

SP-palvelimen rekisteröiminen eduGAIN:iin

Seuraavassa on esitetty [Haka-resurssirekisterissä](#) suoritettavat toimenpiteet, joilla Hakaan rekisteröidyn SP-palvelimen ylläpitäjä pyytää SP-palvelimensa välittämistä eduGAIN:iin.

1. Merkitse SP Basic Information -välilehdellä federaatiot, joihin haluat metadatasia julkaistavan (tässä: eduGAIN).

The Federations this Entity will be published to	
eduGain	☒
eduGain Test	☐
Haka	☒
Haka test	☐
Kalmar Union	☒
Kalmar Union Test	☐

2. Välilehdellä 'Contact Information' oleva yhteyshenkilön sähköpostiosoitteen tulisi olla rooliin perustuva (esim. techadmin@..) eikä henkilökohtainen.
3. Metadata UI -elementit tulisi olla täytetty mahdollisimman täydellisesti. Tämä tapahtuu täyttämällä tiedot 'Ui Extensions' - välilehdellä. Erityisen tärkeät elementit ovat:
 - a. Displayname englanniksi ja itse palvelun kielellä.
 - b. Description englanniksi ja itse palvelun kielellä.
 - c. Privacy Policy URL englanniksi ja itse palvelun kielellä.

Entity Categories

Entity Categoryt ovat [Entity Category Attribute Types](#) -määrittelyn mukaisia kokoelmia samantyyppisistä SAML-palvelimista. Haka-resurssirekisterissä SP-ylläpitäjä voi pyytää SP-palvelimensa sisällyttämistä haluamaansa kategoriaan. Tällä hetkellä Haka-resurssirekisteri tuntee seuraavat kategoriat (kuva alla):

- [GÉANT Data Protection Code of Conduct](#). Rastittamalla tämän kohdan ilmaiset, että organisaatiosi on sitoutunut käsittelemään SP:lle luovutettuja attribuutteja GÉANT-tietosuojakäytännön mukaisesti.
- [Research and Scholarship](#), joka on Entity Category tiedettä ja tutkimusta tukeville palveluille. Kategoriaan pääsemistä varten SP:n ylläpitäjän tulee ottaa yhteyttä Haka-operaattoriin (haka@csc.fi), joka varmistaa että kategorian ehdot täyttyvät.
- [CLARIN member](#), Entity Category, SP-palvelimista, jotka kuuluvat Clarin Service Provider Federation - luottamusverkostoon
- [SIRTFI \(The Security Incident Response Trust Framework for Federated Identity\)](#), Ei käytössä SP-palvelimella.
- [European Student Identifier Entity Category](#), Entity Category, jolla ilmaistaan, että SP noudattaa ESI Entity Categoryn määrittystä schacUniquePersonalCode-attribuutissa (kts: [funetEduPersonSchema2.dot5](#))

Resurssirekisteriin täytettyjen tietojen perusteella resurssirekisteri lisää tarvittavat elementit SP-palvelimesta eduGAIN:iin välitettävään SAML-metatietoon.

Entity Categories

Please visit [Haka Confluence](#) for more information about eduGAIN. About [Entity Categories](#).

Please study the requirements and contact Haka operators before committing to Entity Categories:

1. [Requirements](#) for "Code of Conduct"
2. [Requirements](#) for "Research and Scholarship"
3. [Requirements](#) for "CLARIN member"
4. [Requirements](#) for "SIRTFI (The Security Incident Response Trust Framework for Federated Identity)"
5. [Requirements](#) for "European Student Identifier Entity Category"

Entity Categories this SP is following:

1. GEANT Data Protection Code of Conduct for Service Providers in EU/EEA and countries with adequate protection:
<http://www.geant.net/uri/dataprotection-code-of-conduct/v1> ☐

2. Research and Scholarship:
<http://refeds.org/category/research-and-scholarship> ☐

3. SP is a member of the CLARIN SP Federation:
<http://clarin.eu/category/clarin-member> ☐

4. Sirtfi (The Security Incident Response Trust Framework for Federated Identity):
<https://refeds.org/sirtfi> ☐

This SP follows European Student Identifier Entity Category specification

5. European Student Identifier Entity Category:
<https://myacademicid.org/entity-categories/esi> ☐



Entity Categories

About [Entity Categories](#).

Please study the requirements and contact Haka operators before committing to Entity Categories
[A. Requirements](#) for "Code of Conduct"
[B. Requirements](#) for "Research and Scholarship"

Entity Categories this SP is following:

<http://www.geant.net/uri/dataprotection-code-of-conduct/v1> ☐

<http://refeds.org/category/research-and-scholarship> ☐

SP Trust Rules

Haka-resurssirekisterin eduGAIN Rules -välilehdeltä SP-ylläpitäjä voi poimia ne Identity Provider -palvelimet, joiden suorittamaan käyttäjätunnistukseen ja luovuttamiin attribuutteihin SP luottaa. Resurssirekisteri tuottaa SP-palvelimen käyttöön mainitut Identity Provider -palvelimet sisältävän SAML 2.0 -metadatatiedoston.

Alasvetovalikoissa IdP-palvelimen kotifederaatio ilmaistaan sen eduGAIN-metadatatista poimitun Registration Authority -arvon perusteella. Vaikka arvo on pakollinen, niin valitettavasti ainakin tällä hetkellä kaikki entityt eivät kerro eduGAIN-metadatatissaan kotifederaatiotaan. Haka-resurssirekisteri on niputtanut kyseiset kodittomat 'Homeless'-kotifederaation alle.

Seuraava kuva selvittää yleistä periaatetta. Esimerkkikonfiguraatiota ei tule käyttää tuotantokonfiguraation pohjalla, sen ainoa tarkoitus on valaista sääntöjen käyttöä.

eduGAIN IdPs this SP trusts

eduGAIN trust rules for this Service Provider.

Trust Rule #0	eduGain	All	trusted
Trust Rule #1	http://rr.aai.switch.ch/	All	non-trusted
Trust Rule #2	http://www.swamid.se/	All	non-trusted
Trust Rule #3	http://www.swamid.se/	https://hbidp.hb.se/idp/shibboleth	trusted
Trust Rule #4	Choose authority	Choose entity	Choose action
apply trust rules			

View eduGAIN IdPs

View how your rules target a specific IdP, is the entity trusted.

eduGAIN IdP:	http://www.swamid.se/	https://hbidp.hb.se/idp/shibboleth
View IdP		

Entity	Authority	Trusted	Explanation
https://hbidp.hb.se/idp/shibboleth	http://www.swamid.se/	✓	There is a entity level rule to trust

Esimerkin konfiguraation säännöt tulkitaan seuraavasti: "Luota (#0) kaikkiin eduGAIN IdP entityihin, paitsi niihin, jotka on rekisteröinyt (#1) Sveitsin tai (#2) Ruotsin luottamusverkosto. Ruotsalaisten IdP-palvelinten suhteen tee kuitenkin (#3) poikkeus IdP-palvelimen <https://hbidp.hb.se/idp/shibboleth> kohdalla ja luota siihen".

Luottamus tiettyyn Entityyn evaluoidaan seuraavasti:

1. Tutki *Entity*-tason säännöt (#3). Jos evaluoitavalle Entitylle löytyy sääntö, noudata sitä. Muuten siirry seuraavaan kohtaan.
2. Tutki *Federaatio*-tason säännöt (#1 ja #2). Jos evaluoitavan Entityn kotifederaatiolle löytyy sääntö, noudata sitä. Muuten siirry seuraavaan kohtaan.
3. Noudata eduGAIN-tason (*Authority*-taso) sääntöä (#0).

Voit tarkastella sääntöjesi vaikutusta per eduGAIN IdP "View eduGAIN IdPs" toiminnolla. Esimerkissä on valittu ruotsalainen entity <https://hbidp.hb.se/idp/shibboleth>, jolle esimerkissä löytyy siis *Entity*-tason sääntö (#3), jonka perusteella siihen luotetaan.

Perustelu näinkin monimutkaiselle tavalle filteröidä entityjä sekä itse entityn että entityn kotifederaation (*Authority*) perusteella on eduGAINin käytänteiden monimuotoisuus. Jos olet tyytyväinen esimerkiksi Ruotsin federaation käytänteisiin ja luotat siihen kuin 'Hakaan', voit määrittellä *Federaatio*-tason säännöllä luottavasi automaattisesti kaikkiin Ruotsin federaation eduGAINiin julkaisemiin IdP-palvelimiin. Toisaalta automaattinen luottamussuhteen muodostaminen esimerkiksi brasilialaisiin IdP-palvelimiin ei välttämättä ole kaikille itsestään selvää.

Entity-filtointi on tärkeää myös, jotta voit sulkea pois entityjä, jotka saat duplikaattina esimerkiksi Hakasta tai Kalmarin unionista. Näiden pois sulkeminen ei ole täysin välttämätöntä, jos käytät esimerkiksi Shibboleth SP-palvelinta. Shibbolethin oletustoiminta on käyttää kustakin entiteystä (*entityID:stä*) sitä instanssia, joka sijaitsee metadatalähteissä ensimmäisenä. Tästä syystä määrittele vähintäänkin **Hakan eduGAINiin ilmoittamat jäsenet epäluotetuiksi** *Authority*-tason säännöllä.

Tekemäsi (ja operaattorin hyväksymät) muutokset heijastuvat SP-kohtaiseen eduGAIN-metadatasii noin tunnin viiveellä. SP-kohtainen metadatasii haetaan SP-palvelimen Resurssirekisterin id:n perusteella osoitteesta [http://haka.funet.fi/edugain-nightly/gen-edugain/sp-\[id\]-metadata-eduGain.xml](http://haka.funet.fi/edugain-nightly/gen-edugain/sp-[id]-metadata-eduGain.xml).

SP-palvelimen eduGAIN downstream metadata

Taulukossa käytetyn id-arvon saat SP-palvelimellesi Resurssirekisteristä SP-palvelimen tiedoista (Resource Registry ID). Resurssirekisteri luo jokaiselle eduGAINiin rekisteröidylle SP-palvelimelle räätälöidyn metadata-tiedoston palvelimelle määritettyjen eduGAIN-sääntöjen pohjalta.

Selitys	
SP-palvelimen metadata	https://haka.funet.fi/edugain-nightly/gen-edugain/sp-[id]-metadata-eduGain.xml
eduGAIN metadatan allekirjoitusvarmenne	haka-edugain-sign.csc.fi.2023.pem

Esimerkki SP-palvelimen konfiguroinnista (Shibboleth)

Esimerkki näyttää suuntaa kuinka ottaa käyttöön Resurssirekisterin luoma SP-kohtainen metadata-tiedosto Haka-metadatan rinnalle (mukana allekirjoituksen tarkistus):

shibboleth IdP, relying-party.xml

```
.  
.  
<!-- Haka metadata -->  
<MetadataProvider type="XML" url="https://haka.funet.fi/metadata/haka-metadata.xml" backingFilePath="haka-  
metadata.xml" reloadInterval="3600">  
  <MetadataFilter type="Signature" certificate="/etc/pki/tls/certs/haka-sign-v5.pem"/>  
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="2592000"/>  
  <MetadataFilter type="EntityRoleWhiteList">  
    <RetainedRole xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">md:IDPSSODescriptor</RetainedRole>  
  </MetadataFilter>  
</MetadataProvider>  
  
<!-- eduGAIN metadata -->  
<MetadataProvider type="XML" url="https://haka.funet.fi/edugain-nightly/gen-edugain/sp-XX-metadata-eduGain.xml"   
backingFilePath="sp-XX-metadata-eduGain.xml" reloadInterval="3600">  
  <MetadataFilter type="Signature" certificate="/etc/pki/tls/certs/haka-edugain-sign.csc.fi.2021.pem"/>  
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="2592000"/>  
  <MetadataFilter type="EntityRoleWhiteList">  
    <RetainedRole xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">md:IDPSSODescriptor</RetainedRole>  
  </MetadataFilter>  
</MetadataProvider>  
.  
.
```

Embedded Discovery Service

Loppukäyttäjien palvelussa asiointia voidaan helpottaa konfiguroimalla SP-palvelimen kirjautumissivun yhteyteen EDS (Embedded Discovery Service). Hakan asiointipalvelusta(<https://rr.funet.fi/haka/>) löytyy esimerkki EDS-palvelusta, jossa on hyödynnetty SWITCHin EDS-toteutusta:



For eduGAIN Login, choose your home organization from the box below.
If the selection box doesn't appear, check that your browser has Javascript enabled.

Login with:

haka

CSC - IT Center for Science Ltd.

University of Vaasa
Vaasa University of Applied Sciences
Åbo Akademi University

From other federations

AAI@EduHr Single Sign-On Service
ACOnet staff
AESIR
ARNES
Belnet
BFH - Berner Fachhochschule

SWITCH EDS -toteutuksesta löydät lisätietoja täältä: <https://www.switch.ch/aii/support/serviceproviders/sp-embedded-wayf.html>

Hakan EDS-sivu: <https://wiki.eduuni.fi/display/CSCHAKA/Embedded+DS>

Shibboleth EDS: <https://wiki.shibboleth.net/confluence/display/EDS10/1.+Overview>