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.
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: **Publieke sleutel algoritme (Algorithm):** RSA of ECDSA **Sleutelgrootte (Key Size):** - RSA: minimaal 2048, advies 3072 of hoger - ECDSA: minimaal 224, advies 256 of hoger **Handtekeningsalgoritme (Signature Algoritme):** minimaal SHA-256, advies SHA-384 of hoger **Geldigheidsduur:** heden tot maximaal 5 jaar in de toekomst **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. **Gebruik (Extension Key Usage):** Digital Signature **Basic Constraints:** mag nooit de waarde CA:**TRUE** bevatten.
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.

Revision #32
Created 7 February 2020 12:30:26 by Schmidt, M.S. (Mick)
Updated 21 January 2025 12:53:30 by Schmidt, M.S. (Mick)