< IH Berichtauthenticatie met DigiD

Datum: 16 december 2016
Publicatie: AORTA 2015 (V6.14.0.0)

Inhoudsopgave

1 Inleiding

1.1 Doel en scope

Dit document heeft tot doel een handleiding te geven voor de implementatie van het koppelvlak tussen het goed beheerd patiënten portaal (GBP) en het landelijk schakelpunt (LSP) voor wat betreft de toe te passen technieken voor de authenticatie van patiënten.

Dit document specificeert het SAML (Security Assertion Markup Language) authenticatietoken voor patiënten die zich bij DigiD laten authenticeren.

1.2 Doelgroep voor dit document

Dit document is bedoeld voor softwareontwikkelaars van het goed beheerd patiënten portaal en het LSP, die op grond van de HL7v3 communicatiestandaard en op grond van dit document berichten willen uitrusten met het SAML authenticatietoken. Daarnaast wordt het plaatsen van de digitale handtekening besproken (zie ook [IH tokens generiek]).

1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12 oktober 2011	RfC 46142: SOAP Headers van tokens worden uitgebreid met soap:actor.
6.11.0.1	29 januari 2013	Aanpassingen ten behoeve van DigiD v4.0 koppelvlak SAML
6.12.15.0	14-dec-2015	Ongewijzigd overgenomen in documentset 6.12.15.0
6.14.0.0	16-dec-2016	Ongewijzigd overgenomen in documentset 6.14.0.0

2 Het SAML authenticatietoken

In dit hoofdstuk wordt de inhoud van het gecreëerde SAML authenticatietoken van DigiD besproken die bij berichtauthenticatie voor patiënten wordt gebruikt. Het SAML authenticatietoken bevat informatie over de toegepaste authenticatie en identificatie van de patiënt. Het SAML authenticatietoken is een op XML gebaseerde SAML assertion en heeft tot doel de *assertions* (bewijs van een bewering) over te brengen tussen partijen (service- en identity provider) die een vertrouwensrelatie hebben.

Alle XML voorbeelden in het document dienen door de betrokken partijen tijdens het bouwen van de uitwisseling getest, en waar nodig, in samenspraak met Nictiz aangepast te worden voor een juiste optimale werking.

Voor het verkrijgen van het SAML authenticatietoken en het aanbieden van dit token aan de ZIM worden de volgende profielen gebruikt:

- Een op Web browser gebaseerd profiel van het authenticatie verzoek protocol is gedefinieerd ter ondersteuning van Single Sign-On. Dit profiel raakt de koppelvlakken:
  - patiënt ondersteuning (PC) - goed beheerd patiëntenportaal (GBP)
  - goed beheerd patiëntenportaal (GBP)- identity provider (neemt als vertrouwde autoriteit, de diensten van DigiD waar)

  Dit profiel is niet normatief en is terug te vinden in Het SSO profiel.
- Het gebruik van het SAML authenticatietoken (security token) in het kader van het WSS SOAP berichten profiel voor het veilig stellen en uitwisseling van authentieke SOAP berichten. Dit profiel raakt het koppelvlak:
  - goed beheerd patiëntenportaal (GBP) – het landelijk schakelpunt (LSP)

  Dit profiel wordt in de volgende paragrafen verder uitgewerkt.

2.1 Structuur

Het SAML authenticatietoken is een door een vertrouwde Identity Provider (DigiD) gecreëerde SAML assertion die gebruikt wordt bij berichtauthenticatie van patiënten voor het landelijk EPD. DigiD kan de eigenlijke assertion nog niet ondertekenen. De assertion maakt echter onderdeel uit van de ArtifactResponse. Deze ArtifactResponse kan DigiD wel ondertekenen. Daarom wordt de gehele ArtifactResponse als authenticatietoken in het bericht opgenomen. Aangezien het gebruik van een ArtifactResponse als authenticatietoken feitelijk in strijd is met de WS-Security standaard [WSS] en het daarbinnen gedefinieerde WS-SAML-token profile [SAML Token] moet deze situatie gezien worden als tijdelijk en zo snel mogelijk gecorrigeerd worden op het moment dat DigiD wel in staat is de assertion te ondertekenen.

2.1.1 ArtfactResponse

De ArtifactResponse heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

```
<samlp:ArtifactResponse
      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#"
      InResponseTo="_099440165b7981618772989d92d9aa2c53aa7217"
      Version="2.0"
      ID="_b2728a3aa52c4779c4c77ab8dd8a7dda604c94c7"
      IssueInstant="2012-12-20T18:50:27Z">
```

```
      <saml:Issuer>SamlIssuer</saml:Issuer>
      <ds:Signature>
          <!-- plaats van de digitale handtekening (over de ArtifactResponse) -->
      </ds:Signature>
      <samlp:Status>
          <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </samlp:Status>
      <samlp:Response InResponseTo="_7afa6d9f9ff28ca9233ada1d9ec2aa1bd6c5ce49"
          Version="2.0" ID="_107276b93ba8609c9d0954de6e5d2cd6e36fee96"
          IssueInstant="2012-12-20T18:50:27Z">
          <saml:Issuer>SamlIssuer</saml:Issuer>
          <samlp:Status>
              <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
          </samlp:Status>
          <saml:Assertion
              Version="2.0" ID="_dc9f793e2811b86f8e5cdf43ab5fd47d1fe0e61c"
              IssueInstant="2012-12-20T18:50:27Z">
              <!-- Hier bevind zich de eigenlijke assertion, zie hoofdstuk 2.1.2 -->
          </saml:Assertion>
      </samlp:Response>
  </samlp:ArtifactResponse>
```

2.1.2 Assertion

De assertion heeft de volgende structuur (de waarden die in het token gebruikt worden zijn fictief):

```
<saml:Assertion
    Version="2.0"
    ID="_dc9f793e2811b86f8e5cdf43ab5fd47d1fe0e61c"
    IssueInstant="2012-12-20T18:50:27Z">
    <saml:Issuer>SamlIssuer</saml:Issuer>
    <saml:Subject>
        <saml:NameID>s00000000:12345678</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData
                InResponseTo="_7afa6d9f9ff28ca9233ada1d9ec2aa1bd6c5ce49"
                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>
            <saml:AuthnContextClassRef>
                urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
            </saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
</saml:Assertion>
```

2.2 Namespaces

Het door een vertrouwde Identity Provider afgegeven SAML authenticatietoken dat gebruikt wordt bij berichtauthenticatie, maakt gebruik van de volgende namespaces. De prefixen zijn niet normatief maar worden in dit document als voorbeelden gebruikt.

Tabel AORTA.STK.t3400 - Namespaces

Prefix	Namespace URI
ds	http://www.w3.org/2000/09/xmldsig#
ec	http://www.w3.org/2001/10/xml-exc-c14n#
saml	urn:oasis:names:tc:SAML:2.0:assertion
samlp	urn:oasis:names:tc:SAML:2.0:protocol
wss	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd

Bij het gebruik van de namespace-prefixes is het van belang deze na het ondertekenen niet meer te veranderen, dit maakt de digitale handtekening ongeldig.

2.3 Inhoud

De volgende paragrafen beschrijven de verschillende kenmerken en beveiligingsgerelateerde gegevens die het SAML authenticatietoken onderscheiden, zoals in [IH tokens generiek] beschreven is.

```
<samlp:ArtifactResponse 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#" … >
```

Op de plaats van de drie punten (…) worden Uniekheidattributen opgenomen ten aanzien van de ArtifactResponse. De Assertion die daarbinnen is opgenomen heeft eigen Uniekheidattributen zoals beschreven in paragraaf 2.3.1 Uniekheid.

2.3.1 Uniekheid

```
<saml:Assertion
  Version="2.0"
  ID="_dc9f793e2811b86f8e5cdf43ab5fd47d1fe0e61c"
  IssueInstant="2012-12-20T18:50:27Z">
```

De attributen van het SAML assertion element maken van de afgegeven SAML assertion een uniek gegeven. Het attribuut ID identificeert op een unieke wijze de assertion. Het attribuut IssueInstant is een tijdsmoment van uitgifte van de SAML assertion. De tijdswaarde is gecodeerd in UTC. Het attribuut Version is de gebruikte SAML versie van de SAML assertion. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie is "2.0".

2.3.2 Onderwerp

```
<saml:Subject>
  <saml:NameID>s00000000:12345678</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
     <saml:SubjectConfirmationData
        InResponseTo="_7afa6d9f9ff28ca9233ada1d9ec2aa1bd6c5ce49"
        Recipient="http://example.com/artifact_url"
        NotOnOrAfter="2012-12-20T18:52:27Z"/>
  </saml:SubjectConfirmation>
</saml:Subject>
```

Het onderwerp `<Subject>` bij berichtauthenticatie met DigiD is een referentie naar een authenticatie verzoek van een patiënt dat door het goed beheerd patiëntenportaal is geïnitieerd. Het onderwerp bevat een uniek authenticatie nummer, het `<NameID>` element.

DigiD neemt in het element `<NameID>` het sectoraal nummer op in het formaat <sectorcode>:<sectoraal nummer>

Indien de sectorcode de waarde 'S00000000' heeft, dan is het sectoraal nummer een BurgerServiceNummer.

De bevestiging van het onderwerp `<SubjectConfirmation>` wordt gebruikt om te bevestigen dat het authenticatie verzoek (het `InResponseTo` attribuut) van het patiëntenportaal (het `Recipient` attribuut) kwam. Verder heeft de bevestiging van het onderwerp een geldigheidsduur (het `NotOnOrAfter` attribuut). De geldigheidsduur geeft de duur van een sessie aan tussen het goed beheerd patiëntenportaal en de identity provider (DigiD). Voor deze bevestigingsmethode (het `Method` attribuut) moet de URN waarde "`urn:oasis:names:tc:SAML:2.0:cm:bearer`" (assertion drager) worden gebruikt.

2.3.3 Geldigheid

```
<saml:Conditions
 NotBefore="2012-12-20T18:48:27Z"
 NotOnOrAfter="2012-12-20T18:52:27Z">
  …
</saml:Conditions>
```

Op de plaats van de drie punten (…) kan een AudienceRestriction worden toegevoegd zoals beschreven in paragraaf 2.3.5 Ontvanger).

Het attribuut *NotBefore* is de tijd waarop de afgegeven SAML assertion geldig wordt.

Wordt een bericht ontvangen voor *NotBefore* is aangevangen, dan **moet** dit bericht geweigerd worden.

Het attribuut *NotOnOrAfter* is de tijd waarop de afgegeven SAML assertion vervalt.

Wordt een bericht ontvangen op of nadat *NotOnOrAfter* is verstreken, dan **moet** dit bericht geweigerd worden[1].

Aangezien DigiD deze waarden interpreteert als tijdstip van authenticatie wordt de geldigheidtermijn (d.i. de eindtijd NotOnOrAfter) opgehoogd met een "ZIM-max-BSN-gracetijd" van 15 minuten.

Het tijdsverschil tussen `NotOnOrAfter` en `NotBefore` bedraagt maximaal 4 minuten in DigiDv4.0-SAML. De tijden worden bepaald op het afgiftemoment van de assertion bij DigiD waarbij `NotBefore` de waarde afgiftemoment - 2 minuten en `NotOnOrAfter` de waarde afgiftemoment + 2 minuten krijgt.

De geldigheidsduur van een token (*NotOnOrAfter* minus *NotBefore*) mag niet langer dan 4 minuten zijn. Wordt een bericht ontvangen waarin deze geldigheidsduur overschreden is, dan **moet** dat bericht geweigerd worden, ook al is het tijdstip *NotOnOrAfter* nog niet verstreken.

Van het GBP wordt verwacht dat zij een timer bijhoudt die op het moment dat een gebruiker van het Portaal (de burger) via een redirect vanuit DigiD terugkeert in het LSP-portaal gestart moet worden en de gebruiker na 15 minuten (als de gebruiker op dat moment een nieuwe actie wil doen) weer terugstuurt naar DigiD voor herauthenticatie. Tevens dient het GBP op grond van deze timer een eventueel nog aanwezig ArtefactResponse token te verwijderen.

De subelementen `OneTimeUse` en `ProxyRestriction` worden niet gebruikt binnen het `<Conditions>` element bij Berichtauthenticatie met DigiD.

2.3.4 Afzender

```
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
  https://federatie.overheid.nl/aselectserver/server/
</saml:Issuer>
```

De afzender is de authenticatie autoriteit (DigiD) die de assertion heeft afgegeven en de patiënt heeft geauthenticeerd. De Issuer wordt in dit fictieve voorbeeld uitgedrukt met behulp van een URL.

Noot: In samenspraak met Nictiz en andere betrokken partijen kan het formaat en inhoud van de `Issuer` in de assertion heroverwogen worden, zie volgende opmerking.

De `Issuer` kan ook uitgedrukt worden met behulp van URN (Uniform Resource Name). De URN is opgebouwd uit:

[1] Met de configuratie parameter "*ZIM-max-BSN-gracetijd*" van de ZIM kan de geldigheidtermijn van een SAML assertion vergroot worden waarbij de begintijd *(NotBefore)* vervroegd en de eindtijd (*NotOnOrAfter)* verlaat mag worden.

```
"urn:IIroot:"<OID van het coderingssysteem>":IIext:"<extensie>
```

De URN string is opgebouwd uit een IIroot en een IIext. "II" staat voor Instance Indentifier. Binnen AORTA is de IIroot een oid (Object IDentifier), die een identificatie- of coderingssysteem weergeeft, en dat leidt in HL7v3 XML tot een element met twee attributen, een root met de uitgegeven codering en een extensie (ext). Om de namespace in URN uniek te krijgen is II als prefix voor de root en ext geplaatst.

Indien de keuze door de betrokken partijen gemaakt wordt om de `Issuer` als URN uit te drukken, moet de root en extensie door de GBP organisatie aangevraagd en geregeld worden.

Het goed beheerd patiëntenportaal past een SSL/TLS-sessie toe bij het opvragen van de assertion bij de identity provider.

2.3.5 Ontvanger

```
  <saml:AudienceRestriction>
     <saml:Audience>http://sp.example.com</saml:Audience>
  </saml:AudienceRestriction>
```

```
<saml:AudienceRestriction>
  <!-- Root en extensie van de ZIM en het patiëntenportaal -->
  <saml:Audience>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
  <saml:Audience>urn:IIroot:?:IIext:?</saml:Audience>
</saml:AudienceRestriction>
```

In de `AudienceRestriction` wordt beschreven aan welke ontvangende partijen (service providers) de SAML assertion is gericht. De waarden in de elementen zijn (voorlopig) vaste waarden. Voor de `<Audience>` parameter is (ook) gekozen voor URN, zie voor de opbouw van de URN paragraaf 2.3.4 Afzender.

Het element AudienceRestriction wordt door DigiD nog niet ondersteund. Op het moment dat DigiD wel ondersteuning biedt, dient het element verplicht aanwezig te zijn en dient er controle op het element AudienceRestriction plaats te vinden.

2.3.6 Authenticatie

```
<saml:AuthnStatement
  SessionIndex="17"
  AuthnInstant="2012-12-20T18:50:27Z">
  …
</saml:AuthnStatement>
```

Op de plaats van de drie punten (…) worden de `<SubjectLocality>` en de `<AuthnContext>` toegevoegd zoals hieronder beschreven.

Het onderwerp (Subject), een patiënt, in de SAML assertion is geauthenticeerd doormiddel van een authenticatiemiddel op een gegeven moment.

```
<saml:SubjectLocality Address="127.0.0.1"/>
```

De `SubjectLocality` is gevuld met het IP-adres (`Address` attribuut) van de PC van de gebruiker en is onderdeel van het `AuthnStatement`. Deze wordt gebruikt om te verifiëren of de patiënt een vervolg verzoek vanaf hetzelfde IP-adres doet als zijn initiële verzoek tijdens het benaderen van het patiëntenportaal.

Bij communicatie tussen de computer van de patiënt en het patiëntenportaal mag het adres van de computer van de patiënt tijdens een sessie niet wijzigen. Bij wijziging van het adres (Address attribuut) tijdens de sessie in de SubjectLocality, wordt dit als malafide activiteit aangemerkt en wordt de sessie beëindigd en is herauthenticatie vereist.

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
  </saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Binnen de SAML specificatie is het mogelijk om een authenticatie-context (*AuthnContext*) mee te geven die de context aangeeft van het gebruikte authenticatiemiddel. Binnen de SAML specificatie zijn een aantal contexten gespecificeerd, zie [SAML Authn Context], die gebruikt kunnen worden als referentiekader voor communicatie tussen de ZIM en andere componenten zoals het goed beheerd patiëntenportaal.

Uitgaande van de beveiligingsniveaus van het goed beheerd patiëntenportaal, patiënt en de indentity provider, wordt het "*urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract*" beveiligingsniveau gehanteerd om het AORTA vertrouwensniveau midden weer te geven. Het AORTA vertrouwensniveau midden staat gelijk aan de DigiD authenticatiesterkte 20.

2.4 Algoritmes

Om de integriteit en onweerlegbaarheid van het SAML authenticatietoken te waarborgen wordt een XML Signature geplaatst, zoals beschreven in [IH tokens generiek]. Na plaatsen van de XML Signature kan de ontvanger, met gebruikmaking van het PKIoverheid-certificaat van de verzender onomstotelijk vaststellen dat de getekende SAML assertion ondertekend is met de privé sleutel behorend bij het gebruikte PKIoverheid-certificaat.

De XML Signature van het SAML authenticatietoken die gebruikt wordt bij berichtauthenticatie met behulp van DigiD maakt gebruik van de volgende algoritmes, zoals beschreven in [IH tokens generiek].

- Voor het berekenen van de hashwaarde wordt SHA-256 gebruikt.
- Voor de digitale handtekening in AORTA wordt gebruik gemaakt van een RSA handtekening over een SHA-256 digest.
- Omdat de XML Signature onderdeel is van het SAML authenticatietoken en in het SAML authenticatietoken geplaatst wordt, moet er een "enveloped-signature"

transformatie uitgevoerd worden die de Signature tags uit het SAML authenticatietoken verwijderd.

2.5 Opbouw

2.5.1 Authenticatie en SSO (Single Sign-On)

Deze paragraaf is informatief.

De patiënt kan het goed beheerd patiëntenportaal (GBP) via internet benaderen en daarmee toegang krijgen tot het landelijk schakelpunt (LSP). Eerst zal de patiënt zich echter moeten identificeren bij de Identity Provider (IdP) zijnde DigiD. De IdP verzorgt authenticatie- en single sign-on diensten en levert gebruikerskenmerken (assertion) op die nodig zijn voor autorisatie. De patiënt wordt pas tot het landelijk schakelpunt toegelaten als in het bericht een geldige SAML authenticatietoken voor het LSP is opgenomen.
Dit ontlast het goed beheerd patiëntenportaal van het beheer van authenticatiemiddelen.

De authenticatie- en single sign-on diensten die door de IdP worden aangeboden voor het GBP, worden in Het SSO profiel verder uitgewerkt.

2.5.2 De header

Na authenticatie en toegangsverlening van een patiënt op het GBP moet het GBP er zorg voor dragen dat het SAML authenticatietoken wordt toegevoegd bij de berichten die van het GBP naar het landelijk schakelpunt worden verzonden.

Het SAML authenticatietoken – het `<saml:ArtifactResponse ...>` is aangemaakt en gevuld met die elementen, zoals beschreven in paragraaf 2 Het SAML authenticatietoken.

```
<samlp:ArtifactResponse
    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#"
    InResponseTo="_099440165b7981618772989d92d9aa2c53aa7217"
    Version="2.0"
    ID="_b2728a3aa52c4779c4c77ab8dd8a7dda604c94c7"
    IssueInstant="2012-12-20T18:50:27Z">
    <saml:Issuer>SamlIssuer</saml:Issuer>
    <ds:Signature>
        <!-- plaats van de digitale handtekening (over de ArtifactResponse) -->
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <samlp:Response InResponseTo="_7afa6d9f9ff28ca9233ada1d9ec2aa1bd6c5ce49"
        Version="2.0" ID="_107276b93ba8609c9d0954de6e5d2cd6e36fee96"
        IssueInstant="2012-12-20T18:50:27Z">
        <saml:Issuer>SamlIssuer</saml:Issuer>
        <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion
            Version="2.0" ID="_dc9f793e2811b86f8e5cdf43ab5fd47d1fe0e61c"
            IssueInstant="2012-12-20T18:50:27Z">
            <!-- Hier bevindt zich de assertion (zie paragraaf 2.3 Inhoud)-->
        </saml:Assertion>
```

```
    </samlp:Response>
</samlp:ArtifactResponse>
```

Het XML Signature blok is onderdeel van het SAML authenticatietoken. Het XML Signature blok komt na het `<saml:Issuer>` element van de `<saml:ArtifactResponse>`.

```
<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="#_b2728a3aa52c4779c4c77ab8dd8a7dda604c94c7">
            <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>675ga8KqGFqJSGgSJHzoVU+kgrlWqYLpTxJ28gWLPkQ=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>ecXG...igg==</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:KeyName>e37ee2522de410c633b3700835727ebf1834cd88</ds:KeyName>
    </ds:KeyInfo>
</ds:Signature>
```

2.5.3 Plaats van het SAML token en de digitale handtekening

Het SAML authenticatietoken met daarin de digitale handtekening worden in het WS-Security SOAP Header gezet. Op het `<wss:Security>` element **moet** een `soap:mustUnderstand="1"` vlag opgenomen worden, die aangeeft dat de ontvanger dit security element **moet** verwerken en een `soap:actor="http://www.aortarelease.nl/actor/zim"` die aangeeft dat de ZIM dit security element verwerkt.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ...
  <wss:Security xmlns:wss=
    "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"
    soap:actor="http://www.aortarelease.nl/actor/zim" soap:mustUnderstand="1">
    <saml:ArtifactResponse ...>
    ... Zie paragraaf 2.3 Inhoud ...
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
        ...
        </ds:SignedInfo>
        <ds:SignatureValue>Wuwn...5e4=</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:KeyName>e37ee2522de410c633b3700835727ebf1834cd88</ds:KeyName>
        </ds:KeyInfo>
      </ds:Signature>
    </saml:ArtifactResponse ...>
  </wss:Security>
</soap:Header>
```

Het X509Data element (waar het certificaat in is opgenomen) wordt niet met het bericht meegestuurd maar bevindt zich in het metadocument wat bij DigiD op te halen is.

Het daarin gebruikte entity_id wordt tevens gebruikt als Issuer in de ArtifactResponse.

3 Certificaten

3.1 Te gebruiken certificaat en attributen

Voor het tekenen van het SAML authenticatietoken wordt het authenticiteitcertificaat van de identity provider DigiD gebruikt. Dit certificaat bevat een RSA publieke sleutel. Met de privé sleutel wordt de digitale handtekening gegenereerd.

De attributen in het authenticiteitcertificaat worden gegeven in de vorm van een Distinguished Name (DN) en het serienummer, zie [IH tokens generiek].

De volgende attribuutwaarden zijn voorbeelden en moeten in samenspraak met Nictiz en ander betrokken partijen (zoals de certificaatdienstverlener) nog bepaald en vastgelegd worden.

Tabel AORTA.STK.t3410 – Certificaat attributen

Attribuut	Omschrijving	Waarde
CN	Subject.commonName	as.digid.nl
OU	Subject.organizationalUnitName	Digid
O	Subject.organizationName	Stichting ICTU
C	Subject.countryName	NL
Serienummer	SerialNumber. Wordt door de certificaatdienstverlener vastgelegd	PK070001000868195 (voorbeeld)

Om de digitale handtekening bij de ZIM te verifiëren, moet de ontvanger over de bijbehorende publieke sleutel beschikken, zie [IH tokens generiek]. Voor verificatie is gekozen door een verwijzing naar het authenticiteitcertificaat in het SAML authenticatietoken als KeyInfo mee te zenden; de ontvanger moet deze dan met bijvoorbeeld het LDAP protocol ophalen, zie ook [IH tokens generiek].

Noot: In samenspraak met Nictiz en andere betrokken partijen kan de keuze voor opnemen van een verwijzing naar het certificaat nog heroverwogen worden.

4 Token afhandeling

4.1 Verificatie met het bericht

Het is belangrijk vast te stellen dat velden in het SAML authenticatietoken overeenstemmen met die in het HL7v3 bericht. Wanneer dit niet zou gebeuren, kan een kwaadwillende met een gestolen token nog steeds gegevens opvragen van bv. ieder willekeurig burgerservicenummer.

Voordat het GBP de berichten met de daarbij behorende SAML authenticatietoken doorstuurt naar de ZIM, voert het patiëntenportaal een aantal controles uit op de afgegeven SAML assertion. De controles die het GBP uitvoert staan beschreven in SSO verificatie, omdat deze controles buiten de scope van deze implementatie handleiding vallen.

Na controle door het GBP wordt de SAML assertion door het GBP in de WS-Security SOAP Header geplaatst voor verzending naar de ZIM, zoals beschreven in paragraaf 2.5.3.

De ontvanger controleert of de WS-Security SOAP Header voor hem bestemd is, zie soap attribuut actor.

Het SAML authenticatietoken wordt door de ontvanger uit de WS-Security SOAP Header gehaald indien de WS-Security SOAP Header voor de ontvanger bestemd is en dat de ontvanger deze moet verwerken. Bij gebruik van het SAML authenticatietoken moet de ontvanger controleren of de digitale handtekening over het SAML authenticatietoken geldig is:

- De aanduiding voor de versie van SAML gedefinieerd is op "2.0", zie paragaaf 2.3.1 Uniekheid;
- De verschillende attributen die bij de bevestiging van het onderwerp horen voldoen aan de daarvoor gestelde eisen, zie paragraaf 2.3.2 Onderwerp;
- Het sectoraal nummer een BSN aanduidt en dat het bijbehorende BSN identiek is aan het BSN in de payload van het HL7v3 bericht zie paragraaf 2.3.2 Onderwerp;
- Het bericht ontvangen is binnen de geldigheidsperiode van het token, zie paragraaf 2.3.3 Geldigheid;
- De juiste afzender is vastgelegd, die deze assertion heeft gecreëerd en de patiënt heeft geauthenticeerd, zie paragraaf 2.3.4 Afzender;
- De verschillende afnemers van de assertion (audience) benoemd zijn die dit token mogen ontvangen en verwerken, zie paragraaf 2.3.5 Ontvanger;
- De patiënt geauthenticeerd is door de authenticatie autoriteit (DigiD) met het voorgedefinieerde authenticatiemiddel, de MobileTwoFactorContract (authenticatiesterkte 20 = AORTA vertrouwensniveau midden), vanaf een bepaalde locatie, zoals beschreven in paragraaf 2.3.6 Authenticatie;
- Alleen die attributen zijn gedefinieerd, die zijn beschreven in paragraaf

Als aan één van de bovenstaande condities niet is voldaan, moet het bericht door de ontvanger geweigerd worden en een SOAP foutmelding aan het verzendende systeem afgegeven worden, zie foutafhandeling in [IH tokens generiek].

Als wel aan alle condities is voldaan, wordt het HL7v3 bericht verder verwerkt.

Bijlage A Referenties

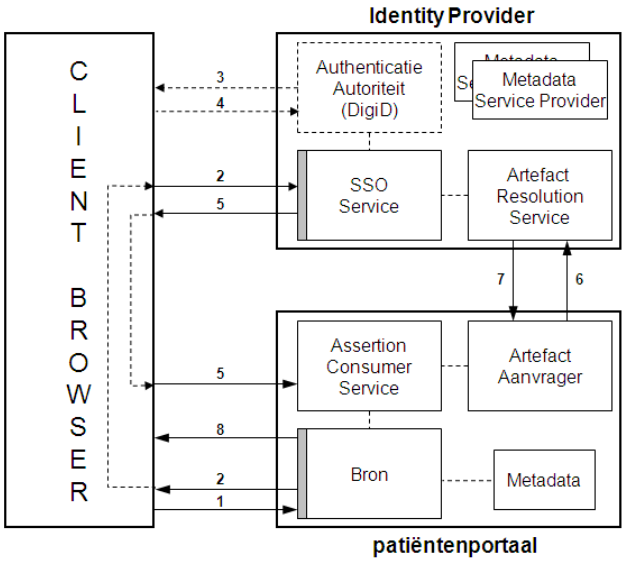
Referentie	Document	Versie
[IH tokens generiek]	Implementatiehandleiding security tokens generiek	6.14.0.0
[SAML Assertion Protocol]	Assertion and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	2.0 15 maart 2005
[SAML Authn Context]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf	2.0 15-mrt-2005
[SAML Profiles]	Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf	2.0 15-mrt-2005
[SAML Token]	SAML Token Profile http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf	1.1 01-feb-2006
[WSS]	WS-Security SOAP Message Security http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf	1.1 01-feb-2006

Bijlage B Het SSO profiel

Het Single Sign-On profiel (SSO) is een SAML profiel dat aangeeft hoe gebruik te maken van het SAML authenticatie vraag en antwoord protocol in combinatie met verschillende SAML-bindings, zoals SOAP en HTTP. De communicatie bij authenticatie gaat tussen een Identity Provider (partij die verantwoordelijk is voor de waarmerking van de gebruiker) en een Service Provider (partij die een applicatie of bron beschikbaar stelt voor de gebruiker).

Noot: Het patiëntenportaal (GBP) vervult de rol van de Service Provider. De Identity Provider (IdP) wordt vervuld door DigiD.

Het volgende figuur illustreert het proces (stappen 1 t/m 8) voor de verwezenlijking van het SSO profiel. De stappen zijn in deze bijlage uitgewerkt.



1. Toegang vragen tot het patiëntenportaal (HTTPS)
2. Doorgeven van <AuthnRequest> naar "SSO Service" bij Identity Provider
3. Identiteit van gebruiker vaststellen door Authenticatie Autoriteit (DigiD)
4. Gebruikerslogin sessie bij Authenticatie Autoriteit
5. Doorgeven van SAML Artefact referentie
6. Artefact Resolve (SOAP) bericht
7. Artefact Response (SOAP) bericht met een ondertekend SAML assertion
8. Toegangverlening tot het patiëntenportaal

Voorbeeld van configuratie waarden voor een fictieve testomgeving:

Entiteit	Waarde
Domein patiëntenportaal	"testportal.aorta-zorg.nl"
Domein Identity Provider	"federatie.overheid.nl"
Assertion Consumer Service	"https://testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO"
SSO Service	"https://federatie.overheid.nl/aselectserver/server/saml20_sso"
Artefact Resolution Service	"https://federatie.overheid.nl/aselectserver/server/saml20_artifact"
Authenticatie Autoriteit	"https://federatie.overheid.nl/aselectserver/server"

Noot: Omdat niet *alle* internet browsers een ongelimiteerde URL ondersteunen, wordt er gebruik gemaakt van HTTP artefact binding (zie de pijlen 6 en 7 in bovenstaand figuur).

Stap 1: Het HTTP Request voor het patiëntenportaal

Een patiënt verzoekt via een cliënt (internet) browser toegang tot het patiëntenportaal (GBP). Dit is een standaard HTTP/SSL verzoek, hiervoor worden geen beperkingen opgelegd.

Stap 2: Het afgeven van een <AuthnRequest>

De 2e stap is implementatie afhankelijk. Voor het authenticeren van burgers is DigiD de aangewezen authenticatie-autoriteit. Het patiëntenportaal stuurt de gebruiker via een HTTP-Redirect door naar een voorgedefinieerde Identity Provider waar de gebruiker wordt geauthenticeerd. Voor dit geval geeft het patiëntenportaal een `<AuthnRequest>` door. De `<AuthnRequest>` is van het complexe type AuthnRequestType dat afgeleid is van het abstracte complexe type RequestAbstractType. Zie voor alle SAML elementen en types [SAML Assertion Protocol].

De locatie van de "SSO Service", die binnen het Identity Provider domein actief is, wordt out-of-band doorgegeven met behulp van een SAML Metadata bestand. Dit bestand bevat tevens de publieke X509-certificaten voor de ondertekening en eventuele encryptie. Encryptie wordt vooralsnog niet gebruikt.

```
<md:IDPSSODescriptor ... >

<!-- Metadata van de SSO Service als onderdeel van de Identity Provider -->
   <md:SingleSignOnService
   Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://federatie.overheid.nl/aselectserver/server/saml20_sso"/>
  ...
</md:IDPSSODescriptor>
```

Het `<SingleSignOnService>` element is van het complexe type IndexedEndpointType en onderdeel van het `<IDPSSODescriptor>` element uit het metadata bestand dat een specifiek profiel (dienstverlening) reflecteert ter ondersteuning van het SSO profiel van de Identity Provider.

Het `<SingleSignOnService>` metadata element bestaat uit de volgende attributen:

Naam (@=attribuut)	Omschrijving	Vereist
@Binding	Specificeert de binding dat door de "SSO Service" wordt ondersteund. De binding wordt via een URI geïdentificeerd. Bijvoorbeeld: "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect".	Ja
@Location	De locatie van de "SSO Service". Ook een URI attribuut.	Ja

Het patiëntenportaal initieert de SAML binding. In antwoord op het authenticatie verzoek wordt een antwoord aan het patiëntenportaal geleverd als onderdeel van de "SSO Service".

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Authenticatie verzoek via HTTP Redirect -->
```

```
<samlp:AuthnRequest AssertionConsumerServiceURL="https://testportal.aorta-zorg.nl:443/topa-
prototype/saml/SSO"
 Destination="https://federatie.overheid.nl/aselectserver/server/saml20_sso"
 ID="authntoken_2.16.528.1.1007.3.3.1234567.1_0123456789"
 IssueInstant="2009-06-24T11:46:53Z"
 ProviderName="testportal.aorta-zorg.nl"
 Version="2.0"
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">


<!-- Aanvrager van het authenticatie verzoek -->
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
>https://testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>

 <!-- Authenticatie-context -->
 <samlp:RequestedAuthnContext Comparison="exact">
  <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
>urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract</saml:AuthnContextClassRef>
 </samlp:RequestedAuthnContext>

 <!-- Partijen waar toegang voor gevraagd wordt -->
 <saml:Conditions>
  <saml:AudienceRestriction>
   <saml:Audience
>urn:IIroot:2.16.840.1.113883.2.4.6.6:IIext:1</saml:Audience>
<!-- Root en extensie van het GBP -->
   <saml:Audience>urn:IIroot:?:IIext:?</saml:Audience>
  </saml:AudienceRestriction>
 </saml:Conditions>

</samlp:AuthnRequest>
```

Het SAML authenticatie verzoek `<AuthnRequest>` bestaat uit verschillende attributen en elementen. De elementen worden in hiërarchische (top-down) volgorde beschreven en hebben de volgende betekenis:

Naam (@=attribuut)	Omschrijving	Vereist
@ID	Unieke identificatie van het (authenticatie) verzoek. De waarden van de ID-attribuut in een verzoek en de InResponseTo attribuut in het bijbehorende antwoord moeten overeenkomen.	Ja
@Version	De SAML versie van dit (authenticatie) verzoek. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie wordt "2.0".	Ja
@IssueInstant	Tijdsmoment van uitgifte van het (authenticatie) verzoek. De tijdswaarde is gecodeerd in UTC.	Ja
@Destination	Een URI referentie waarnaar het (authenticatie) verzoek wordt verzonden, dit om malafide activiteiten te voorkomen. De ontvangende partij dient de URI verwijzing te controleren met de	Nee

	locatie waar het bericht is ontvangen. Indien dit niet overeenkomt, moet het bericht genegeerd en verwijderd worden.	
@AssertionConsumerServiceURL	Hiermee wordt aangegeven waar het antwoord van het (authenticatie) verzoek heen gestuurd moet worden, De responder moet ervoor zorgen dat de opgegeven waarde in feite verbonden is aan het verzoek.	Nee
@ProviderName	Leesbare naam van de aanvrager van het (authenticatie) verzoek. Wordt gebruikt door de gebruiker van de Identity Provider.	Nee
saml:Issuer	Geeft de entiteit die het (authenticatie) verzoek heeft gegenereerd.	Ja
saml:Conditions	Via de condities kan de aanvrager van het (authenticatie) verzoek de geldigheid en/of gebruik van de verkregen assertion beperken. De responder *kan* wijzigingen of aanvullingen in de assertion invoeren als zij dit nodig acht aan de hand van de gegeven condities. Paragraaf 2.3.3 Geldigheid Geldigheid beschrijft kaders van de SAML condities waaraan het (authenticatie) verzoek moet voldoen	Ja
saml:Subject	De entiteit die het (authenticatie) verzoek genereert kan een `<Subject>` element toevoegen waarin het onderwerp van de verklaring(en) staat voor de ontvangende assertion. Dit element mag geen `<SubjectConfirmation>` elementen in het verzoek bevatten.	Nee
samlp:RequestedAuthnContext	Specificeert in welke context de authenticatie statement wordt afgegeven, in antwoord op het (authenticatie) verzoek. Indien dit element aanwezig is, *moet* het antwoord een `<AuthnContext>` bevatten.	Nee

`<AuthnContext>` (authenticatie-context) wordt gedefinieerd als de informatie, naast de authenticatie assertion zelf, dat een vertrouwde partij kan eisen voordat zij een besluit neemt over het afgeven van een assertion. De authenticatie-context kan informatie

bevatten over de actuele authenticatie methode (de "sterkte" van het gebruikte authenticatiemiddel) die gebruikt wordt.

Binnen de SAML specificatie zijn verschillende mogelijke authenticatie-contexten gespecificeerd die gebruikt kunnen worden als referentiekader voor de communicatie tussen de aanvrager en uitvoerder van het authenticatieverzoek. Dit moet met de software leverancier verder afgestemd worden, zie ook AuthnContextClassRef. Het `<RequestedAuthnContext>` element is van het complexe type RequestedAuthnContextType en bevat één of meerdere elementen en attributen. Zie ook [SAML Assertion Protocol] en [SAML Authn Context] voor de verschillende voorgedefinieerde context klassen voor authenticatie.

Naam (@=attribuut)	Omschrijving	Vereist
@Comparison	Specificeert welke vergelijkingsmethode gebruikt wordt om de gevraagde context klasse te evalueren. Standaard is de waarde "exact". Dit houdt in dat de inhoud van de authenticatie assertion exact moet matchen met tenminste een van de opgegeven authenticatie-context klassen. Andere mogelijke waarden zijn: "minimum", "maximum", of "better".	Nee
saml:AuthnContextClassRef	Is een URI naar een voorgedefinieerde context klasse voor authenticatie, zie [SAML Authn Context]. De URI waarde die nu bij DigiD als voorbeeld wordt gebruikt is "urn:oasis:names:tc:SAML:2.0:ac:classes :PasswordProtectedTransport". De PasswordProtectedTransport klasse is van toepassing wanneer een opdrachtgever een authenticatie autoriteit een gebruiker laat verifiëren met een wachtwoord dialoog via een beveiligde sessie.	Nee

Noot: DigiD kan verschillende authenticatiemiddelen hanteren om de identiteit van een gebruiker vast te stellen. Bij wijziging van de SAML contexten (saml:AuthnContextClassRef) kan de authenticatiesterkte wijzigen.

Noot: De huidige PasswordProtectedTransport heeft een te lage authenticatiesterkte en (AORTA) niveau voor patiënten die gebruik willen maken van het patiëntenportaal. Voor het patiëntenportaal moet de burger zich bij DigiD op AORTA vertrouwensniveau midden (laten) authenticeren, waarbij de afgegeven authenticatiesterkte 20 is. Zie volgende tabel.

Mogelijke keuze (moet met de software leverancier afgestemd worden)

Authenticatieniveau (AORTA)	AuthnContextClassRef (SAML)	Comparison (SAML)	Authenticatie sterkte (DigiD)
Laag, waarbij een burger aan de hand van een wachtwoord wordt geauthenticeerd	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	exact	10
Midden, waarbij een burger aan de hand van een wachtwoord en een tijdelijk eenmalige code, die hij per SMS ontvangt (per authenticatiepoging), authenticeert;	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract	exact	20
AORTA vertrouwensniveau midden, gelijk aan het vorige niveau waarbij de burger eenmalig op zijn fysieke verschijning tegen zijn WID is geverifieerd (een zogeheten face2face controle)	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract	better	22
Hoog. geeft de zekerheid dat alleen de desbetreffende persoon (zoals de patiënt, of zijn vertegenwoordiger of de zorgverlener) via eNIK wordt geauthenticeerd. eNiK staat voor elektronische Nederlandse Identiteitskaart.	urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI	exact	30

AuthnContextClassRef, zie [SAML Authn Context].

Stap 3 en 4: Identificeren van een Gebruiker door de Identity Provider

De authenticatie-autoriteit bij de Identity Provider moet de identiteit van de gebruiker vast stellen. Het authenticatie verzoek hiertoe wordt gedaan door het patiëntenportaal die het element `<RequestedAuthnContext>` in het verzoek toevoegt. De authenticatie-autoriteit start een dialoog op met de gebruiker om deze te identificeren aan de hand van het `<RequestedAuthnContext>`, zie [SAML Authn Context] .

Eis: Voor het patiëntenportaal **moet** het authenticatieniveau of betrouwbaarheidsniveau **"20"** door de authenticatie-autoriteit afgegeven worden, voordat een patiënt toegang krijgt tot het portaal.

Stap 5: Het antwoord van de Identity Provider

Ongeacht of de identificatie van een patiënt door de Identity Provider wel of niet lukt, wordt er een antwoord naar het patiëntenportaal gestuurd in de vorm van een artefact. Het patiëntenportaal maakt gebruik van het artefact resolution profiel. Het patiëntenportaal maakt hierbij gebruik van een callback aanroep naar de Identity Provider, om het `<Response>` bericht met behulp van een SOAP binding over authenticatie op te halen. De locatie van de "Assertion Consumer Service" kan met behulp van metadata van het patiëntenportaal worden bepaald. De Identity Provider moet middelen hebben om vast te stellen dat deze locatie wordt gecontroleerd door het patiëntenportaal.

Het patiëntenportaal geeft aan welke SAML binding en specifieke "Assertion Consumer Service" gebruikt wordt voor het `<AuthnRequest>` bericht. De Identity Provider moet deze instellingen volgen.

Wanneer de authenticatie via de "SSO Service" van de Identity Provider succesvol verlopen is, wordt de gebruiker terug naar het patiëntenportaal gedirigeerd.

```
Redirect to https://aselectserver/server/saml20_assertion?
SAMLart=AAQAABhQELuXX%3D
```

Bovenstand voorbeeld toont en SAML artefact referentie afgegeven door de "SSO Service" voor de "Assertion Consumer Service".

Stap 6: Het opvragen van een Artefact

Het patiëntenportaal maakt gebruik van het artefact resolution profiel, zie [SAML Profiles], om via een callback de `<AuthnRequest>` bericht te achterhalen waarin het uiteindelijke SAML authenticatie antwoord staat. Het artefact resolution profiel maakt gebruik van SOAP binding, wat ook in het SAML metadata bestand van de Identity Provider voor het patiëntenportaal is vastgelegd.

```
<md:IDPSSODescriptor ... >
  <md:ArtifactResolutionService
   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
   Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://federatie.overheid.nl/aselectserver/server/saml20_artifact"
   index="0"
   isDefault="true" />
  ...
</md:IDPSSODescriptor>
```

Het `<ArtifactResolutionService>` element is van het complexe type IndexedEndpointType en onderdeel van het `<IDPSSODescriptor>` element uit het SAML metadata bestand dat weer een specifiek profiel (dienstverlening) reflecteert ter ondersteuning van het SSO profiel van de Identity Provider.

Het <ArtifactResolutionService> element bestaat uit de volgende attributen en elementen:

Naam (@=attribuut)	Omschrijving	Vereist
@Binding	Specificeert de binding dat door de "Artefact Resolution Service" wordt ondersteund. De binding wordt via een URI geïdentificeerd. Bijvoorbeeld: "urn:oasis:names:tc:SAML:2.0:bindings:SOAP ".	Ja
@Location	De locatie van de "Artefact Resolution Service". Ook een URI attribuut.	Ja
@index	Een unieke integer waarde die aan de "Artefact Resolution Service" wordt toegekend, waarnaar in het protocol bericht wordt verwezen.	Ja
@isDefault	Wordt gebruikt om een standaard (Artefact Resolution) Service aan te wijzen uit een geïndexeerde set van diensten.	Nee

Het patiëntenportaal stuur een <ArtifactResolve> bericht met het gegeven <Artifact> referentie naar een "Artefact Resolution Service". De locatie van deze service kan weer met behulp van het SAML metadata bestand worden bepaald. Het opvragen van het artefact gebeurd via een beveiligde sessie met behulp van SOAP over HTTP.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/"
         xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
         xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
   <soap11:Body>
     <samlp:ArtifactResolve
      ID="samlart_2.16.528.1.1007.3.3.1234567.1_0123456789"
      IssueInstant="2009-06-24T11:47:01Z"
      Version="2.0">
      <saml:Issuer
        Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity"
>https://testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>
      <samlp:Artifact>AAQAABhQELuXX=</samlp:Artifact>
     </samlp:ArtifactResolve>
   </soap11:Body>
</soap11:Envelope>
```

Het <ArtifactResolve> element is van het complexe type ArtifactResolveType dat is afgeleid van RequestAbstractType en bestaat uit de volgende attributen en elementen:

Naam (@=attribuut)	Omschrijving	Vereist
@ID	Unieke identificatie van het Artefact verzoek. De waarde van het ID-attribuut in een verzoek en het InResponseTo attribuut in het bijbehorende antwoord moeten overeenkomen.	Ja
@IssueInstant	Tijdsmoment van uitgifte van het Artefact verzoek. De tijdswaarde is gecodeerd in UTC.	Ja
@Version	De versie van dit SAML Artefact verzoek. De aanduiding voor de versie van SAML gedefinieerd in deze specificatie wordt "2.0".	Ja
saml:Issuer	Geeft de entiteit die het Artefact verzoek doet.	Ja
samlp:Artifact	Artefact (referentie) waarde die de aanvrager heeft ontvangen en deze wenst te vertalen in het protocol boodschap die zij vertegenwoordigd. In dit geval is dat het antwoord op een authenticatie verzoek.	Ja

Eis: Er wordt bij een unieke artefact verzoek, maximaal één en eenmalig een artefact response bericht gegeven door de "Artefact Resolution Service", in antwoord op het verzoek.

Stap 7: De ArtifactResponse met de SAML assertion

Het uiteindelijke antwoord betreffende de authenticatie van een gebruiker staat in het <ArtifactResponse>. De "Artefact Resolution Service" geeft altijd een <Status> terug over de <ArtifactResponse>. De <ArtifactResponse> bevat de <Response> van de Identity Provider, of de identificatie en authenticatie van een gebruiker wel of niet gelukt is. Dit wordt ook weer met een <Status> aangegeven, maar dan voor de <Response>. Verder bevat de <Response> het uiteindelijke SAML assertion element <Assertion>.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/"
         xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
         xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <soap11:Body>
   <samlp:ArtifactResponse
    Destination="Destination unknown"
    ID="_b2d765569da660eff830c352d5bb4da2"
    InResponseTo="samlart_2.16.528.1.1007.3.3.1234567.1_0123456789"
    IssueInstant="2009-06-24T11:47:05Z" Version="2.0">
     <saml:Issuer
      Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity"
>https://testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>
     <samlp:Status>
      <samlp:StatusCode
       Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
     </samlp:Status>
     <samlp:Response ID="EE7E3DF7EBC86438"
      InResponseTo="authntoken_2.16.528.1.1007.3.3.1234567.1_0123456789"
```

```
      IssueInstant="2009-06-24T11:46:59Z" Version="2.0">
      <saml:Issuer
       Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity"
>https://testportal.aorta-zorg.nl:443/topa-prototype/saml/SSO</saml:Issuer>
      <samlp:Status>
        <samlp:StatusCode
         Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </samlp:Status>
      <saml:Assertion
       ID="_2c81606885bf79c716eb2c082a2249a5"
       IssueInstant="2009-06-24T11:46:59Z"
       Version="2.0"
       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        ...
      </saml:Assertion>
     </samlp:Response>
   </samlp:ArtifactResponse>
  </soap11:Body>
</soap11:Envelope>
```

Het `<ArtifactResponse>` element is van het complexe type ArtifactResonseType dat een uitbreiding is van StatusResponseType en bestaat uit de volgende attributen en elementen:

Naam (@=attribuut)	Omschrijving	Vereist
@ID	Unieke identificatie van het antwoord van de "Artefact Resolution Service".	Ja
@Version	De aanduiding voor de SAML versie gedefinieerd in deze specificatie wordt "2.0".	Ja
@IssueInstant	Tijdsmoment van uitgifte van het antwoord. De tijdswaarde is gecodeerd in UTC.	Ja
@InResponseTo	Moet de waarde bevatten die overeen komt met het ArtifactResolve@ID bericht.	Nee
saml:Issuer	Geeft de entiteit die het artefact verzoek heeft ingediend.	Nee
samlp:Status	Een code die de status van het desbetreffende verzoek weergeeft. Dit element heeft weer verplicht het samlp:Statuscode element in zich. Als het opvragen van het artefact geslaagd is, wordt de waarde "urn:oasis:names:tc:SAML:2.0:status:Success" teruggeven. Als het opvragen van het artefact niet geslaagd is wordt een foutcode gegenereerd, zie verder SSO meldingen voor de verschillende foutcodes.	Ja
samlp:Response	Het bericht element dat bestaat uit 0 of meerdere assertions die aan een (authenticatie) verzoek voldoen.	Nee

Het `<Response>` element is van het complexe type ResponseType en bevat de volgende elementen en attributen:

Naam (@=attribuut)	Omschrijving	Vereist
@ID	Unieke identificatie van het antwoord op het authenticatie verzoek.	Ja
@Version	De aanduiding voor de SAML versie gedefinieerd in deze specificatie wordt "2.0".	Ja
@IssueInstant	Tijdsmoment van uitgifte van het antwoord. De tijdswaarde is gecodeerd in UTC.	Ja
@InResponseTo	Moet de waarde bevatten die overeen komt met het AuthnRequest@ID bericht.	Ja
saml:Issuer	Geeft de entiteit die het authenticatie verzoek heeft gegenereerd.	Ja
samlp:Status	Een code die de status van het desbetreffende verzoek weergeeft. Dit element heeft weer verplicht het samlp:Statuscode element in zich. Als het authenticatie verzoek geslaagd is, wordt de waarde "urn:oasis:names:tc:SAML:2.0:status:Success" teruggeven. Als het authenticatie verzoek niet geslaagd is wordt een foutcode gegenereerd, zie verder SSO meldingen voor de verschillende foutcodes.	Ja
saml:Assertion	Dit type specificeert de basis informatie die gemeenschappelijk is voor alle afgegeven beweringen (assertion) door een vertrouwde partij of autoriteit.	Nee

Eis: Indien de samlp:Status <> "urn:oasis:names:tc:SAML:2.0:status:Success" moet er geen saml:Assertion element teruggegeven worden.

Het `<Assertion>` element is van het complexe type AssertionType. De opbouw en inhoud van het `<Assertion>` element wordt in paragraaf 2 Het SAML authenticatietoken besproken.

Het `<Assertion>` element valt in de gedeclareerde namespace van "urn:oasis:names:tc:SAML:2.0:assertion".

Eis: Indien er een Assertion wordt afgegeven **moet** de Identity Provider deze Assertion signeren in het daarvoor aangewezen Signature veld, zie paragraaf 2.4 Algoritmes.

Stap 8: Toegang verlening

Ter voltooiing van het SSO profiel, verwerkt het patiëntenportaal de `<Response>` en de daarbij behorende `<Assertion>`, en verleent of weigert hij de gebruiker of patiënt toegang tot het patiëntenportaal door antwoord te geven op het HTTP Request waarmee bij stap 1 werd begonnen.

De verleende `<Assertion>` is het locaal geldig toegangsbewijs voor de patiënt om bepaalde handelingen te mogen uitvoeren op het patiëntenportaal, die in verbinding staat met de ZIM, die als (web)service fungeert waartussen beveiligde SOAP berichten worden uitgewisseld met behulp van SAML authenticatietokens.

Eis: De verleende assertion moet door het patiëntenportaal verwijderd worden na afloop van een SSL/TLS-sessie met het LSP respectievelijk na afloop van gebruik van de sessie door een patiënt of na het verstrijken van 15 minuten gerekend vanaf het afgiftemoment door DigiD.

Bijlage C SSO verificatie

Het goedbeheerde patiëntenportaal (GBP) moet voor elk bericht dat naar de ZIM doorgestuurd wordt een bijbehorende SAML authenticatietoken hebben. Deze tokens worden opgevraagd bij de Identity Provider (IdP) met behulp van een artefact referentie, zie stap 6 van Het SSO profiel. Het uiteindelijke antwoord van de IdP, een artefact response, bevat een SAML assertion over een patiënt, zie stap 7 van Het SSO profiel.

Voordat het GBP de assertion als SAML authenticatietoken gebruikt, moeten onderstaande controles uitgevoerd worden. Als het uiteindelijke antwoord van de IdP hieraan niet voldoet, mag de assertion niet gebruikt worden als SAML authenticatietoken tussen het GBP en het LSP.

De volgende controles moeten door het patiëntenportaal uitgevoerd worden:

- Controleer of het attribuut "InResponseTo" van het `<ArtifactReponse>` gelijk is aan de ID van het oorspronkelijke `<ArtifactResolve>` bericht;
- Controleer of het attribuut "InResponseTo" van het `<Response>` gelijk is aan de ID van het oorspronkelijke `<AuthnRequest>` bericht;
- Verifieer het attribuut "Issuer" van het `<ArtifactResponse>` element of die overeenkomt met de Assertion Consumer Service URL;
- Verifieer het attribuut "Status" van het `<ArtifactResponse>` element of die overeenkomt met de waarde "urn:oasis:names:tc:SAML:2.0:status:Success";
- Verifieer het attribuut "Issuer" van het `<Response>` element of die overeenkomt met de Assertion Consumer Service URL;
- Verifieer het attribuut "Status" van het `<Response>` element of die overeenkomt met de waarde "urn:oasis:names:tc:SAML:2.0:status:Success".

Bijlage D SSO meldingen

De volgende statuscodes (URI referenties) worden door SAML onderkend en geretourneerd binnen het SSO profiel waar van toepassing (De volgende tabel is deels overgenomen uit [SAML Assertion Protocol]).

De SAML meldingen worden alleen binnen het SSO profiel gebruikt. Dat wil zeggen dat de meldingen alleen voorkomen tussen het patiëntenportaal (GBP) en de Identity Provider (IdP).

Een statuscode is een Uniforme Resource Name (URN) en is als volgt opgebouwd:

"urn:"<Namespace Identifier>":"<Name Specific String>

Voorbeeld: "urn:oasis:names:tc:SAML:2.0:status:Success"

In de statuscode tabel wordt alleen de omschrijving en de specifieke string getoond.

Omschrijving	Namespace Specific String
The request could not be performed due to an error on the part of the requester.	Requester
The request could not be performed due to an error on the part of the SAML responder or SAML	Responder
The SAML responder could not process the request because the version of the request message was incorrect.	VersionMismatch
The responding provider was unable to successfully authenticate the principal.	AuthnFailed
The specified authentication context requirements cannot be met by the responder.	NoAuthnContext
The SAML responder or SAML authority is able to process the request but has chosen not to respond.	RequestDenied
The SAML responder or SAML authority does not support the request.	RequestUnsupported
The SAML responder cannot process any requests with the protocol version specified in the request.	RequestVersionDeprecated
The SAML responder cannot process the request because the protocol version specified in the request message is a major upgrade from the highest protocol version supported by the responder.	RequestVersionTooHigh
The SAML responder cannot process the request because the protocol version specified in the request message is too low.	RequestVersionTooLow
The resource value provided in the request message is invalid or unrecognized.	ResourceNotRecognized
The response message would contain more elements than the SAML responder is able to return.	TooManyResponses
The responding provider does not recognize the	UnknownPrincipal

principal specified or implied by the request.	
The SAML responder cannot properly fulfill the request using the protocol binding specified in the request.	UnsupportedBinding