Veranderingen aanbrengen bestaande Identity Provider

Soms is het onvermijdelijk dat je iets moet veranderen aan de configuratie van je Identity Provider-systeem, bijvoorbeeld door een overstap naar een ander softwarepakket, of vanwege een fusie van je organisatie met een andere organisatie. Je loopt een grote kans dat deze verandering zorgt voor verstoring van de dienst, variërend van een aantal (werk)dagen tot twee weken. SURFnet raadt dan ook aan alleen wijzigingen door te voeren als dit strikt noodzakelijk is. Op deze pagina vind je richtlijnen hoe om te gaan met aanpassingen aan je IdP en welke procedures er zijn voor aanpassingen.

Impact wijziging

De impact van een wijziging of upgrade van je Identity Provider-systeem is erg afhankelijk van de omstandigheden en hangt nauw samen met welke diensten je gebruikt via SURFconext. De onderstaande lijst geeft een indruk van wat de impact die wijzigingen kunnen hebben:

- Het veranderen van het attribuut **'urn:mace:dir:attribute-def:uid**', '**urn:mace:terena.org:attribute-def:schacHomeOrganization**' of '**urn:mace:dir:attribute-def:eduPersonPrincipalName**' kan ertoe leiden dat de toegang tot diensten wordt ontzegt en wel hierom:
    - Het **NameID**, zoals gebruikt in de SAML assertion naar de service provider bij het aanmelden op de dienst, is een samenstelling van de attributen **uid**, **schacHomeOrganization**, het **Entity ID** van de **service provider** samen met een geheim wat gebruik maakt van een SHA algoritme. Als een instelling of dienstverlener er voor kiest bij een dienst die al in productie is één van deze attributen aan te passen zal het er toe leiden dat SURFconext een nieuw **NameID** en **eduPersonTargetedID** gaat genereren. Dit kan tot gevolg hebben dat gebruikers geen toegang meer hebben tot hun profielen bij diensten.
    - Gebruikers kunnen hun teamlidmaatschap kwijt raken, waardoor zij niet meer bij diensten kunnen die op groepsniveau zijn afgeschermd.

- Het veranderen van het 'EntityID' van de organisatie leidt ertoe dat sommige Service Providers het oude 'EntityID' moeten vervangen door het nieuwe 'EntityID'. Dit is het geval bij diensten die gebruik maken van een eigen WAYF. Dit komt vaak voor omdat de upgrade van een IdP dit doorgaans tot gevolg heeft en hier hebben we een werkinstructie voor opgesteld. Dit zou niet hoeven te lijden tot onderbreking van toegang tot diensten.

Dit zijn een paar voorbeelden. SURFnet weet niet van elke Service Provider hoe zij elk attribuut gebruiken. Een Service Provider kan er bijvoorbeeld voor kiezen om aan de hand van bepaalde attributen zelf een unieke identifer te maken. Hierdoor is het moeilijk om van tevoren in te schatten welke impact een wijziging van een attribuut heeft.

Voordat je wat gaat wijzigen aan je Identity Provider, moet je contact opnemen met het SURFconext-team. Doe dit op tijd. Wij zullen je informeren over de impact van de voorgestelde wijziging, een schattig geven van de duur van eventuele onderbrekingen van toegang tot diensten en aangeven welke stappen je moet doorlopen. Ook als je advies wilt inwinnen of de wijziging misschien op een andere manier opgelost kan worden, kun je dat aangeven. Stuur een e-mail naar support@surfconext.nl.

Procedure

Als je jouw Identity Provider-systeem wilt vervangen door een nieuw Identity Provider-systeem, dan moet je de onderstaande stappen doorlopen:

1. Neem contact op met support@surfconext.nl om de planning van de migratie af te stemmen.
2. Richt het nieuwe Identity Provider-systeem in en koppel deze aan de SURFconext testomgeving.
3. Het SURFconext-team neemt het nieuwe Identity Provider-systeem op in de productieomgeving van SURFconext. Hiervoor voert het SURFconext-team onderstaande acties uit:
    a. Het nieuwe Identity Provider-systeem koppelen aan de productie-omgeving van SURFconext.
    b. De toegang naar de huidige diensten openzetten voor het nieuwe Identity Provider-systeem.
    c. Het oude Identity Provider-systeem 'verbergen' in de WAYF op de SURFconext gateway. Transparant aangesloten Service Providers die (nog) gebruikmaken van het oude Identity Provider-systeem blijven werken. Een transparant aangesloten Service Provider maakt gebruik van een eigen WAYF-scherm (bijvoorbeeld SURFspot).
4. Het SURFconext team stuurt transparant aangesloten Service Providers een verzoek om de nieuwe Identity Provider te gaan gebruiken. De gemiddelde doorlooptijd hiervan is 2 weken maar soms ook langer. In de logs op de SURFconext-gateway kan het SURFconext-team zien welke Service Providers het oude Identity Provider-systeem nog gebruiken.
5. Het oude Identity Provider-system wordt uit de productie-omgeving van SURFconext verwijderd als alle Service Providers over zijn op het nieuwe Identity Provider-systeem.