Rajapintakuvaus

Rajapinnat ja tämä kuvaus tarkentuvat, kun organisaatiot liittyvät yhdistämispalvelun käyttäjiksi.

- Yhdistämispalveluun liittyminen
  - Testaus ja kehittäminen
  - Tuotanto
- Skeema ja rajapinnan käyttäytyminen
  - Pyyntö (request)
    - XML
    - JSON
  - Vastaus (response)
    - XML
    - JSON
- Rajapinnan tiedot
  - Push
    - SOAP
    - REST

Yhdistämispalvelusta siirretään käyttäjän kotiorganisaatioon kirjautumistapahtumissa saadut SAML-federaation yksilöllinen tunniste (Hakassa eduPersonPrincipalName) ja OAuth2-rajapinnasta saatu tunniste (ORCID iD). Ensivaiheessa toteutetaan push-metodi, jossa tunnistepari työnnetään kotiorganisaation toteuttamaan rajapintaan.

Rajapinnan toteutukset löytyvät koodiprojektin push-haarasta.

Unknown macro: 'lucidchart'

Yhdistämispalveluun liittyminen

Liittyäkseen yhdistämispalvelun käyttäjäksi organisaation on suoritettava seuraavat toimenpiteet.

Testaus ja kehittäminen

1. Organisaation testi-IdP:n liittäminen Hakan testiympäristöön
   a. Yhdistämispalvelussa noudatetaan skenaariota, jossa rajapintoja organisaatioihin on n-kappaletta. Organisaatio kytketään yhdistämispalvelun rajapintaan organisaation IdP-palvelimen entityId:llä. Kutakin osallistuvaa organisaatiota kohden toteutetaan täsmälleen yksi rajapinta ja kullakin organisaatiolla on täsmälleen yksi SAML IdP-palvelin. Yhdistämispalveludemon SAML SP on liitetty Hakan testiympäristöön. SP hyödyntää Hakan testiympäristön DS-palvelua, josta käyttäjä valitsee kotiorganisaationsa. Yhdistämispalvelun demoon voidaan liittää kotiorganisaation testi-IdP suoraan Haka testimetadatasta, jolloin simuloidaan tuotannon asetelmaa. Jos organisaatiolla ei ole testi-IdP -palvelinta ja sellaisen pystyttäminen ei pienellä vaivalla onnistu, voidaan testaamisessa hyödyntää CSC:n ORCID-osaamiskeskuksen toteuttamaa tilapäistä testi-IdP -palvelinta.
   b. Luottosuhteen muodostaminen organisaation testi-IdP:n ja yhdistämispalvelun demon välille vaatii Hakan testiympäristön tavanomaisesta prosessista poikkeavan metadatavaihdon. Poikkeavan metadatatiedoston osoitteen organisaatio saa liittymisen yhteydessä.
2. Tunnisteparin vastaanottavan rajapinnan toteuttaminen
   a. Organisaatio varaa rajapinnan IdM-järjestelmästään tai toteuttaa muulla tavoin palvelun, johon yhdistämispalvelun selvittämä tunnistepari toimitetaan. Organisaaton rajapinnasta tarvittavat tiedot on kuvattu taulukoissa kohdassa #rajapinnat .
      i. jos wsdl-kuvaus sisältää laajan skeeman (message) ja useita toiminteita (porttype, operation, binding), organisaatio ilmoittaa, mitä näistä käytetään yhdistämispalvelun tietoparin toimittamiseen
   b. Organisaatio suojaa rajapintansa HTTP Basic Auth tunnistuksella, jota varten organisaatio ilmoittaa käytettävän tunnus- ja salasanaparin.
   c. Rajapinta on suojattava kulloinkin tietoturvaltaan riittäväksi todetulla salauksella, joten HTTPS URL:n käyttö on pakollista. Suositellaan, että rajapinnan suojauksessa käytetään yleisesti tunnettua varmenneketjua (esim. Funetin varmennepalvelusta hankittua varmennetta).

Tuotanto

- Tuotantovaiheessa hyödynnetään Haka-metadataa luottosuhteen muodostamiseen. Sekä organisaation IdP, että yhdistämispalvelu ovat Haka-metadatassa. Yhdistämispalvelu tarvitsee IdP:ltä vain eppn-attribuutin.
- Muutoin noudatetaan testivaiheen mallia, mutta organisaatio ilmoittaa tuotantoympäristöään vastaavat rajapintamääritykset

Skeema ja rajapinnan käyttäytyminen

Yhdistämispalvelun suunnittelussa on toteutettu esimerkkikuvaus siirrettävästä viestistä. Rajapintatoteutuksessa suositellaan käytettäväksi suunniteltua skeemaa, mutta jos organisaation rajapinta edellyttää muuta tietomallia, organisaation on kuvattava, missä muodossa haluaa tiedon vastaanottaa.

Välitettävien attribuuttien niminä (Name, FriendlyName) käytetään kyseisen federaation määrittämiä nimiä (Hakassa funetEduPerson-skeema). ORCID iD:n nimenä käytettävä eduPersonOrcid-attribuutti on virallisessa eduPerson-skeemassa vielä experimental-tilassa, mutta hyväksytty käyttöön Hakan attribuuttiskeemassa.

Pyyntö (request)

Yhdistämispalvelu tekee pyynnön organisaation rajapintaan. Tunnistepari välitetään pyynnössä.

XML

XML-skeematiedoston esimerkki löytyy tästä. Skeemaan perustuva esimerkki XML-tiedostosta löytyy tästä. Varsinaisessa SOAP-pyynnössä viesti paketoidaan SOAP-viestikäytännön mukaiseen kuoreen. Viesti voi näyttää esimerkiksi seuraavalta:

XML-esimerkki

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
        <SOAP-ENV:Header/>
        <SOAP-ENV:Body>
                <ns2:receiveRequest xmlns:ns2="http://www.novell.com/provisioning/service">
                        <ns2:arg0>teppo@yliopisto.fi</ns2:arg0>
                        <ns2:arg1>0000-0003-0833-4032</ns2:arg1>
                </ns2:receiveRequest>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Yhdistämispalvelussa muodostetaan pyyntöviesti skeemanmukaisesta luokkakokoelmasta käyttötapaukseen perustuvaa muuntokirjastoa (MessageConverter) hyödyntäen. Demopalvelusta on saatavilla kirjautumisen jälkeen XML-näkymä käyttäjän tiedoista URL:sta: https://orcid-connect01.csc.fi/app/shib/iddescriptor.xml

JSON

Mallin mukainen JSON-viesti voi näyttää esimerkiksi seuraavalta:

JSON-esimerkki

```
{
        identifier: [
        {
                name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.16",
                nameFormat: "urn:oasis:names:tc:SAML:2.0:attrname-format:uri",
                friendlyName: "eduPersonOrcid",
                issuer: "https://sandbox.orgid.org",
                issueInstant: null,
                mediator: "https://connect.tutkijatunniste.fi",
                mediationInstant: 1457545085621,
                identifierValue: "0000-0003-0833-4032"
        },
        {
                name: "urn:oid:1.3.6.1.4.1.5923.1.1.1.6",
                nameFormat: "urn:oasis:names:tc:SAML:2.0:attrname-format:uri",
                friendlyName: "eduPersonPrincipalName",
                issuer: "https://idp.testshib.org/idp/shibboleth",
                issueInstant: null,
                mediator: "https://connect.tutkijatunniste.fi",
                mediationInstant: 1457545085621,
                identifierValue: "myself@testshib.org"
        }]
}
```

Yhdistämispalvelussa muodostetaan pyyntöviesti skeemanmukaisesta luokkakokoelmasta käyttötapaukseen perustuvaa muuntokirjastoa (MessageConverter) hyödyntäen. Demoversiosta on saatavilla kirjautumisen jälkeen JSON-näkymä käyttäjän tiedoista URL:sta: https://orcid-connect01.csc.fi/app/shib/iddescriptor.json

Vastaus (response)

Organisaation rajapinta vastaa yhdistämispalvelulle ja raportoi tunnisteparin siirtämisen onnistumisesta tai epäonnistumisesta. Onnistumiseksi tulkitaan, että organisaatio on tallentanut tunnisteen henkilöhakemistoonsa ja se on loppukäyttäjän hyödynnettävissä organisaation tarjoamissa palveluissa. Paluuviesti sisältää käyttäjälle näytettäväksi sopivan ohjeen, kuten: "tunniste on tallennettu henkilöhakemistoon ja se on välittömästi käytettävissä Haka-kirjautumisessa".

Organisaation rajapinta ilmaisee siirron onnistumisen HTTP vastauksen numerolla 2 alkavalla tilakoodilla. Virhe ilmaistaan HTTP vastauksen numerolla 5 alkavalla tilakoodilla. Virheviestiin sisältyy loppukäyttäjälle näytettäväksi sopiva selkokielinen ohje, miten virhetilanne voidaan korjata, kuten: "taustajärjestelmä ei ollut saatavilla, yritä 5 minuutin päästä uudelleen".

> Vastauspyynnön käsittely ja erityisesti virheenkäsittelyn toteuttaminen on kesken ja tarkentuu, kun organisaatiot liittyvät palvelun käyttäjiksi.

XML

Organisaation rajapinnan vastaus saattaa näyttää esimerkiksi seuraavalta:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ser="http://www.novell.com
/provisioning/service">
   <soapenv:Header/>
   <soapenv:Body>
      <ser:receiveResponse/>
   </soapenv:Body>
</soapenv:Envelope>
```

JSON

Organisaation rajapinnan vastaus saattaa näyttää esimerkiksi seuraavalta:

```
{
        "status":"identities stored"
}
```

Rajapinnan tiedot

Organisaation rajapinnasta tarvittavat tiedot yhdistämispalvelun liitoksen toteuttamiseksi

Push

SOAP

Tieto	Esimerkki
WSDL	http://demo9650738.mockable.io/mockProvisioningBinding?wsdl
Käytettävä Binding URI	https://demo9650738.mockable.io/mockProvisioningBinding
Tarvitaanko SOAPAction (on noudatettava skeemassa käytettävää XMLNS nimiavaruutta)	http://www.novell.com/provisioning/service/receive
Pyyntösanomassa noudatettava skeema	https://bitbucket.org/klaalo/orcidconnect/raw/9ad4c4c7e1dda64362fc62d9f33846267d47addc/src/main/resources/xml_example.xsd
Vastaussanoman skeema	
IdP:n entityId	https://testidp.funet.fi/idp/shibbolet
IdP:n SAML Metadata	https://haka.funet.fi/metadata/haka_test_metadata_signed.xml
Metadatan allekirjoitusvarmenne	https://confluence.csc.fi/download/attachments/31195585/haka_testi_2015_sha2.crt

REST

Tieto	Esimerkki

Käytettävä URI	https://demo9650738.mockable.io/identities
Käytettävä metodi	HTTP POST
Pyyntösanomassa noudatettava skeema	#json
Vastaussanoman skeema	
IdP:n entityId	https://idp.testshib.org/idp/shibboleth
IdP:n SAML Metadata	https://haka.funet.fi/metadata/haka_test_metadata_signed.xml
Metadatan allekirjoitusvarmenne	https://confluence.csc.fi/download/attachments/31195585/haka_testi_2015_sha2.crt