

IdP-palvelimen rekisteröiminen eduGAIN:iin

Seuraavassa on esitetty Haka-resurssirekisterissä suoritettavat toimenpiteet, joilla Hakaan rekisteröidyn IdP-palvelimen ylläpitäjä saa IdP-palvelimensa näkymään eduGAIN:iin.

1. Merkitse **IdP's Basic Information** -välilehdellä federaatiot, joihin haluat metatiasi julkaistavan (tässä: eduGAINiin).

The Federations this Entity will be published to	
eduGain	☒
eduGain Test	☐
Haka	☒
Haka 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.

IdP Trust Rules

eduGAIN Rules -välilehdellä IdP-ylläpitäjä voi määrittellä, mihin Service Provider palvelimiin IdP-palvelin luottaa (luovuttaa attribuutteja). Määritysten perusteella resurssirekisteri tuottaa IdP-palvelimen tarvitseman SAML-metadatatiedoston.

Määrittely voidaan tehdä kahdella tavalla:

- **Basic eduGAIN Rules:** IdP luottaa kaikkiin SP-palvelimiin, jotka ovat sitoutuneet tiettyyn Entity Category -ryhmään
- **Advanced eduGAIN Rules:** IdP-ylläpitäjä määrittelee yksitellen, mihin SP-palvelimiin IdP luottaa

Muistathan määrittelyjä tehdessäsi, että kyse on henkilötietojen luovuttamisesta toiselle rekisterinpitäjälle, mitä säätelee henkilötietolaki.

Basic eduGAIN Rules: Entity Categories

Entity Categoryt ovat [Entity Category Attribute Types](#) -määrittelyn mukaisia kokoelmia samantyyppisistä SAML-palvelimista. Haka-resurssirekisterissä IdP-ylläpitäjä voi yksinkertaisesti konfiguroida IdP:n luottamaan (luovuttamaan attribuutteja) kaikille SP-palvelimille, jotka kuuluvat tiettyyn Entity Categoryyn. Tällä hetkellä Haka-resurssirekisteri tuntee seuraavat kategoriat:

- [GÉANT Data Protection Code of Conduct](#), EU/ETA-maissa tai niihin rinnastuvissa maissa sijaitsevat SP-palvelimet, jotka ovat sitoutuneet GÉANT-tietosuojakäytäntöön.
- [Research and Scholarship](#), globaali Entity Category SP-palvelimista, jotka paikallisen federaation näkemyksen mukaan tukevat tiedettä ja tutkimusta.
- [CLARIN member](#), Entity Category, SP-palvelimista, jotka kuuluvat Clarin Service Provider Federation - luottamusverkostoon
- [SIRTFI \(The Security Incident Response Trust Framework for Federated Identity\)](#), Entity Category, SP-palvelimista, jotka ilmoittavat olevansa Sirtfi-kehikon vaatimusten mukaisia
- [European Student Identifier Entity Category](#), Entity Category, jolla ilmaistaan, että IdP noudattaa ESI Entity Categoryn määrittystä schacUniquePersonalCode-attribuutissa (kts: [funetEduPersonSchema2.dot5](#))

Tällöin resurssirekisteri tuottaa IdP-ylläpitäjälle SAML-metadatatiedoston, joka sisältää valittuun kategoriaan kuuluvat SP-palvelimet. Jos valitset useamman kategorian, SP-palvelin tulee poimituksi mukaan, jos se kuuluu ainakin yhteen valitsemistasi kategorioista (joukko-opillisesti kyse on siis unionista).

Basic EduGAIN Rules, trust EduGAIN SPs committed to Entity Categories

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

Please study the requirements before committing to Entity Categories:

1. Requirements for [Data Protection 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](#).

This IdP will trust all EduGAIN SPs which are committed to:

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 IdP follows European Student Identifier Entity Category specification (Does not affect entity selection)

5. European Student Identifier Entity Category:

<https://myacademicid.org/entity-categories/esi> ☐

Advanced eduGAIN Rules

Basic-tason sääntöjen lisäksi/sijaan IdP-ylläpitäjä voi poimia yksitellen ne SP-palvelimet, joihin haluaa luottaa. Advanced-tason säännöt ohittavat aina Basic-tason säännöt, jos sellaisia on tehty. Toimintaperiaate on sama kuin "SP Trust Rules" sivulla [SP:n luottamat Identity Provider -palvelimet](#).

'Advanced eduGAIN Rules' - kohdan alasvetovalikoissa SP-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-metadatatassaan 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.

Advanced EduGAIN Rules

Advanced EduGAIN trust rules for this IdP. These rules are dominant and will override Basic EduGAIN Rules(Code of Conduct).

Trust Rule #0

Trust Rule #1

eduGain	▼	All	▼	trusted	▼
http://cafe.rnp.br	▼	All	▼	non-trusted	▼
apply trust rules					

Esimerkin konfiguraation säännöt tulkitaan seuraavasti: "Luota (#0) kaikkiin eduGAIN SP -entiteihin, paitsi niihin, jotka on rekisteröinyt (#1) Brasilian Café-luottamusverkosto."

Luottamus tiettyyn Entiteettiin evaluoidaan seuraavasti:

1. Tutki Entity-tason säännöt. Jos evaluoitavalle Entiteetille löytyy sääntö, noudata sitä. Muuten siirry seuraavaan kohtaan.
2. Tutki federaatiotason säännöt (#1). Jos evaluoitavan Entiteetin kotifederaatiolle löytyy sääntö, noudata sitä. Muuten siirry seuraavaan kohtaan.
3. Noudata eduGAIN-tason sääntöä (#0).

Attribuuttien luovutuksen konfiguroiminen

Sen lisäksi, että IdP-ylläpitäjä voi määritellä entity-, kotifederaatio- tai eduGAIN-tason säännöt niistä SP-palvelimista, joihin IdP-palvelin luottaa, IdP-ylläpitäjä voi myös asettaa perälaudan kullekin SP-palvelimille luovutettavien attribuuttien listalle. 'eduGAIN Rules' -välilehdellä on toiminto, jolla voi rakentaa sääntöjä attribuutti- ja SP-kohtaisesti.

Alla oleva esimerkkikonfiguraatio selvittää sääntöjen toimintaa eikä ole sellaisenaan malli tuotantokonfiguraatiolle.

Attributes this IdP releases to eduGAIN			
Mark attribute release rules for eduGain SPs			
nationalIdentificationNumber [urn:oid:1.2.246.21]			
Rule #0	Choose authority	Choose entity	Choose action
preferredLanguage [urn:oid:2.16.840.1.113730.3.1.39]			
Rule #0	http://feide.no/	https://foodl.org/simplesaml/module.php/saml/sp/metadata.php/saml	allow
Rule #1	Choose authority	Choose entity	Choose action
cn [urn:oid:2.5.4.3]			
Rule #0	http://feide.no/	https://foodl.org/simplesaml/module.php/saml/sp/metadata.php/saml	allow
Rule #1	Choose authority	Choose entity	Choose action
sn [urn:oid:2.5.4.4]			
Rule #0	http://feide.no/	https://foodl.org/simplesaml/module.php/saml/sp/metadata.php/saml	allow
Rule #1	Choose authority	Choose entity	Choose action

Periaattena, on, että kukin attribuutti luovutetaan,

- jos kohdasta IdP Trust Rules (ks. yllä) seuraa, että IdP ylipäätään luottaa kyseiseen SP-palvelimeen JA
- jos SP pyytää kyseistä attribuuttia (käyttämällä SAML-metadatan md:RequestedAttributes-elementtiä) JA
- jos "Attributes this IdP releases to eduGAIN" -kohta sallii kyseisen attribuutin luovuttamisen kyseiselle SP-palvelimelle.

Attribuuttien luovutussäännöt evaluoidaan entity-tasolta ylöspäin seuraavasti:

1. Tutki Entity-tason säännöt (#2). Jos evaluoitavalle Entiteyille löytyy sääntö, noudata sitä. Muuten siirry seuraavaan kohtaan.
2. Tutki federaatiotason säännöt (#1). Jos evaluoitavan Entiteyn kotifederaatiolle löytyy sääntö, noudata sitä. Muuten siirry seuraavaan kohtaan.
3. Noudata eduGAIN-tason sääntöä (#0).

Kuvan esimerkikikonfiguraatio ilmaisee, että "Lähetä attribuutti 'cn' kaikille sitä pyytävälle (#0) eduGAIN SP-palvelimille paitsi, jos palvelun kotifederaatio on (#1) Norjan Feide. Norjan federaation palveluiden joukossa (#2) tee kuitenkin poikkeus foodl.org-palvelun osalta ja lähetä sille cn pyydettyessä".

Näiden sääntöjen perusteella Haka-resurssirekisteri muodostaa kunkin IdP-palvelimen metadatatiedostoon 'RequestedAttribute' osuudet kullekin SP:lle. Tämän perusteella Shibboleth IdP-palvelin päättää, mitä attribuutteja lähetetään kullekin SP-palvelimelle.

Luottamuksen ja attribuuttien luovutuksen testaaminen

IdP-ylläpitäjä voi tarkastella omien sääntöjensä vaikutusta kunkin eduGAIN SP-palvelimen kohdalla:

View eduGAIN SPs			
View how your rules target a specific SP, are you releasing the requested attributes and is the entity trusted at all.			
eduGAIN SP:			
		http://ukfederation.org.uk	
		https://sso.ft.com/sso/sp/oa/metadata	
		View SP	
Entity	Authority	Trusted	Explanation
https://sso.ft.com/sso/sp/oa/metadata	http://ukfederation.org.uk	✓	There is a entity level rule to trust

Ensimmäinen taulukko kertoo, että foodl.org -niminen SP on sääntöjen perusteella luotettu ja sisällytetty IdP-palvelimen saamaan eduGAIN-metadataan. Toisesta taulukosta näet attribuutisääntöjesi vaikutuksen luovutettaviin attribuutteihin.

Tekemäsi muutokset heijastuvat IdP-kohtaiseen eduGAIN-metadatasii noin tunnin viiveellä siitä, kun Haka-operaattori on hyväksynyt ne. Haka-resurssirekisteri generoi kerran tunnissa IdP-palvelimellesi näiden sääntöjen perusteella metadatan (ks. alla), joka sisältää valitsemasi eduGAIN-SP-palvelimet. Jos tiettyä attribuuttia ei sääntöjesi mukaan saa luovuttaa kohteelle, kyseinen attributti kommentoidaan ulos metadatatista.

IdP-palvelimen eduGAIN downstream metadata (Shibboleth)

Alla taulukossa käytetyn id-arvon saat IdP-palvelimellesi Resurssirekisteristä IdP-palvelimen tiedoista (Resource Registry ID) . Resurssirekisteri luo jokaiselle eduGAINiin rekisteröidylle IdP-palvelimelle räätälöidyn tiedoston palvelimelle määritetyjen eduGAIN-sääntöjen pohjalta. Erillisestä attribute-filter.xml tiedoston luomisesta on luovuttu koska sama tieto on nyt saatavilla IdP:n metadata tiedostosta.

Selitys	URL
IdP-palvelimelle räätälöity metadata	https://haka.funet.fi/edugain-nightly/gen-edugain/idp-[id]-metadata-eduGain.xml
eduGAIN metadatan allekirjoitusvarmenne	haka-edugain-sign.csc.fi.2023.pem

Esimerkki IdP-palvelimen konfiguroinnista (Shibboleth)

Esimerkki näyttää suuntaa kuinka ottaa käyttöön Resurssirekisterin luoma IdP-kohtainen metadata-tiedosto Haka-metadatan rinnalle (mukana allekirjoituksen tarkistus), huomaathan myös vaihtaa oman IdP:si ID:n edugain osioon.

shibboleth IdP, metadata-providers.xml

```
.
.
<!-- Haka MetadataProvider -->
<MetadataProvider backingFile="%{idp.home}/metadata/haka-metadata.xml" id="HTTPHakaMetadata" maxRefreshDelay="
PT2H" metadataURL="https://haka.funet.fi/metadata/haka-metadata.xml" refreshDelayFactor="0.5" xsi:type="
FileBackedHTTPMetadataProvider">
  <MetadataFilter certificateFile="%{idp.home}/credentials/haka-sign-v5.pem" xsi:type="SignatureValidation"/>
  <MetadataFilter xsi:type="EntityRoleWhiteList">
    <RetainedRole>md:SPSSODescriptor</RetainedRole>
  </MetadataFilter>
  <MetadataFilter xsi:type="Algorithm"> <!-- Legacy algorithm for these entities -->
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
    <Entity>http://enit.id.com/adfs</Entity>
  </MetadataFilter>
</MetadataProvider>

<!-- eduGAIN MetadataProvider -->
<MetadataProvider backingFile="%{idp.home}/metadata/edugain-metadata.xml" id="HTTPEdugainMetadata"
maxRefreshDelay="PT2H" metadataURL="https://haka.funet.fi/edugain-nightly/gen-edugain/idp-XX-metadata-eduGain.
xml" refreshDelayFactor="0.5" xsi:type="FileBackedHTTPMetadataProvider">
  <MetadataFilter certificateFile="%{idp.home}/credentials/haka-edugain-sign.csc.fi.2021.pem" xsi:type="
SignatureValidation"/>
  <MetadataFilter xsi:type="EntityRoleWhiteList">
    <RetainedRole>md:SPSSODescriptor</RetainedRole>
  </MetadataFilter>
</MetadataProvider>
.
.
```

Esimerkki näyttää suuntaa kuinka ottaa käyttöön eduGain attribute-filter-edugain.xml -tiedoston Haka-filtterin rinnalle, mukana myös erillinen exceptions tiedosto kustomoituja sääntöjä varten:

shibboleth IdP, services.xml

```
.
.
<util:list id="shibboleth.AttributeFilterResources">
  <value>%{idp.home}/conf/attribute-filter.xml</value>
  <value>%{idp.home}/conf/attribute-filter-edugain.xml</value>
  <value>%{idp.home}/conf/attribute-filter-exceptions.xml</value>
</util:list>
.
.
```

Esimerkki eduGain filteri säännöstöstä jossa kaikille IdP:n eduGain metadatatassa löytyville entiteeteille sallitaan joukko attribuutteja jos niitä SP on ilmoittanut tarvitsevana:

shibboleth IdP, attribute-filter-edugain.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<AttributeFilterPolicyGroup id="edugain-coc-onlyifrequired" xmlns="urn:mace:shibboleth:2.0:afp" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.net
/schema/idp/shibboleth-afp.xsd">

<AttributeFilterPolicy id="releaseToCoC">

<PolicyRequirementRule xsi:type="AND">
  <Rule xsi:type="InEntityGroup" groupID="http://edugain.org/" />
</PolicyRequirementRule>

<AttributeRule attributeID="eduPersonTargetedID">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="eduPersonPrincipalName">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="eduPersonAffiliation">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="eduPersonScopedAffiliation">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="eduPersonEntitlement">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="eduPersonAssurance">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="schacHomeOrganization">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="schacHomeOrganizationType">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="mail">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="sn">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="cn">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="displayName">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="givenName">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="o">
  <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>

</AttributeFilterPolicy>
</AttributeFilterPolicyGroup>
.
.
```

eduGAINin palvelut ja IdP-palvelimen kirjautumissivu (Shibboleth)

eduGAINiin rekisteröitävän IdP-palvelimen kirjautumissivu kannattaa muokata siten, että palveluun kirjautuva loppukäyttäjä näkee ainakin palvelun nimeen (<idpui:serviceName>) ja kuvaukseen (<idpui:serviceDescription>) ja että hänellä on mahdollisuus tutustua palvelun tietosuojaselosteeseen (<idpui:servicePrivacyURL>) ennen attribuuttien luovutusta. Shibboleth IdP -ohjelmiston kirjautumissivun muokkaamista koskevat tarkemmat ohjeet löytyvät [täältä](#).

eduGAIN-kirjautumisen testaaminen

Haka IdP -palvelimen oikeanlaista konfiguraatiota ja attribuuttien luovutuksen onnistumista voi testata vaikkapa [Sveitsin SWITCHaai-luottamusverkoston testipalvelinta](#) vasten. Testipalvelin on sitoutunut GÉANT-tietosuojakäytäntöön.