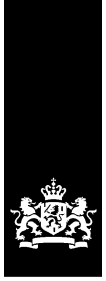


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakspecificatie DigiD SAML

Authenticatie

Versie 3.3

Datum 31 augustus 2016
Status Definitief

Colofon

Projectnaam DigiD 4
Organisatie Logius
Postbus 96810
2509 JE Den Haag
servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur(s)	Opmerkingen
06-03-2012	2.2	Logius	-
01-08-2013	2.3	Logius	Enkele fouten en onduidelijkheden verbeterd. Nieuwe voorbeeldberichten toegevoegd. Verduidelijking van algemene afspraken met eisen aan dienstaanbieders.
05-08-2013	2.4	Logius	404 beschrijving verbeterd.
12-12-2013	3.0	Logius: GvB, EP, JJ	• Nieuwe documentstructuur (NB: het koppelvlak zelf is ongewijzigd) • Elementen uit de Checklist testen opgenomen • Nieuwe Saml voorbeelden • Bijlage DigiD SAML bindings toegevoegd.
17-11-2015	3.1	Logius: JvdB	• Toevoegingen voor DigiD niveau Hoog
10-12-2015	3.2	Logius: JvdB, TR	• Enkele kleine correcties doorgevoerd
31-08-2016	3.3	Logius: TR, DK	• Toevoegingen voor DigiD niveau Substantieel

Met enige regelmaat zal dit document worden verbeterd, verduidelijkt en aangevuld. Logius zal kleine verbeteringen met beperkte gevolgen niet via de mail communiceren. Controleer daarom zelf of er inmiddels een nieuwe versie van dit document te vinden is op www.logius.nl.

Inhoud

1 Inleiding

1.1 Introductie

Via DigiD kunnen eindgebruikers inloggen bij (overheids-) dienstaanbieders, bijvoorbeeld om de aangifte van de inkomstenbelasting te doen. Dit document is bestemd voor ontwikkelaars die in opdracht van een dienstaanbieder een koppeling willen maken tussen een webdienst en DigiD, via het SAML v2.0 koppelvlak van DigiD.

SAML, ofwel Security Assertion Markup Language, is een internationale standaard voor het uitwisselen van berichten met beveiligingsgegevens en informatie over eindgebruikers.

Dit document bevat technische informatie over hoe de SAML standaard door DigiD gebruikt wordt en welke eisen er aan deze koppeling gesteld worden. Dit document geeft geen complete beschrijving van de SAML v2.0.standaard. Uitgangspunt van dit document is dat de lezer bekend is met de SAML v2.0 standaard of anders tijdens het lezen de internationale SAML v2.0 documentatie zal raadplegen.

1.2 Gebruikte termen en afkortingen

Aansluiting = Koppeling tussen Dienstaanbieder en DigiD.

Artifact = Een betekenisloze verwijzing naar een SAML bericht dat via het front channel wordt verstuurd, om te vermijden dat gegevens over de Eindgebruiker kunnen worden onderschept door de browser van de Eindgebruiker.

Assertion = Een verklaring over 1) een attribuut (eigenschap) van een persoon of systeem; 2) een authenticatie van een persoon of systeem of 3) een authorisatie van een persoon of systeem.
Assertions zijn in de context van DigiD verklaringen over een persoon: “Deze persoon heeft BSN 123456789 en is om 9.30 ingelogd met niveau DigiD Midden.”

Back channel = Communicatiekanaal direct tussen Dienstaanbieder en DigiD. Zie stap 6 en stap 7 in Figuur 1: SAML authenticatiestappen.

Dienstaanbieder = De dienstaanbieder waarbij de Eindgebruiker inlogt via DigiD. Dit is de Nederlandse vertaling van de SAML term Service Provider. Voorbeelden van dienstaanbieders zijn de Belastingdienst, de gemeente Amsterdam en Achmea.

Eenmalig Inloggen (EI) = de Single Sign On (SSO) dienst van DigiD, waarmee een gebruiker van meerdere gerelateerde diensten gebruik kan maken zonder steeds opnieuw voor iedere dienst te hoeven inloggen.

Eindgebruiker = De burger/klant die zich met zijn DigiD authenticeert. De Nederlandse vertaling van de SAML term User.

Front channel = Communicatie tussen Dienstaanbieder en DigiD via de User Agent (UA). Zie stap 2 en stap 5 in Figuur 1: SAML authenticatiestappen.

Identity Provider (IDP)
= in deze specificatie altijd DigiD.

Metadata = Voordat een SAML aansluiting tot stand gebracht kan worden, moeten de de Dienstaanbieder en DigiD elkaar eenmalig van configuratiegegevens over de aansluiting voorzien. Dit gebeurt via twee zogenaamde metadata bestanden: één van de Dienstaanbieder en één van DigiD. Hierin wordt aangeven welke diensten, locaties van diensten en certificaten gebruikt worden voor de aansluiting.

SAML = De SAML v 2.0 standaard, ook SAML2.0 genoemd. SAML staat voor Security Assertion Markup Language.
SLO = Single Log Off, federatief uitloggen.

Service Provider (SP)
= Zie Dienstaanbieder.

SSO = Single Sign On, zie Eenmalig Inloggen.

UA = User Agent, ofwel de browser van de Eindgebruiker.

User = Zie Eindgebruiker.

Webdienst = Webdienst van de Dienstaanbieder.

Betrouwbaarheidsniveau
= Het betrouwbaarheidsniveau waarmee de Eindgebruiker zich authenticeert. DigiD kent betrouwbaarheidsniveaus Basis (wachtwoord & gebruikersnaam), Midden (wachtwoord, gebruikersnaam en een extra SMS ter controle), Substantieel (authenticatie met een middel waarbij bij uitgifte een identiteitsdocument is gecontroleerd) en Hoog (authenticatie met een persoonlijk certificaat op een identiteitsdocument)

Zie ook de Engelstalige SAML definitielijst van OASIS.

1.3 Gerelateerde documenten

Document (met vindplaats)	**Inhoud**
Handleiding voor aansluiten (www.logius.nl)	Een stappenplan dat moet worden doorlopen om een aansluiting op DigiD te realiseren. **Let op: vraag op tijd de PKI-overheid certificaten aan!**
Checklist testen (www.logius.nl)	Een lijst met eisen waaraan een nieuwe aansluiting op het SAML koppelvlak moet voldoen. **Let op: bekijk vóór het ontwikkelen van de aansluiting vast deze checklist!**
De SAML v 2.0 standaard (http://saml.xml.org/saml-specifications)	De internationale SAML specificaties.
De PKIoverheid standaard (http://www.pkioverheid.nl/voor-organisaties/)	De standaard die gebruikt wordt voor de beveiligde verbindingen in het DigiD SAML v2.0 koppelvlak.
SAML technical overview (http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf)	De technische beschrijving van SAML 2.0 Zie met name hoofdstuk 5.1 (SSO profile), paragraaf 5.1.3 en paragraaf 5.4.3 (federated identities), zie figuur 13.
SAML profiles (http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)	Een toelichting op de SAML profiles. Zie met name hoofdstuk 4.1 (web browser SSO profile)

1.4 Ondersteuning voor ontwikkelaars & verbetersuggesties

Beheerders van webdiensten die vragen hebben over deze specificatie, of de werking van dit koppelvlak kunnen contact opnemen met het Servicecentrum van Logius.
Indien u verbetersuggesties voor dit document heeft, dan horen wij dat graag.

1.5 Leeswijzer

Dit document is als volgt opgebouwd:

- In hoofdstuk 2 wordt er een kort overzicht gegeven van uit welke SAML onderdelen de SAML implementatie van DigiD bestaat. Er wordt bovendien een keuzewijzer gegeven voor of een dienstaanbieder DigiD met of zonder Eenmalig inloggen wil implementeren.
- In hoofdstuk 3 worden de authenticatiestappen van SAML toegelicht.

- Hoofdstuk 4 beschrijft de extra onderdelen van SAML die nodig zijn indien er voor een implementatie mét Eenmalig inloggen gekozen wordt.
- Hoofdstuk 5 beschrijft diverse eisen en aanwijzingen als toevoeging op de eerdere hoofdstukken.
- In de bijlagen staan diverse XML voorbeeldberichten die in de eerdere hoofdstukken worden beschreven.

2 Over de SAML implementatie van DigiD

2.1 Inhoud van de berichten

Een DigiD authenticatiebericht bevat als belangrijkste de volgende gegevens:

- Het **betrouwbaarheidsniveau** waarmee de eindgebruiker geauthenticeerd is. DigiD kent vier betrouwbaarheidsniveaus: niveau Basis voor het authenticeren met gebruikersnaam en wachtwoord, het niveau Midden met gebruikersnaam, wachtwoord en sms-code, niveau Substantieel waarbij geauthenticeerd wordt met een middel waarbij bij uitgifte een identiteitsdocument is gecontroleerd en Hoog waarbij geauthenticeerd wordt met een persoonlijk certificaat op een identiteitsdocument.Een combinatie van een sectorcode en een **sectoraal nummer** van de eindgebruiker. Een sectoraal nummer is het persoonlijke nummer van de eindgebruiker (namelijk het burgerservicenummer of het sofinummer). De sectorcode geeft aan of het om een burgerservicenummer (BSN) of sofinummer gaat.

2.2 Gebruikte profiles van SAML

Een SAML profile is een specifieke set regels die gebruikt worden voor een bepaalde use case.
DigiD gebruikt twee profiles van de SAML standaard, te weten:

- **Webbrowser SSO profile**, met een HTTP Redirect of HTTP Post binding voor het front channel verkeer, en een HTTP artifact binding voor het back channel verkeer.
- **Single Logout profile**, issued by Session Participant to Identity Provider. Een gedetailleerde uitleg van dit profiel is te vinden in de *SAML profiles* zoals genoemd onder paragraaf 1.3 Gerelateerde documenten.

2.3 Gebruikte bindings

De DigiD SAML implementatie maakt gebruik van de volgende bindings:

- **SP Initiated: HTTP-redirect binding** (Location HTTP header contains SAMLRequest AuthnRequest).
- **SP Initiated: HTTP-post binding** (HTML form contains SAMLRequest AuthnRequest).
- **SP Initiated: HTTP-SOAP binding** (SOAP ArtifactResolve & ArtifactResponse) t.b.v. stap 6 en 7.

Let op: Uit veiligheidsoverwegingen ondersteunt DigiD *geen* AuthenticatieResponse over een POST binding. Gebruik altijd de http-artifact binding.

Zie voor meer informatie de *SAML technical overview* en de *SAML profiles* zoals genoemd onder paragraaf 1.3 Gerelateerde documenten.

2.4 Keuzewijzer: SAML met of zonder Eenmalig Inloggen (EI)?

Indien een eindgebruiker gebruik wil maken van een aantal gerelateerde diensten, is het handig voor de eindgebruiker als hij niet steeds voor iedere dienst opnieuw hoeft in te loggen wanneer hij van de ene dienst naar de andere navigeert. Als een eindgebruiker bijvoorbeeld via DigiD ingelogd is op de persoonlijke internetpagina MijnOverheid, dan hoeft hij meestal niet opnieuw in te loggen als hij naar de site van een van de achterliggende dienstaanbieders navigeert. Dit is mogelijk via SAML met ondersteuning voor Eenmalig Inloggen.
Een dienstaanbieder kan dus kiezen of hij met of zonder Eenmalig Inloggen wil aansluiten op DigiD:

- Bij een dienstaanbieder zonder EI-aansluiting ondersteunt DigiD alleen de authenticatiefunctie voor het inloggen op de webdienst van de dienstaanbieder. Dit wordt toegelicht in hoofdstuk 3 - Interactie via SAML.
- Bij een dienstaanbieder met een EI-aansluiting biedt DigiD de functies federatief inloggen, federatief uitloggen en herauthenticatie aan. Daarnaast toont DigiD bij gebruik van EI ook informatieve tussenschermen aan de eindgebruiker waarin wordt aangegeven waar hij/zij is ingelogd. Wie voor een EI-aansluiting kiest moet de federatief uitloggen functionaliteit implementeren. Dit wordt toegelicht in hoofdstuk 4 - Interactie via SAML mét Eenmalig Inloggen.

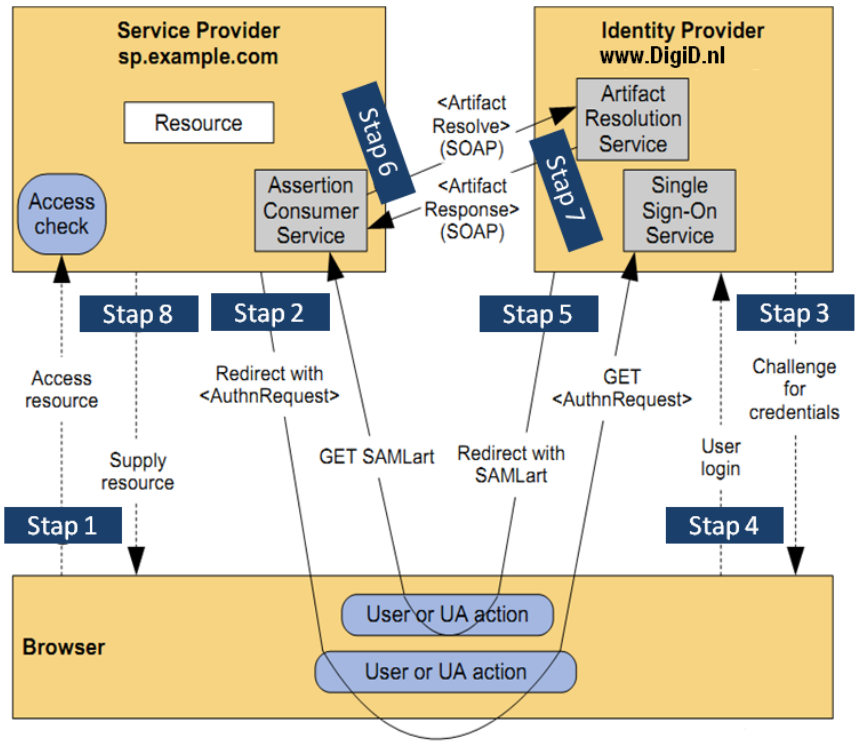
3 Interactie via SAML

3.1 Leeswijzer

In dit hoofdstuk worden de SAML authenticatiestappen toegelicht. In de eerstvolgende paragraaf worden de stappen in hoofdlijnen toegelicht, waarna in de paragraaf daarna dieper op elk van de stappen wordt ingegaan. Merk op dat in de bijlagen diverse voorbeeldberichten ter verduidelijking van elke stap staan.
Tot slot gaan we in op de metadatabestanden van DigiD en de dienstaanbieders en gaan we kort in op de beveiligingsmechanismen van het koppelvlak.

3.2 SAML authenticatiestappen in hoofdlijnen

Het onderstaande schema bevat de authenticatiestappen die worden gemaakt wanneer een eindgebruiker zich bij een dienstaanbieder (in het Engels: Service Provider (SP)) door middel van DigiD (de Identity Provider) authenticeert. *Merk op: hierna worden alleen de termen dienstaanbieder en DigiD gebruikt.*



Figuur 1: SAML authenticatiestappen

Merk op: Bovenstaand schema is omwille van de herkenbaarheid overgenomen uit de internationale SAML v2.0 specificaties en voorzien van blauwe genummerde stappen waarnaar vanuit dit hele document wordt verwezen.

Voordat de bovenstaande authenticatiestappen worden toegelicht, is het van belang om een onderscheid te maken tussen het front channel en het back channel.
Het **front channel** is de communicatie tussen de dienstaanbieder en DigiD *via de Browser van de eindgebruiker*, ofwel Stap 1 en Stap 5 in

bovenstaand figuur. Het **back channel** is de *directe* communicatie tussen de Dienstaanbieder en DigiD, ofwel Stap 6 en Stap 7 in bovenstaand figuur. Dit onderscheid is van belang omdat de gebruikersattributen (zoals het BSN) nooit via het front channel worden verstuurd, zodat deze nooit kunnen worden onderschept of gewijzigd door de browser van de eindgebruiker. Alle SAML backchannel berichten worden in een SOAP envelope geplaatst.

Toelichting bij de stappen in het figuur:

Stap 1
De eindgebruiker met browser als User Agent (UA) wil de webdienst van de dienstaanbieder gebruiken.

Stap 2
De dienstaanbieder wil de identiteit van de eindgebruiker vaststellen. De webdienst stuurt daarom de eindgebruiker door naar DigiD. De webdienst vraagt hierbij om het minimaal gewenste betrouwbaarheidsniveau waarmee de eindgebruiker zich moet authenticeren bij DigiD.

Stap 3 & 4
De eindgebruiker krijgt het DigiD inlogscherm gepresenteerd en voert zijn gebruikersnaam en wachtwoord in. Eventueel moet de eindgebruiker nog een SMS-code invoeren.

Stap 5
DigiD stuurt de eindgebruiker *via een redirect* terug naar de webdienst. Hier wordt een betekenisloos artifact dat door DigiD is gegenereerd, meegestuurd. Dit artifact verwijst naar het daadwerkelijke SAML bericht dat in stap 7 via de *back channel* naar de Dienstaanbieder wordt gestuurd.

Stap 6
De webdienst presenteert het SAML artifact aan DigiD.

Stap 7
DigiD antwoordt direct met het ArtifactResponse bericht dat bij het SAML artifact hoort. In dit bericht geeft DigiD een assertion mee met daarin onder meer het authenticatieresultaat en bij een succesvolle authenticatie het BSN (sectorale nummer) van de eindgebruiker.

Stap 8
De Dienstaanbieder verwerkt de assertion uit het authenticatiebericht van DigiD, en stelt zo de identiteit van de eindgebruiker vast. Alleen bij een succesvolle authenticatie krijgt de eindgebruiker toegang tot de webdienst van de dienstaanbieder.

In de volgende paragraaf worden deze SAML authenticatiestappen in detail beschreven.

3.3 SAML authenticatiestappen in detail

3.3.1 Stap 1 Toegang tot webdienst

De eindgebruiker vraagt toegang tot de webdienst van de Dienstaanbieder. Deze stap vindt plaats zonder tussenkomst van DigiD en valt daarom buiten de scope van dit document.

3.3.2 Stap 2 Authenticatievraag

De dienstaanbieder vraagt in deze stap aan DigiD om de gebruiker te authenticeren met een minimum betrouwbaarheidsniveau. De authenticatievraag van de webdienst (SAML AuthnRequest) bevat in ieder geval de velden die door de standaard als verplicht zijn aangegeven. Daarnaast bevat de authenticatievraag ook optionele velden die DigiD gebruikt. De overige elementen die in SAML optioneel zijn, worden niet door DigiD gebruikt. Overige optionele velden, anders dan die in dit document staan aangegeven, mogen meegestuurd worden, maar worden niet verwerkt door DigiD.

Eisen:
Wanneer een webdienst een eindgebruiker doorstuurt naar DigiD, dan moet dit op zo'n wijze gebeuren dat het voor de gebruiker duidelijk is dat hij op de website van DigiD is en dat hij dit ook daadwerkelijk kan controleren. Daarom gelden de volgende eisen:

1. De eindgebruiker moet naar DigiD worden doorgestuurd in hetzelfde scherm als waarin de gebruiker op "Inloggen op DigiD" heeft geklikt.
2. De eindgebruiker moet een browserwindow zien met daarin de volledige adresbalk. Hiermee kan een gebruiker zien dat hij zijn gegevens op de DigiD website invoert. De gebruiker kan dit controleren door het certificaat (Groene slotje) te inspecteren.
3. Het is niet toegestaan om DigiD in een frame of iframe aan te roepen, danwel DigiD op een andere wijze in te bedden in een pagina van de webdienst.

Twee mogelijkheden: HTTP Redirect of HTTP Post
DigiD ondersteunt zowel de HTTP Redirect als de HTTP Post binding voor de ontvangst van requests van de dienstaanbieder. De dienstaanbieder kan zelf kiezen welke van deze bindings te gebruiken. Bij gebruik van de HTTP Redirect binding worden gegevens in de URL geplaatst. In de praktijk kan een URL maar een beperkte hoeveelheid karakters bevatten, dus op het moment dat een dienstaanbieder zelf veel extra parameters in URLs opneemt, of grote berichten verstuurt, wordt aanbevolen de HTTP Post binding te gebruiken.

De velden en waarden zoals aangegeven in de tabellen voor HTTP Redirect en HTTP Post zijn verplicht, tenzij expliciet anders gespecificeerd.

Mogelijkheid 1: HTTP Redirect
De signature over het bericht wordt bij een HTTP Redirect niet in het SAML bericht opgenomen, maar in de parameters van het GET request meegestuurd. De signature tekent daarmee ook de parameters van de URL en niet alleen het bericht. De signature wordt in de URL opgenomen. Zie [1], specifiek het hoofdstuk over de HTTP Redirect binding uit het saml-bindings-2.0-os document.

Verplicht XML element of attribuut	**Inhoud**
IssueInstant	Het moment waarop het bericht is vervaardigd door de webdienst. Tijdsnotatie dient in UTC te gebeuren. Let op: de datum in deze notatie eindigt op een 'Z', bijvoorbeeld: "2012-02-28T09:01:13Z"
Issuer	De naam van de webdienst. Deze naam wordt gebruikt voor het controleren van de handtekening, en het controleren van autorisaties (zoals de autorisatie om sectorale nummers uit bepaalde sectorcodes te ontvangen). De waarde moet gelijk zijn aan het EntityID in de metadata van de dienstaanbieder..
RequestedAuthnContext	Bevat een attribuut "Comparison = minimum" en een <AuthnContextClassRef> met daarin opgenomen het door de dienstaanbieder vereiste minimale betrouwbaarheidsniveau. Zie het einde van deze paragraaf voor de mogelijke waarden.
ForceAuthn	Dit veld staat standaard op "false". Wanneer er gebruik gemaakt wordt van EI dan heeft de webdienst de mogelijkheid om met dit veld expliciet aan te geven dat de eindgebruiker zich (nogmaals) moet authenticeren, middels de waarde "true".
ProviderName	Optioneel, bevat de naam van de webdienst die wordt getoond aan de eindgebruiker tijdens het authenticeren bij DigiD.
AssertionConsumerServiceIndex Of AssertionConsumerServiceURL	De index uit de metadata waar de eindgebruiker naar terug wordt gestuurd na de authenticatie of als de authenticatie door de eindgebruiker wordt afgebroken. Of als alternatief, direct de URL waar deze eindgebruiker naar terug wordt gestuurd. Slechts één van beide varianten kan gebruikt worden in een bericht. NB: DigiD prefereert de index-variant. Wanneer niet de index-variant wordt gebruikt, maar de URL variant, dan kan Logius een controle doen of de return-URL wel voldoet aan de verwachte return-URL (voor wat betreft het FQDN deel) die voor deze dienstaanbieder wordt toegestaan.

Mogelijkheid 2: HTTP Post
Bij gebruik van de HTTP Post binding wordt de signature in het bericht opgenomen.

XML element of attribuut	**Inhoud**
IssueInstant	Het moment waarop het bericht is vervaardigd door de webdienst. Tijdsnotatie dient in UTC te gebeuren.
Issuer	De naam van de webdienst. Deze naam wordt gebruikt voor het controleren van de handtekening, en het controleren van autorisaties (zoals de autorisatie om sectorale nummers uit bepaalde sectorcodes te ontvangen). De waarde moet gelijk zijn aan het EntityID in de metadata.
Signature	De handtekening van de webdienst over het hele bericht, die wordt gecontroleerd door DigiD . Zie paragraaf 5.1.
Destination	URL van DigiD waarop het bericht wordt aangeboden. Deze URL moet overeenkomen met URL in de metadata van DigiD.
RequestedAuthnContext	Bevat een attribuut "Comparison = minimum" en een <AuthnContextClassRef> met daarin opgenomen het door de dienstaanbieder vereiste minimale betrouwbaarheidsniveau. Zie het einde van deze paragraaf voor de mogelijke waarden.
ForceAuthn	Dit veld staat standaard op "false". De webdienst heeft de mogelijkheid om met dit veld expliciet aan te geven dat de eindgebruiker zich (nogmaals) moet authenticeren.
ProviderName	Optioneel Bevat de naam van de webdienst die wordt getoond aan de eindgebruiker tijdens het authenticeren bij DigiD.
AssertionConsumerServiceIndex Of AssertionConsumerServiceURL	De index uit de metadata waar de eindgebruiker naar terug wordt gestuurd na de authenticatie of als de authenticatie door de eindgebruiker wordt afgebroken. Of als alternatief direct de URL waar deze eindgebruiker naar terug wordt gestuurd. Slechts één van beide varianten kan gebruikt worden in een bericht. NB: DigiD prefereert de index-variant. Wanneer niet de index-variant wordt gebruikt, maar de URL variant, dan kan Logius een controle doen of de return-URL wel voldoet aan de verwachte return-URL (voor wat betreft het FQDN deel) die voor deze dienstaanbieder wordt toegestaan.

< AuthnContextClassRef>: Betrouwbaarheidsniveau
In het AuthnRequest wordt door de dienstaanbieder in het element AuthnContextClassRef het minimaal vereiste betrouwbaarheidsniveau meegegeven. Om de betrouwbaarheidsniveaus van DigiD in de berichten mee te geven bevat het element AuthnContext een van de volgende declarations.

DigiD betrouwbaarheidsniveau	**SAML2 AuthnContextClassRef**
Basis	`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
Midden	`urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract`
Substantieel	`urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard`
Hoog	`urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI`

De dienstaanbieder moet er op controleren dat het betrouwbaarheidsniveau in de ontvangen Assertion voldoet aan het minimaal gevraagde betrouwbaarheidsniveau. Als hier niet aan voldaan wordt, dan moet de inlogpoging worden afgebroken.

Mogelijk kunnen in de toekomst andere betrouwbaarheidsniveaus worden toegevoegd.
Zie ook de SAML specificaties, meer specifiek de documenten saml-authn-context en saml-core.

3.3.3 Stap 5 Artifact

DigiD antwoordt op de authenticatievraag met een SAML-artifact bericht via het front channel. Een artifact is een verwijzing naar een SAML bericht. Ook als er geen authenticatie heeft plaatsgevonden, wordt er een SAML-artifact verstuurd.
Dit SAML-artifact bericht wordt niet getekend door DigiD. SAML stelt dat een SAML-artifact bericht via een HTTP Redirect verstuurd moet worden; dat mag niet via een HTTP Post.

Eis
Om misbruik te voorkomen dient de artifact altijd gestuurd te worden naar een pagina in hetzelfde subdomein als waarvan de redirect van authnrequest is verzonden naar gebruiker. Bijvoorbeeld: de pagina voor het inloggen is https://secure.webpagina.nl/start; de pagina na het inloggen met DigiD is https://secure.webpagina.nl/ingelogd.

3.3.4 Stap 6 Artifact resolution

Met het artifact uit het SAML-artifact bericht haalt de webdienst het authenticatiebericht bij DigiD op via het back channel.

Met het artifact uit het SAMLartifact bericht kan het resultaat van de (gelukte of niet gelukte) authenticatie via de back channel worden opgehaald.

Artifacts worden door DigiD hoogstens 15 minuten bewaard, en kunnen maar één keer door de webdienst worden gebruikt. Er zijn situaties mogelijk (afbreken van processen, vroegtijdig uitloggen) waarbij DigiD een artifact korter dan 15 minuten bewaart.

3.3.5 Stap 7 ArtifactResponse

Het antwoord op de artifact resolution in stap 6 is een artifact response dat een SAML Assertion bevat. Dit assertion bevat het sectorale nummer (BSN of sofinummer) van de eindgebruiker.
Hieronder lichten we het artifact response met de daarin vervatte assertion toe. Zie de bijlage voor een voorbeeldbericht bij deze stap.

<ArtifactResponse>

XML element / attribuut	**Inhoud**
IssueInstant	Het moment waarop het bericht is vervaardigd en ondertekend door DigiD. Tijdsnotatie is in UTC.
Issuer	DigiD
Signature	De handtekening van DigiD die moet worden gecontroleerd door de webdienst. DigiD zet een handtekening over het SAML-bericht. Zie 5.1
Assertion	Een (optioneel getekende) verklaring over de authenticatie, uitgegeven door DigiD. Zie de volgende paragraaf voor de definitie van deze Assertion.
Status	Bevat een element StatusCode met daarin de status van de authenticatie.

<Assertion>

XML element / attribuut	**Inhoud**
IssueInstant	Het moment waarop het bericht (assertion) is vervaardigd en ondertekend door DigiD.
Issuer	DigiD
Signature	De handtekening van DigiD die moet worden gecontroleerd door de webdienst. DigiD zet optioneel een handtekening over de assertion. Zie 5.1
NotBefore en NotOnOrAfter	Geldigheid van de Assertion, gesteld op -2 en +2 minuten vanaf het verzendmoment.

NameID	Sectorcode en sectoraal nummer van de eindgebruiker (bijvoorbeeld: S00000000:123456789). Subject Confirmation wordt door DigiD conform de SAML standaard gebruikt.
AuthnContext	Bevat een AuthnContextClassRef met het betrouwbaarheidsniveau (DigiD basis, DigiD midden, DigiD Substantieel of DigiD hoog) waarmee de eindgebruiker zich heeft geauthenticeerd. Dit betrouwbaarheidsniveau zal gelijk of groter zijn dan het door de webdienst gevraagde minimum niveau. Zie stap 2 voor meer informatie.
AudienceRestriction	Optioneel. Indien gevuld, moet de dienstaanbieder controleren of het bericht (assertion) voor de dienstaanbieder tot de bedoelde Audience behoort; indien controle inhoudelijk niet mogelijk is, of negatief uitvalt, moet de dienstaanbieder het bericht (de assertion) weigeren.
AuthnInstant	Het moment waarop de eindgebruiker zich heeft geauthenticeerd bij DigiD. Dit tijdstip valt vaak samen met IssueInstant.
SubjectLocality	Het IP adres van de eindgebruiker.

In dit SAML koppelvlak geldt dat:

- Het sectoraal nummer met sectorcode wordt direct als subject gebruikt.
- Het betrouwbaarheidsniveau is geen user-attribuut maar een SAML-sessie attribuut: bij een volgende authenticatie kan de waarde immers anders zijn.

De overige optionele elementen die volgens de SAML-standaard in authenticatieberichten kunnen worden gebruikt, worden door DigiD niet gebruikt en genegeerd.

<NameID>: Sectoren

DigiD kent meerdere sectoren, elk met hun eigen sectorcode. Binnen een sector worden personen geïdentificeerd met hun sectorale nummer. Om er voor te zorgen dat een eindgebruiker uniek geïdentificeerd kan worden wordt daarom zowel het sectoraal nummer van de eindgebruiker als de sectorcode meegestuurd in het Subject veld van de responseberichten. Voorbeelden van sectorcodes zijn:

Sectorcode	**Soort Sectoraalnummer**	**Sectorbeschrijving**
S00000000	BSN	Burgerservicenummer
S00000001	SOFI	Sofinummer, gebruikt door bv. de Sociale Verzekeringsbank (SVB) voor Nederlanders die voor de invoering van het BSN uit Nederland zijn geëmigreerd,

Hiervoor wordt de URI syntax gebruikt waarbij sectorcode:sectoraal_nummer worden meegestuurd. Deze URI wordt opgenomen in een <saml2:NameID>. Bijvoorbeeld: <saml:NameID>s00000000:12345678</saml:NameID>

De dienstaanbieder moet een correcte interpretatie van de sectorcode door voeren in zijn aansluiting met DigiD. De dienstaanbieder moet controleren of de sectorcode zoals die in de Assertion is teruggekregen voldoet aan de verwachte sectorcode en daar passend mee omgaan; als niet een verwachte sectorcode is teruggekregen dan moet de authenticatie worden afgebroken.

Als een eindgebruiker wil inloggen bij een webdienst, dan zal DigiD controleren of de eindgebruiker wel een persoonsnummer heeft in een sector waarmee de webdienst van de dienstaanbieder uit de voeten kan. Als DigiD de keus heeft uit meerdere overeenkomende sectoren dan hanteert DigiD de geadministreerde prioriteit voor deze dienstaanbieder voor de terug te geven sector.

3.3.6 Stap 8 Toegang tot de webdienst

In deze stap geeft de dienstaanbieder al dan niet toegang tot de webdienst.

Eisen

Een webdienst moet aan de hand van de assertion besluiten of een gebruiker toegang krijgt tot zijn webdienst of in het geval van een herauthenticatie (van toepassing bij Saml Eenmalig inloggen) zijn sessie mag voortzetten.

Indien de status in de Assertion niet succesvol is of de gebruiker heeft niet het vereiste betrouwbaarheidsniveau (AuthnContext in Assertion) dan:

1. Is de dienstaanbieder verplicht de lopende sessie op diens webdienst direct te beëindigen.
2. Dient er een melding te worden gegeven met eventueel een reden (zie paragraaf 5.13 Foutmeldingen en statussen).

3.4 Metadata

Voordat een SAML aansluiting tot stand gebracht kan worden, moeten de de Dienstaanbieder en DigiD elkaar eenmalig van configuratiegegevens over de aansluiting voorzien. Dit gebeurt via twee zogenaamde metadata bestanden: één van de Dienstaanbieder en één van DigiD. Hierin wordt aangeven welke diensten, locaties van diensten en certificaten gebruikt worden voor de aansluiting. Logius verstrekt de DigiD metadata zodra de aansluitingsaanvraag is goedgekeurd.

De metadata van de dienstaanbieder wordt als volgt aangeboden:

- Best Known Location (voorkeur). Hierbij staat de metadata online beschikbaar via een url. De metadata moet met gebruik van SSL (PKIoverheid) worden aangeboden. Voorbeeld: https://apps.organisatie.nl/metadata.xml

- Bestand. Hierbij wordt de metadata out-of-band uitgewisseld in de vorm van een XML-bestand in het door de SAML2.0 standaard voorgeschreven formaat

De dienstaanbieder moet de metadata gesigned aanleveren. Voor de signature moet daarbij het PKIoverheidcertificaat worden gebruikt dat bij DigiD is geregistreerd voor de webdienst.

De verantwoordelijkheid voor de actualiteit van de inhoud van de metadata ligt bij de dienstaanbieder. De dienstaanbieder moet er zorg voor dragen dat wijzigingen worden gecommuniceerd met de beheerorganisatie van DigiD. Omgekeerd geldt ook dat de beheerorganisatie van DigiD een bericht stuurt in het geval de metadata van DigiD verandert. Aanleiding voor het aanpassen van de metadata is bijvoorbeeld het verlopen van een PKIoverheid-certificaat.

Metadata bij DigiD wordt niet automatisch vernieuwd, maar op basis van een handmatige beheeractie opnieuw ingelezen. De dienstaanbieder geeft door aan DigiD wanneer een verversing van de metadata wenselijk is.

Het (optionele) veld CacheDuration wordt niet gebruikt door DigiD, en mag dan ook niet voorkomen in de door de dienstaanbieder aangeleverde metadata.

Het veld AssertionConsumerServiceIndex wordt gebruikt om de locatie(s) door te geven waar de eindgebruiker naar terug wordt gestuurd na de authenticatie, of waar de eindgebruiker naar terug wordt gestuurd als de authenticatie door de eindgebruiker wordt afgebroken. Het is ook mogelijk om een AssertionConsumerServiceURL mee te geven in de Authentication Request.

Tot slot: DigiD gebruikt het certificaat uit de meta-data van de SP, zelfs als een optioneel veld in berichten een certificaat-info veld betreft: het overrulen van het certificaat uit de metafile is niet mogelijk.

Voor meer informatie over metadata die de dienstaanbieder beschikbaar moet stellen aan DigiD, zie het document saml-metadata-2.0-os.pdf uit de SAML2.0 specificatiebundel. Een voorbeeld van een metadata bestand van een dienstaanbieder staat in de bijlage.

3.5 Beveiliging

De dienstaanbieder moet beveiligingscontroles conform SAML 2.0 uit voeren. Voor een overzicht van deze uit te voeren beveiligingscontroles, zie hoofdstuk 5 - Berichtafhandeling.

Globaal gesproken zijn er beveiligingsmaatregelen getroffen op drie niveaus: Op transportniveau, op berichtniveau, en op protocolniveau.

3.5.1 Transport

Vertrouwelijkheid en integriteit van de HTTP-berichten worden beschermd middels TLS 1.0 of TLS 1.2 met PKIoverheid-certificaten [2]. Dit geldt zowel voor berichten tussen DigiD en webdienst (2-zijdig SSL), als tussen DigiD en eindgebruiker (1-zijdig SSL).

3.5.2 Bericht

Webdiensten en DigiD ondertekenen de authenticatievraag en de assertion in het artifact-respons (ofwel authenticatiebericht) met een digitale handtekening. Ook de SOAP-berichten voor de artifact resolve, en de artifact response (stap 6 en 7) worden beveiligd met een digitale handtekening.
Handtekeningen worden gezet volgens de SAML-standaard (zie hoofdstuk)

3.5.3 SAML Protocol

Ook het protocol bevat een vorm van beveiliging. Voor het transport van het authenticatiebericht wordt gebruik gemaakt van een SAML-artifact die via het front channel naar de dienstaanbieder wordt verstuurd en via het back channel wordt geresolved bij DigiD. Dit wordt gedaan als beveiligingsmaatregel tegen eventuele zwakheden in de computer van de eindgebruiker.

4 Interactie via SAML mét Eenmalig Inloggen

Dit hoofdstuk is alleen bedoeld voor dienstaanbieders die gebruik willen maken van Eenmalig Inloggen. Zie daarom eerst paragraaf 0 – "

Keuzewijzer: SAML met of zonder Eenmalig Inloggen (EI)?".

4.1 Federatief inloggen

Een dienstaanbieder die zijn diensten wil ontsluiten middels Single Sign On kan dat doen via de dienst Eenmalig Inloggen (EI) van DigiD. Deze dienstaanbieder neemt dan deel aan een EI-domein waarin meerdere dienstaanbieders zijn opgenomen die allen gebruik willen maken van de EI functionaliteit die binnen het EI-domein[1] wordt geboden.

Eenmalig inloggen ondersteunen betekent vooral gebruiksgemak. Wanneer bij DigiD bekend is dat een eindgebruiker zich al recent geauthenticeerd heeft binnen het EI-domein, dan wordt deze eindgebruiker namelijk niet opnieuw gevraagd zijn credentials te verstrekken (stap 3 en stap 4 in Figuur 1: SAML authenticatiestappen). Voor de rest werken de authenticatiestappen met eenmalig inloggen hetzelfde als de authenticatiestappen in Figuur 1.

In een aantal uitzonderingsgevallen geldt dat de eindgebruiker alsnog gevraagd wordt zijn credentials te verstrekken:

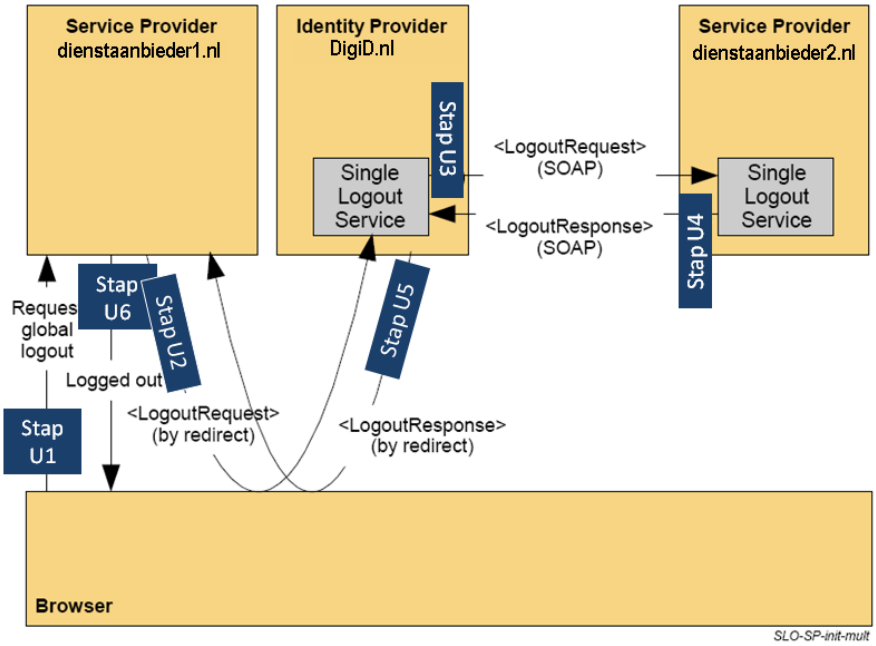
- Het kan zijn dat het betrouwbaarheidsniveau waar de dienstaanbieder om vraagt hoger is dan het betrouwbaarheidsniveau dat is opgeslagen in de bestaande EI sessie.
- De bestaande EI sessie kan voor een ander EI domein gelden dan waar de dienstaanbieder lid van is.
- De dienstaanbieder kan zelf het veld ForcedAuthn meesturen in het authenticatieverzoek, met de waarde True.

[1] *Technisch kunnen er meerdere EI-domeinen worden ingericht. DigiD kent voor de aansluitende dienstaanbieders één EI domein.*

4.2 Federatief uitloggen (door de eindgebruiker geïnitieerd)

4.2.1 Stappen bij federatief uitloggen

In Figuur 2: Federatief uitloggen is een overzicht te vinden van stappen die tijdens de uitlogprocedure gevolgd worden.



Figuur 2: Federatief uitloggen

Toelichting bij de stappen in het figuur:

Stap U1
De eindgebruiker geeft aan uit te willen loggen bij de webdienst van de dienstaanbieder.

Stap U2
De dienstaanbieder beëindigt de lokale sessie. De eindgebruiker wordt doorgestuurd naar DigiD. Het doorsturen gebeurt door een GET of een POST bericht. Hierbij stuurt de webdienst van de dienstaanbieder een LogoutRequest (dienstaanbieder → Browser → DigiD).

DigiD toont de eindgebruiker een uitlogscherm, met vermelding van de dienstaanbieders waar de eindgebruiker gaan uitloggen (dit is niet in de figuur aangegeven, zie voor meer informatie paragraaf 4.4).

Stap U3
DigiD stuurt, indien de eindgebruiker bij meerdere webdiensten binnen dezelfde EI-federatie is ingelogd, via de HTTP-SOAP koppeling een uitlogbericht naar alle andere webdiensten waar de eindgebruiker ingelogd is. Dit is het LogoutRequest (dienstaanbieder → DigiD).

Stap U4
De webdienst van de dienstaanbieder verwijdert de lokale sessie van de eindgebruiker, en stuurt een bevestiging. Dit is de LogoutResponse (dienstaanbieder → DigiD).

Stap U5
DigiD verwijdert de EI-sessie bij DigiD, en stuurt de eindgebruiker terug naar de webdienst waar de eindgebruiker aan het uitloggen is. Het doorsturen gebeurt door een HTTP-GET Hier wordt een LogoutResponse door DigiD meegestuurd (DigiD → Browser > dienstaanbieder).

Stap U6
De webdienst van de dienstaanbieder bevestigt aan de eindgebruiker dat hij is uitgelogd, en stuurt de eindgebruiker naar een uitgelogde pagina (waarvoor geen DigiD Authenticatie nodig is) naar keuze bij deze webdienst.

Gebruikte bindings:
- SP Initiated: HTTP Redirect en HTTP Post (LogoutRequest)
- IDP Initiated: Synchronized (HTTP-SOAP LogoutRequest)

Relevante SAML 2.0 documentatie:
- sst-saml-tech-overview-2.0-cd-02.pdf (Hoofdstuk 5.3, paragraaf 5.3.2, zie figuur 17).
- saml-profiles-2.0-os.pdf (Hoofdstuk 4.4).

4.2.2 Stap U2 Logout request

De signature over het logout-request bericht wordt bij een HTTP Redirect niet in het SAML-bericht opgenomen, maar in de parameters van het GET request meegestuurd. De signature signed daarmee ook de parameters van de URL en niet alleen het bericht. Zie [1], specifiek het hoofdstuk over de HTTP Redirect binding uit het saml-bindings-2.0-os document.

XML element of attribuut	**Inhoud**
IssueInstant	Het moment waarop het bericht is vervaardigd door de webdienst.
Issuer	De naam van de webdienst. Deze naam wordt gebruikt voor het controleren van de handtekening, en het controleren van autorisaties (zoals de autorisatie om sectorale nummers uit bepaalde sectorcodes te ontvangen).
NameID (subject uit de assertion)	Het NameID bevat de identificatie van het subject (eindgebruiker) door de sectorcode en het sectoraal nummer (bijvoorbeeld: S0000000:123456789 . Zie 0 NB: Het NameID kan in de toekomst verplicht zijn als EncryptedID.

4.2.3 Stap U3 SOAP logout request

Het uitlogbericht van DigiD naar de aangesloten SP's waar de eindgebruiker ingelogd is bevat het sectorale nummer en de sectorcode van de eindgebruiker. Het uitlogbericht bevat de door de SAML 2.0 standaard verplicht gestelde elementen en de optionele velden die door DigiD worden gebruikt.

XML element of attribuut	**Inhoud**
IssueInstant	Het moment waarop het bericht is vervaardigd en ondertekend door DigiD.
Issuer	Identity Provider die het bericht uitgeeft (zie metadata van DigiD voor exacte waarde per omgeving)
Digital Signature	De handtekening van DigiD die kan worden gecontroleerd door de webdienst. DigiD zet een handtekening over het SAML-uitlogbericht.
NameID (subject uit de assertion	Sectorcode en sectoraal nummer van de eindgebruiker (bijvoorbeeld: S0000000:123456789). Zie 3.2.5

4.3 Herauthenticatie en timers

Herauthenticatie zorgt ervoor dat de sessietimer die bij DigiD EI wordt bijgehouden, opgehoogd wordt. Zonder herauthenticatie wordt de eenmalig inloggen sessie bij DigiD na 15 minuten ongeldig.

Om de EI-sessietimer te verhogen stuurt de dienstaanbieder binnen dit tijdsinterval de eindgebruiker naar DigiD voor een herauthenticatie. Vervolgens wordt de EI-sessietimer bij DigiD opnieuw op 15 minuten gezet, en stuurt DigiD de eindgebruiker terug naar de website van de dienstaanbieder zonder opnieuw om credentials te vragen. Via het back channel verstrekt DigiD opnieuw de identificerende gegevens van de eindgebruiker aan de webdienst van de dienstaanbieder.

Om DigiD niet over te belasten met herauthenticatie verzoeken mag een eindgebruiker niet binnen 10 minuten terug naar DigiD gestuurd worden met als enig doel om de EI-sessietimer te verhogen. Een herauthenticatie verzoek moet dus tussen de 10 en 15 minuten van de sessietijd plaatsvinden.

Een authenticatieverzoek of herauthenticatieverzoek kan ook worden voorzien van het veld ForceAuthn. Deze 'force authentication' zorgt ervoor dat een eindgebruiker, los van het al dan niet bestaan van een sessie, opnieuw gevraagd wordt zijn credentials op te geven.

Er worden door DigiD twee timers bijgehouden.

Timer	**Waarde**
Sessie timeout	15 minuten (instelbaar door DigiD)
Absolute timeout	3 uur (instelbaar door DigiD)

Deze waardes zijn vast, en alleen door DigiD in te stellen voor de hele EI-federatie (voor alle dienstaanbieders gelden dezelfde waardes).

Voor een eindgebruiker die langer dan de sessie timeout periode (15 minuten) bekend is bij DigiD EI zonder zijn sessie te verlengen wordt de sessie geïnactiveerd. Vanaf dat moment werkt EI niet meer; bij een authenticatie verzoek vanuit de webdienst van een andere dienstaanbieder zal de eindgebruiker opnieuw zijn credentials moeten invoeren.

Er bestaat een absolute timer op het bestaan van de EI sessie van 3 uur. Na deze periode wordt de EI sessie bij DigiD verwijderd.

DigiD verstuurt bij het verlopen van timers geen IDP initiated logout request naar dienstaanbieders. Elke dienstaanbieder heeft zijn eigen verantwoordelijkheid om sessies bij te houden, en dient binnen de aansluitvoorwaarden van DigiD een eigen afweging te maken of een eindgebruiker nog toegang krijgt tot het eigen systeem.

4.4 Partial Logout

Het kan voorkomen dat de dienstaanbieder een partial logout melding ontvangt van DigiD. Door een onvoorziene foutsituatie kan het voorkomen dat de burger bij een SP niet uitgelogd kan worden. DigiD zal dan in het logout response bericht aangeven dat de burger niet bij alle SP's maar bij een deel van SP's is uitgelogd.(zie SAML urn:oasis:names:tc:SAML:2.0:status:PartialLogout)

Dienstaanbieders dienen de partial logout message als een reguliere uitlog response te behandelen.

4.5 Tussenschermen

Indien een burger inlogt bij een dienstaanbieder die is aangesloten op het EI-domein, zullen er in het authenticatieproces specifieke EI - tussenschermen getoond worden door DigiD. Het gaat hierbij om twee tussenschermen: bij het inloggen en bij het uitloggen.

4.5.1 Tussenscherm bij inloggen

Wanneer de eindgebruiker van dienstaanbieder A naar dienstaanbieder B gaat (een herhaling van stap 1 in figuur 2) wordt aan de eindgebruiker een scherm getoond met uitleg waarom er niet opnieuw ingelogd hoeft te worden bij dienstaanbieder B. Daarnaast wordt in dit scherm aangegeven bij welke dienstaanbieder de eindgebruiker nog meer is ingelogd in de huidige EI-sessie.

Het tussenscherm wordt ook getoond bij het navigeren naar andere EI-domeinen. Het tussenscherm wordt alleen getoond aan een eindgebruiker die van EI gebruik maakt (ingesteld in MijnDigiD), tenzij de dienstaanbieder het attribuut 'ForceAuthn' met de waarde 'true' doorgeeft. In dat geval krijgt de eindgebruiker een inlogscherm te zien.

4.5.2 Tussenscherm bij uitloggen

Wanneer de eindgebruiker bij een dienstaanbieder op uitloggen klikt, krijgt deze een scherm te zien waarop wordt uitgelegd wat uitloggen precies betekent. Federatief uitloggen houdt in dat er bij alle dienstaanbieders en bij alle EI-domeinen waarbij is ingelogd ook uitgelogd wordt. In dit tussenscherm wordt aangegeven bij welke dienstaanbieders er uitgelogd wordt.

5 Berichtafhandeling: extra aanwijzingen en eisen

In dit hoofdstuk worden extra aanwijzingen en eisen gegeven voor berichtafhandeling door de dienstaanbieder. Een aantal van de eisen komt terug in de Checklist testen die door Logius gebruikt wordt om nieuwe aansluitingen te testen.

5.1 Signing, vercijferalgoritmes en hash functies

Bij de HTTP Redirect binding wordt, conform huidige SAML 2.0 specificaties, gebruik gemaakt van RSAwithSHA1. Bij de HTTP Post binding wordt gebruik gemaakt van de hashfunctie SHA256 en het vercijferalgoritme RSA-SHA256. Ook DSA met SHA1 en SHA256 wordt ondersteund door DigiD.

In de nabije toekomst zal Logius het gebruik van SHA1 niet meer toestaan. De nieuwste versie van de SAML standaard voorziet ook in het gebruik van SHA256 voor de Redirect binding.

Alle SAML-berichten die de dienstaanbieder naar DigiD stuurt, worden verplicht ondertekend met een Enveloped XML signature volgens de SAML standaard.

Assertions worden *op verzoek van de dienstaanbieder* apart voorzien van een XML signature. Dit om de authenticiteit en integriteit van de assertion als zelfstandig object te kunnen valideren. De dienstaanbieder geeft in zijn metadata bestand aan of de assertions wel of niet door DigiD getekend moeten worden (via wantAssertionsSigned).

Dienstaanbieders zijn verplicht om handtekeningen en bijbehorende berichten volledig te controleren volgens standaarden inclusief controle van de juistheid van de afzender. Dit geldt ook voor logout requests van DigiD en voor de metadata.

5.2 SSL transport

DigiD vereist dat een dienstaanbieder altijd al het http verkeer beveiligt met SSL. Het certificaat wat hiervoor gebruikt wordt dient een PKI-overheid certificaat te zijn.
De Saml berichten die via de browser van de gebruiker verlopen (front channel) hebben alleen een Server certificaat nodig.
De Saml berichten direct tussen DigiD en de dienstaanbieder (back channel) dienen beide een PKI overheidcertificaat toe te passen. Dit wordt ook wel two-sided SSL genoemd. Hiermee is het in beide richtingen onmogelijk om berichten af te luisteren en is het gegarandeerd van de veronderstelde afzender afkomstig.

5.3 Scheiding bericht- en metadata-signing

De scheiding tussen transport-encryptie en bericht-signing is aangebracht door toepassing van twee aparte certificaten bij DigiD. De DigiD metadata is gesigned met hetzelfde certificaat als waarmee de berichten gesigned worden.

Scheiding tussen transport-encryptie en bericht-signing wordt mogelijk een toekomstige eis aan dienstaanbieders.

In de architectuur voor DigiD zijn alle back channel berichten 2-zijdig SSL beveiligd.

5.4 Certificaten

PKI-sleutelparen worden gebruikt door DigiD en de webdienst op drie manieren:

- Voor de SSL-verbinding met de eindgebruiker,
- voor de SSL-verbinding tussen DigiD en de webdienst,
- en voor het ondertekenen van de SAML-berichten volgens de SAML 2.0 standaard.

DigiD accepteert alleen PKI-Overheid-certificaten voor het authenticeren van webdiensten van dienstaanbieders. Het PKI-Overheid-certificaat dat is gebruikt om de SSL-verbinding op te zetten kan worden hergebruikt voor het ondertekenen van SAML-berichten

5.5 Authenticatievragen, en authenticatieberichten

Webdiensten moeten authenticatieresponses met een IssueInstant te ver in het verleden negeren.

De NotBefore en NotOnOrAfter bij DigiD zijn gesteld op respectievelijk -2 en + 2 minuten vanaf het verzendmoment. Dit is de geldigheid voor het verkrijgen en verwerken van de SAML-artifacts/assertions. Hiervoor is het aan te raden gebruikt te maken van NTP-servers (bijvoorbeeld uit de nl.pool.ntp.org verzameling NTP servers). Het achterlopen kan de webdienst kwetsbaar maken voor bepaalde aanvallen op het authenticatieprotocol.

Bij een herauthenticatie dient het volledige protocol afhandeling plaats te vinden en moet het ArtifactResponse ofwel de AuthenticatieResponse worden gecontroleerd voordat de eindgebruiker verder kan met zijn lokale sessie.

5.6 Betrouwbaarheidsniveaus

DigiD vermeldt in het authenticatiebericht altijd het gevraagde authenticatieniveau. Webdiensten moeten erop zijn voorbereid dat de SAML-authenticatieberichten ook hogere betrouwbaarheidsniveau's kunnen bevatten dan het gevraagde betrouwbaarheidsniveau.

De webdienst van de dienstaanbieder is verplicht om te controleren of het betrouwbaarheidsniveau voldoet. Als blijkt dat het gekozen betrouwbaarheidsniveau van de gebruiker niet afdoende is, mag er door de webdienst geen toegang verleend worden.

5.7 Sectoraal nummer en sectorcode

Identiteiten van eindgebruikers worden door DigiD als een combinatie van een sectoraal nummer en een sectorcode doorgegeven. De dienstaanbieder is verplicht om te controleren of de sectorcode de verwachte sectorcode is. Is de sectorcode niet conform de verwachting dan dient de gebruiker geen toegang te krijgen tot de webdienst.

5.8 Audience Restriction

Het veld Audience Restriction moet indien gevuld inhoudelijk gecontroleerd worden. Alleen als de Audience Restriction een verwachte waarde heeft mag een Assertion in behandeling worden genomen.

Dienstaanbieders die geen gebruik maken een Audience Restriction dienen berichten met een ingevulde waarde af te keuren.

5.9 Lokale sessie

De dienstaanbieder is verplicht om een lokale sessie voor de ingelogde eindgebruiker bij te houden. Voor deze lokale sessie geldt een maximale inactiviteit van 15 minuten (zie aansluitvoorwaarden en Checklist testen van DigiD).

Bij de lokale sessie bewaking worden ook de DigiD sessie gegevens conform de SAML standaard opgeslagen en bewaakt.

De dienstaanbieder moet replay attacks herkennen en deze aanvallen afweren.

5.10 Controle op IP adressen

Bij een constatering door DigiD van een verandering van het IP-adres van een eindgebruiker gedurende de EI-sessie, wordt dit als een mogelijke malafide activiteit aangemerkt en breekt DigiD de EI-sessie af.

De SubjectLocality is ingevuld met het IP-adres van de eindgebruiker. Aangesloten partijen kunnen de SubjectLocality gebruiken voor logging of het bijhouden van een audit trail, en tevens kunnen aangesloten partijen dit gegeven gebruiken om in de gaten te houden of het IP-adres van de eindgebruiker gedurende de sessie nog verandert. Het stelt aangesloten partijen in staat om hierop te monitoren, en hier zelf adequaat op te reageren.

Wanneer de IP adres controle niet slaagt, dan moet de eindgebruiker opnieuw inloggen. Er wordt geen foutcode terug gegeven.

5.11 RelayState

Dienstaanbieders mogen een RelayState meegeven voor hun eigen sessie-bewaking. DigiD retourneert de meegegeven RelayState waarde zonder enige controle. De bewaking van inhoud en integriteit van de RelayState moet door de dienstaanbieder zelf worden gedaan.

De SAML standaard hanteert een maximum van 80 karakters voor de RelayState (zie de SAML standaard).

5.12 Cookies

DigiD maakt bij het aanbieden van de EI-functionaliteit gebruik van cookies. Het cookie wordt gebruikt om vast te stellen dat de eindgebruiker bij een EI-domein is aangemeld. Als de browser van een eindgebruiker geen cookies accepteert is de consequentie voor de eindgebruiker dat hij elke keer dat een herauthenticatie gevraagd wordt opnieuw dient in te loggen. Als de eindgebruiker het cookie zelf handmatig aanpast of verwijdert, is de consequentie ook dat een herauthenticatie bij DigiD benodigd is. Eindgebruikers die geen cookies accepteren kunnen gebruik maken van de EI opt-out om daarmee geheel af te zien van Single Sign On; de eindgebruiker geeft dat in MijnDigiD aan.

5.13 Foutmeldingen en statussen

Toplevel code
De standaard SAML foutmeldingen worden gebruikt. De volgende drie foutmeldingen hebben bovendien een eigen betekenis in DigiD.

urn:oasis:names:tc:SAML:2.0:status:Success	Bij ieder succesvol bericht.
urn:oasis:names:tc:SAML:2.0:status:Requester	Bij ieder fout bericht veroorzaakt door de dienstaanbieder.
urn:oasis:names:tc:SAML:2.0:status:Responder	Bij ieder bericht dat niet succesvol is.

Substatus codes
Deze codes worden in combinatie met de Requester en Responder Top level code gebruikt.

urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	Wanneer de eindgebruiker het inloggen annuleert. Wanneer de eindgebruiker niet de juiste sector heeft.
urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext	Wanneer de eindgebruiker niet kan voldoen aan het gevraagde betrouwbaarheidsniveau.
urn:oasis:names:tc:SAML:2.0:status:PartialLogout	Wanneer de eindgebruiker niet uitgelogd kan worden bij alle dienstaanbieders (Bijv. als een dienstaanbieder niet reageert).
urn:oasis:names:tc:SAML:2.0:status:RequestDenied	Een SAML responder die weigert een bericht-uitwisseling met de SAML aanvrager uit te voeren moet een reactie bericht geven met een deze foutcode.

Bij een fout, zal DigiD normaliter een SAML-artifact terugsturen. De dienstaanbieder kan met dit SAML-artifact de DigiD SAML foutmelding ophalen bij DigiD (met een artifact-resolve bericht via het back channel).

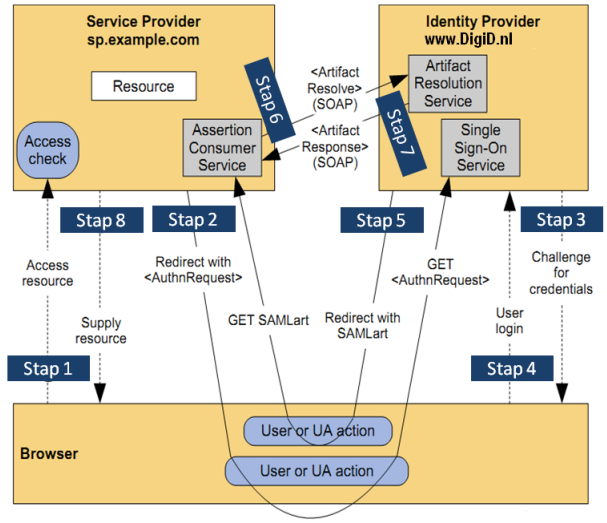
5.13.1 DigiD 404-melding

Naast fouten die binnen het SAML protocol geconstateerd worden, zijn er ook systeemfouten waarop DigiD met een 404-melding reageert. Dit komt voor bij de volgende twee situaties:

- Wanneer de XML parser van DigiD weigert en blokkeert (dus het bericht van de SP kan niet worden gelezen)
- Wanneer er door DigiD niet geverifieerd kan worden, van wie het bericht afkomstig is. Dit wijst vaak op een probleem met de waarde van het veld "Issuer" (deze dient gelijkt te zijn aan de waarde "EntityID" uit de metadata van de SP).

1 Bijlage: Voorbeeldberichten SAML zonder Eenmalig inloggen.

In deze bijlage vindt u voorbeeldberichten bij de stappen in Figuur 1: SAML authenticatiestappen.



1.1 Xml Signature

Saml berichten moeten worden voorzien van een signature.
Deze wordt in het saml bericht zelf opgenomen indien u gebruik maakt van de POST-binding:

```
<ds:Signature>
  <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="#_1330416073">
      <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#">
          <ec:InclusiveNamespaces PrefixList="ds saml samlp xs"/>
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>irsh4GNXQcsbkUmex22XsUejBTXyDdHfaUL/MFFWQHs=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>YJ0V4gCTwRYvgy <INGEKORT> LnOEvyF2ddwBFwILL4nCpw==</ds:SignatureValue>
</ds:Signature>
```

1.2 Soap Envelope

Al het Saml back-channel verkeer wordt in een Soap envelope geplaatst

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <!—SAML BERICHT -->
  </soapenv:Body>
</soapenv:Envelope>
```

1.3 Voorbeeldbericht bij Stap 2: AuthnRequest Redirect Binding

Dit bericht bevat geen xml Signature. Deze wordt in de URI meegezonden.

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_1330416073" Version="2.0" IssueInstant="2012-02-28T09:01:13Z"
  AssertionConsumerServiceIndex="0" ProviderName="provider name">
  <saml:Issuer>http://sp.example.com</saml:Issuer>
  <samlp:RequestedAuthnContext Comparison="minimum">
    <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Redirect Binding url parameter voorbeeld:

https://idp.example.com/SAMLRequest=eJx9kl9LwzAUxd%2F3KUJeZW3a6ZiXtWNMhIHKcNNXCenVFZo%2F5qazH9%2B0rDBQ9hSSnHPv7x7uctXphp3QU21NwbNEcIZG2ao2XwV%2FOzxOF3xVTpYkdeNg3YajecXvFimwaDQEw0fBW2%2FASqoJjNRIEBTs189PkCcCnLfBKtvwC8t1hyRCHyIRZ9uHgn9ks5m4zeZ32Zyz95E171m3RC1uDQVpQnwSWT4V%2BTRfHMQ9iAXM5jciAxGF67HkxhpqNfo9%2BlOtorfCruBRsfP2VFfoXyJOwd35xno6Xk4YGzKAoaEvjyE4SFNyCXZSuwYTZfUyvZSMFgfnxLAa8osAAbvANlY76WvqZ9G1qXWrhz5jp0vxpomRvOJneTU1BarXxeddPH6sr%2BJMAVXsfPDSkLM%2BnBn%2FLd4Tp1eQ4x6kfxehnPwC7bfIIw&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signatur=EN42CtFVVfwO5t9mVBJuPZ3h2WKzEb2ZtC1mdCorXMryDGIf0W9PEArYjMdKz25u4aXcaTJyj0JGz53SKv3SN2okDUQIIpUKVNvKzSLkEiyfQei3PER7dfPoJgPWhFPE4gtIB0JdlwSkvmO0fVlan/GdBwpDdKwh1CAFIONrvU7zMuRe+uSb3Pi6FxM3VPSEUNkEhEh5Oah/uyDCm819KmMPAH13ge5Bxkx/jcw7RNSR2V3Sna57ozlxkQR6O/2bfIY+ueiX7sTh6TmIYHgciMiqnuFQCdW/7ackjNIvutvAVnVd34L98RNOicwVI9r/m6KjYIv7iB8dtUGf8O7Fxw

1.4 Voorbeeldbericht bij Stap 2: AuthnRequest Post Binding

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  Destination="https://example.com" ForceAuthn="false" ID="_1330416073" Version="2.0"
  IssueInstant="2012-02-28T09:01:13Z" AssertionConsumerServiceIndex="0"
  ProviderName="provider name">
  <saml:Issuer>https://sp.example.com</saml:Issuer>
  <ds:Signature><!—Zie XML Signature--></ds:Signature>
  <samlp:RequestedAuthnContext Comparison="minimum">
    <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

1.5 Voorbeeldbericht bij Stap 6: Artifact Resolve (SOAP)

In een Soap envelope:

```
<samlp:ArtifactResolve
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  ID="_1330416073" Version="2.0" IssueInstant="2012-02-28T09:01:13Z">
  <saml:Issuer>http://sp.example.com</saml:Issuer>
    <ds:Signature><!—Zie XML Signature--></ds:Signature>
    <samlp:Artifact>AAQAAMh48/1oXIMRdUmllwn9jJHyEgIi8=</samlp:Artifact>
</samlp:ArtifactResolve>
```

1.6 Voorbeeldbericht bij Stap 7: Artifact Response (SOAP)

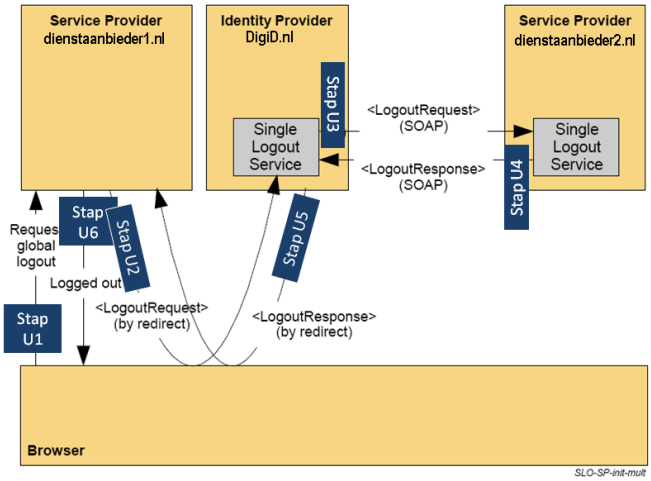
In een Soap envelope. Voor de leesbaarheid is de Saml Assertion uit de Response genomen.

```
<samlp:ArtifactResponse
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  ID="_1330416516" Version="2.0" IssueInstant="2012-12-20T18:50:27Z"
  InResponseTo="_1330416516">
  <saml:Issuer>https://idp.example.com</saml:Issuer>
  <ds:Signature><!-- Zie XML Signature --></ds:Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <samlp:Response InResponseTo="_7afa5ce49" Version="2.0" ID="_1072ee96"
    IssueInstant="2012-12-20T18:50:27Z">
    <saml:Issuer>https://idp.example.com</saml:Issuer>
    <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion><!—ZIE ASSERTION HIERONDER --></saml:Assertion>
  </samlp:Response>
</samlp:ArtifactResponse>

<saml:Assertion Version="2.0" ID="_dc9f70e61c" IssueInstant="2012-12-20T18:50:27Z">
  <saml:Issuer>https://idp.example.com</saml:Issuer>
  <ds:Signature><!—Optioneel Zie XML Signature --></ds:Signature>
  <saml:Subject>
    <saml:NameID>s00000000:12345678</saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData InResponseTo="_7afa5ce49"
        Recipient="http://example.com/artifact url" NotOnOrAfter="2012-12-20T18:52:27Z"/>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2012-12-20T18:48:27Z" NotOnOrAfter="2012-12-20T18:52:27Z">
    <saml:AudienceRestriction>
      <saml:Audience>http://sp.example.com</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement SessionIndex="17" AuthnInstant="2012-12-20T18:50:27Z">
    <saml:SubjectLocality Address="127.0.0.1"/>
    <saml:AuthnContext Comparison="minimum">
      <saml:AuthnContextClassRef>
         urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

2 Bijlage: Voorbeeldberichten bij SAML met Eenmalig inloggen

In deze bijlage vindt u voorbeeldberichten bij de stappen in Figuur 2: Federatief uitloggen.



2.1 Voorbeeldbericht bij Stap U2: Logout Request

Dit is een http redirect bericht. De signing wordt in de URI meegezonden.

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:LogoutRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_1330416516" Version="2.0" IssueInstant="2012-02-28T09:08:36Z">
  <saml:Issuer>http://sp.example.com</saml:Issuer>
  <saml:NameID>s00000000:12345678</saml:NameID>
</samlp:LogoutRequest>
```

2.2 Voorbeeldbericht bij Stap U3: LogoutRequest (SOAP)

In een Soap envelope.

```
<samlp:LogoutRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  ID="_1331125262" Version="2.0" IssueInstant="2012-03-07T14:01:02Z">
  <saml:Issuer>http://sp.example.com</saml:Issuer>
  <ds:Signature><!-- Zie XML Signature --></ds:Signature>
  <saml:NameID>s00000000:12345678</saml:NameID>
</samlp:LogoutRequest>
```

2.3 Voorbeeldbericht bij Stap U4: LogoutResponse (SOAP)

In een Soap envelope.

```
<?xml version="1.0"?>
<samlp:LogoutResponse
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  Version="2.0" Destination=""
  InResponseTo="_43faa9487db98daa757214c2d233d31a8ac043be"
  ID="_882ff30b8fcaba5d2dfdfa1" IssueInstant="2011-08-31T08:57:47Z">
  <saml:Issuer>https://idp.example.com</saml:Issuer>
  <ds:Signature><!-- Zie XML Signature --></ds:Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
</samlp:LogoutResponse>
```

2.4 Voorbeeldbericht bij Stap U5: Response Redirect

Dit is een http redirect bericht. De signing wordt in de URI meegezonden.

```
<?xml version="1.0"?>
<samlp:LogoutResponse
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  Version="2.0" Destination="" InResponseTo="_43faa9487043be"
  ID="_882ff30b891047ca111" IssueInstant="2011-08-31T08:57:47Z">
  <saml:Issuer>https://idp.example.com</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
</samlp:LogoutResponse>
```

3 Bijlage: Voorbeeld van metadata van een dienstaanbieder

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
  ID="_052c51476c9560a429e1171e8c9528b96b69fb57" entityID="http://test.local">
  <ds:Signature><!-- Zie XML Signature --></ds:Signature>
  <md:SPSSODescriptor WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:KeyName>4g4lgk4gk4g44sf3921293</ds:KeyName>
        <ds:X509Data>
          <ds:X509Certificate>MIIGBI<!—Base64 encoderen, ingekort --> 41caj3gg=
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService <!—Alleen voor Saml EI -->
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://test.local/saml/sp/logged_out"/>
    <md:SingleLogoutService <!—Alleen voor Saml EI -->
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="http://test.local/saml/sp/logout"/>
    <md:AssertionConsumerService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
      Location="http://test.local/saml/sp/artifact resolution" index="0"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

4 Bijlage: DigiD Saml bindings sheet

Overzicht van alle Saml stappen, de route (en richting) van de berichten.
Waar (en in welke metadata) ze zijn gedefinieerd in de metadata (binding en protocol).

Hierbij geldt:
SP (Service Provider) = Dienstaanbieder.
Client = De eindgebruiker van DigiD.
IDP (Identity Provider) = DigiD.

Front-channel (Her)authenticatie.

#	Route	Bericht	Binding	Protocol	Meta-data
2	SP => client =>IDP	Authnrequest	SingleSignOnService	HTTP-Redirect of HTTP-Post	IDP
5	IDP => client => SP	Artifact	AssertionConsumerService	HTTP-artifact	SP

Back-channel (Assertion)

#	Route	Bericht	Binding	Protocol	Meta-data
6	SP => IDP	Artifact Resolve	ArtifactresolutionService	SOAP	IDP
7	IDP => SP	Artifact Response	geen binding is direct antwoord	SOAP	

SAML EI

#	Route	Bericht	Binding	Protocol	Meta-data
U2	SP => client => IDP	Logout Request	SingleLogoutService	HTTP-Redirect	IDP
U3	IDP => SP	Logout Request	SingleLogoutService	SOAP	SP
U4	SP => IDP	Logout Response	geen binding is direct antwoord	SOAP	
U5	IDP=>client=>SP	Logout Response	SingleLogoutService	HTTP-Redirect	SP