

Validatie van schacHomeOrganization en eduPersonPrincipalName

Samenvatting

Voor betrouwbare authenticatie is het noodzakelijk dat nauwkeurig kan worden vastgesteld dat bepaalde attributen ook echt van de instelling afkomstig zijn. Daarom gaat SURFconext de waarde die een IdP stuurt voor schacHomeOrganization ("uniharderwijk.nl") en het achtervoegsel dat een IdP gebruikt voor eduPersonPrincipalName ("fetze@uniharderwijk.nl") valideren tegen een lijst van toegestane waarden voor die IdP. Hiermee kan beter gewaarborgd worden dat er geen onverwachte waarden gestuurd worden.

Op dit moment zijn voor elke IdP waarden geconfigureerd bij SURFconext die toegestaan zijn. Afwijkingen worden gelogd en waar nodig overlegd met de IdP-beheerder. Vanaf begin 2019 zal een gebruiker met niet-geregistreerde waarden geblokkeerd worden en een foutmelding van SURFconext getoond worden.

Achtergrond

Het attribuut schacHomeOrganization geeft aan bij welke instelling een gebruiker hoort. eduPersonPrincipalName is een unieke identificatie van een gebruiker. (Zie: [Attributen in SURFconext \(NL\)](#).) Beide worden door Service Providers vaak gebruikt voor autorisatie: de schacHomeOrganization geeft vaak toegang tot zaken die aan een bepaalde instelling voorbehouden zijn. Het is ook een input voor het unieke NameID/eduPersonTargetedID van de gebruiker; evenals de eduPersonPrincipalName bepaalt één van die id's wie de gebruiker is en dus tot welke gegevens hij/zij toegang krijgt.

In SURFconext/SURFfederatie werden attribuutwaarden in het algemeen niet gevalideerd. De IdP van universiteit A kan dus technisch gezien een schacHomeOrganization sturen die behoort aan hogeschool B. Aan de basis van de federatie ligt het vertrouwen dat een identity provider kloppende gegevens verstrekt over zijn gebruikers, en dit is ook contractueel vastgelegd. Met het toenemende belang van federatieve login ontstond de behoefte om dit ook technisch meer af te dwingen. Daarom is ervoor gekozen om deze belangrijke identificerende kenmerken per IdP te beperken tot waarden die bekend zijn voor die IdP. Zo kan een probleem met een verkeerd geconfigureerde of gecompromitteerde IdP nooit bredere impact hebben dan de context van die betreffende instelling.

Implementatie

Voor de validatie maken we gebruik van het metadata-veld `shibmd:scope`. Dit veld, dat meerdere waarden kan hebben, bevat alle schacHomeOrganization-waarden en achtervoegsels van eduPersonPrincipalName die toegestaan zijn voor de IdP. Als het veld bijvoorbeeld bevat: (uniharderwijk.nl, unihw.edu, student.uniharderwijk.nl) dan worden gebruikers met schacHomeOrganization=uniharderwijk.nl, eduPersonPrincipalName=frits@student.uniharderwijk.nl toegelaten. Andere attributen dan de twee genoemde worden niet onderworpen aan controles en werken dus als vanouds. Elke instelling zal dus een eindige lijst met mogelijke waarden hebben.

SURFconext slaat de toegestane waarden op in haar configuratie. Initieel zijn de waarden gevuld op basis van in het recente verleden waargenomen waarden uit onze logging. Indien er opmerkelijke waarden tussenzitten, wordt daarover contact opgenomen met de IdP-beheerder.

Alle door ons geconfigureerde waarden zijn terug te zien in de `idps-metadata` van SURFconext. Een IdP kan hierin zijn eigen entityID opzoeken en zien welke waarden SURFconext zal accepteren. De SURFconext-verantwoordelijke kan gewenste waarden doorgeven aan SURFconext.

SURFconext monitort de resterende mismatches. Op dit moment is dat aantal zeer laag (enkele per dag, op 500.000 logins per dag). De juiste waarden zullen per 26 maart 2019 gehandhaafd worden. Een gebruiker die vanaf dat moment nog met een waarde aankomt die bij SURFconext niet bekend is voor die IdP, krijgt een foutmelding gepresenteerd: `Error - Attribuutwaarde niet toegestaan / Attribute value not allowed`.

Technische details

De waarde van het shibmd:scope-attribuut wordt ook gepubliceerd in de metadata die SURFconext genereert voor aangesloten SP's en in eduGAIN. SP's die dat willen kunnen hiermee zelf ook de gestuurde attributen valideren. Veel Shibboleth-SP's vereisen zelfs dat het attribuut aanwezig is.

De waarden van shibmd:scope worden kastengevoelig vergeleken met de attribuutwaarden. De shibmd:scope-definitie ondersteunt ook reguliere expressies. Deze functionaliteit wordt in SURFconext om compatibiliteitsredenen niet gebruikt.

De IdP-beheerder kan het shibmd:scope-attribuut opnemen in zijn metadata zodat SURFconext die kan inlezen. Het verschilt per IdP-product hoe dit moet (en of het überhaupt kan). Na het aanpassen kun je SURFconext-support vragen de metadata opnieuw in te lezen, of indien de metadata-route geen optie is, kan de SURFconext-verantwoordelijke de juiste waarden sturen in een mail aan support@surfconext.nl.

Vragen

Zoals altijd zijn alle vragen welkom via support@surfconext.nl.