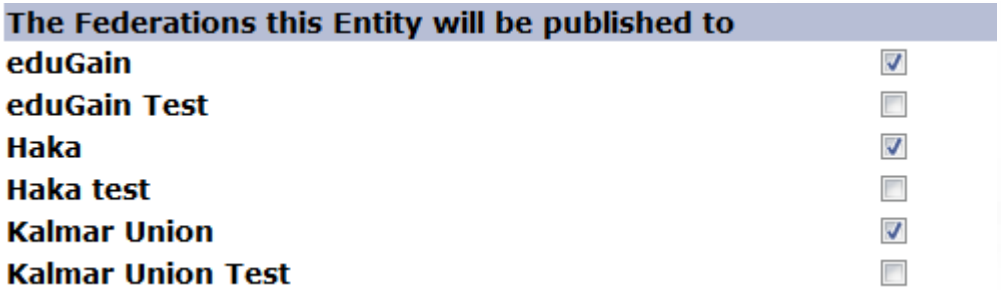
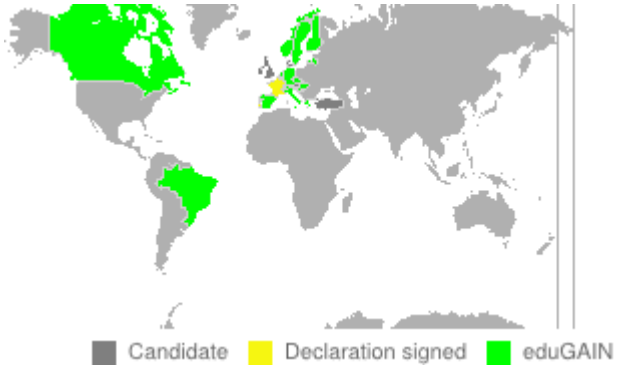
eduGAIN

Janne Lauros / CSC – Haka seminaari 14.02.2013

Haka, Kalmar, eduGain ja RR



- ”ruksi päälle ja uusi ”metadatasource”

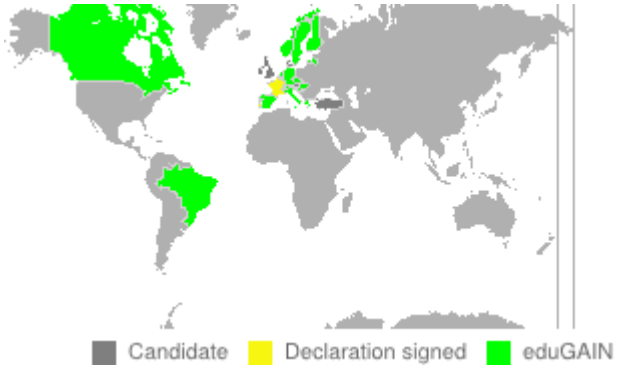


eduGAIN

PART OF THE GÉANT SERVICES PORTFOLIO

CSC

- SAML2 profiilina on SAML2int 0.2
  - Haka yhteensopiva
- Suositellut attribuutit: displayName,cn,mail,eduPerson(Scoped)Affiliation, schacHomeOrganization ja schacHomeOrganizationType
- Teknisesti kaikki ”OK”



CSC

eduGAIN

PART OF THE GÉANT SERVICES PORTFOLIO

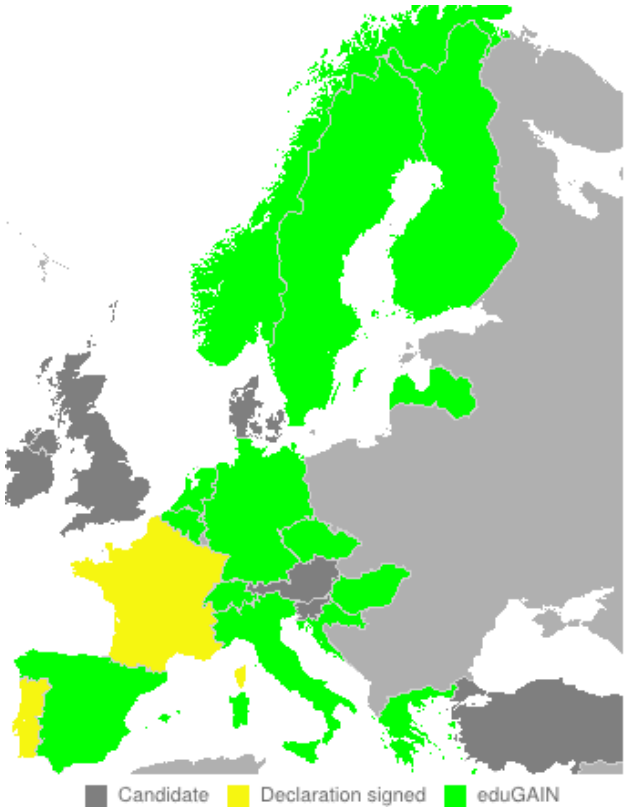
- Jokainen eduGain federaatio julkaisee käytänteensä sivulla http://www.edugain.org/federation_status.php

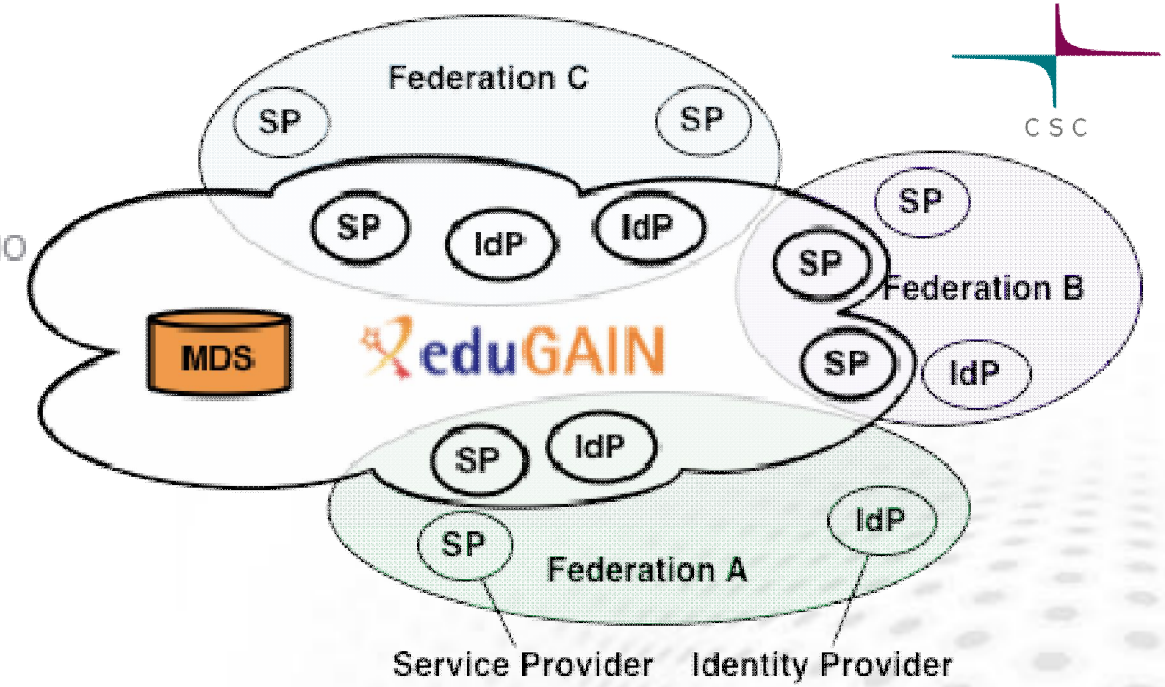
Brazil - CaFe

eduGAIN policy
see the scan
Metadata URL
https://ds.cafe.rnp.br/metadata/cafe-metadata.xml
Federation page
http://www.rnp.br/en/services/cafe.html
Contact email
operacao@cafe.rnp.br
TSG delegate
Jean Carlo Faustino
TSG deputy
Leandro Guimarães
Policy
http://www.rnp.br/_arquivo/en/CAFe_Usage_Policy_Identity_Providers.pdf
http://www.rnp.br/_arquivo/en/CAFe_Usage_Policy_Service_Providers.pdf
Supplied English version of the Policy
yes
Policy hardcopy received
yes
Registration practice statement
http://www.rnp.br/en/services/joincafe.html

eduGAIN

PART OF THE GÉANT SERVICES PORTFOLIO





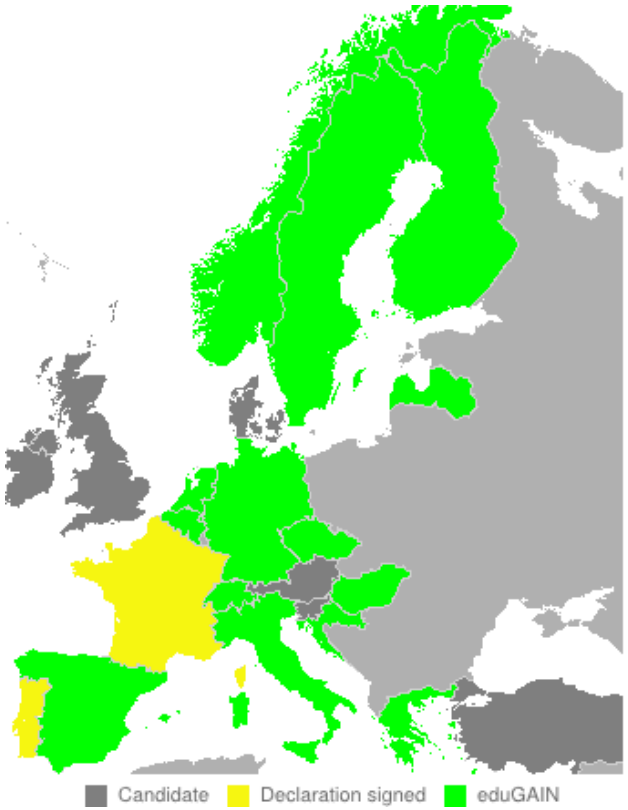
CSC

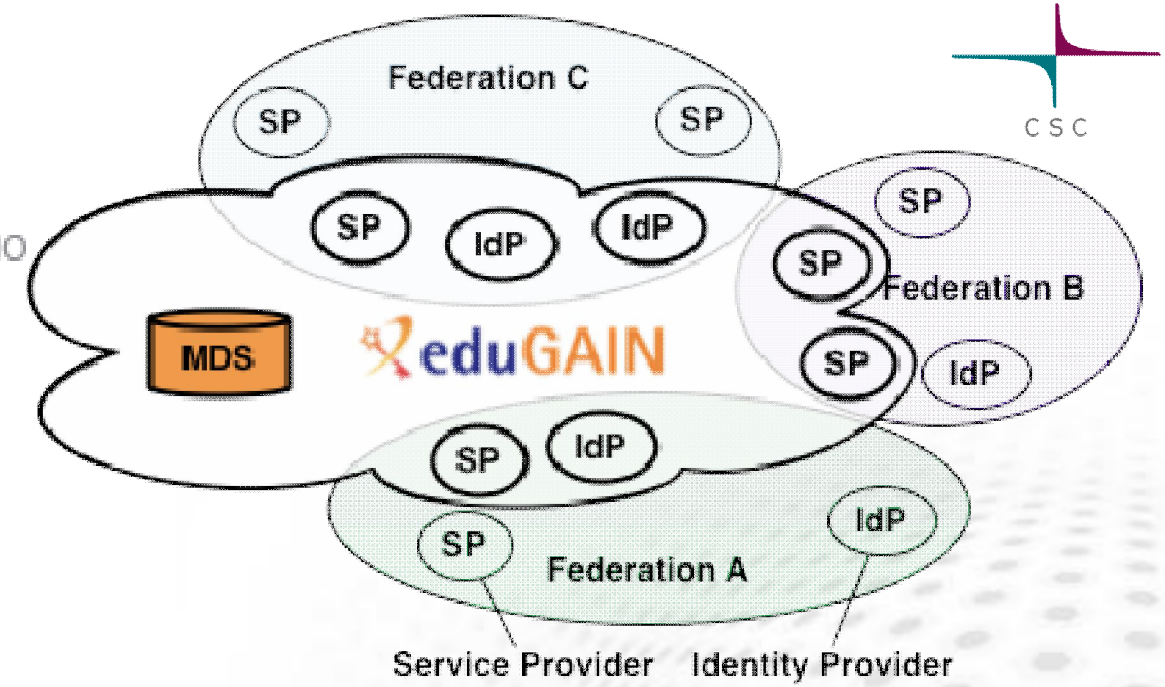
Federaatiot julkaisevat upstreamin

eduGain aggregaatti validoi ja yhdistää upstreamit yhdeksi isoksi köntiksi, http://mds.edugain.org

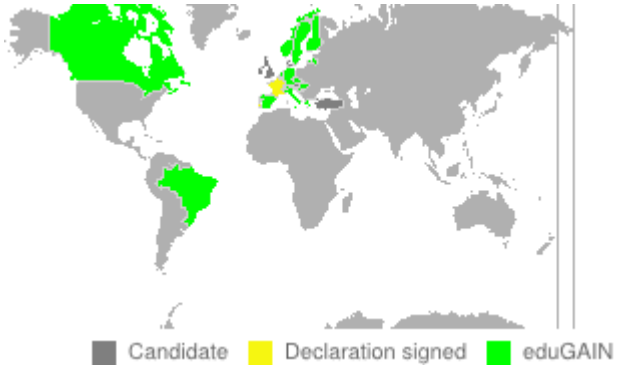
eduGAIN

PART OF THE GÉANT SERVICES PORTFOLIO





- Federaatoiden operaattorit siivoavat edugain köntin
  - Federaatio tasolle tai
  - Entity tasolle
- Federaatiot julkaisevat oman versionsa eduGain metadatasta



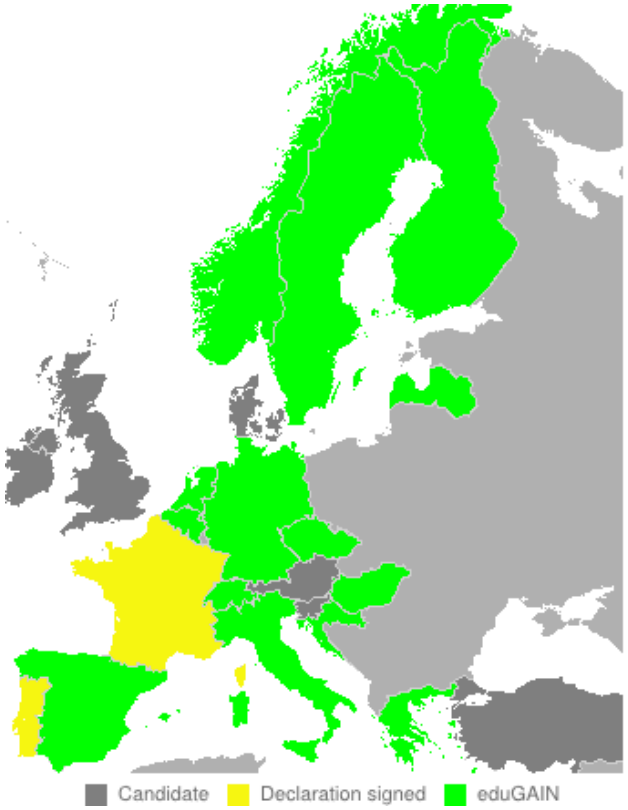
eduGAIN

PART OF THE GÉANT SERVICES PORTFOLIO

CSC

- Haka + Kalmar + eduGain.. Metadata kontrollista tulee haastava.
- Yksi yksittäinen entity voi tulla useammastakin lähteestä mikä vähintäänkin on ei-suositeltavaa
- Useamman lähteen ongelma ratkaistu vain osittain Hakassa

eduGain Haka metadata



Voit luoda säännöstön kehen luottaa eduGainissa

Voit luoda IdP:lle säännöstön mitä attribuutteja luovuttaa eduGainissa

Kontrolloidaan entity kohtaisilla metadata ja afp julkaisuilla

eduGain / Haka RR / Kehen luottaa

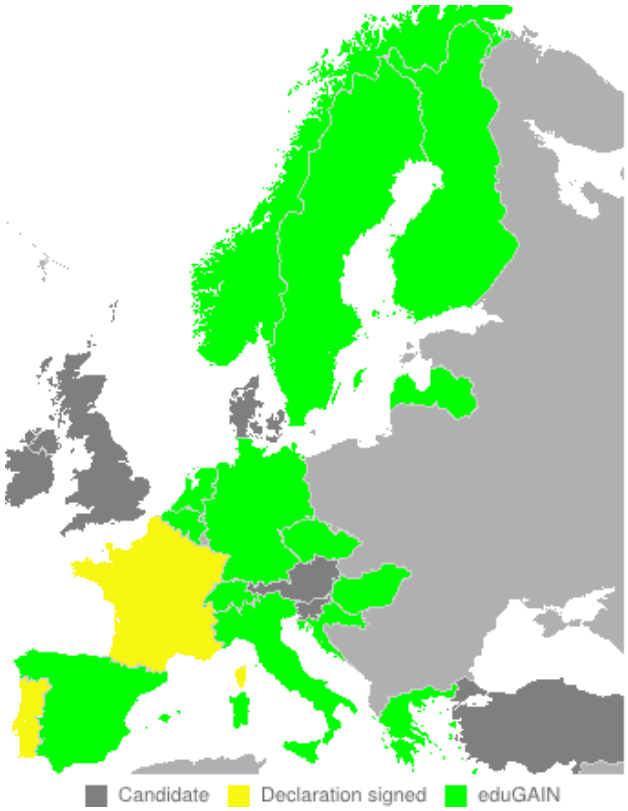
eduGain SPs this IdP trusts

eduGain trust rules for this Identity Provider.

Trust Rule #0

eduGain | All | trusted

apply trust rules



- ”Luotan kaikkiin eduGain entityihin”

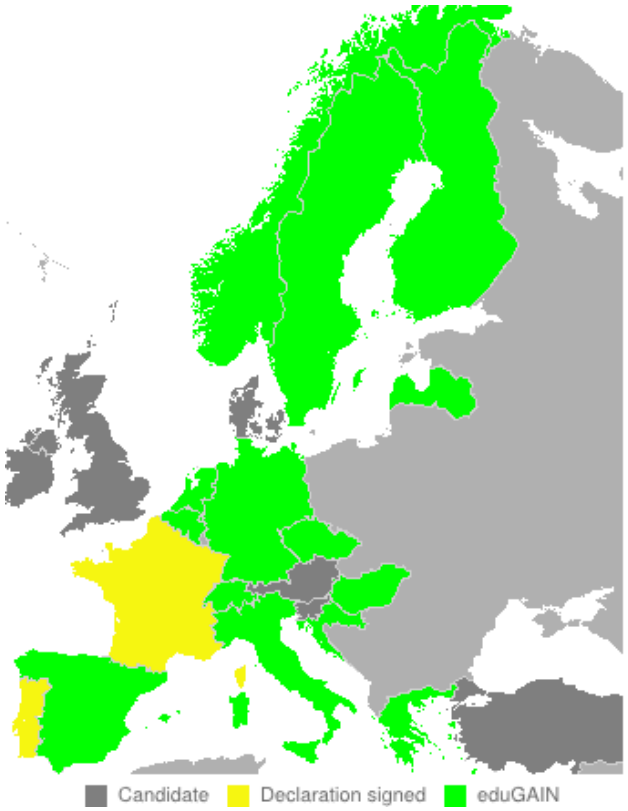
eduGain / Haka RR / Kehen luottaa

eduGain SPs this IdP trusts

eduGain trust rules for this Identity Provider.

Trust Rule #0	eduGain	All	non-trusted
Trust Rule #1	http://feide.no/	All	trusted
Trust Rule #2	http://www.swamid.se/	All	trusted

apply trust rules



”Luotan ainoastaan Norjan ja Ruotsin federaatioiden entityihin”

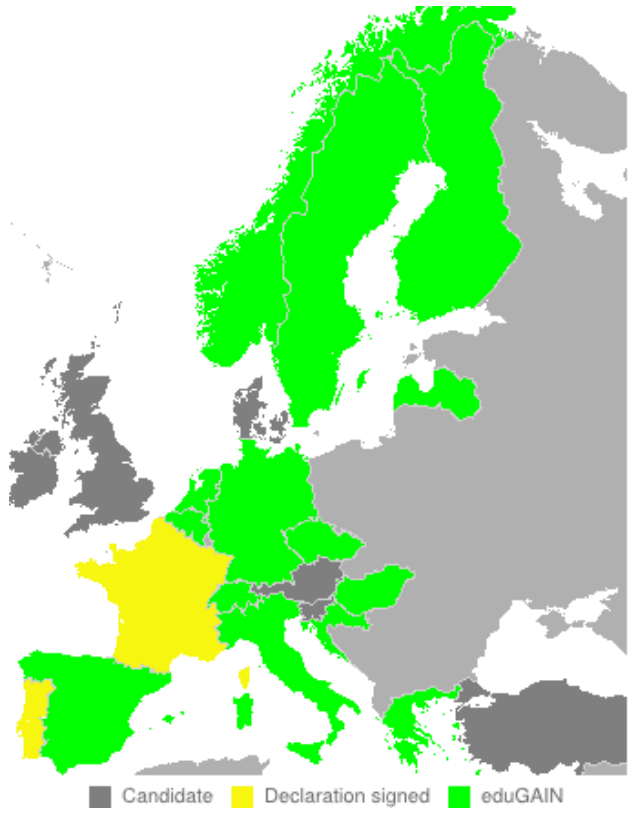
eduGain / Haka RR / Kehen luottaa

eduGain SPs this IdP trusts

eduGain trust rules for this Identity Provider.

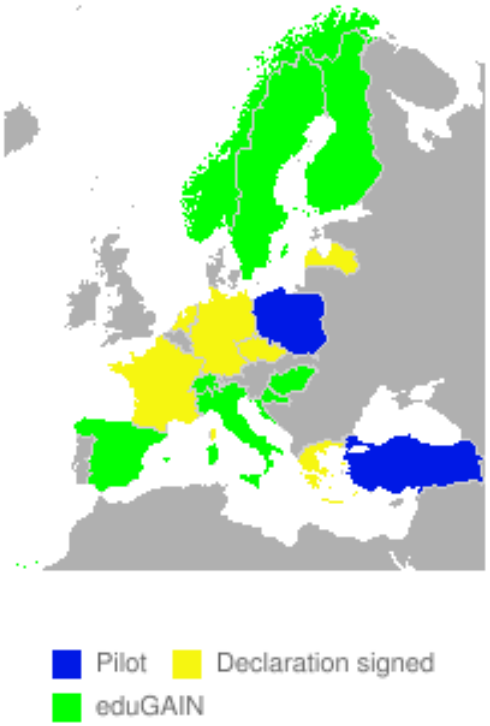
Trust Rule #0	eduGain	All	trusted	
Trust Rule #1	Homeless	All		non-trusted
Trust Rule #2	Homeless	https://terena.org/sp		trusted

apply trust rules



”Luotan kaikkiin eduGain entityihin paitsi niihin joille ei ole merkitty kotifederaatiota. Niiden joukossa teen poikkeuksen ja luotan https://terena.org/sp entityyn”

eduGain / Haka RR / Attribuutti säännöt

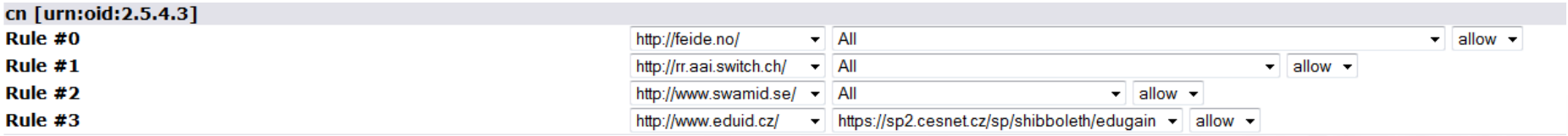


- Luottamussuhteen lisäksi IdP voi määritellä säännöt luovutettaville attribuuteille.
- Attribuuttisäännöt ovat hierarkiset samoin kuin luottamussäännöt: eduGain taso, Federaatio taso ja Entity taso.
- Attribuuttisäännöt tehdään per attribuutti.

eduGain / Haka RR / Attribuutti säännöt

- Kaikki IdP:n populoimat attribuutit listattuna
- ”Luovuta attribuutti pyydettäessä kenelle tahansa”
- ”Haka malli”

eduGain / Haka RR / Attribuutti säännöt



- ”Luovuta attribuutti *cn* pyydettäessä kaikille Norjan, Sveitsin ja Ruotsin federaatioiden jäsenille. Näiden lisäksi attribuutin *cn* saa lähettää Tsekin federaation jäsenelle https://sp2.cesnet.cz/sp/shibboleth/edugain.”
- IdP:n ylläpitä tekee ikään kuin statementin että hän luottaa kyseisten kolmen federaation policyjen olevan riittävällä tasolla.

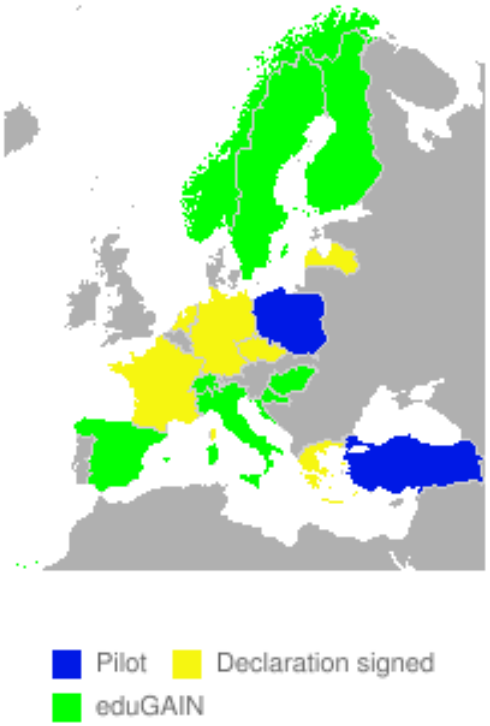
eduGain / Haka RR / SP View

Entity	Authority	Trusted	Explanation
https://forge.switch.ch/shibboleth	http://rr.aai.switch.ch/	Trusted	There is a entity level rule to trust

Requested attribute	Release	Explanation
mail [urn:oid:0.9.2342.19200300.100.1.3]	Released	There is a authority level rule to allow relase of the attribute.
sn [urn:oid:2.5.4.4]	Released	There is a eduGain level rule to allow relase of the attribute.
givenName [urn:oid:2.5.4.42]	Not Released	There is no release rule for the attribute. Your IdP does not list attribute as supported.

- Näkymä yksittäisen eduGain SP:n tilanteesta suhteessa määriteltyihin sääntöihin
- IdP Luottaa SP:hen, spesifisti ’entity tasolla’.
- Attribuuttien *mail* lähetetään koska SP kuuluu Sveitsin federaation.
- Attribuutti *sn* lähetetään koska SP on eduGainissa.
- Attribuuttia *givenName* ei lähetetä koska sitä koskevaa sääntöä ei löydy. Attribuutti ei ole myöskään IdP:n ilmoitetussa ’repertuaarissa’.

CoC



- Toivoa on.. Mikael Linden on mukana työstämässä lisäyksiä eduGain käytänteisiin.
- SP:t voivat ilmoittaa noudattavansa tiettyjä yhteisiä tietosuojakäytänteitä.