AD's in het netwerk.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV. 2. Kies een AD uit de lijst die door de HM wordt getoond. 3. Annuleer het authenticeren door op de annuleer knop van de AD te klikken. 4. Controleer op de HM of het annuleren correct wordt afgehandeld en de gebruiker de keuze krijgt om opnieuw een AD te kiezen. Noteer de bevindingen in de checklist. 5. Selecteer nogmaals dezelfde AD uit de lijst die door de HM wordt getoond. 6. Voltooi de authenticate bij de AD. 7. Controleer of de HM de geslaagde authenticatie correct afhandelt en de gebruiker doorstuurt. Noteer de bevindingen in de checklist. 8. Herhaal de stappen 1 t/m 4 voor elke AD.



Succes:	De test is een succes als alle AD's bij de HM het verwachte resultaat opleveren.
Requirements:	<ul style="list-style-type: none"> De te testen HM moet de meest recente acceptatie metadata verwerkt hebben. De AD's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

215

Testcase naam:	04 – HM – Normale flow, controle ID's – Geeft de HM de ID's van de gebruikte AD en MR correct door.
Beschrijving:	De normale flow afhandeling voor een HM. Controleert correcte afhandeling van RFC 98.
Stappen:	<ul style="list-style-type: none"> Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV. Doorloop een volledige authenticatie en autorisatie keten. Controleer in het door de gesimuleerde DV ontvangen bericht de attributen NameQualifier, deze moet het EntityID van de gebruikte MR bevatten en AuthenticatingAuthority, deze moet het EntityID van de gebruikte AD bevatten. Herhaal de stappen 1 t/m 3 voor elke AD/MR combinatie.
Succes:	De test is een succes als de HM de EntityID's correct doorgeeft.
Requirements:	<ul style="list-style-type: none"> De te testen HM moet de meest recente acceptatie metadata verwerkt hebben. De AD's en MR's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. De Tester moet de EntityID's van de AD's en MR's kennen. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

216

Testcase naam:	05 – HM – SSO
----------------	---------------



Beschrijving:	De SSO flow afhandeling voor een HM. Controleert correcte afhandeling van RFC 200.
Stappen:	<ol style="list-style-type: none"> 1 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV. 2 Doorloop een volledige authenticatie en autorisatie keten. 3 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV binnen 10 minuten, zet het @IsPassive op true en @ForceAuthn op false 4 Doorloop een authenticatie keten 5 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV binnen 10 minuten, zet het @IsPassive op false en @ForceAuthn op false 6 Doorloope een volledige authenticatie en autorisatie keten 7 Controleer in het door de gesimuleerde DV ontvangen bericht de attributen NameQualifier, deze moet het EntityID van de gebruikte MR bevatten en AuthenticatingAuthority, deze moet het EntityID van de gebruikte AD bevatten. 8 Herhaal de stappen 1 t/m 7 voor elke AD.
Succes:	De test is een succes als de HM de EntityID's correct doorgeeft.
Requirements:	<ul style="list-style-type: none"> • De te testen HM moet de meest recente acceptatie metadata verwerkt hebben. • De AD's en MR's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • De Tester moet de EntityID's van de AD's en MR's kennen. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0200	

217

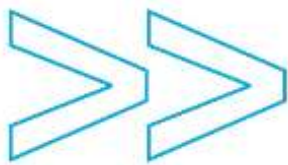
Testcase naam:	06 – HM – Ketenmachtiging (Optioneel)
Beschrijving:	De Ketenmachtiging flow afhandeling voor een HM. Controleert correcte afhandeling van RFC 188.
Stappen:	<ol style="list-style-type: none"> 1 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV. 2 Doorloop de authenticatie bij een AD (mag de simulator AD zijn). Gebruik een pseudoniem dat een ketenmachtiging registratie bij een MR heeft. 3 Doorloop de ketenmachtiging 4 Controleer in het door de gesimuleerde DV ontvangen bericht de attributen NameQualifier, deze moet het EntityID van de gebruikte MR bevatten, AuthenticatingAuthority, deze moet het EntityID van de gebruikte AD bevatten en IntermediateEntityID deze moet OIN van de intermediare partij



	die voorkomt in de ketenmachtiging bevaten. 5 Herhaal de stappen 1 t/m 4 voor elke MR dat ketenmachtiging ondersteunt.
Succes:	De test is een succes als de HM de ketenmachtiging correct doorloopt.
Requirements:	<ul style="list-style-type: none"> De te testen HM moet de meest recente acceptatie metadata verwerkt hebben. De AD's en MR's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. De Tester moet de EntityID's van de AD's en MR's kennen. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0188	

218

Testcase naam:	07 – HM – B2C (Optioneel)
Beschrijving:	De flow afhandeling van B2C use case voor een HM. Controleert correcte afhandeling van RFC 204.
Stappen:	<ol style="list-style-type: none"> 1 Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV. 2 Doorloop de authenticatie bij een AD, en gebruik een middel voor een beroepsoefenaars waar geen sprake van vertegenwoordiging is 3 Controleer in het door de gesimuleerde DV ontvangen bericht de attributen NameQualifier, deze moet het EntityID van de AD bevatten, AuthenticatingAuthority, deze moet het EntityID van de gebruikte AD bevatten en een EntityConcernedID dat de dienstafnemer identificeert. 4 Herhaal de stappen 1 t/m 3 voor elke AD dat B2C ondersteunt.
Succes:	De test is een succes als de HM de flow correct doorloopt.
Requirements:	<ul style="list-style-type: none"> De te testen HM moet de meest recente acceptatie metadata verwerkt hebben. De AD's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. De Tester moet de EntityID's van de AD's kennen. Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0204	



219 6.3 Ketentest testcases Authenticatiedienst

220 In dit geval heeft de toetreder (of een deelnemer met een nieuwe release) een authenticatiemiddel verstrekt
221 aan de beheerorganisatie en voor de tester een soortgelijk testmiddel aangemaakt. Het authenticatiemiddel
222 MAG worden gekoppeld aan een machtiging in een MR. Met dit authenticatiemiddel worden voor iedere
223 eHerkenningmakelaar HM in het A-netwerk de volgende testen uitgevoerd:

Doel:	Het testen van interoperabiliteit tussen de systemen in het netwerk en een nieuwe authenticatiedienst (AD).
Samenvatting:	De ketentesten controleren de interoperabiliteit binnen het afsprakenstelsel, door het doorlopen van de hele flow tussen de verschillende systemen.

224

Testcase naam:	01 – AD – Normale flow – Correcte bericht afhandeling en verzending door de AD.
Beschrijving:	De normale flow afhandeling voor een AD. Handelt de AD de verzoeken van de verschillende HM's goed af en reageren de verschillende HM's correct op de berichten van de AD.
Stappen:	<ol style="list-style-type: none">1. Genereer een bericht een van de HM's vanuit de gesimuleerde DV, begin met het hoogste betrouwbaarheidsniveau waarvoor de AD gecertificeerd wordt/is (saml:AuthnContextClassRef).2. Kies de te testen AD uit de lijst die door de HM wordt getoond.3. Controleer of de AD gewenst reageert en authenticceert bij de AD.4. Controleer of de HM de gebruiker doorstuurt naar de bij het middel geregistreerde MR of de gebruiker de mogelijkheid geeft de bijbehorende MR zelf te selecteren (in het geval er geen MR geregistreerd staat). Noteer de bevindingen in de checklist.5. Herhaal de stappen 1 t/m 4 voor elk relevant betrouwbaarheidsniveau.6. Herhaal de stappen 1 t/m 5 voor elke HM.
Succes:	De test is een succes als alle HM's in combinatie met de te testen AD het verwachte resultaat opleveren.



Requirements:	<ul style="list-style-type: none"> • De tester moet in het bezit zijn van een geldig authenticatiemiddel van de te testen AD. • De tester MAG ook de interactie met MR's testen, hiervoor moet de tester in het bezit zijn van een geldige machtiging. • De te testen AD moet de meest recente acceptatie metadata verwerkt hebben. • De HM's (en MR's) in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

225

Testcase naam:	02 – AD – Normale flow – Correcte bericht afhandeling bij annuleren door gebruiker op de AD.
Beschrijving:	De normale flow afhandeling voor een AD. Handelt de AD de verzoeken van de verschillende HM's goed af en reageren de verschillende HM's correct op de berichten van de AD.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht een van de HM's vanuit de gesimuleerde DV. 2. Kies de te testen AD uit de lijst van AD's en vervolg naar de AD. 3. Annuleer het authenticeren bij de AD door op de knop annuleren te klikken. 4. Controleer of de HM het AuthnFailed bericht correct afhandelt en of de gebruiker een nieuwe keuze voor AD mag maken. Noteer de bevindingen in de checklist. 5. Herhaal de stappen 1 t/m 4 voor elke HM in het netwerk.
Succes:	De test is een succes als alle HM's in combinatie met de te testen AD het verwachte resultaat opleveren.
Requirements:	<ul style="list-style-type: none"> • De te testen AD moet de meest recente acceptatie metadata verwerkt hebben. • De HM's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	



--

226

Testcase naam:	03 – AD – Normale flow – Correcte bericht afhandeling bij annuleren door gebruiker op de AD, waarna replay.
Beschrijving:	De normale flow afhandeling voor een AD. Handelt de AD de verzoeken van de verschillende HM's goed af en reageren de verschillende HM's correct op de berichten van de AD.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht een van de HM's vanuit de gesimuleerde DV. 2. Kies de te testen AD uit de lijst van AD's en vervolg naar de AD. 3. Annuleer het authenticeren bij de AD door op de knop annuleren te klikken. 4. Controleer of de HM het AuthnFailed bericht correct afhandelt en of de gebruiker een nieuwe keuze voor AD mag maken. 5. Kies nogmaals dezelfde AD als bij 2 en controleer of de flow precies zo gaat als normaal (02 –AD). Noteer de bevindingen in de checklist. 6. Herhaal de stappen 1 t/m 5 voor elke HM in het netwerk.
Succes:	De test is een succes als de te testen AD precies hetzelfde reageert op een replay van een user als op een nieuwe user. Hierbij moeten alle HM's in combinatie met de te testen AD het verwachte resultaat opleveren.
Requirements:	<ul style="list-style-type: none"> • De te testen AD moet de meest recente acceptatie metadata verwerkt hebben. • De HM's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

227

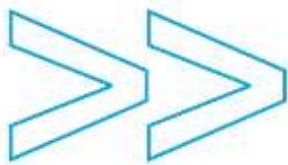
Testcase naam:	04 – AD – SSO (Optioneel)
Beschrijving:	De SSO flow afhandeling voor een AD. Controleert correcte afhandeling van RFC 200.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht voor een HM vanuit de gesimuleerde DV. 2. Kies de te testen AD bij de HM 3. Doorloop een volledige authenticatie en autorisatie keten.



	<p>4 Genereer een bericht voor de te testen AD vanuit de gesimuleerde DV binnen 10 minuten, zet het @IsPassive op true en @ForceAuthn op false</p> <p>5 Kies de te testen AD bij de HM</p> <p>6 Doorloop een authenticatie keten</p> <p>7 Genereer een bericht voor de te testen AD vanuit de gesimuleerde DV binnen 10 minuten, zet het @IsPassive op false en @ForceAuthn op false</p> <p>8 Kies de te testen AD bij de HM</p> <p>9 Doorloop een volledige authenticatie en autorisatie keten (als de AD SSO ondersteunt, dan moet de authenticatie zonder gebruikers interactie gebeuren)</p> <p>10 Controleer in het door de gesimuleerde DV ontvangen bericht de attributen NameQualifier, deze moet het EntityID van de gebruikte MR bevatten en AuthenticatingAuthority, deze moet het EntityID van de gebruikte AD bevatten.</p> <p>11 Herhaal de stappen 1 t/m 10 voor elke HM.</p>
Succes:	De test is een succes als alle HM's in combinatie met de te testen AD het verwachte resultaat opleveren.
Requirements:	<ul style="list-style-type: none"> • De te testen AD moet de meest recente acceptatie metadata verwerkt hebben. • De MR's en HM's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • De Tester moet de EntityID's van de AD's en MR's kennen. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0200	

228

Testcase naam:	05 – HM – B2C (Optioneel)
Beschrijving:	De flow afhandeling van B2C use case voor een AD. Controleert correcte afhandeling van RFC 204.
Stappen:	<p>1 Genereer een bericht voor een HM vanuit de gesimuleerde DV.</p> <p>2 Doorloop de authenticatie bij de te testen AD, en gebruik een middel voor een beroepsoefenaars waar geen sprake van vertegenwoordiging is</p> <p>3 Controleer in het door de gesimuleerde DV ontvangen bericht de attributen NameQualifier, deze moet het EntityID van de AD bevatten, AuthenticatingAuthority, deze moet het EntityID van de gebruikte AD bevatten en een EntityConcernedID dat de dienstafnemer identificeert.</p>



	4 Herhaal de stappen 1 t/m 3 voor elke HM dat B2C ondersteunt.
Succes:	De test is een succes als alle HM's in combinatie met de te testen AD het verwachte resultaat opleveren.
Requirements:	<ul style="list-style-type: none">• De te testen AD moet de meest recente acceptatie metadata verwerkt hebben.• De HM's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben.• De Tester moet de EntityID's van de AD's kennen.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0204	

229

230 **6.4 Ketentest testcase Machtigingenregister**

231 In dit geval heeft de toetreder (of een deelnemer met een nieuwe release) een machtiging, eventueel
232 gekoppeld aan een authenticatiemiddel, verstrekt aan de beheerorganisatie en voor de tester een soortgelijk
233 testmiddel aangemaakt. Met dit testmiddel worden voor iedere eHerkenningmakelaar (HM) in het A-
234 netwerk de volgende testen uitgevoerd:

Doel:	Het testen van interoperabiliteit tussen de systemen in het netwerk en een nieuw machtigingenregister (MR).
Samenvatting:	De ketentesten controleren de interoperabiliteit binnen het afsprakenstelsel, door het doorlopen van de flow tussen de verschillende systemen.

235

Testcase naam:	01 – MR – Normale flow – Handelt de MR de berichten van de verschillende HM's correct af.
Beschrijving:	De normale flow afhandeling voor een MR. Controleert correcte afhandeling en interoperabiliteit tussen de MR en andere systemen in het netwerk.



Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht voor de te testen HM vanuit de gesimuleerde DV, begin met het hoogste betrouwbaarheidsniveau van het bijbehorende middel. 2. Selecteer op de HM de bij het middel behorende AD of als het middel niet aan een authenticatiemiddel gekoppeld is de simulator AD. 3. Rond de authenticatie succesvol af, in het geval van de simulator AD, voer de locatie van de MR in bij "@Destination" en het persistente pseudoniem bij "...saml:NameID". 4. Vervolg naar de bij het testmiddel horende MR. 5. Rond indien nodig de stappen bij de MR af voor correcte machtiging. 6. Controleer in de gesimuleerde DV de correctheid van het ontvangen bericht en noteer de bevindingen in de checklist. 7. Herhaal de stappen 1 t/m 6 ook voor lagere betrouwbaarheidsniveaus. 8. Herhaal de stappen 1 t/m 7 ook voor de andere HM's in het netwerk.
Succes:	De test is een succes als alle HM's in combinatie met de te testen MR het verwachte resultaat opleveren.
Requirements:	<ul style="list-style-type: none"> • De te testen MR moet de meest recente acceptatie metadata verwerkt hebben. • De HM's, (en AD's) in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
<p>Notities / opmerkingen:</p> <p>RFC0105/RFC0245: Bij uitvoeren van stap 3 dient specifiek gecontroleerd te worden dat er EntityConcernedIDs gevuld wordt met het KvKNr, het vestigingsnummer en het SubdossierNr (dat laatste tot 1/4/2014 verplicht).</p>	

236

Testcase naam:	02 – MR – Foutieve flow – Handelt de MR foutieve berichten, te laag betrouwbaarheidsniveau, van de HM's correct af.
Beschrijving:	Controleert correcte afhandeling van foutieve berichten.
Stappen:	<ol style="list-style-type: none"> 1. Genereer een bericht vanuit de gesimuleerde DV, met een te laag betrouwbaarheidsniveau voor het bijbehorende middel (machtiging). 2. Selecteer op de HM de simulator AD. 3. Rond de authenticatie succesvol af voer de locatie van de MR in bij "@Destination" en het persistente pseudoniem bij "...saml:NameID". 4. Vervolg naar de bij het testmiddel horende MR.



	5. Rond indien nodig de stappen bij de MR af voor correcte machtiging. 6. Controleer in de gesimuleerde DV de correctheid (status:deny) van het ontvangen bericht en noteer de bevindingen in de checklist. 7. Herhaal stappen 1 t/m 6 voor elke HM in het netwerk.
Succes:	De test is een succes als de te testen MR het de te lage betrouwbaarheidsniveau weigert. En dit elke keer met elke HM doet.
Requirements:	<ul style="list-style-type: none"> • De te testen MR moet de meest recente acceptatie metadata verwerkt hebben. • De HM's, (en AD's) in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben. • Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen:	

237

Testcase naam:	03 – MR – Ketenmachtiging (Optioneel)
Beschrijving:	De Ketenmachtiging flow afhandeling voor een MR. Controleert correcte afhandeling van RFC 188.
Stappen:	1 Genereer een bericht voor een HM vanuit de gesimuleerde DV. 2 Doorloop de authenticatie bij een AD (mag de simulator AD zijn). Gebruik een pseudoniem dat een ketenmachtiging registratie bij de MR heeft. 3 Doorloop de ketenmachtiging 4 Controleer in het door de gesimuleerde DV ontvangen bericht de attributen NameQualifier, deze moet het EntityID van de gebruikte MR bevatten, AuthenticatingAuthority, deze moet het EntityID van de gebruikte AD bevatten en IntermediateEntityID deze moet OIN van de intermediare partij die voorkomt in de ketenmachtiging bevatten. 5 Herhaal de stappen 1 t/m 4 voor elke HM dat ketenmachtiging ondersteunt.
Succes:	De test is een succes als de MR in combinatie met de HM de ketenmachtiging correct doorloopt.



Requirements:	<ul style="list-style-type: none">• De te testen MR moet de meest recente acceptatie metadata verwerkt hebben.• De AD's en HM's in het netwerk moeten de meest recente acceptatie metadata verwerkt hebben.• De Tester moet de EntityID's van de AD's en MR's kennen.• Tester moet toegang hebben tot de eHerkenning simulator.
Notities / opmerkingen: RFC0188	

238



239 7 Ketentest Checklist

240 Deze ketentest bestaat een aantal testcases. De toetreder dient, voor de relevante rollen en niveaus, de
241 verschillende testcases te doorlopen.

242 Bij resultaat kunnen de waardes S (succes), F (fail), of N (niet getest) en een toelichting worden ingevuld.

Testcases	Resultaat	Toelichting
HM – Testcases		
01 – HM met AD & MR Digidentity	S / F / N	
01 – HM met AD & MR Connectis	S / F / N	
01 – HM met AD & MR Zetsolutions	S / F / N	
01 – HM met AD & MR KPN	S / F / N	
01 – HM met AD & MR CreAim	S / F / N	
01 – HM met AD & MR QuoVadis	S / F / N	
--Insert eventuele nieuwe AD & MR		
02 – HM met AD Digidentity	S / F / N	
02 – HM met AD Connectis	S / F / N	
02 –HM met AD Zetsolutions	S / F / N	
02 – HM met AD KPN	S / F / N	
02 – HM met AD CreAim	S / F / N	
02 – HM met AD QuoVadis	S / F / N	
--Insert eventuele nieuwe AD & MR		
03 – HM met AD & MR Digidentity	S / F / N	
03 – HM met AD & MR Connectis	S / F / N	



03 – HM met AD & MR Zetsolutions	S / F / N	
03 – HM met AD & MR KPN	S / F / N	
03 – HM met AD & MR CreAim	S / F / N	
03 – HM met AD & MR QuoVadis	S / F / N	
--Insert eventuele nieuwe AD & MR		
04 – HM met AD & MR Digidentity	S / F / N	
04 – HM met AD & MR Connectis	S / F / N	
04 – HM met AD & MR Zetsolutions	S / F / N	
04 – HM met AD & MR KPN	S / F / N	
04 – HM met AD & MR CreAim	S / F / N	
04 – HM met AD & MR QuoVadis	S / F / N	
--Insert eventuele nieuwe AD & MR		
05 – HM met AD & MR Digidentity	S / F / N	
05 – HM met AD & MR Connectis	S / F / N	
05 – HM met AD & MR Zetsolutions	S / F / N	
05 – HM met AD & MR KPN	S / F / N	
05 – HM met AD & MR CreAim	S / F / N	
05 – HM met AD & MR QuoVadis	S / F / N	
--Insert eventuele nieuwe AD & MR		
06 – HM met AD & MR Digidentity	S / F / N	
06 – HM met AD & MR Connectis	S / F / N	
06 – HM met AD & MR Zetsolutions	S / F / N	



06 – HM met AD & MR KPN	S / F / N	
06 – HM met AD & MR CreAim	S / F / N	
06 – HM met AD & MR QuoVadis	S / F / N	
--Insert eventuele nieuwe AD & MR		
07 – HM met AD & MR Digidentity	S / F / N	
07 – HM met AD & MR Connectis	S / F / N	
07 – HM met AD & MR Zetsolutions	S / F / N	
07 – HM met AD & MR KPN	S / F / N	
07 – HM met AD & MR CreAim	S / F / N	
07 – HM met AD & MR QuoVadis	S / F / N	
--Insert eventuele nieuwe AD & MR		
Testcases	Resultaat	Toelichting
AD – Testcases		
01 – AD met HM Connectis	S / F / N	
01 – AD met HM KPN	S / F / N	
01 – AD met HM GEMNET	S / F / N	
01 – AD met HM iWelcome	S / F / N	
01 – AD met HM Digidentity	S / F / N	
01 – AD met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		
02 – AD met HM Connectis	S / F / N	
02 – AD met HM KPN	S / F / N	



02 – AD met HM GEMNET	S / F / N	
02 – AD met HM iWelcome	S / F / N	
02 – AD met HM Digidentity	S / F / N	
02 – AD met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		
03 – AD met HM Connectis	S / F / N	
03 – AD met HM KPN	S / F / N	
03 – AD met HM GEMNET	S / F / N	
03 – AD met HM iWelcome	S / F / N	
03 – AD met HM Digidentity	S / F / N	
03 – AD met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		
04 – AD met HM Connectis	S / F / N	
04 – AD met HM KPN	S / F / N	
04 – AD met HM GEMNET	S / F / N	
04 – AD met HM iWelcome	S / F / N	
04 – AD met HM Digidentity	S / F / N	
04 – AD met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		
05 – AD met HM Connectis	S / F / N	
05 – AD met HM KPN	S / F / N	
05 – AD met HM GEMNET	S / F / N	



05 – AD met HM iWelcome	S / F / N	
05 – AD met HM Digidentity	S / F / N	
05 – AD met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		
Testcases	Resultaat	Toelichting
MR – Testcases		
01 – MR met HM Connectis	S / F / N	
01 – MR met HM KPN	S / F / N	
01 – MR met HM GEMNET	S / F / N	
01 – MR met HM iWelcome	S / F / N	
01 – MR met HM Digidentity	S / F / N	
01 – MR met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		
02 – MR met HM Connectis	S / F / N	
02 – MR met HM KPN	S / F / N	
02 – MR met HM GEMNET	S / F / N	
02 – MR met HM iWelcome	S / F / N	
02 – MR met HM Digidentity	S / F / N	
02 – MR met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		
03 – MR met HM Connectis	S / F / N	
03 – MR met HM KPN	S / F / N	



03 – MR met HM GEMNET	S / F / N	
03 – MR met HM iWelcome	S / F / N	
03 – MR met HM Digidentity	S / F / N	
03 – MR met HM CreAim	S / F / N	
--Insert eventuele nieuwe HM		

243