Palvelun rekisteröinti Virtu - luottamusverkostoon / testipalveluun

Tässä ohjeessa kerrotaan, miten lisäät uuden Identity Provider (IdP) palvelun kotiorganisaatioksi Virtu-luottamusverkostoon käyttäen Resurssirekisteriä.

Käyttöä koskevat kysymykset sähköpostitse osoitteeseen helpdesk@csc.fi.

Identity Provider (IdP) -palvelun rekisteröinti luottamusverkostoon

1. Mene Resurssirekisterin aloitussivulle *[1]* (https://virtus.csc.fi/) ja valitse linkki "***Add a new Identity Provider***"

2. Valitse palvelun omistavan organisaation tiedot "***Organization Information***" -kohdassa. Mikäli haluttua organisaatiota ei ole listassa tai palvelu tulee testaukseen, valitse ”Virtu Test Organization”.

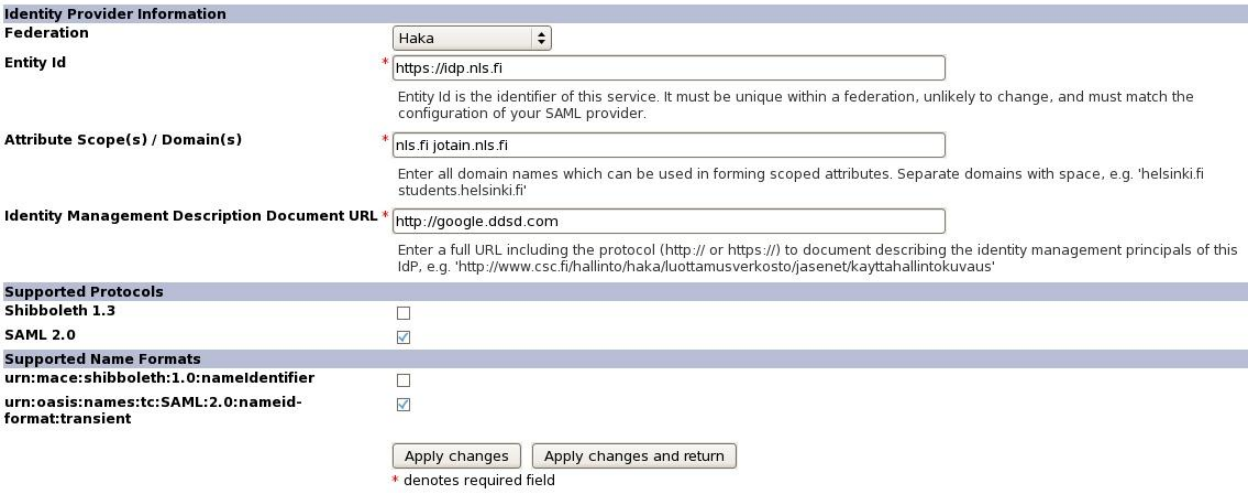
Kuva 1: Organisaation perustiedot

Uuden organisaation lisäämiseksi valintalistaan, ota yhteys sähköpostitse helpdesk@csc.fi.

3. Syötä IdP:n perustiedot kohdassa "***IdP Basic Information***". Valitse ensin luottamusverkosto, johon haluat palvelun liittää. Entity Id -kenttään tulee täyttää palvelun entityid, eli sen SAML-protokollassa yksilöivä tunniste. Tunnisteen on oltava uniikki ja sen on täsmättävä käytettävän SAML-toteutuksen konfiguraatiossa määriteltyyn entityid -arvoon. Entity Id -arvo kannattaa valita siten, ettei sitä tarvitse myöhemmin muuttaa, sillä muuttaminen jälkeenpäin voi olla työlästä.

Anna virtuHomeOrganization-attribuutissa käytettävä domain-nimi kenttään Attribute Scope(s) / Domain(s).

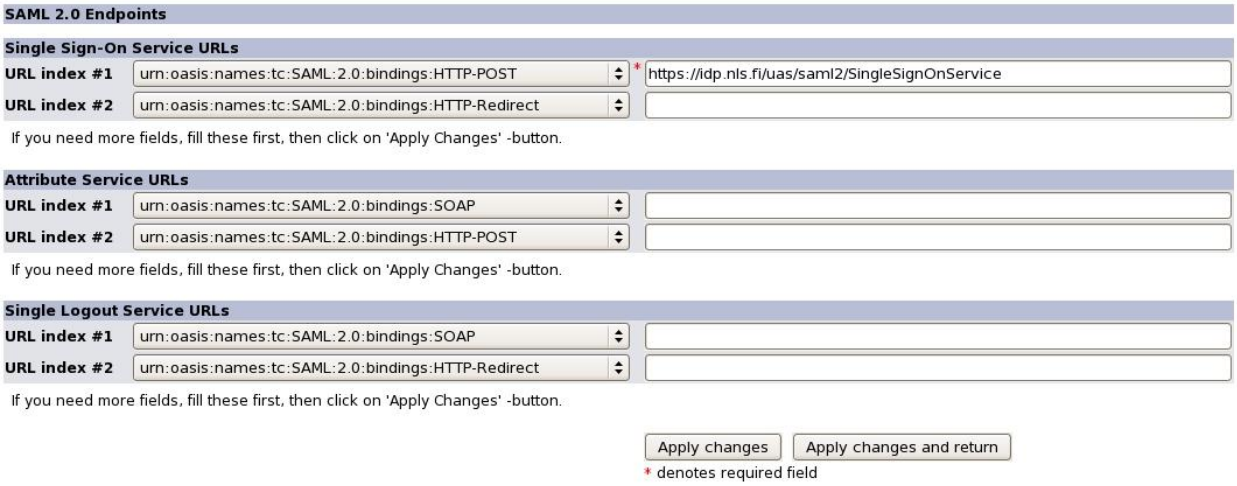
Valitse tuetut protokollat ja Name Format -arvot. Vähintään "SAML 2.0" protokolla ja "urn:oasis:names:tc:SAML:2.0:nameid-format:transient " Name Format on syytä olla tuettuna, ks. Virtu SAML - profiili *[2]*.



Kuva 2: IdP:n perustiedot

4. Syötä IdP:n SAML-osoitteet kohdassa "***IdP SAML Endpoints***". Vähintään HTTP-POST -muotoinen SSO-osoite on oltava syötettynä. Muut osoitteet ovat Virtu SAML-profiilin mukaisesti valinnaisia, eikä pidä olettaa, että Virtuun liittyneet SP:t osaavat niitä hyödyntää.

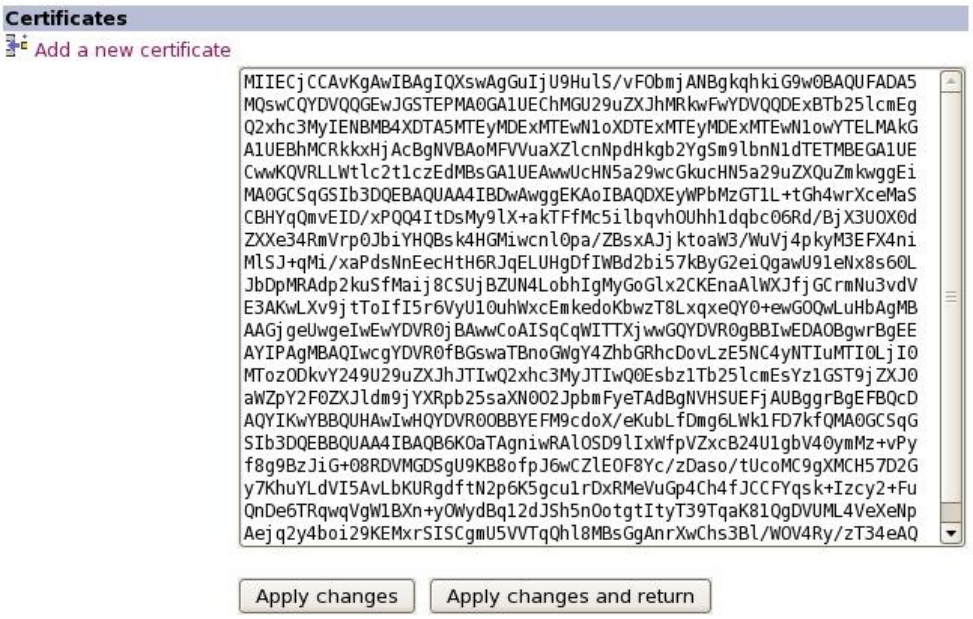
Kaikkien osoitteiden on käytettävä HTTPS-prokollaa, joten palvelu tarkistaa, että osoitteet alkavat "https://".



Kuva 3: SAML-osoitteiden syöttäminen

5. Syötä varmenne, jota IdP käyttää SAML-assertioiden allekirjoittamiseen kohdassa "***Certificates***". Huomaa varmenteelle asetetut tekniset vaatimukset, jotka on kerrottu vielä kyseisellä sivulla. Palvelu ei anna syöttää varmennetta, jonka se havaitsee virheelliseksi.

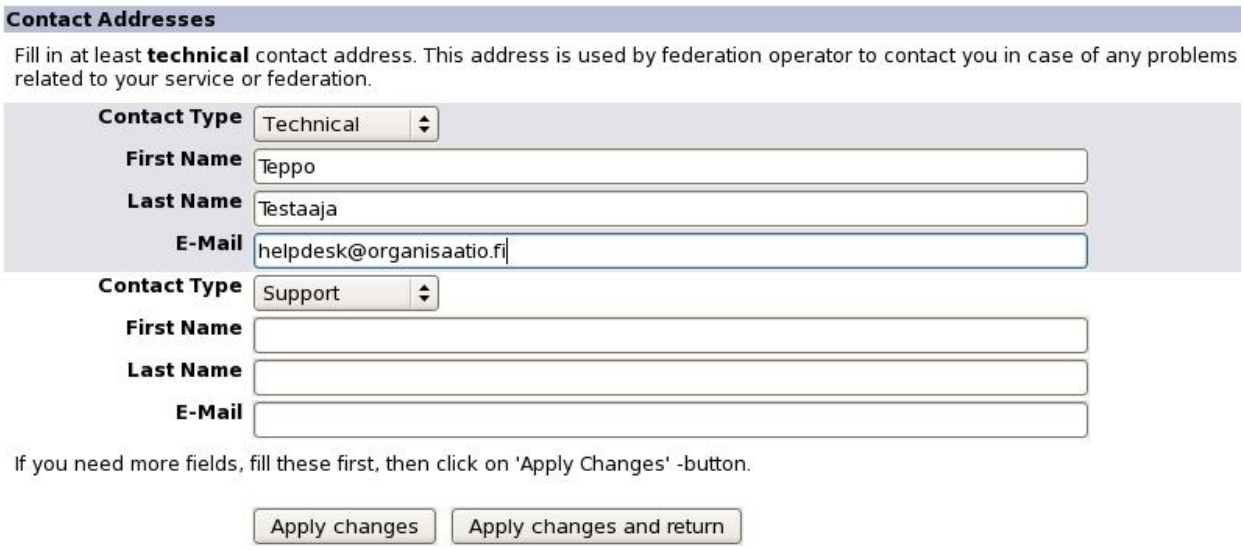
Syötettyäsi varmenteen hyväksytysti voit vielä muuttaa varmenteen käyttötarkoitusta tai lisätä muita varmenteita. Tämä on harvemmin tarpeen.



Kuva 4: Varmenteen syöttäminen

6. Valitse ne attribuutit, joita IdP tukee sivulla "***Supported Attributes***". Huomaa, että vähintään luottamusverkoston pakolliset attribuutit on oltava valittuna. Ajantasainen tieto saatavilla olevista attribuuteista on tärkeää palveluntarjoajille, joten muistathan päivittää tätä tietoa kun lisäät uusia attribuutteja IdP:iisi.

7. Syötä palvelun yhteystiedot sivulla "***Contact Information***". Vähintään tekninen kontaktiosoite on annettava. Osoitteen on syytä olla palveluosoite, jolla tavoittaa IdP:n ylläpidon myös loma-aikana. Luottamusverkoston operaattori käyttää tätä osoitetta teknisissä yhteydenotoissa esimerkiksi vikatilanteissa tai tietoturvaan liittyvissä tiedotteissa. Yhteystiedot julkaistaan luottamusverkoston SAML-metadatassa, jotta myös muille luottamusverkoston osapuolille on tarjolla kontaktipiste mahdollisia ongelmatilanteita varten.



Kuva 5: Yhteystietojen syöttäminen

8. Syötettyäsi yhteystiedot palvelu tarkistaa rekisteröintitiedot. Huomioi mahdolliset varoitukset ja korjaa niiden syy, mikäli aiheellista.

9. Voit tarkastella syöttämiesi tietojen pohjalta generoitua SAML-metadataa kohdasta "***View Metadata***".

10. Voit perua kaikki tekemäsi muutokset kohdassa "***Cancel modifications***".

11. Kun olet tarkistanut, että kaikki tiedot ovat oikein täytetty, lähetä rekisteröintitiedot painamalla "***Submit IdP Description***" -linkkiä. Tämän jälkeen tiedot menevät luottamusverkoston operaattorin sekä VIP:n tarkistettavaksi. Voit vielä tarkistaa syöttämäsi tietoja, ja ota yhteyttä operaattoriin mahdollisimman pikaisesti, mikäli havaitset virheitä.

12. Saat sähköpostitse kuittauksen, kun rekisteröinti ja valtuutesi rekisteröinnin tekemiseen on tarkistettu. Mikäli operaattori tarvitsee lisätietoja tai rekisteröinnissä on puutteita, niitä kysytään myös tässä vaiheessa.

13. Kun rekisteröinti on operaattorin ja VIP:n hyväksymä, IdP:si lisätään luottamusverkostoon.

Viitteet

1. Virtu Resurssirekisteri, ***https://virtus.csc.fi***
2. Virtu-käyttäjätunnistusjärjestelmän tekniset määritykset, ***http://www.csc.fi/sivut/virtu/tekniikka/maaritykset/***