Technische koppeling voorbereiden

Op deze pagina geven we een introductie in de techniek die SURFconext gebruikt. We geven een aantal handleidingen die je kunt gebruiken om je Identity Management-systeem geschikt te maken voor SURFconext. Op de pagina 'technische koppeling realiseren', leggen we uit welke stappen je precies moet doorlopen om SURFconext te kunnen gebruiken.

SAML 2.0 ondersteunen

SURFconext maakt gebruik van het SAML 2.0 protocol voor de uitwisseling van informatie tussen jouw instelling als Identity Provider en de (externe) Service Provider. Deze informatie neemt de vorm van attributen aan. Een attribuut is een stukje informatie over de eindgebruiker dat vanuit jouw organisatie via SURFconext bij de Service Provider belandt. Dit kan bijvoorbeeld een user-id zijn, om de gebruiker uniek te kunnen identificeren, maar ook een naam of een e-mailadres.

Om je organisatie geschikt te maken voor SURFconext moet je huidige Identity Management systeem om kunnen gaan met de SAML-technologie. Er is een aantal producten op de markt dat hiervoor kan zorgen. Welk product voor jou het beste werkt, hangt af van de software die je momenteel gebruikt voor Identity Management. Van de meest gebruikte producten hebben we een handleiding beschikbaar:

- SimpleSAMLphp
- NetIQ Access Manager
- Microsoft Windows Server 2012 R2 - ADFS 3.0
- Microsoft Windows Server 2016 - ADFS 4.0
- Microsoft Azure Active Directory (Azure AD)

De SAML 2.0 specificatie laat veel vrijheid over om bepaalde keuzes te maken. Bijvoorbeeld hoe attributen doorgegeven moeten worden, welke informatie wel en niet gesigneerd moet worden, enzovoort. Als dit niet goed wordt afgestemd tussen alle deelnemers, kan het ertoe leiden dat het systeem niet goed functioneert. SURFconext maakt daarom gebruik van het 'Interoperable SAML2.0 Profile' (afgekort tot SAML2int). Dit is een document met eisen en richtlijnen op het gebied van SAML. Momenteel volgt SURFconext versie 0.2 van dat profiel. Het volledige profiel staat beschreven op de website https://saml2int.org/profile/current/.

Valide metadata uitgeven

SAML maakt gebruik van metadata om informatie uit te wisselen. Buiten de attributen hebben we metadata nodig. Hierin staan gegevens over je instelling, zoals de naam van de instelling en contactpersonen. Wat je daar moet invullen om aan SURFconext te koppelen vind je op deze pagina

Attributen vrijgeven

De uitwisseling van gebruikersgegevens via SAML gaat via 'attributen'. Als je organisatie gaat aansluiten op SURFconext, moet je in ieder geval een aantal van deze attributen uitgeven. Welke dat precies zijn, staat beschreven op de pagina Vereiste attributen. Naast de minimale set attributen kent SURFconext er nog veel meer. Als een Service Provider dit vereist, moet je de vereiste attributen vrijgeven. Een compleet overzicht van alle attributen die SURFconext ondersteunt, vind je op de pagina Attributen in SURFconext. Via het dashboard van SURFconext kun je zien welke dienst om welke attributen vraagt. Merk op dat je pas kunt aanmelden op het dashboard van SURFconext als je organisatie een werkende koppeling heeft met SURFconext. Meer informatie over het dashboard van SURFconext vind je op de pagina Beschikbare diensten activeren.

Een Single Sign On-URL beschikbaar hebben

SURFconext moet weten waar de gebruikers precies heen gestuurd moeten worden als zij willen inloggen bij jouw organisatie. Deze URL moet je bekend maken aan het SURFconext-team. In de verschillende handleidingen wordt genoemd waar je de URL kunt vinden en configureren voor elk Identity Provider-product.

Metadata-URL bereikbaar maken voor SURFconext

Het metadata-bestand moet gelezen kunnen worden door SURFconext. Zorg er dus voor dat het bestand van buitenaf (of in ieder geval vanaf SURFconext) bereikbaar is.

Alle endpoints beveiligen

Alle eindpunten in SURFconext moeten https gebruiken, en worden beveiligd met een geldig certificaat, uitgegeven door een bekende Certificate Authority. Op de pagina SSL certificaten lees je hier meer over. Het is verstandig om hierbij geen wildcard certificaat (*.domeinnaam.nl) te gebruiken, maar een certificaat specifiek voor domein van de inlogpagina. Als een wildcardcertificaat voor *.domeinnaam.nl in andere handen komt, dan zijn direct alle services achter domeinnaam.nl gecompromitteerd. Het is dan verstandiger om om een certificaat voor bijv. 'inloggen. domeinnaam.nl' of 'adfs.domeinnaam.nl' aan te vragen.

Een NTP-server instellen

Door een NTP-server in te stellen weet je zeker dat de tijd van je server(s) synchroon loopt met SURFconext. Als deze teveel afwijkt ontstaan er problemen met inloggen.