

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/) (<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".

Organization Information	
Select organization	Virtu Test Organization ▾
Descriptive Name (Finnish)	Virtu Test Organization
(English)	Virtu Test Organization
(Swedish)	Virtu Test Organization
Organization's home page URL	http://www.csc.fi/sivut/virtu

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 täsmäyttävä 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 [\[2\]](#).

Identity Provider Information	
Federation	Haka
Entity Id	* https://idp.nls.fi <small>Entity Id is the identifier of this service. It must be unique within a federation, unlikely to change, and must match the configuration of your SAML provider.</small>
Attribute Scope(s) / Domain(s)	* nls.fi jotain.nls.fi <small>Enter all domain names which can be used in forming scoped attributes. Separate domains with space, e.g. 'helsinki.fi students.helsinki.fi'</small>
Identity Management Description Document URL *	http://google.ddsd.com <small>Enter a full URL including the protocol (http:// or https://) to document describing the identity management principals of this IdP, e.g. 'http://www.csc.fi/hallinto/haka/luottamusverkosto/jasenet/kayttahallintokuvaus'</small>
Supported Protocols	
Shibboleth 1.3	<input type="checkbox"/>
SAML 2.0	<input checked="" type="checkbox"/>
Supported Name Formats	
urn:mace:shibboleth:1.0:nameidentifier	<input type="checkbox"/>
urn:oasis:names:tc:SAML:2.0:nameid-format:transient	<input checked="" type="checkbox"/>
<input type="button" value="Apply changes"/> <input type="button" value="Apply changes and return"/>	
* denotes required field	

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://".

SAML 2.0 Endpoints	
Single Sign-On Service URLs	
URL index #1	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST * https://idp.nls.fi/uas/saml2/SingleSignOnService
URL index #2	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
<small>If you need more fields, fill these first, then click on 'Apply Changes' -button.</small>	
Attribute Service URLs	
URL index #1	urn:oasis:names:tc:SAML:2.0:bindings:SOAP
URL index #2	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
<small>If you need more fields, fill these first, then click on 'Apply Changes' -button.</small>	
Single Logout Service URLs	
URL index #1	urn:oasis:names:tc:SAML:2.0:bindings:SOAP
URL index #2	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
<small>If you need more fields, fill these first, then click on 'Apply Changes' -button.</small>	
<input type="button" value="Apply changes"/> <input type="button" value="Apply changes and return"/>	
* denotes required field	

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 lisää 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-metadatatassa, jotta myös muille luottamusverkoston osapuolille on tarjolla kontaktipiste mahdollisia ongelmatilanteita varten.

Contact Addresses

Fill in at least **technical** contact address. This address is used by federation operator to contact you in case of any problems related to your service or federation.

Contact Type	Technical
First Name	Teppo
Last Name	Testaaja
E-Mail	helpdesk@organisaatio.fi
Contact Type	Support
First Name	
Last Name	
E-Mail	

If you need more fields, fill these first, then click on 'Apply Changes' -button.

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 kiittauksen, 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/>