

eduGAIN OID Federation Pilot

Niels van Dijk (SURF), Davide Vaghetti (GARR)

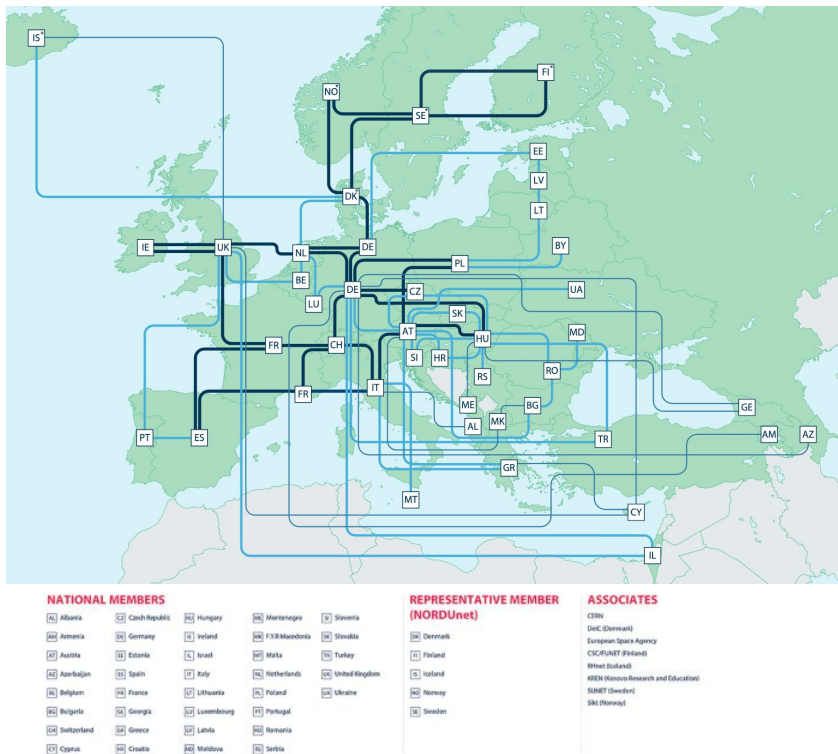
FIM4R - December 8, 2024

Public (PU)

Membership Association

GÉANT Association supports and represents 38 NRENs and NORDUnet across Europe.

Together they support over 10,000 institutions and 50 million academic users.



Trust and Identity in GEANT

Services, Standards & Community



EnCo



(EUDI) Wallet in global R&E

2003

2010

2017

2018

2020

2022

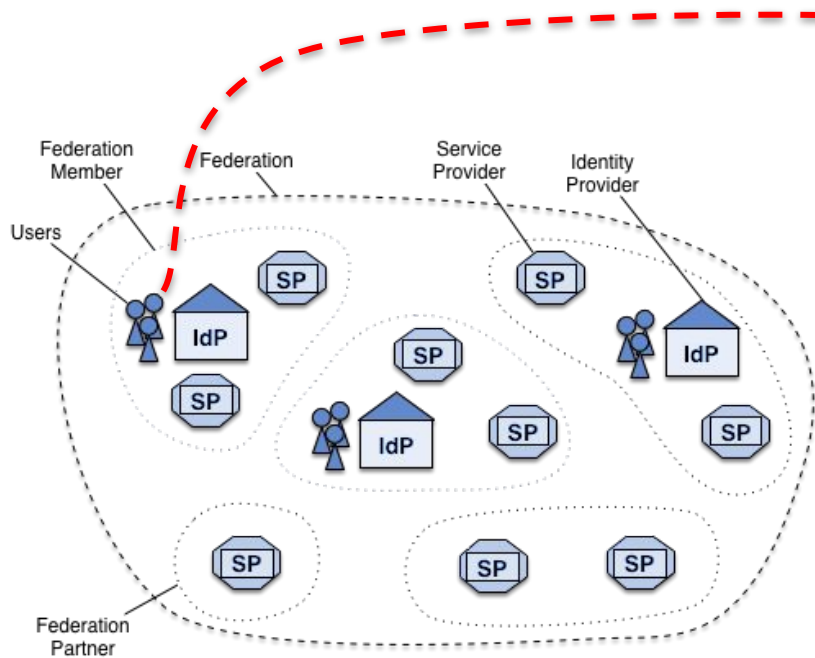
2024

TRUST & IDENTITY
INCUBATOR

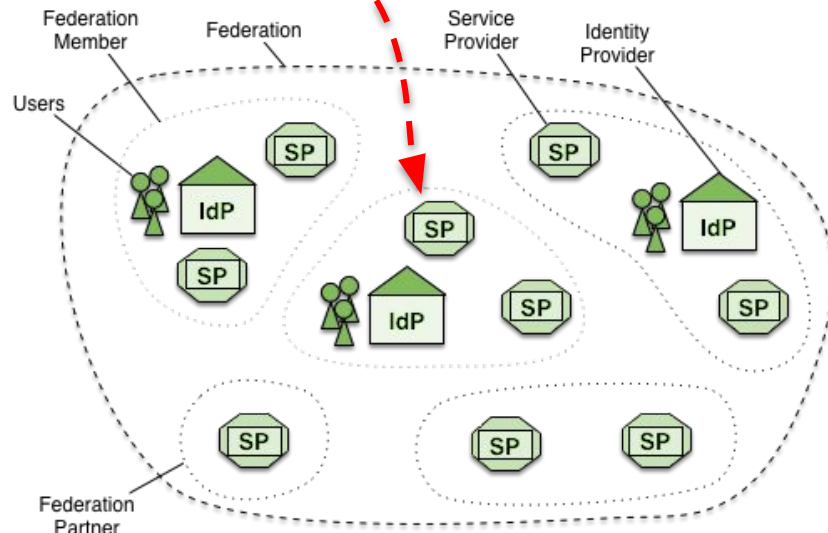


*“eduGAIN **interfederation service** connects identity federations around the world, simplifying **access** to content, services and resources for the **global** research and education community”*

Inter-federated Access

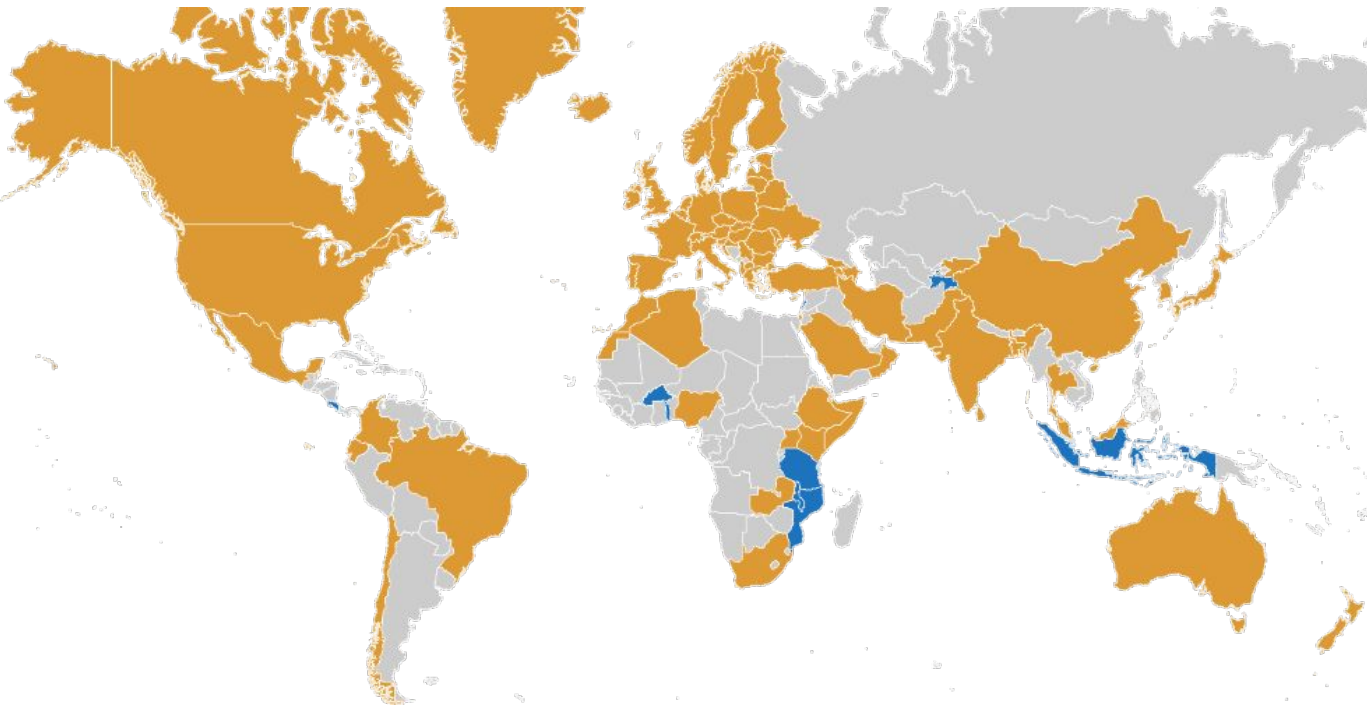


Federation Blue



Federation Green

eduGAIN Global Coverage



78 Federations

9552 Entities

5775 Identity Providers

3795 Service Providers

Last update November 26th 2024

What do we use it for?

Elsevier Clinical Skills

Sign in to Elsevier Clinical Skills

Find your institution

Examples: Science Academy, sue@uni.ac.uk, London.



National Institutes of Health
(NIH)



Lawrence Berkeley National
Laboratory



National Distance Education
University



National Library of Spain



National Agency for Quality
Assessment and Accreditation of
Spain



eduID.hu Virtual Home (VHO)



National University Hospital of
Iceland



rometer Gravitational-Wave Observatory, **LIGO**, comprises more than 1,500 scientists, all of whom
ards a single goal: to capture signs of gravitational waves and decode their meaning. The data
ns at massive observatories in the USA and Italy, but the analysis is done in countries all over the



thentication, Authorisation and Identification (AAI) technologies and the expansion of
etween organisations and identity federations using eduGAIN has allowed these rapid collaborations to take place by allowing
se their existing institutional identities to access data on remote systems and securely share results.

om 11 participating countries and around 3,000
d from mobility under Erasmus by 2017. The
n Commission under the **European Student Card**
ically at higher education institutions within the EU
nd paperwork". Under this initiative Erasmus
for student mobility exchange.

emicID project (co-funded by Connecting Europe
ne the specifications of the eID scheme, including
l the functioning of the Service Provider (SP) Proxy

Erasmus Student M

In the last years the Era
students in 1987, to 33
procedures in place ho
Initiative aims to "enabl
when moving abroad for
Without Paper project v

Since 2019, GÉANT with
Facilities, INEA/CEF/ICT
the bridges between ell
that will connect key ele

eduGAIN provides

- A **governance model** and body for global collaboration between the national federations
- A **policy** for participating federations and entities
- A **technical infrastructure** which publishes metadata
- **Tools** to view, test and validate participants
- **Specifications** for global interoperability,
 - specifically a **SAML profile**

eduGAIN provides

- A **governance model** and body for global collaboration between the national federations
- A **policy** for participating federations and entities
- A **technical infrastructure** which publishes metadata
- **Tools** to view, test and validate participants
- **Specifications** for global interoperability,
 - specifically a **SAML profile**

**A trust layer for cross border access
to R&E resources**

eduGAIN Technological Profiles: SAML 2.0

An open standard

Extremely successful and adopted

87 R&E Federations + eduGAIN

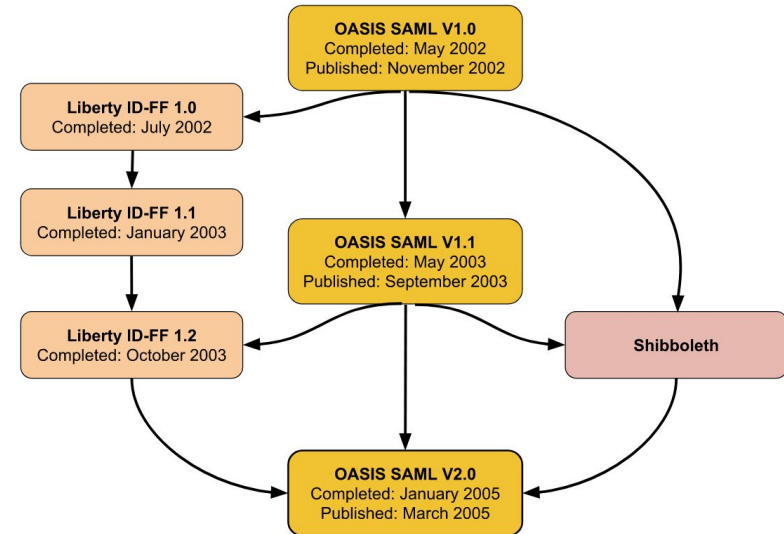
Legacy Protocol: no new devs in the last 5 years

No support for Mobile App, REST/API flows, etc.

Decentralized identity and Verifiable Credentials?

Post-quantum cryptography support?

A History of the Security Assertion Markup Language



eduGAIN OpenID Federation Pilot Overview



WHY

- SAML is a legacy protocol
- Mobile clients
- Post-quantum cryptography
- Verifiable credentials and DID
- etc, etc



HOW

- OpenID Fed set up kit based on T&I Incubator tools
- **DRAFT** eduGAIN OpenID Federation Technological Profile



WHO

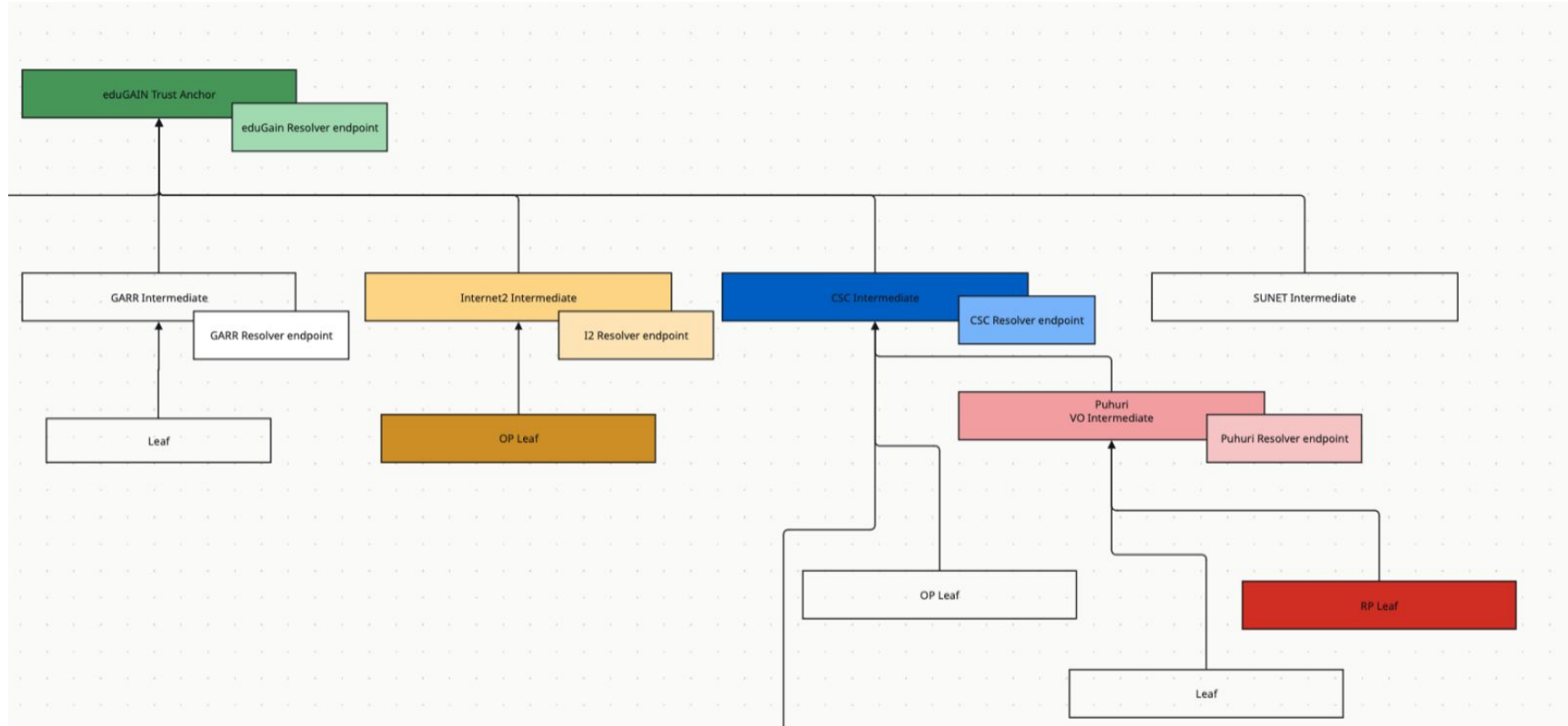
- eduGAIN service and T&I Incubator
- Federation Operators
- Research Community AAls
- Any other interested stakeholder



WHEN

- As soon as the dev work is done (end 2024)
- 12 Months

eduGAIN OpenID Federation Trust model



The eduGAIN OpenID Connect Profile - work in progress



TRUST is based on trust chains with eduGAIN as Trust Anchor, Federations as Intermediates and Entities as Leaves

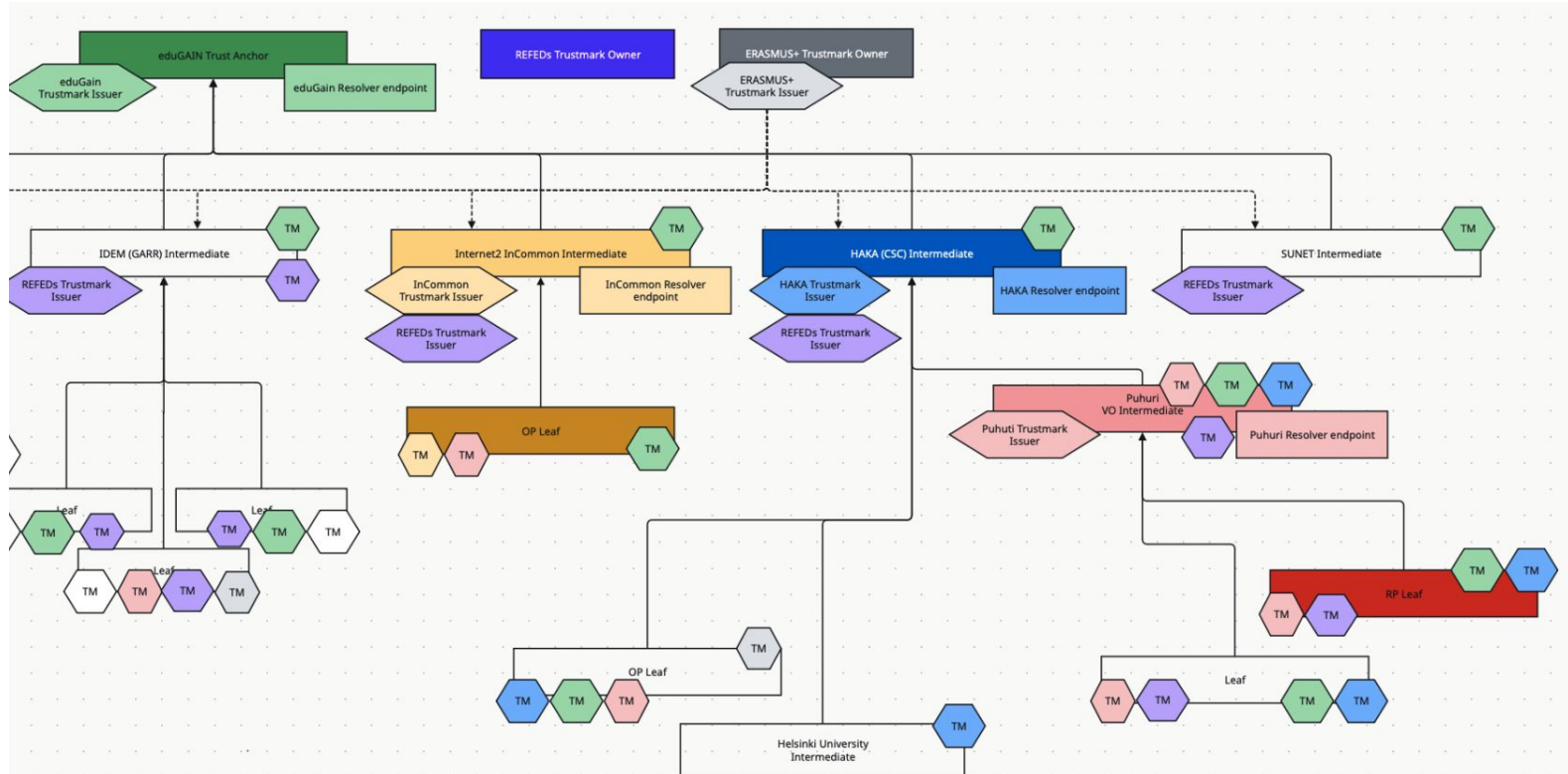


ENTITY VALIDATION is based the eduGAIN Trust Mark. **Only validated entities can be part of trust chains with eduGAIN as Trust Anchor**

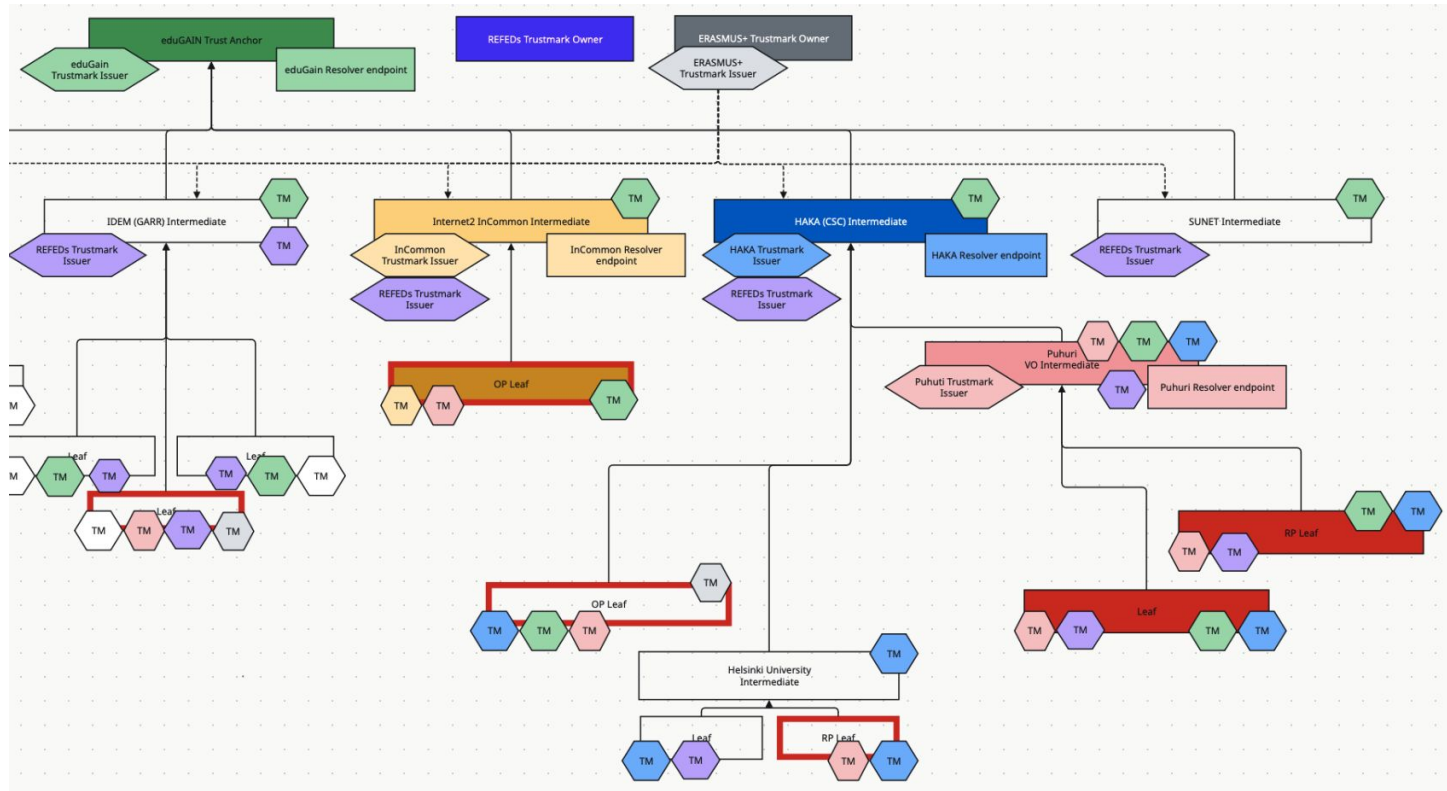


ENTITY RESOLUTION is provided by a resolver endpoint at federation and inter-federation level that provides metadata about entities

Trust hierarchy 'remix' using Trustmarks



Trust hierarchy 'remix' using Trustmarks



Benefits for using OID Fed in eduGAIN

- A route to start moving away from SAML, while retaining multilateral federation
- Simplify federation management due to increased automation
- **End to end trust**
- More **transparent trust**, specifically wrt proxies
- One **unique trust infrastructure** that may support SAML, OIDC and Wallets

Some of our software projects

- OFcli - command line tool for inspecting OID Federation topology, entities, evaluate trust chains and trust marks - <https://github.com/dianagudu/ofcli>
- OID Fed library for GO - <https://github.com/zachmann/go-oidfed>
OID Fed RP in Go - <https://github.com/zachmann/go-oidfed/tree/master/examples/rp>
- OpenID Federation into SimpleSAMLphp - <https://github.com/simplesamlphp/openid>
- Started with an implementation for Shibboleth OP - <https://git.shibboleth.net/view/?p=java-idp-oidc.git;a=summary> (dev/JOIDC-222 branch, still heavy in development!)

Shibboleth IdP OIDC OP plugin - OIDfed support

- The development branch 'dev/JOIDC-222' in <https://git.shibboleth.net/git/java-idp-oidc> is used for the OIDfed feature
- The plugin already exploits Nimbus OAuth2/OIDC SDK for standard OP/AS functionality
- The approach is to exploit it for the OIDfed as well, but in a way that it integrates to the existing Shibboleth building blocks (metadata caching, security configuration, etc)
- First implemented (proof of concept) features:
 - Entity configuration endpoint
 - Metadata caches for:
 - entity configurations (keyed with subject entity ID)
 - subordinate statements (keyed with issuer and subject entity IDs)
 - trust chains (list of trust chains keyed with subject entity ID)
- Automatic registration in the authorization endpoint
- Upcoming features (current/next work items):
 - Trust mark support in registration limiting and e.g. in the attribute filtering engine
 - Explicit registration (fairly simple as the plugin already supports standard OIDC dynamic client registration)
 - Automatic registration in the PAR endpoint

Shibboleth IdP OIDC OP plugin - OIDfed support - Demo

SimpleSAMLphp Module OIDC

<https://github.com/simplesamlphp/simplesamlphp-module-oidc>

- OpenID Federation capabilities are being introduced for v6 of the module which is WIP:
<https://github.com/simplesamlphp/simplesamlphp-module-oidc/tree/wip-version-6>
- Automatic client registration is implemented
 - new federation endpoints for issuing configuration entity statement and subordinate statements
 - new properties for clients
 - new capabilities like support for request objects on authorization endpoint, support for `private_key_jwt` client authentication method at token endpoint...
- WIP federation participation (limiting) based on Trust Marks
- Underlying library <https://github.com/simplesamlphp/openid> introduced, with capabilities like:
 - trust chain resolving
 - metadata (policy) resolving
 - abstractions and factories for entity statements, trust chains, trust marks ...
 - http fetchers for entity statements, jwks ...
 - optional built-in caching
- Authentication can be tested on <https://gorp.testbed.oidcfed.incubator.geant.org/> RP, by selecting "https://maiv1.incubator.geant.org" OP (u: testuser, p: testpass).

SimpleSAMLphp Module OIDC - Demo



Thank You

Niels van Dijk, niels.vandijk@surf.nl

Davide Vagheti, davide.vagheti@garr.it

www.geant.org



Co-funded by
the European Union