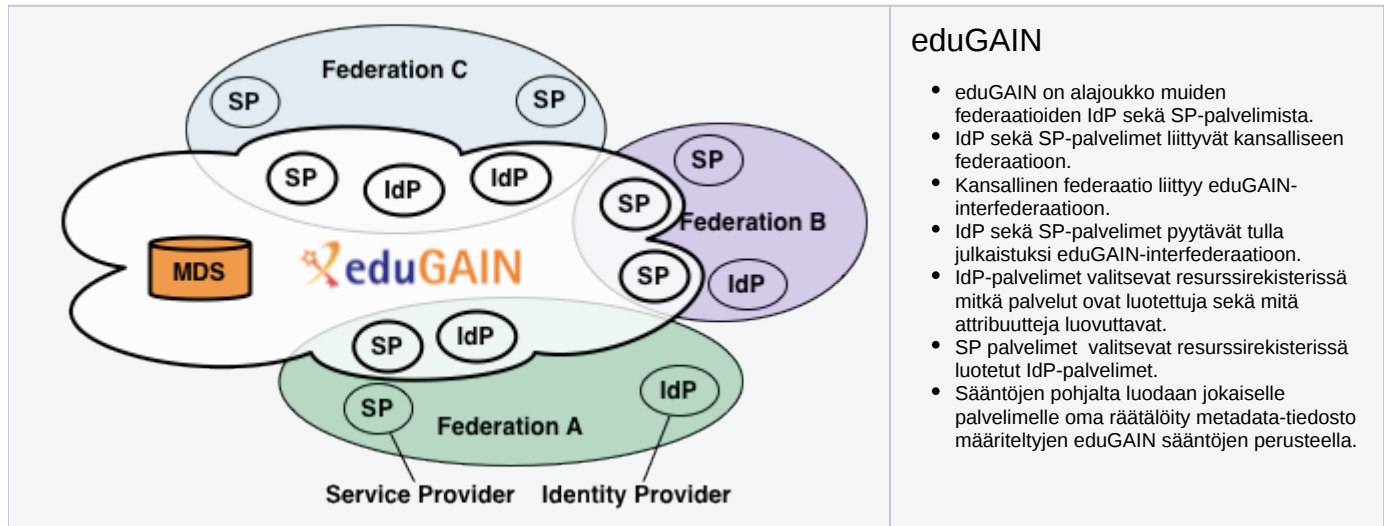


Liittyminen eduGAIN:iin

[eduGAIN-interfедераatio](#) eli luottamusverkostojen verkosto mahdollistaa luotettavan metadatan vaihdon jäsenfederaatioidensa välillä. Identity tai Service Provider tulee ensin rekisteröidä johonkin jäsenfederaatioon (kuten Hakaan), josta se voidaan ylläpitäjän pyynnöstä välittää myös eduGAIN:iin.

Alkujaan eduGAIN on eurooppalainen palvelu, mutta avoinna kaikille akateemisille federaatioille maailmassa. Tämän hetken jäsentilanteen voi tarkistaa eduGAIN:in [teknisiltä sivulta](#).



eduGAIN:n toimintakäytännöistä

eduGAIN:iin rekisteröidyt palvelimet ovat sitoutuneet kukin oman federaationsa käytänteisiin, jotka eivät ole yhteismitallisia. Lisätietoa asiasta on [eduGAIN-toimintakäytännöissä](#), jotka sitovat eduGAIN:iin liittyneitä federaatioita.

Luottosuhteen automaattisuus

- Hakassa lähtökohta on, että Haka IdP:t luottavat (luovuttavat attribuutteja) kaikkiin Haka SP:iin ja päinvastoin
- eduGAIN:ssä ei voi automaattisesti olettaa, että kaikki eduGAIN:iin rekisteröidyt IdP:t ja SP:t luottavat toisiinsa

Hakaan rekisteröidyn SP:n ylläpitäjän tulee lisäksi huomioida mm. seuraavaa

- **Kattavuus.** eduGAIN:in kautta saattaa kirjautua myös käyttäjiä, jotka eivät ole liitoksissa korkeakouluun (esim. alemmat koulutusasteet)
- **Tunnistuksen tukevuus.** eduGAIN:in kautta kirjautuvien käyttäjien tunnistuksen luotettavuus saattaa olla Hakaan heikompi. Myös ryhmätunnukset ovat mahdollisia, samoin erilaiset testitunnukset ja -palvelimet
- **Attribuutit.** Käyttäjien attribuuttien saatavuus, semantiikka ja luotettavuus saattaa olla erilainen eduGAIN:n kautta kirjautuville käyttäjille

Tietosuoja-asiat. Hakaan rekisteröidyn IdP:n ylläpitäjän tulee huomioida

- eduGAIN:iin rekisteröitynyt SP ei välttämättä ole sitoitunut yhtä kattaviin tietosuoja koskeviin pelisääntöihin kuin Hakaan rekisteröidyt (katso GÉANT-tietosuojakäytäntö)
- eduGAIN:iin rekisteröidyt SP:t eivät välttämättä ole EU/ETA-alueella, mikä tulee huomioida henkilötietoja luovutettaessa

Hakan SAML-profiiliin mukaiset IdP ja SP -palvelimet täyttävät pääosin eduGAIN:in tekniset vaatimukset. Lähinnä eroavaisuuksia on Hakan ja eduGAIN:in edellyttämän SAML 2.0 -metadatan sisällössä.

eduGAIN-käyttöönoton vaiheet

Sekä Identity että Service Provider -palvelinten eduGAIN-rekisteröintiin ja -käyttöön liittyy neljä vaihetta. Vaiheet 1-3 konfiguroidaan Haka-resurssirekisterissä:

1. Tietosuojakäytäntö (lisätietoa)

- Service Providerin ylläpitäjä päättää, haluaako hän sitoutua GÉANT-tietosuojakäytäntöön.
- Identity Providerin ylläpitäjä päättää, haluaako hän luovuttaa attribuutteja GÉANT-tietosuojakäytäntöön sitoutuneille Service Providereille.

2. Metadata export. Providerin ylläpitäjä pyytää Haka-resurssirekisterissä, että Provider välitetään eduGAIN:iin.

3. Metadata import. Providerin ylläpitäjä valitsee Haka-resurssirekisteristä, mihin eduGAIN:iin rekisteröityihin vastapuoliin hän haluaa luottaa.

- Service Provider -ylläpitäjä valitsee, minkä Identity Provider -palvelinten suorittamaan käyttäjätunnistukseen hän luottaa.
- Identity Provider -palvelinten ylläpitäjä valitsee, mihin Service Provider -palvelimiin hän haluaa luovuttaa attribuutteja.

4 Tekniset konfiguraatit.

- Identity ja Service Provider -ylläpitäjät konfiguroivat palvelimeensa lukemaan Haka-metadatan rinnalla myös eduGAIN-metadatatiedostoa, jonka Haka-resurssirekisteri räätälöi erikseen kullekin Providerille kohtien 1-3 valintojen perusteella
- Service Provider -ylläpitäjä asentaa palvelimeensa Discovery Servicen (eduGAIN:ssä ei ole Hakan tapaista keskitettyä DS-palvelintä)

Yksityiskohtaiset ohjeet IdP- ja SP-ylläpitäjille

- [Ohjeet IdP-ylläpitäjille](#)
- [Ohjeet SP-ylläpitäjille](#)