Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakspecificatie DigiD SAML Authenticatie

Koppelvlakspecificatie DigiD SAML Authenticatie

Via DigiD kunnen eindgebruikers inloggen bij (overheids-)dienstaanbieders, bijvoorbeeld om de aangifte van de inkomstenbelasting te doen. Deze pagina is bestemd voor ontwikkelaars die in opdracht van een dienstaanbieder een koppeling willen maken tussen een webdienst en DigiD, via het SAML 3.X koppelvlak van DigiD.

Met enige regelmaat wordt dit document verbeterd en aangevuld. Logius zal kleine wijzigingen met beperkte gevolgen niet via de mail communiceren. Controleer daarom zelf regelmatig of er inmiddels een nieuwe versie van dit document beschikbaar is.

Versiegegevens

Publicatiedatum: 19 juli 2022

Versie: 3.7

Inleiding

Introductie

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

Deze pagina bevat technische informatie over hoe de SAML V2.0 standaard door DigiD gebruikt wordt en welke eisen er aan deze koppeling gesteld worden. Deze pagina geeft geen complete beschrijving van de SAML v2.0.standaard waarop dit koppelvlak is gebaseerd. Uitgangspunt van de pagina 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.

Gebruikte termen en afkortingen

Term/Afkorting	Omschrijving
Aansluiting	Koppeling tussen dienstaanbieder en DigiD.
Artifact	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 autorisatie 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)	Single Sign On (SSO) dienst van DigiD, waarmee een gebruiker van meerdere gerelateerde diensten gebruik kan maken zonder voor iedere dienst opnieuw te hoeven inloggen.
Eindgebruiker	De burger/klant die zich met zijn DigiD authentiseert. 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 is DigiD altijd de SAML Identity Provider.
Metadata	Voordat een SAML-aansluiting tot stand gebracht kan worden, moeten 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	SAML v2.0 standaard, ook SAML2.0 genoemd. SAML staat voor Security Assertion Markup Language. SLO = Single Log Off, federatief uitloggen. Het SAML 3.X koppelvlak van DigiD maakt gebruik van de SAML v2.0 standaard.
Service Provider (SP)	Zie Dienstaanbieder.
SSO	Single Sign On, zie Eenmalig Inloggen.
UA	User Agent, ofwel de browser/app van de eindgebruiker.
User	Zie Eindgebruiker.
Webdienst	Webdienst van de dienstaanbieder.
Betrouwbaarheidsniveau	Betrouwbaarheidsniveau waarmee de eindgebruiker zich authentiseert. DigiD kent betrouwbaarheidsniveaus *Basis* (wachtwoord & gebruikersnaam), *Midden* (wachtwoord, gebruikersnaam en een extra SMS ter controle, of de DigiD app), *Substantieel* (authenticatie met de DigiD app waarbij bij uitgifte een identiteitsdocument is gecontroleerd) en Hoog (authenticatie met een persoonlijk eID op een identiteitsdocument).

Zie ook de Engelstalige SAML-definitielijst van OASIS.

Gerelateerde pagina's

Document (met vindplaats)	Inhoud
Handleiding aansluiten op DigiD (https://www.logius.nl/diensten/digid/aansluiten-op-digid)	Stappenplan om een aansluiting op DigiD te realiseren. **Let op: vraag op tijd de PKI-overheid certificaten aan!**
DigiD checklist testen (https://www.logius.nl/diensten/digid/documentatie/digid-checklist-testen)	Lijst met eisen waaraan een aansluiting op het SAML-koppelvlak moet voldoen. **Let op: bekijk vóór het ontwikkelen van de aansluiting vast deze checklist!**
SAML v2.0 standaard (https://wiki.oasis-open.org/security/FrontPage)	De internationale SAML specificaties.
PKIoverheid standaard (https://www.logius.nl/diensten/pkioverheid)	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)

Ondersteuning voor ontwikkelaars & verbetersuggesties

Beheerders van webdiensten die vragen hebben over deze specificatie, of de werking van dit koppelvlak kunnen contact opnemen met Logius.

Indien u verbetersuggesties heeft voor deze pagina, dan horen wij dat graag.

Leeswijzer

Deze pagina is als volgt opgebouwd:

- In hoofdstuk Over de SAML-implementatie van DigiD 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 Interactie via SAML worden de authenticatiestappen van SAML toegelicht.
- Hoofdstuk Interactie via SAML mét Eenmalig Inloggen beschrijft de extra onderdelen van SAML die nodig zijn indien er voor een implementatie mét Eenmalig inloggen gekozen wordt.
- Hoofdstuk Interactie via SAML voor app2app-authenticatie beschrijft de authenticatiestappen van SAML in het geval van app2app.
- Hoofdstuk Berichtafhandeling: extra aanwijzingen en eisen 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.

Over de SAML-implementatie van DigiD

Inhoud van de berichten

Een DigiD authenticatiebericht bevat als belangrijkste de volgende gegevens:

- Het **betrouwbaarheidsniveau** waarmee de eindgebruiker geauthentiseerd is. DigiD kent vier betrouwbaarheidsniveaus: Basis voor authenticaties met gebruikersnaam en wachtwoord; Midden voor authenticaties

met gebruikersnaam, wachtwoord en sms-code, of met de DigiD app; Substantieel voor authenticaties met de DigiD app waarbij een identiteitsdocument is gecontroleerd en Hoog voor authenticaties met een persoonlijk eID 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 (het burgerservicenummer of het sofinummer). De sectorcode geeft aan of het om een burgerservicenummer (BSN) of sofinummer gaat.

Gebruikte profiles van SAML

Een SAML profile is een specifieke set regels die gebruikt wordt 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. (Het front channel is de communicatie tussen de dienstaanbieder en DigiD via de browser van de eindgebruiker. Het back channel is de directe communicatie tussen de dienstaanbieder en DigiD).
- **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 hoofdstuk Gerelateerde pagina's.

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 Artifact binding** (SOAP Artifact Resolve & Artifact Response) t.b.v. het back channel verkeer (de directe communicatie tussen de dienstaanbieder en DigiD).

Let op: Uit veiligheidsoverwegingen ondersteunt DigiD geen authenticatie Response 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 hoofdstuk Gerelateerde pagina's.

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 kiezen of hij met of zonder Eenmalig Inloggen aansluit 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 Interactie via SAML mét Eenmalig Inloggen.

Interactie via SAML

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.

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) authentiseert. 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 deze hele pagina 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 (HTTP Post of HTTP Redirect binding). Het back channel is de directe communicatie tussen de dienstaanbieder en DigiD, ofwel Stap 6 en Stap 7 in bovenstaand figuur (HTTP Artifact binding). 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 back channel 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 authentiseren bij DigiD.
- Stap 3 & 4: De eindgebruiker krijgt het DigiD inlogscherm gepresenteerd en authentiseert zich met één van de beschikbare inlogmiddelen op het minimaal gewenste betrouwbaarheidsniveau.
- 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 hierna in stap 6 en 7 via de back channel wordt uitgewisseld.
- Stap 6: De webdienst maakt een beveiligde verbinding met DigiD via de back channel en stuurt een Artifact Resolve-bericht met daarin het SAML-Artifact.
- Stap 7: DigiD antwoordt direct met het Artifact Response-bericht dat bij het SAML-Artifact hoort. In dit bericht geeft DigiD de 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.

SAML-authenticatiestappen in detail

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 deze pagina.

Stap 2 Authenticatievraag

De dienstaanbieder vraagt in deze stap aan DigiD om de gebruiker te authentiseren 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 op deze pagina 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 terecht is gekomen en dat hij dit ook daadwerkelijk kan controleren. Daarom gelden de volgende eisen:

1. De eindgebruiker moet naar DigiD worden doorgestuurd in hetzelfde browserscherm als waarin de gebruiker op "Inloggen op DigiD" heeft geklikt.
2. De eindgebruiker moet een browserscherm 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 (bijvoorbeeld groene slotje) te inspecteren.1
3. Het is niet toegestaan om DigiD in een frame of iframe aan te roepen, dan wel DigiD op een andere wijze in te bedden in een pagina van de webdienst.

Twee mogelijkheden: HTTP Redirect binding of HTTP Post binding

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. 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 authentiseren, middels de waarde “true”.
ProviderName	Optioneel, bevat de naam van de webdienst die wordt getoond aan de eindgebruiker tijdens het authentiseren 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 hoofdstuk Signing, vercijferalgoritmes en hashfuncties.
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 authentiseren.
ProviderName	Optioneel Bevat de naam van de webdienst die wordt getoond aan de eindgebruiker tijdens het authentiseren 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.

Betrouwbaarheids- niveau	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 controleren of 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, specifiek de documenten saml-authn-context en saml-core.

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*.

Stap 6 Artifact Resolution

Met het Artifact uit het SAML-Artifact bericht haalt de webdienst het authenticatiebericht (Assertion) bij DigiD op via het back channel.

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

Stap 7 Artifact Response

Het antwoord op de Artifact Resolution in stap 6 is een Artifact response dat een SAML Assertion bevat.2 Dit Assertion bevat het sectorale nummer (BSN of sofinummer) van de eindgebruiker, mits de authenticatie geslaagd is.

Als de eindgebruiker er niet in geslaagd is, zich te authenticeren, heeft de dienstverlener weliswaar een Artifact van DigiD ontvangen, maar zal dat niet naar een geldig sectoraalnummer kunnen resolven. De Artifact Response bevat dan GEEN Assertion.

Hieronder lichten we het Artifact response met de daarin opgenomen Assertion toe. Zie de bijlage voor een voorbeeldbericht bij deze stap.

Tabel: <Artifact Response>

XML-element of -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 hoofdstuk Signing, vercijferalgoritmes en hashfuncties.
Assertion	Een verklaring over de authenticatie, uitgegeven door DigiD. Zie de volgende tabel voor de definitie van deze Assertion.
Status	Bevat een element StatusCode met daarin de status van de authenticatie.

Tabel: <Assertion>

XML-element of -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 hoofdstuk Signing, vercijferalgoritmes en hashfuncties.
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 geauthentiseerd. Dit betrouwbaarheidsniveau zal gelijk of groter zijn dan het door de webdienst gevraagde minimum niveau. Zie Stap 2 Authenticatievraag 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 geauthentiseerd 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 userattribuut maar een SAML-sessieattribuut: 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 een eindgebruiker uniek te kunnen identificeren, wordt daarom zowel het sectoraal nummer van de eindgebruiker als de sectorcode meegestuurd in het veld Subject 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 wordt 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.

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 minimaal 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 hoofdstuk Foutmeldingen en statussen).

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 out-of-band aan de beheerorganisatie van DigiD aangeboden 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. Dit geldt ook voor aansluitingen op de preproductie-omgeving van DigiD.

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. Meerdere indexen opgeven is mogelijk. Het is ook mogelijk om een AssertionConsumerServiceURL mee te geven in de Authentication Request.

Tot slot: Om de signature van berichten te valideren, gebruikt DigiD het certificaat uit de meta-data van de SP, zelfs als een optioneel veld in berichten certificaat-info bevat: het overrulen van het certificaat uit de metadata 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.

Beveiliging

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

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

Transport

Vertrouwelijkheid en integriteit van het HTTP-verkeer wordt beschermd middels TLS met certificaten. Dit geldt zowel voor berichten tussen DigiD en webdienst (2-zijdig TLS), als tussen DigiD en eindgebruiker (1-zijdig TLS).

De ondersteuning van TLS-versies en ciphersuites volgt de standaarden zoals aangegeven door NCSC-richtlijnen voor TLS. Indien er (belangrijke) wijzigingen zijn in deze ondersteuning zal de dienstaanbieder tijdig geïnformeerd worden. Vanwege de onderhoudbaarheid van deze pagina is daarom geen lijst van ondersteunde versies of ciphersuites opgenomen; die kan indien nodig opgevraagd worden bij de beheerorganisatie van DigiD.

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 stap 7) worden beveiligd met een digitale handtekening.

Handtekeningen worden gezet volgens de SAML-standaard (zie hoofdstuk Signing, vercijferalgoritmes en hashfuncties)

SAML-protocol

Ook het protocol bevat een vorm van beveiliging. Voor het transport van het authenticatiebericht wordt gebruik gemaakt van een SAML-Artifact dat 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.

Interactie via SAML mét Eenmalig Inloggen

Dit hoofdstuk is alleen bedoeld voor dienstaanbieders die gebruik willen maken van Eenmalig Inloggen. Zie daarom eerst hoofdstuk “Keuzewijzer: SAML met of zonder Eenmalig Inloggen (EI)?”.

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 wordt geboden.Technisch kunnen er meerdere EI-domeinen worden ingericht. DigiD kent voor de aansluitende dienstaanbieders één EI domein.

Eenmalig inloggen ondersteunen betekent vooral gebruiksgemak. Wanneer bij DigiD bekend is dat een eindgebruiker zich recent geauthentiseerd heeft binnen het EI-domein, dan wordt deze eindgebruiker 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 van 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.

N.B. In het app2app-scenario kan geen gebruik worden van eenmalig inloggen (SSO).

Federatief uitloggen (door de eindgebruiker geïnitieerd)

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:

1. Stap U1: De eindgebruiker geeft aan uit te willen loggen bij de webdienst van de dienstaanbieder.
2. 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 naar Browser naar 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 hoofdstuk Partial logout).
3. 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).
4. Stap U4: De webdienst van de dienstaanbieder verwijdert de lokale sessie van de eindgebruiker, en stuurt een bevestiging. Dit is de LogoutResponse (dienstaanbieder DigiD).
5. 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).
6. 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).

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. NB: Het NameID kan in de toekomst verplicht zijn als EncryptedID.

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 Stap 7 Artifact Response.

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.

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.

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.

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, tenzij de dienstaanbieder het attribuut 'ForceAuthn' met de waarde 'true' doorgeeft. In dat geval krijgt de eindgebruiker een inlogscherm te zien.

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.

Interactie via SAML voor app2app-authenticatie

Leeswijzer

DigiD biedt app2app-authenticatie aan via het SAML-protocol. Hierbij schakelt een burger van de app van een dienstaanbieder naar de DigiD app om in te loggen. Na een succesvolle authenticatie wordt de burger teruggeleid naar de app van de dienstaanbieder. Dit hoofdstuk beschrijft de SAML-stappen die hierbij van toepassing zijn, eerst in hoofdlijnen, vervolgens in detail. Daarbij wordt waar mogelijk verwezen naar andere hoofdstukken op deze pagina; alleen de punten waarop app2app afwijkt van de reguliere aansluiting komen hier aan bod.

SAML-authenticatiestappen voor app2app in hoofdlijnen

Het onderstaande schema bevat de authenticatiestappen die worden doorlopen wanneer een eindgebruiker zich in een dienstaanbieder app (Service Provider app) authentiseert door middel van de DigiD app.

Figuur 3: SAML-authenticatiestappen voor app2app

Het is van belang om een onderscheid te maken tussen het front channel en het back channel. De communicatie tussen dienstaanbieder (Service Provider) en DigiD (Identity Provider) die via de dienstaanbieder app en de DigiD app loopt, noemen we het front channel (Stap 2 en Stap 5 in bovenstaand figuur). De directe communicatie tussen de backends van dienstaanbieder en DigiD verloopt via het back channel, ofwel Stap 6 en Stap 7. Gebruikersattributen (zoals het BSN) worden nooit via het front channel verstuurd, zodat deze nooit kunnen worden onderschept of gewijzigd. Alle SAML back channel berichten worden in een SOAP envelope geplaatst.

Toelichting bij de stappen in figuur 3:

- Stap 1: De eindgebruiker wil de dienstaanbieder app gebruiken.
- Stap 2: De dienstaanbieder wil de identiteit van de eindgebruiker vaststellen.
  - 2a De dienstaanbieder backend vraagt via de dienstaanbieder app de gebruiker te authentiseren met een minimum betrouwbaarheidsniveau via een AuthnRequest.
  - 2b De dienstaanbieder app stuurt dit verzoek door naar de DigiD app. Dit gebeurt via een iOS Universal link of een Android App link.
  - 2c De DigiD app start vervolgens een authenticatiesessie via de DigiD backend.
- Stap 3 & 4: Via de DigiD app wordt de identiteit van de eindgebruiker geverifieerd. De app vraagt de eindgebruiker om zijn pincode en controleert deze in de DigiD backend.
- Stap 5: Na een succesvolle authenticatie vraagt de DigiD app om het resultaat:
  - 5a De DigiD backend genereert een SAML-Artifact en stuurt het naar de DigiD app. Dit SAMLart verwijst naar het daadwerkelijke SAML-bericht dat de dienstaanbieder backend via de back channel ophaalt bij de DigiD backend in Stap 6 en Stap 7.
  - 5b De DigiD app stuurt de eindgebruiker via een iOS Universal link of Android App link terug naar de dienstaanbieder app en stuurt daarbij het SAMLart mee.
  - 5c De dienstaanbieder app stuurt het SAMLart door naar zijn backend.
- Stap 6: De dienstaanbieder backend presenteert het SAMLart aan de DigiD backend.
- Stap 7: DigiD antwoordt direct met het Artifact Response-bericht dat bij het SAMLart 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 op minimaal het vereiste betrouwbaarheidsniveau geeft de dienstaanbieder de eindgebruiker toegang tot de gevraagde informatie via de app.

In de volgende paragraaf worden de relevante SAML-authenticatiestappen in detail beschreven.

SAML-authenticatiestappen in detail

In deze paragraaf worden alleen de interacties tussen dienstaanbieder en DigiD nader toegelicht.

Stappen 1, 2a en 5c betreffen communicatie tussen de backend en de app van de dienstaanbieder. Deze stappen vinden plaats zonder tussenkomst van DigiD en vallen daarom buiten de scope van deze pagina. Voor stap 8 geldt dit in feite ook, maar omdat DigiD aan deze stap eisen stelt, komt deze hier toch aan de orde.

Stappen 2c, 3, 4 en 5a spelen zich af binnen DigiD (tussen DigiD app en de DigiD backend) en zijn dus voor deze pagina niet van belang: ze lopen niet via een koppelvlak tussen DigiD en dienstaanbieder.

Stap 2b Authenticatieverzoek

De dienstaanbieder app vraagt in deze stap aan de DigiD app om de gebruiker te authentiseren met een minimum betrouwbaarheidsniveau. Hij stuurt het authenticatieverzoek (SAML AuthnRequest) via een iOS Universal link of een Android App link naar de DigiD app. Zie onderstaande eisen voor meer details.

Het authenticatieverzoek bevat in ieder geval de velden die door de standaard als verplicht zijn aangegeven. Daarnaast bevat het ook enkele optionele elementen die DigiD gebruikt. Overige optionele velden, anders dan die op deze pagina staan aangegeven, mogen meegestuurd worden, maar verwerkt DigiD niet.

Eisen

iOS Universal link of Android App link

De afnemer app roept iOS Universal link of Android App link aan op de URL https://app.digid.nl/digid-app?app-app={JSON_REQUEST}, waarbij JSON_REQUEST een BASE64 encoded JSON object is met UTF-8 character encoding en de volgende informatie (de veldnamen zijn hoofdlettergevoelig).

Veldnaam	Formaat	Verplicht	Omschrijving
Icon	string	X	De URL waar de DigiD app het icoon van de dienstaanbieder app kan vinden voor weergave in het bevestigingsscherm. Dit icoon moet zich binnen het domein van de dienstaanbieder bevinden.
ReturnUrl	string	X	Het iOS Univeral Link of Android App Link adres van de dienstaanbieder app waar de DigiD app na het authentiseren van de gebruiker het SAML-Artifact heen stuurt.
SAMLRequest	string	X	Het SAML-verzoek tot authenticatie met DigiD bij de dienstaanbieder backend. Hierin geeft de dienstaanbieder in het element AuthnContextClassRef het minimaal vereiste betrouwbaarheidsniveau mee (zie Stap 2 Authenticatievraag).

Host	string	De omgeving van de DigiD backend waarmee de DigiD app communiceert, alleen in het geval van een testomgeving. Op productie moet dit veld leeg zijn.
RelayState	string	Optionele SAML-parameter die door de dienstaanbieder mee mag worden gestuurd voor zijn eigen sessiebewaking. Zie hoofdstuk RelayState.
SigAlg	string	Het vercijferalgoritme dat wordt gebruikt bij het maken van de handtekening (zie parameter 'Signature'). SAML parameter, benodigd bij HTTP Redirect binding.
Signature	string	De handtekening van de dienstaanbieder over het hele bericht, die wordt gecontroleerd door DigiD. Zie hoofdstuk Interactie via SAML voor app2app-authenticatie. SAML parameter, benodigd bij HTTP Redirect binding.

Fallback bij falen iOS Universal links

In bepaalde iOS-versies kan het na een installatie of update van de DigiD app tot 8 uur duren voordat de Universal link registratie is voltooid. Ook kan het voorkomen dat iOS Universal links in z'n geheel niet werkt op bepaalde devices of versies van iOS.

Daarom heeft DigiD een fallbackscenario toegepast: Als de DigiD app niet gevonden wordt met Universal links, leidt het OS de gebruiker naar de browser, waar hij de DigiD app alsnog handmatig kan starten, gebruikmakend van URL-schemes.

SAML binding: HTTP Redirect

Vanwege het hierboven beschreven fallbackscenario ondersteunt DigiD in geval van app2app-aansluitingen **alleen HTTP Redirect binding** voor de ontvangst van requests van de dienstaanbieder. Omdat de alternatieve route via een browser loopt, is het aantal toegestane karakters van het SAML-bericht beperkt (een browser kan ongeveer een maximum van 2000 karakters aan).

Bij gebruik van de HTTP Redirect binding ontbreekt het certificaat in het bericht, waardoor het binnen de toegestane lengte blijft. (Het certificaat is al eerder uitgewisseld in de metadata in de contacten tussen dienstaanbieder en DigiD en hoeft niet in elk SAML-request opnieuw meegestuurd te worden.)

Check op geïnstalleerde app

Voor een optimale gebruikerservaring kan de dienstaanbieder app controleren of de DigiD app op hetzelfde device als de dienstaanbieder app is geïnstalleerd en afhankelijk hiervan de gebruiker informeren.

- Voor iOS kan hiervoor de methode canOpenURL worden gebruikt (url = "digid://").
- Voor Android kan hiervoor de methode packageManager.getPackageInfo worden gebruikt (packageName = "nl.rijksoverheid.digid.pub" (productie – neem voor de packageName voor testomgevingen contact op met uw Logius contactpersoon)).

Stap 5b Artifact

DigiD antwoordt op de authenticatievraag met een SAMLart bericht. Dit bericht wordt via de DigiD app naar de app van de dienstaanbieder gestuurd via een iOS Universal link of Android App link.

Het Artifact is een verwijzing naar een SAML-bericht. Ook als er geen authenticatie heeft plaatsgevonden, wordt er een SAML-Artifact verstuurd.

Eisen

iOS Universal link of Android App link

Om misbruik te beperken, dient de iOS Universal link of Android App link zich binnen hetzelfde domein als de dienstaanbieder te bevinden. Bijvoorbeeld: het domein van de dienst is *https://secure.webpagina.nl*; de iOS Universal link of Android App link is *https://secure.webpagina.nl/app2app*.

De URL van de iOS Universal link of Android App link die wordt aangeroepen door de DigiD app is:

{RETURN_URL}?app-app={JSON_RESPONSE}

- RETURN_URL is de waarde van ReturnUrl die door de dienstaanbieder is opgenomen in het verzoek
- JSON_RESPONSE is een BASE64 encoded JSON object met UTF-8 character encoding.

JSON_RESPONSE bevat de volgende velden:

Antwoord-type	Veldnaam	Formaat	Meer informatie
succes	SAMLart	string	Het SAML-Artifact dat de dienstaanbieder gebruikt om het resultaat van de (gelukte of niet gelukte) authenticatie via de back channel op te halen.
	RelayState	string	De waarde van RelayState die de dienstaanbieder app in het verzoek heeft doorgegeven. Indien de dienstaanbieder dit veld niet heeft gevuld bij in stap 2b, heeft dit veld in het antwoord de waarde null (niet de string "null").

fout	ErrorMessage string	Een ‘plain tekst’ foutmelding in geval van technische fouten, waarbij het niet mogelijk is een SAMLart te versturen, meldt de app dat via deze ErrorMessage. Ook in enkele functionele foutsituaties stuurt de DigiD app via deze ErrorMessage een melding naar de dienstaanbieder, zodat die daar direct op kan reageren: • **_by_user**: bij annuleren door de gebruiker. • **not_activated**: als de app niet geactiveerd is. • **timeout**: als het AuthNRequest van de dienstaanbieder blijkt te zijn verlopen. • **icon_missing**: als het verzoek van de dienstaanbieder geen icon bevat. NB In overige foutsituaties stuurt de DigiD app een succes-response met een niet te resolven SAMLart.

Zoals in Stap 2b Authenticatieverzoek beschreven, kunnen er problemen optreden bij het aanroepen van een iOS Universal link. De dienstaanbieder kan overwegen een fallbackscenario te implementeren: leid de gebruiker, als vanuit de DigiD app de dienstaanbieder app niet gevonden wordt via Universal links, naar een webpagina, waar hij de app handmatig kan proberen te openen d.m.v. URL-schemes. Omdat URL-schemes minder veilig zijn dan Universal links, dient de dienstaanbieder hierin een eigen risicoafweging te maken.

Stap 6 Artifact Resolution

Met het Artifact uit het SAML-Artifact bericht haalt de dienstaanbieder het authenticatiebericht bij DigiD op via het back channel. Daarin staat het resultaat van de authenticatie (gelukt of niet gelukt).

DigiD bewaart een Artifact hoogstens 15 minuten, en de dienstaanbieder kan het maar één keer gebruiken. Er zijn situaties mogelijk (afbreken van processen, vroegtijdig uitloggen) waarbij DigiD een Artifact korter dan 15 minuten bewaart.

Stap 7 Artifact response

Het antwoord op de Artifact Resolution is een Artifact response dat een SAML Assertion bevat. Zie voor een beschrijving Stap 7 Artifact Response.

Stap 8 Toegang tot de gevraagde dienst

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

Eisen

Authenticatieresultaat controleren

Een dienstaanbieder moet aan de hand van de Artifact response besluiten of een gebruiker toegang krijgt tot zijn dienst. Als de status in de Artifact response niet succesvol is of als de gebruiker niet het vereiste betrouwbaarheidsniveau heeft, dan:

- Is de dienstaanbieder verplicht de lopende sessie direct te beëindigen.
- Dient er een melding te worden gegeven met eventueel een reden (zie hoofdstuk Foutmeldingen en statussen).

Eenmalig inloggen

In het app2app-scenario kan geen gebruik worden van eenmalig inloggen (SSO). Als de eindgebruiker in een andere afnemer-app wil inloggen, moet hij altijd opnieuw via de DigiD app inloggen, ongeacht of de afnemer aan eenmalig inloggen doet of niet.

Beveiliging

Zie voor de beveiligingsspecificaties op gebied transport, berichtondertekening en SAML-protocol hoofdstuk Beveiliging.

DigiD app in demostand

De DigiD app kan voor test- en instructiedoeleinden in demostand geactiveerd worden. In de demostand legt de DigiD app geen verbinding met de DigiD backend. Een authenticatie met de DigiD app in demostand is dus slechts een simulatie en leidt niet daadwerkelijk tot inloggen bij (een app van) een dienstaanbieder.

Dienstaanbieders die op app2app willen aansluiten, kunnen deze demostand gebruiken om het inloggen in hun eigen app te testen, zonder dat zij daarvoor een echt DigiD account nodig hebben. Zij zullen daarvoor ook een demostand in hun eigen app moeten introduceren. In het app2app-scenario beantwoordt de DigiD app het authenticatieverzoek van de app van de dienstaanbieder niet met een geldig SAMLart. In plaats daarvan stuurt hij de string “demo” terug. De app van de dienstaanbieder moet daarop kunnen anticiperen.

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.

Signing, vercijferalgoritmes en hashfuncties

DigiD ondersteunt zowel bij de HTTP Redirect als bij de HTTP Post binding het gebruik van RSA-SHA256, conform huidige SAML 2.0 specificaties. Bij de HTTP Redirect binding ondersteunt DigiD ook RSA met SHA1, in verband met de maximale lengte van de URL.

In de toekomst zal Logius het gebruik van SHA1 mogelijk niet meer toestaan. Indien deze wijziging wordt doorgevoerd zal de dienstaanbieder hierover tijdig geïnformeerd worden.

Alle SAML-berichten die de dienstaanbieder naar DigiD stuurt, moet hij verplicht ondertekenen 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 metadatabestand aan of DigiD de Assertions wel of niet moet ondertekenen (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.

TLS transportbeveiliging

Het HTTP-verkeer dat via de browser van de gebruiker loopt (front channel) dient beveiligd te zijn met een publiek vertrouwd browser-certificaat. Deze certificaten moeten onder een root vallen, welke in alle grote browsers opgenomen is.

Het HTTP-verkeer tussen de dienstaanbieder en DigiD (back channel) dient gebruik te maken van twee-zijdig TLS. Hierbij wordt zowel de partij die de verbinding opzet (afzender) als de partij die de verbinding accepteert (ontvanger) gecontroleerd op basis van het certificaat.

Het client-certificaat dat u als afzender aanbiedt, moet een machine-2-machine certificaat zijn, welke onder de G1-root van PKIoverheid valt.

TLS- en SAML-certificaten

In principe zijn er drie verschillende functies waarvoor u als dienstaanbieder voor DigiD certificaten gebruikt::

1. Het ondertekenen van SAML berichten (SAML-signing)
2. Het vercijferen van SAML berichten en elementen (SAML-encryption)
3. Het vercijferen van HTTP-verkeer (TLS-encryption)

Bij SAML3.x worden alleen de certificaten onder punt 1 in de metadata opgenomen. Type 2 gebruikt DigiD niet bij SAML3.x en TLS certificaten worden niet via de metadata verzonden.

Er kan een scheiding aangebracht worden tussen transport-encryptie (TLS) en bericht-signing (SAML) certificaten door toepassing van twee aparte certificaten. Meer informatie hierover vindt u in de Factsheet - SAML certificaten en metadata.

De DigiD metadata is gesigned met hetzelfde certificaat als waarmee de berichten gesigned.

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 niet synchroon lopen van de tijd kan de webdienst kwetsbaar maken voor bepaalde aanvallen op het authenticatieprotocol.

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

Betrouwbaarheidsniveaus

DigiD vermeldt in de response op het authenticatiebericht altijd het authenticatieniveau waarop de gebruiker is ingelogd. Webdiensten moeten erop zijn voorbereid dat dit ook een hoger betrouwbaarheidsniveau kan zijn 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.

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.

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.

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 sessiebewaking worden ook de DigiD sessiegegevens conform de SAML-standaard opgeslagen en bewaakt.

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.

RelayState

Dienstaanbieders mogen een RelayState meegeven voor hun eigen sessiebewaking. DigiD retourneert de waarde van de RelayState 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).

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. Ook is het mogelijk dat bepaalde privacy-instellingen van de browser (bijv. een “in-private” browsing venster) het gebruik van cookies onmogelijk maakt en daarmee de EI-functionaliteit verstoort.

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 berichtuitwisseling 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).

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 DigiD niet kan verifiëren, 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).
- Wanneer DigiD de signature van het XML-bericht niet (op de juiste wijze) kan controleren. Dit kan wijzen op een probleem met het certificaat of met de metadata.

Bijlage: Voorbeeldberichten SAML zonder Eenmalig inloggen.

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

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>

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>

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%2B0r

DBQ9hSSnHPv7x7uctXphp3QU21NwbNEcIZG2ao2XwV%2FOzxOF3xVTpYkdeNg3YajecXvFimwaDQEw0fBW2%2FASqoJj

NRIEBTs189PkCcCnLfBKtvwC8t1hyRCHyIRZ9uHgn9ks5m4zeZ32Zyz95E171m3RC1uDQVpQnwSWT4V%2BTRfHMQ9iAX

M5jciAxGF67HkxhpqNfo9%2BlOtorfCruBRsfP2VFfoXyJOwd35xno6Xk4YGzKAoaEvjyE4SFNyCXZSuwYTZfUyvZSMFgfnxL

Aa8osAAbvANlY76WvqZ9G1qXWrhz5jp0vxpomRvOJneTU1BarXxeddPH6sr%2BJMAVXsfPDSkLM%2BnBn%2FLd4Tp1eQ

4x6kfxehnPwC7bfIIw&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=EN42CtF

VVfwO5t9mVBJuPZ3h2WKzEb2ZtC1mdCorXMryDGIf0W9PEArYjMdKz25u4aXcaTJyj0JGz53SKv3SN2okDUQIIpUKVNvKzS

LkEiyfQei3PER7dfPoJgPWhFPE4gtIB0JdlwSkvmO0fVlan/GdBwpDdKwh1CAFIONrvU7zMuRe+uSb3Pi6FxM3VPSEUNkEhE

h5Oah/uyDCm819KmMPAH13ge5Bxkx/jcw7RNSR2V3Sna57ozlxkQR6O/2bfIY+ueiX7sTh6TmIYHgciMiqnuFQCdW/7ackjNIv

utvAVnVd34L98RNOicwVI9r/m6KjYIv7iB8dtUGf8O7Fxw

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>

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>

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>

Bijlage: Voorbeeldberichten bij SAML met Eenmalig inloggen

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

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>

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>

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>

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>

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" AuthnRequestsSigned=”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>

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.

SAML

Tabel: 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

Tabel: Back channel (Assertion)

#	Route	Bericht	Binding	Protocol	Meta- data
6	SP IDP	Artifact Resolve	ArtifactResolutionService	SOAP	IDP
7	IDP SP	Artifact Response	Geen binding (direct antwoord)	SOAP	

Tabel: 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 (direct antwoord)	SOAP	
U5	IDP client SP	Logout Response	SingleLogoutService	HTTP Redirect	SP

SAML app2app

Tabel: Front channel ((Her)authenticatie)

#	Route	Bericht	Binding	Protocol	Meta- data
2	SP SP app IDP app IDP	Authnrequest	SingleSignOnService	HTTP Redirect	IDP
5	IDP IDP app SP app SP	Artifact	AssertionConsumerService	HTTP Artifact	SP

Tabel: Back channel (Assertion)

#	Route	Bericht	Binding	Protocol	Meta- data
6	SP IDP	Artifact Resolve	ArtifactResolutionService	SOAP	IDP
7	IDP SP	Artifact Response	Geen binding (direct antwoord)	SOAP	

N.B. In het app2app-scenario kan geen gebruik worden van eenmalig inloggen (SSO).

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	• 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	• Toevoegingen voor DigiD niveau Hoog.
10-12-2015	3.2	Logius	• Enkele kleine correcties doorgevoerd.
31-08-2016	3.3	Logius	• Toevoegingen voor DigiD niveau Substantieel.
22-02-2019	3.4	Logius	• Toevoegingen voor app2app.

06-05-2020	3.5	Logius	• Aanpassingen app2app. • AuthnRequestsSigned="true" atttribuut toegevoegd als vereiste in metadata. • Verwijzing naar TLS 1.0 verwijderd.
07-06-2021	3.6	Logius	• Functionele foutmeldingen toegevoegd in SAMLart-bericht van DigiD app naar afnemer app (app2app).
19-07-2022	3.7	Logius	• App2app: Demostand toegevoegd • Functionele foutmeldingen toegevoegd in SAMLart-bericht van DigiD app naar afnemer app (app2app).

Website url: https://www.logius.nl
Print datum: 29/03/2024 06:56:26