

SAML 2.0

- Inleiding
- Verantwoordelijkheden
- Authenticatie & Autorisatie
- Metagegevens
- Vereiste instellingen
- Attributen

Inleiding

Dit boek beschrijft de procesmatige realisatie van een federatie tussen een Service Provider (SP) en een Identity Provider (IdP) via het Security Assertion Markup Language 2.0 (SAML 2.0) protocol.

Verantwoordelijkheden

De aanvrager is gemandateerd om namens de applicatie eigenaar een federatie tussen de Service Provider en Identity Provider aan te vragen. De applicatie eigenaar is formeel eindverantwoordelijk en dient zelf een functioneel en technisch team aan te stellen voor werkzaamheden aan de Service Provider die voortvloeien uit de totstandkoming van deze federatie.

Voor het in stand houden van een federatie moet de metadata periodiek worden verversd. Een belangrijk onderdeel is het certificaat van de applicatie. Dit certificaat wordt gebruikt voor ondertekening van het berichtenverkeer. Deze certificaten hebben meestal een houdbaarheid van 1 tot 2 jaar en moeten daarom periodiek vernieuwd worden. Het is aan de verantwoordelijke van de applicatie om de vervaldatum in de gaten te houden en de certificaten tijdig te vervangen. Stem de vervanging tijdig af met het Identity and Access Management (IAM) team via de ITS Servicedesk. Ook andere wijzigingen in de metadata aan de kant van de applicatie moeten worden afgestemd met het IAM team. Soms zijn er ook wijzigingen aan de kant van de Identity Provider. In dat geval neemt het IAM team contact op met de aangewezen functioneel beheerder(s) van de applicatie.

Het IAM team communiceert niet direct met leveranciers. Contact met een leverancier over de federatie dient te allen tijde via een medewerker van de Universiteit Utrecht te verlopen. Dit kan de applicatie eigenaar dan wel een functioneel beheerder zijn.

Authenticatie & Autorisatie

In onderstaande tabel worden de alle beschikbare instellingen voor authenticatie en autorisatie aangegeven. Een combinatie van verschillende authenticatie en autorisatie instellingen is mogelijk.

Authenticatie	Gebruikersnaam en wachtwoord
	Kerberos (soliscom.uu.nl)
	Multi-factor methode (instelbaar via mysolisid.uu.nl)
Autorisatie	Op basis van een algemeen kenmerk
	Op basis van een groepslidmaatschap

Metagegevens

De Universiteit prefereert het gebruik van het dynamisch uitwisselen van metagegevens tussen de Identity Provider en de Service Provider zoals gespecificeerd in OASIS Standard.

Metadata Identity Provider

De metadata van de Identity Provider kan via de volgende URL's worden verkregen:

Productie	https://login.uu.nl/nidp/saml2/metadata
Acceptatie	https://login.acc.uu.nl/nidp/saml2/metadata

Metadata Service Provider

De metadata van de Service Provider kan op twee verschillende manieren worden aangeleverd.

1. Via een publiek beschikbare URL (voorkeur)
2. Via een XML-geformatteerd bestand

De volgende gegevens dienen minimaal in de metadata te zijn beschreven:

Element	Type	Waarden
entityID	EntityDescriptor	Uniform Resource Identifier
protocolSupportEnumeration	SPSSODescriptor	urn:oasis:names:tc:SAML:2.0:protocol
AuthnRequestsSigned	SPSSODescriptor	TRUE
WantAssertionsSigned	SPSSODescriptor	TRUE
use	KeyDescriptor	signing
certificate	KeyDescriptor, KeyInfo, X509Data, X509Certificate	Base64 geëncodeerd
use	KeyDescriptor	encryption
certificate	KeyDescriptor, KeyInfo, X509Data, X509Certificate	Base64 geëncodeerd
Binding	SingleLogoutService	POST of Redirect
Location	SingleLogoutService	URL

	NameIDFormat	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:transient
Binding	AssertionConsumerService	POST, Redirect of Artifact
Location	AssertionConsumerService	URL

Vereiste instellingen

Voor een federatie met de Identity Provider van de Universiteit gelden aanvullende instellingen.

Identity Provider
De response en assertion worden ondertekend.
Voor de assertion wordt gebruik gemaakt van een SHA256 hashing algoritme.

Service Provider
De elementen: AuthnRequestsSigned en WantAssertionsSigned bevatten enkel de waarde: true.
<p>De certificaten voor 'signing' en 'encryption' zijn door een door de Universiteit vertrouwde Certificate authority (CA)* uitgegeven of het betreft een zelf uitgegeven certificaat wat voldoet aan de volgende eisen:</p> <p>Publieke sleutel algoritme (Algorithm): RSA of ECDSA</p> <p>Sleutelgrootte (Key Size):</p> <ul style="list-style-type: none">- RSA: minimaal 2048, advies 3072 of hoger- ECDSA: minimaal 224, advies 256 of hoger <p>Handtekeningsalgoritme (Signature Algorithm): minimaal SHA-256, advies SHA-384 of hoger</p> <p>Geldigheidsduur: heden tot maximaal 5 jaar in de toekomst</p> <p>Algemene naam (Common Name): bevat de naam of 'volledig gekwalificeerde domeinnaam' (FQDN) van de applicatie. De FQDN is te herleiden naar minimaal één AssertionConsumerServiceURL (ACS) zoals vermeld in de metadata.</p> <p>Gebruik (Extension Key Usage): Digital Signature</p> <p>Basic Constraints: mag nooit de waarde CA:TRUE bevatten.</p>
De Service Provider ondersteunt en maakt gebruik van Single Logout (SLO) indien deze kritiek scoort op de BIV-classificatie**. Voor overige Service Providers is dit een dringende aanbeveling.
Indien de Service Provider gebruikmaakt van SLO, dient de implementatie conform OASIS SAML2.0 specificatie te zijn ingericht***. Deze is te vinden op https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf en https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

* De Universiteit vertrouwt de volgende CA's inclusief een tweetal eigen CA's welk in pem formaat aan deze pagina zijn toegevoegd.

** De BIV classificatie wordt door de diensteigenaar uitgevoerd, in samenwerking met Informatiebeveiliging: <https://intranet.uu.nl/security/informatiebeveiliging-gegevensclassificatie>

*** Dit geldt voor logouts die worden geïnitieerd door zowel de Service Provider als de Identity Provider.

Attributen

In de assertion die vanuit de Identity Provider wordt verzonden kunnen meerdere kenmerken van een gebruiker worden meegegeven. Voor alle persoonsgebonden kenmerken geldt dat de applicatie eigenaar vooraf de benodigde grondslagen heeft laten toetsen bij de functionaris gegevensbescherming of daarvoor gemandateerde vervanger.