IdP-geïnitieerde login

Gewoonlijk wordt een login vanuit de dienst (SP) geïnitieerd: De eindgebruiker probeert bij een SP in te loggen en deze begint het proces door een SAML AuthenticationRequest te versturen via het bekende WAYF-scherm van SURFconext (als er meer dan één IdP is aangesloten op de betreffende dienst). IdP-geïnitieerde login (IdP initiated, IdP-first, unsolicited of ongevraagde login) maakt het mogelijk om in te loggen op een SP zonder dat de SP een SAML AuthenticationRequest stuurt.

De IdP stuurt zelf een SAML Assertion op naar de SP waardoor er geen WAYF-scherm verschijnt. Dit kan worden gebruikt voor bijvoorbeeld een instellingsportal of een bookmark. Voor een dergelijke login is een 'deeplink' noodzakelijk waarbij de IdP en de SP al van te voren zijn bepaald. Op deze pagina wordt uitgelegd hoe een dergelijke deeplink kan worden gemaakt.

> **Let Op!**
>
> Niet alle SP's ondersteunen deze, van hun kant, ongevraagde login.

Dit is alleen in specifieke gevallen een wenselijke oplossing en heeft als nadeel dat zowel gegevens over de IdP en SP in de URL opgenomen worden; wijzigt hier iets dan moet ook de URL aangepast worden. Er zijn betere manieren om een WAYF over te slaan, die de SP kan implementeren. Bijvoorbeeld het gebruik van de transparante metadata (idps-metadata) van SURFconext, of inzet van het scoping-element in het authenticatierequest. Unsolicited SSO is met name nuttig voor instellingen (IdP's) die een deeplink willen maken als de SP zelf hier geen ondersteuning voor biedt.

Opbouw Deeplink

Voor bijvoorbeeld de IdP SURFnet BV en de SP "SURFfilesender | SURF" maakt de volgende deeplink een IdP-geïnitieerde login mogelijk:

https://engine.surfconext.nl/authentication/idp/unsolicited-single-sign-on/key:20230503/ba573f07093978e3852ddef0d2465b84?sp-entity-id=https://filesender.surf.nl/simplesaml/module.php/saml/sp/metadata.php/default-sp

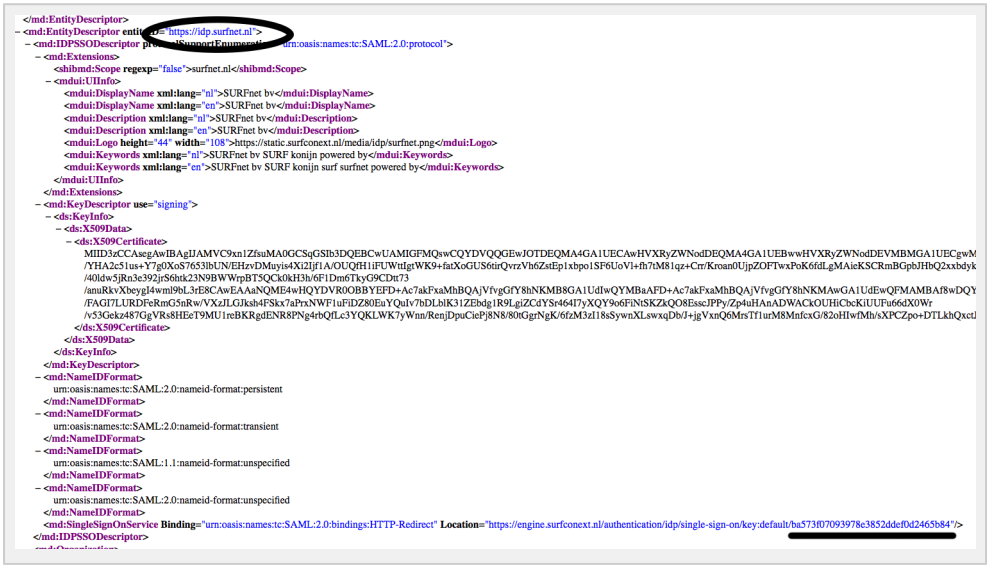
Deze link bestaat uit de basis:

https://engine.surfconext.nl/authentication/idp/unsolicited-single-sign-on/key:20230503/**IdP-key**?sp-entity-id=**SP-connection-ID**

IdP-key

Het vinden van de IdP-key is relatief eenvoudig:

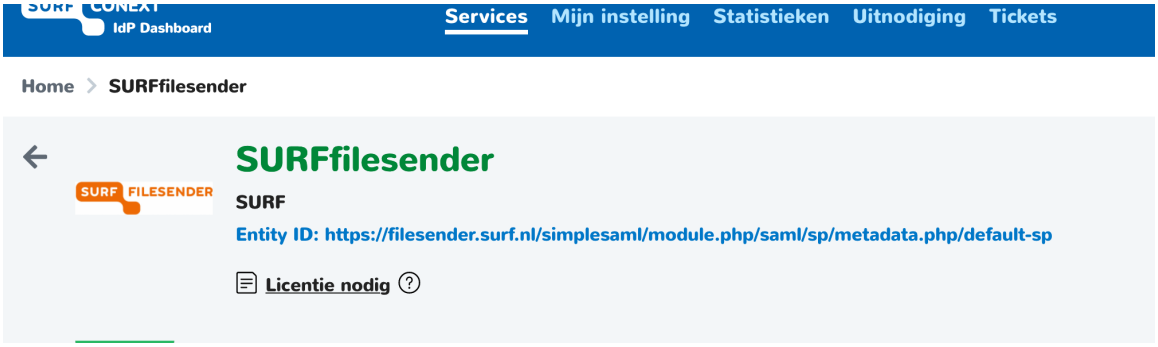
- Ga naar https://metadata.surfconext.nl/idps-metadata.xml
- Zoek hier op de instelling van je keuze
- Kijk vervolgens bij SingleSignOnService



> **Let Op!**
>
> Deze IdP-key verandert als de entity-ID van je IdP wijzigt, bijvoorbeeld na een migratie van de software. De oude link zal dan niet meer werken.

SP-connection-ID

De "SP-connection-ID" moet het EntityID van de gewenste Service Provider zijn. Deze vind je in SURFconext IdP Dashboard. Zoek de betreffende Service Provider op. Je vindt de benodigde entityID (een URL) in het blauw direct onder de naam van de aanbieder van de dienst. In het voorbeeld hieronder is het "`https://filesender.surf.nl/simplesaml/module.php/saml/sp/metadata.php/default-sp`".



Optionele configuratie

Indien de SP hier iets mee kan, kan ook een "&RelayState=" parameter toegevoegd worden met een voor de SP relevante waarde.

Als er een key rollover gaande is, is het ook mogelijk direct na "unsolicited-single-sign-on/" de te gebruiken keyid op te geven:

https://engine.surfconext.nl/authentication/idp/unsolicited-single-sign-on/key:20181213/**IdP-key**?sp-entity-id=**SP-connection-ID**