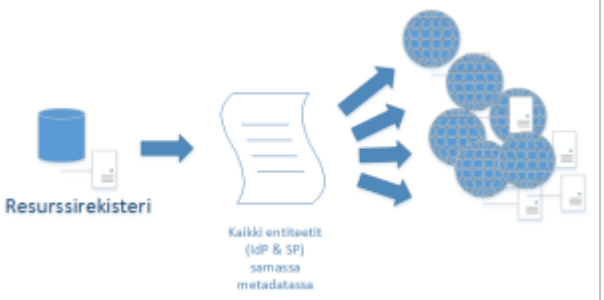
Testiympäristöön liittäminen

Määrittele IdP käyttämään Haka-testiympäristön metadataa

MetadataProvider -ohje	IdP 3.0#metadataProvider
Haka-testiympäristön metadata	https://haka.funet.fi/metadata/haka_test_metadata_signed.xml
Testimetadatan allekirjoitusvarmenne	haka_testi_2015_sha2.crt

Lisää IdP-palvelimesi testiympäristöön

Tavanomainen federaation metadata	Testiympäristön metadata
	

Lisää uusi IdP

Kirjaudu ensin	https://rr.funet.fi/rr/
Manage IdPs -> Add New Entity Provider	https://rr.funet.fi/rr/idp_edit.php?id=new

Organization Information

Valitse organisaatioksi	ShibIdPv3WorkShop

IdP's Basic Information

Paina mieleen tai kirjoita ylös, mitä määrittelet tähän osioon. Joudut käyttämään arvoja myöhemmin IdP:n konfiguraatiossa.

EntityId	Muodosta entityId virtuaalikoneesi host-nimen perusteella siten, että allaolevan esimerkin tilalle korvaat oman virtuaalikoneesi nimen: `https://vmXXXX.kaj.pouta.csc.fi/ShibIdPv3WorkShop/KLa` Lisää URL:n polulle myös oman työryhmäsi nimikirjaimet tai muu sellainen tunniste, josta ryhmäsi on koulutuksessa erotettavissa. Huomioi, että testimetadata on julkisesti jaossa. EntityId:n on oltava globaalisti yksikäsitteinen. Silloin, kun palvelu on lisätty vain yhteen federaatioon, periaatteessa riittää metadatan kattava yksikäsitteisyys. Haka on mukana kansainvälisissä Kalmar2 ja eduGAIN-verkostoissa. Hakassa entityId:n on oltava URI, joka on organisaation omistamasta nimiavaruudesta. Useimmat organisaatiot käyttävät URL, koska eivät ole ottaneet käyttöön muuta omaa nimijärjestelmää (kuten URN). EntityId:n ei tarvitse resolvoitua, eli sitä vastaavaa osoitetta ei tarvitse löytyä esim. DNS-järjestelmästä. SAML-määritykset mahdollistavat entiteetin metadatan löytämisen entityId:n perusteella. Tällainen menettely ei vielä ole käytössä Hakassa. Tulevaisuuden kehityksen mahdollistamiseksi kannattaa varata entityId:ksi sellainen nimi, joka ei myöhemmin törmää esim. tuotenimien tai organisaation julkisten www-osoitteiden kanssa.

AttributeScope(s) / Domain(s)	Valitse IdP:lle skooppi, jonka myöhemmin määrittelet attribuuteille.
	IdP voi luovuttaa skoopattuja attribuutteja, joissa skooppi määrittelee attribuutin voimassaoloalueen. Attribuuttien muoto on:
	`arvo@skooppi`
	Skoopattuja attribuutteja on Hakassa:
	• eduPersonPrincipalName
	• eduPersonScopedAffiliation
	• eduPersonUniqueId
	Haka-metadatassa skooppi ilmaistaan IdPSSODescriptorin Extensiona.
	`<IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">`
	`<Extensions>`
	`<shibmd:Scope regexp="false">funet.fi</shibmd:Scope>`
	`<shibmd:Scope regexp="false">yliopisto.fi</shibmd:Scope>`
	Hakassa on myös vatimus, että yksi IdP saa luovuttaa vain yhden arvon schacHomeOrganization -attribuutissa. Arvo on oltava sama kaikille käyttäjille. Arvon on vastattava jotakin metadataan määritettyä skooppia.
	schacHomeOrganization ja skoopattuja attribuutteja hyödyntävien on tarkistettava, että attribuuttien skoopit vastaavat jotakin metadataan ilmoitettua skooppia. Yksi IdP voi julkaista useamman skoopin. Suositus kuitenkin on, että skooppi on organisaation domain-nimi ja, että sama korkeakoulu ei käytä kuin yhtä skooppia. Siirtymävaiheessa sallitaan useampia skooppeja esim. silloin, kun IdM-järjestelmän vaihdoksen yhteydessä halutaan vanhentaa vanhojen käyttäjien skoopit luonnollisesti.
	mail-attribuutin sähköpostiosoitetta ei pidä sekoittaa skoopattuihin attribuutteihin. Esim. eppn näyttää sähköpostiosoitteelta ja eppn:n arvo voi olla sama, kuin mail-attribuutilla. Ei kuitenkaan voi olettaa, että eppn toimisi sähköpostiosoitteena.

Supported Protocols

Valitse aina SAML 2.0. Shibboleth 1.3 on jäänne menneisyydestä.

Supported Name Formats

> Luovuta palveluille vain niiden tarvitsemia tietoja. Jos käyttäjän henkilöllisyys ei ole palvelulle tarpeellinen tieto, se voi yksilöidä käyttäjän nimitunnisteen avulla. Persistent-nimitunniste on Hakassa suositeltu fep-versiosta 2.2 alkaen.

SAML-nimitunniste yksilöi käyttäjän identifioimatta (unique opaque identifier). Nimitunniste luovutetaan SAML-assertiossa Subject-kenttässä, kun attribuuttien arvot luovutetaan AttributeStatementissa. SP määrittelee metadatassa, mitä nimitunnisteita se tukee. Mikäli IdP ei pysty tuottamaan SP:n tukemaa nimitunnistetta, kirjautuminen voi päätyä virheeseen. Näin käy esim. silloin, kun IdP luovuttaa Hakassa aiemmin ainoana pakollisena nimitunnisteena transient-tunnisteen, mutta SP:n metadataan on kirjattu tuetuksi tunnisteeksi persistent.

NameIdentifier SAML-autentikaatiovastauksessa

```
<saml2:Subject>
      <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="https://testidp.funet.fi/idp/shibboleth" SPNameQualifier="https://testsp.funet.fi/Shibboleth.sso"
>_e50dd4f79c473b970d82d2ef80b29a2b</saml2:NameID>
```

Nimitunniste on jokaisen IdP/SP -paria ja käyttäjää kohden yksilöllinen. Tällä tavalla palvelut (SP) eivät voi identifioida käyttäjää nimitunnisteita vertaamalla.

Identifioimatonta nimitunnistetta käytetään palveluissa (SP) esim. silloin, kun halutaan mahdollistaa käyttäjälle pääsy samaan käyttäjäprofiiliin, mutta ei ole tarvetta tallentaa käyttäjän henkilötietoja. Henkilötietosäädösten ja Haka-palvelusopimuksen perusteella palvelut (SP) saavat käsitellä ja IdP luovuttaa vain tarpeellisia henkilötietoja. Esimerkiksi aineistotietopalvelussa tai metatietojen hakupalvelussa voi olla tarpeen rajata pääsy aineistoon vain tutkijoille. Tällöin ei tarvita henkilötietoa käyttäjistä, vain ainoastaan tieto henkilön suhteesta organisaatioon. Tutkijastatus voidaan Hakassa luovuttaa käyttäen eduPersonAffiliation-attribuuttia.

Identifioimattomien tunnisteiden käyttö helpottaa palvelun (SP) toteuttamista, sillä palveluun ei muodostu henkilörekisteriä. Palvelun suojaus voidaan toteuttaa kevyemmin.

urn:mace:shibboleth:1.0:nameIdentifier	Ei käytössä, jäänne menneisyydestä
urn:oasis:names:tc:SAML:2.0:nameid-format:transient	Sessioiden välillä vaihtuva nimitunniste. Pakollinen Hakassa. Valitse vähintään tämä.
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	Pysyvä nimitunniste, joka ei saa muuttua. Suositeltu Hakassa (fep v 2.2) Arvo voi olla sama, kuin eduPersonTargetedId-attribuutissa, mutta ei tarvitse olla. Shibboleth IdP tukee, mutta vaatii erillistä konfiguraatiota, jossa muodostetut nimitunnisteet joko tallennetaan tietokantaan ja tunnisteet muodostetaan laskemalla siemen-attribuutista ja kiinteästä siemenmerkkijonosta (salt).

The Federations this Entity will be published to

Cirrus test	CSC:n sisäinen, ei yleisessä käytössä
CSC Internal	CSC:n sisäinen, ei yleisessä käytössä
eduGain test	eduGainilla on testi-metadata, mutta Haka-IdP:llä on sille vähän käyttöä. Toistaiseksi ei ole tiedossa ulkomaista palvelua (SP), joka olisi kaikkien IdP:iden käytössä. Käytännössä testaaminen edellyttää jonkin ulkomaisen tahon kanssa sopimista.
Kalmar union test	Kuten edellinen, mutta pohjoismaisen Kalmar2-federaation metadata.
Haka test	**Vain tähän rasti.** IdP lisätään koulutuksessa Hakan testiympäristöön.

IdP's SAML Endpoints

Single Sign-On Service URLs

SSO URL määrittää palvelulle (SP) sen päätepisteen (endpoint), johon lähettää autentikaatiopyynnön. Osoite julkaistaan metadatassa.

```
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTPRedirect"
Location="https://testidp.funet.fi/idp/profile/SAML2/Redirect/SSO"/>
```

Hakassa käytetään SAML 2.0 Web Browser SSO Profiilia. Käytössä on vain HTTP-Redirect päätepiste. Hakassa on käytettävä suojattua HTTPS-liikennettä kaikkien SAML-viestien välittämiseen. Viimeistään keväällä 2016 on siirryttävä käyttämään vähintään SHA2-tasoisella menetelmällä allekirjoitettuja varmenteita HTTPS-päätepisteessä. Funetin Varmennepalvelusta saatavat uudet varmenteet ovat SHA2-allekirjoitettuja.

HTTP-Redirect	Muokkaa mallin mukaan oman IdP:si URL `https://vmXXXX.kaj.pouta.csc.fi/idp/profile/SAML2/Redirect/SSO`
HTTP-Post	Ei käytössä Hakassa

Attribute Service URLs

Ei käytetä tässä harjoituksessa. Jätä tyhjäksi.

Attribute Service URL määritetään silloin, kun IdP toimii nk. attribuuttirikastimena, eli AttributeProviderina. Käyttöoikeuksien valtuutuspalvelu REMS on esimerkki tällaisesta käyttötapauksesta. REMS ei autentikoi käyttäjää, vaan tunnistaminen tapahtuu käyttäjän oman kotiorganisaation IdP:llä. Kun käyttäjä kirjautuu palveluun (SP), joka tarvitsee käyttövaltuustietoa REMS:ltä, SP pyytää REMS-IdP:ltä lisäattribuutteja. REMS-IdP antaa autentikaatiovastauksen, jossa ei ole AuthenticationStatementia. Vastauksessa on AttributeStatement, jossa luovutetaan eduPersonEntitlement-attribuutti. Tämän attribuutin arvoon perustuen palvelu tekee ratkaisun, annetaanko käyttäjälle pääsy hänen hakemaansa aineistoon.

Lisätietoa REMS:stä: https://confluence.csc.fi/display/REMS/Home

IdP:t voidaan myös ketjuttaa niin, että käyttäjän autentikoiva IdP noutaa lisäattribuutteja toisen IdP:n AttributeProviderilta.

Single Logout Service URLs

Single Logout ei ole pakollinen Hakassa ja siihen liittyy hankaluuksia. SLO ei kuulu koulutuksen skooppiin, mutta voit määrittää omaa testailua varten metadataan seuraavat tiedot.

Shibboleth IvP v 3:een on suunniteltu laajempaa logout-tukea. Vielä sitä ei ole toteutettu ja v3 IdP:n käyttäytyminen LogoutRequesteihin saattaa olla ennalta-arvaamatonta ja todennäköisesti päättyy virheeseen. Seuraavissa versioissa tuki saattaa parantua.

Hakan käyttämä SAML-profiili asettaa vaatimuksia Single Logoutin toteutukselle. Single logout toteutetaan Hakassa nk. front channel kommunikaatiolla käyttäjän selaimessa. Päätepisteenä käytetään vain HTTP-Redirect. Jos logout ei toteudu täydellisesti, IdP:n on ohjeistettava käyttäjää logoutin loppuun saattamisessa.

Single Logout ei ole Hakassa pakollinen. Siitä syystä operoinnin ohjeitus onkin, että Single Logout -tukea ei kannata mainostaa metadatassa, ellei ole täyttä varmuutta, että SLO-vaatimukset täyttyvät. Shibboleth-IdP v3:n perustoteutuksella SLO-URL:ia ei pidä kirjata Haka-metadataan.

HTTP-Redirect	`https://vmXXXX.kaj.pouta.csc.fi/idp/profile/SAML2/Redirect/SLO`
SOAP	Ei käytössä Hakassa

Certificates

Muodosta salainen avain ja varmenne turvallisessa paikassa. Koulutuksessa on tarkoituksenmukaista muodostaa salainen avain virtuaalikoneympäristössä.

Käytä SAML-viestien suojaamiseen tarkoitettua salaista avainta ainoastaan SAML-käytössä IdP-palvelimella. Älä käytä samaa salaista avainta SAML-viestien ja HTTPS-liikenteen suojaamiseen. Koulutuksessa varmenne voi olla lyhytikäinen, mutta tuotannossa voit suunnitella varmenteen voimassaoloajan organisaatiosi ohjeistuksen perusteella.

Hakan varmennekäytännön mukaisesti:

- Palvelun DNS-nimen on vastattava varmenteen CN (common name) -kenttää
- Varmenteiden julkiselta avaimelta edellytetään vähintään 2048 bitin pituutta

Hakassa käytettävä varmenne voi siis olla myös itseallekirjoitettu.

SAML:ssa varmennetta käytetään vain julkisen avaimen toimittamiseen. Varmenteen muut ominaisuudet jätetään huomiotta. Siitä huolimatta varmenteen on oltava voimassa. Mikäli syntyy epäilys salaisen avaimen vaarantuneen, tai varmenne on vanhenemassa on avain vaihdettava prosessin mukaan.

Sijoita salainen avain palvelimelle asianmukaiseen paikkaan ja varmista, että siihen on lukuoikeus vain sillä käyttäjällä, jolla IdP-suoritusympäristöä ajetaan. Varmista, että `idp.properties` -tiedostossa on määritelty oikea avain ja varmenne käyttöön. Haka-resurssirekisterissä ei voi määritellä eri avainta ja varmennetta allekirjoituksen (signing) ja salaukseen (encryption), vaan on käytettävä samaa paria molemmissa tarkoituksissa.

Itseallekirjoitetun varmenteen muodostaminen (esimerkki)

```
openssl genrsa -out key.pem 2048
openssl req -new -key key.pem -out csr.pem
openssl req -x509 -days 365 -key key.pem -in csr.pem -out certificate.pem
mv key.pem /opt/shibboleth-idp/credentials/shibTrSamlKey.pem
chown root.jetty /opt/shibboleth-idp/credentials/shibTrSamlKey.pem
chmod 440 /opt/shibboleth-idp/credentials/shibTrSamlKey.pem
mv certificate.pem /opt/shibboleth-idp/credentials/shibTrSamlCert.pem
chown root.jetty /opt/shibboleth-idp/credentials/shibTrSamlCert.pem
chmod 444 /opt/shibboleth-idp/credentials/shibTrSamlCert.pem
less /opt/shibboleth-idp/credentials/shibTrSamlCert.pem
```

Kopioi varmenne resurssirekisteriin PEM-muodossa ilman BEGIN ja END -rivejä. Tarkista, että avainpituus ja CN vastaavat vaatimuksia ja varmenteen voimassaolo vastaa suunnitelmaa.

Supported attributes

Tämä osio on informatiivinen, jota käytetään attribuuttiluettelon muodostamiseksi tuotannon IdP-palvelimista. Koulutuksessa ei tarvitse rastittaa attribuutteja. Paina "Apply Changes and return".

Tuotannossa listan ajan tasalla pitäminen vähentää tarpeettomia kysymyksiä IdP-ylläpidolle.

UI Extensions

Täydennä IdP:n käyttöliittymätiedot. DS-palvelut hyödyntävät UI-tietoja vaihtelevasti. Hakan DS-palvelussa organisaation nimi otetaan DisplayName-kentästä ja valikossa tulostetaan organisaation kuvake, jos se on saatavilla HTTPS-URL:sta ja lisätty 16x16 kokoisena.

Koulutuksessa valitse IdP:llesi **erottuva DisplayName** kaikilla kolmella kielellä.

Statistics

Kirjautumistilastojen keräämistä ei käsitellä koulutuksessa. Lue lisää Haka-wikistä.

Contact Information

Tuotannossa on ilmoitettava vähintään tekninen kontakti. Sekä etunimi- ja sukunimikentät on täytettävä kaikille syötettäville kontakteille UTF-8 -merkistössä.

Submit IdP Description

Kun olet vamistunut tietojen oikeellisuudesta, **muista tallentaa muutokset** lähettämällä ne tarkastettavaksi Haka-operoinnille.