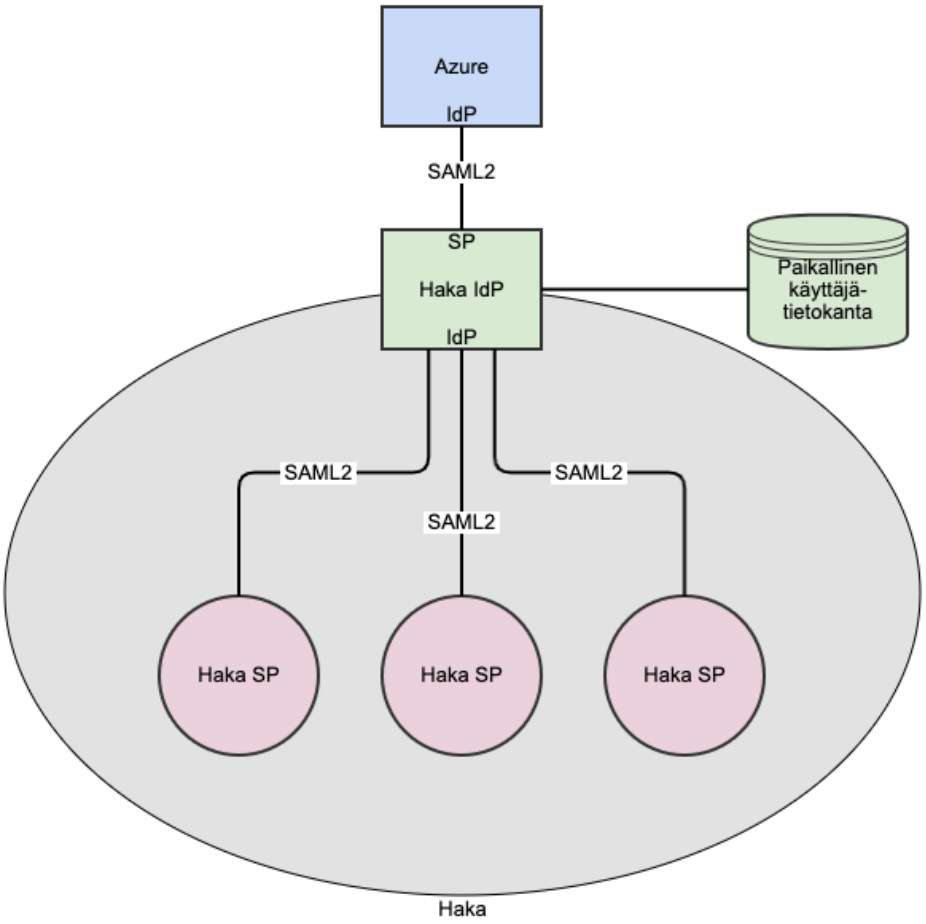
Azuren käyttäminen tunnistusvälineenä Haka IdP:ssa

Shibboleth IdP versiossa 4 alkaen mahdollistaa sisäänrakennettuna lähettää palveluilta tulevat tunnistuspyynnöt eteenpäin toiselle SAML2 IdP:lle. Shibboleth IdP4 siis sisältää SAML2 SP -toiminnallisuuden, jolloin se esiintyy palveluna muille SAML2 IdP:lle.

Tätä toiminnallisuutta voi hyödyntää Azuren kanssa, jolloin käyttäjät tunnistetaan Azuressa, mutta Shibboleth IdP hoitaa federaatioiden luottosuhteet yms. jotka eivät onnistu kovin hyvin Azuressa.



Käyttäjien tunnistaminen tapahtuu Azuressa ja voidaan tällöin käyttää sen tarjoamana monivaiheista tunnistamista. Tosin tähän liittyy joitakin rajoitteita, joita on dokumentoitu alla.

Azuren lisäksi IdP:iin voidaan kytkeä paikallinen käyttäjätietokanta tai -hakemisto, josta voidaan haluattessa hakea käyttäjäattribuutteja Azureen tallennettujen lisäksi. Samaten IdP:ssa voidaan muokata Azuresta saatuja attribuuteja ja luoda kokonaan uusia paikallisesta hakemistosta haettujen lisäksi. Esimerkiksi Azuresta voitaisiin ottaa henkilön nimi ja sähköpostiosoite, opiskelijan opiskelutietoja haetaan lisähakemistosta ja IdP:ssa tehdään käyttäjälle kotiorganisaatio-attribuutti.

Käyttöönotto

Ohjedokumentit

- Yleinen ohje proxyttaa tunnistuspyynnöt toiselle IdP:lle:
  - https://wiki.shibboleth.net/confluence/display/KB/Using+SAML+Proxying+to+another+IdP
- Ohje Azuren käytöstä proxytuksen kohteena:
  - https://wiki.shibboleth.net/confluence/display/KB/Using+SAML+Proxying+in+the+Shibboleth+IdP+to+connect+with+Azure+AD

Yllä oleviin ohjeisiin perustuvaa ratkaisua on Suomessa testattu TUNI:n sekä Certia & CSC toimesta erilaisissa ympäristöissä.

Koska yllä olevassa ohjeessa on tarkat kuvaukset tehtävistä, esitellään tässä vaiheet pääpiirteittäin ilman kaikkia yksityiskohtia. Tehtävissä on kaksi osaa:

1. Rakennetaan luotto Shibboleth IdP:n ja Azure välille
2. Konfiguroidaan Shibboleth IdP lähettämään Azuresta saatuja tietoja Haka SP:lle

Käytännön tasolla IdP:lle aktivoidaan tunnistusmenetelmäksi SAML (https://wiki.shibboleth.net/confluence/display/IDP4/SAMLAuthnConfiguration). Tässä menetelmässä IdP pyytää autentikointia toiselta IdP:lta SAML2-protokollan avulla. Yleisimmin aiemmin Shibboleth IdP on konfiguroitu tekemään tunnistusta LDAP-hakemistoa vasten Password -menetelmällä. Alla oleva ohjeistus kuvaa askeleet, mitä SAML -tunnistusmeneltemän käyttöönotto edellyttää. Lisäksi tulee olla riittävät tiedot Azuren konfiguroinnista käyttäjien tunnistamiseen sekä SAML Service Provider -liitoksen tekemiseen.

Tehtävät

Luottosuhde Azure Shibboleth IdP

Tehtävät, jotka kuvattu https://wiki.shibboleth.net/confluence/display/KB/Using+SAML+Proxying+in+the+Shibboleth+IdP+to+connect+with+Azure+AD Trust Task 1-4 kohdissa. Tarkoitus on siis muodostaa luottosuhde ensin Azuren ja Shibboleth IdP:n SP-rajapinnan kanssa. Azure lähettää omilla nimillään ja omalla formaatilla attribuutteja, joten ne pitää pystyä käsittelemään Shibboleth IdP:lla, jotta niitä voidaan jatkokäyttää. Yksi huomattava asia on, ett Azure lähettää attribuutit nameformat:lla unspesified ja tätä ei voida käyttää Hakassa. Täten jokainen attribuutti pitää käsitellä uudelleen.

1. Muodostetaan metadatatiedosto, joka kuvaa Shibboleth IdP:n SP-rajapinnan
2. Rekisteröidään Shibboleth IdP:n metadata Azuren käyttöön
    a. Viedään shibboleth IdP:n SP-rajapinnan metadata Azurelle käytettäväksi.
3. Rekisteröidään Azuren IdP:n metadata Shibbolethin käyttöön
    a. Ladataan azuresta metadatatiedosto, joka otetaan käyttöön Shibboleth IdP:ssa
4. Konfiguroidaan attribuuttien luovutus Azuresta Shibboleth IdP:lle
    a. Azuressa päätetään mitkä attribuutit halutaan lähettää tunnistetuista käyttäjistä Shibbolethilla.

Konfiguroidaan Shibboleth IdP proxy-toiminto

Tehtävät, jotka kuvattu https://wiki.shibboleth.net/confluence/display/KB/Using+SAML+Proxying+in+the+Shibboleth+IdP+to+connect+with+Azure+AD Proxy Task 1-6 kohdissa.

Näiden avulla saadaan käyttäjä ohjattua tunnistautumaan Azuressa. Lisäksi välitetään mahdollinen pyyntö MFA-tunnistusmenetelmästä. Huomaa, että Azuren MFA logiikka ohittaa osin pyydetyt menelmät ja niitä on syytä tarkastella Azuressa erikseen.

Lisäksi Azuren lähettämät käyttäjäattribuutit tulee saada IdP:n käsittelyyn ja lähteiksi eteenpäin lähetettäville attribuuteille.

1. Ohjataan tunnistukset Azurelle
    a. Konfiguroidaan SAML-tunnistusmenetelmän pyynnöt menemään Azurelle.
2. Vastaanotetaan Azuren lähettämät attribuutit
    a. Tehdään filtteri, jolla Azurelta tulevat attrbuutit hyväksytään jatkokäsitelyyn
3. Konfiguroidaan IdP ymmärtämään Azuren attribuutit
    a. Luodaan attribuuttisäännöt Azuresta vastaanotetuille attribuuteille
4. Subjektin eli käyttäjätunnisteen muodostaminen
    a. Tarvitaan joku tunniste, jolla käyttäjä identifioidaan IdP:n sisällä
5. Attribuuttien välittäminen
    a. Säännöt, joilla Azuresta saatu attribuutti voidaan välittää eteenpäin käsittelyn jälkeen
6. Lisätään REFEDS MFA-profiilin käsittely
    a. Sanasto tunnistusmenetelmäpyyntöjen välittämiseen Azurelle

Hakan konfiguraatiot

Edellä listattujen tehtävien lisäksi miten tunnistaminen proxytetaan Azurelle, on joitakin Hakaan liittyviä asioita, jotka on hyvä huomioida.

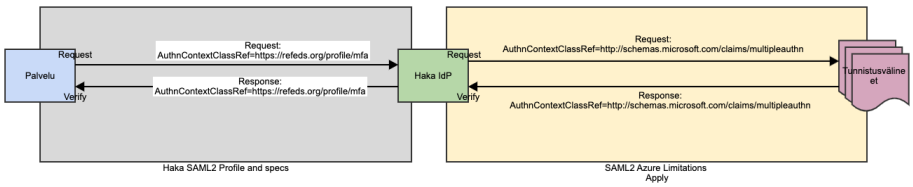
Attribuutit

Azuren toimittamia attribuutteja ei voida sellaisenaan välittää Hakaan, koska Azure lähettää ne ilman oikeaa NameFormat:ia eikä sitä voi Azuren päässä konfiguroida. Täten pitää joko jokainen attribuutti Azuresta on käsitellä IdP:ssa uudelleen, vähintään asetettava oikea NameFormat. Tai vaihtoehtoisesti Haka-palveluille välitettävät attribuutit haetaan organisaation hakemistosta ja Azuren toimittamia tietoja käytetään vain sitomaan tunnistustapahtuma hakemiston tietoihin.

IdP4:ssa attribuutteja voidaan konfiguroida Attribute Registry ominaisuuden avulla. Sen edellyttämiä Haka-attribuuttien pohjatiedostoja IdP4:lle löytyy: https://github.com/CSCfi/ansible-role-shibboleth-idp/tree/idp4/templates/opt/shibboleth-idp/conf/attributes ja kuvaukset yleisellä tasolla FuneEduPerson-skeemassa.

Tunnistusmenetelmät

Hakassa on keväällä 2021 vahvistettu REFEDS:n mfa- ja sfa-sanastot tunnistusmenetelminä aiemmin käytössä olleiden SAML2-määrityksistä löytyvien (mm. PasswordProtected) rinnalla. Näiden käyttäminen onnistuu pääosin Azuren kanssa sopivalla konfiguraatiolla. Kirjoitushetkellä ei ole kuitenkaan tiedossa, miten Azuren saisi kunnioittamaan tunnistusmenetelmäpyyntöjä täydellisesti.



Jotta Haka SP:ltä tulevat tunnistuspyynnöt saadaan välitettyä Azurelle, voidaan tunnistusmenetelmä sanastoa muokata proxytettaessa pyynnöt. Azurea ei ole mahdollista konfiguroida REFEDS-sanaston mukaiseksi vaan sille täytyy lähettää Azuren ymmärtämiä tunnistuspyyntöjä. Sanaston muokkaaminen hoidetaan ohjeen mukaisesti Proxy Task 6.

Lisätietoja tunnistusmenetelmistä: Vahvemman tunnistamisen sanasto