eduGAIN OpenID Federation POC

Davide Vaghetti (GARR)

eduGAIN Service Owner

FIM4R Copenhagen January 2024

www.geant.org

A new identity federations standard - TL;DR

R&E Identity Federations and **eduGAIN** are based on **SAML 2.0.**

Industry, Web and Cloud services are based on **OAuth 2.0** and **OpenID Connect 1.0.**

The **OpenID Federation** specification is an holistic attempt to define modern federations targeting **OAuth 2.0** and **OpenID Connect 1.0,** but in principle open to any group of entities with trust relationships and a common set of rules.

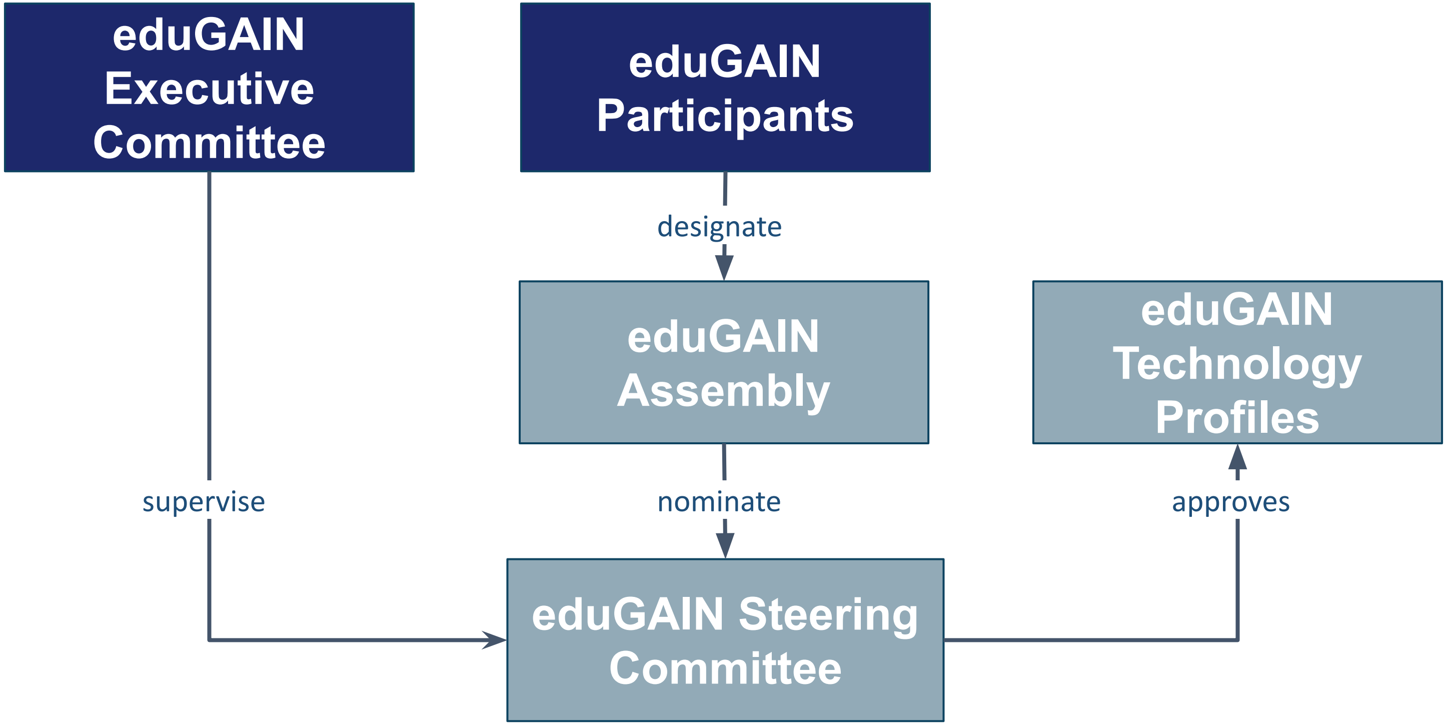
The eduGAIN Service started a Proof of Concept activity to develop tools to build OpenID Federations and define a R&E implementation profile for NRENs and Research Collaborations.

In **Q2 2024** we will start an eduGAIN OpenID Federation pilot.

OpenID Federation is also currently being tested as one of the trust framework for the EUID Wallet.

eduGAIN Many Contributors

eduGAIN Governance and Tech Profiles


eduGAIN Executive Committee
eduGAIN Participants
designate
eduGAIN Assembly
eduGAIN Technology Profiles
supervise
nominate
approves
eduGAIN Steering Committee

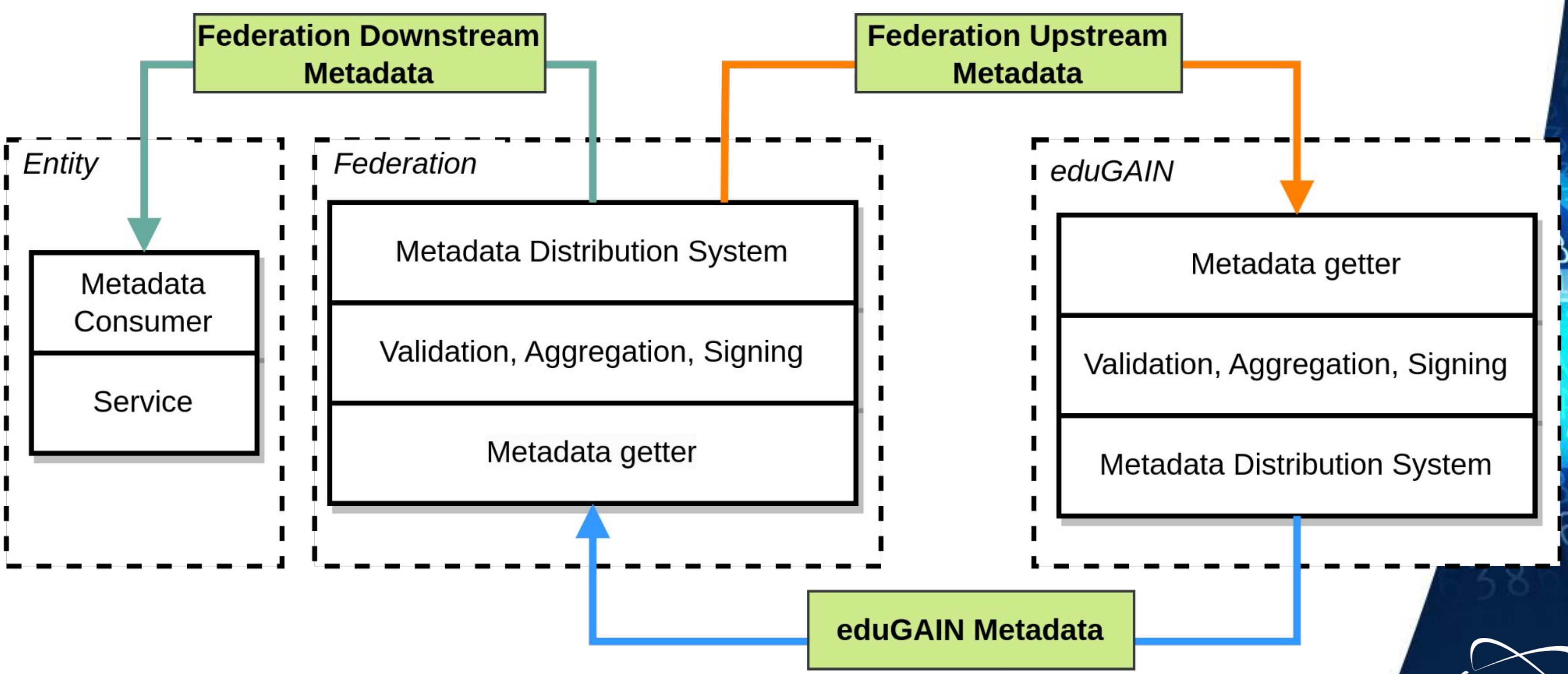
ref https://technical.edugain.org/documents

eduGAIN SAML Profile

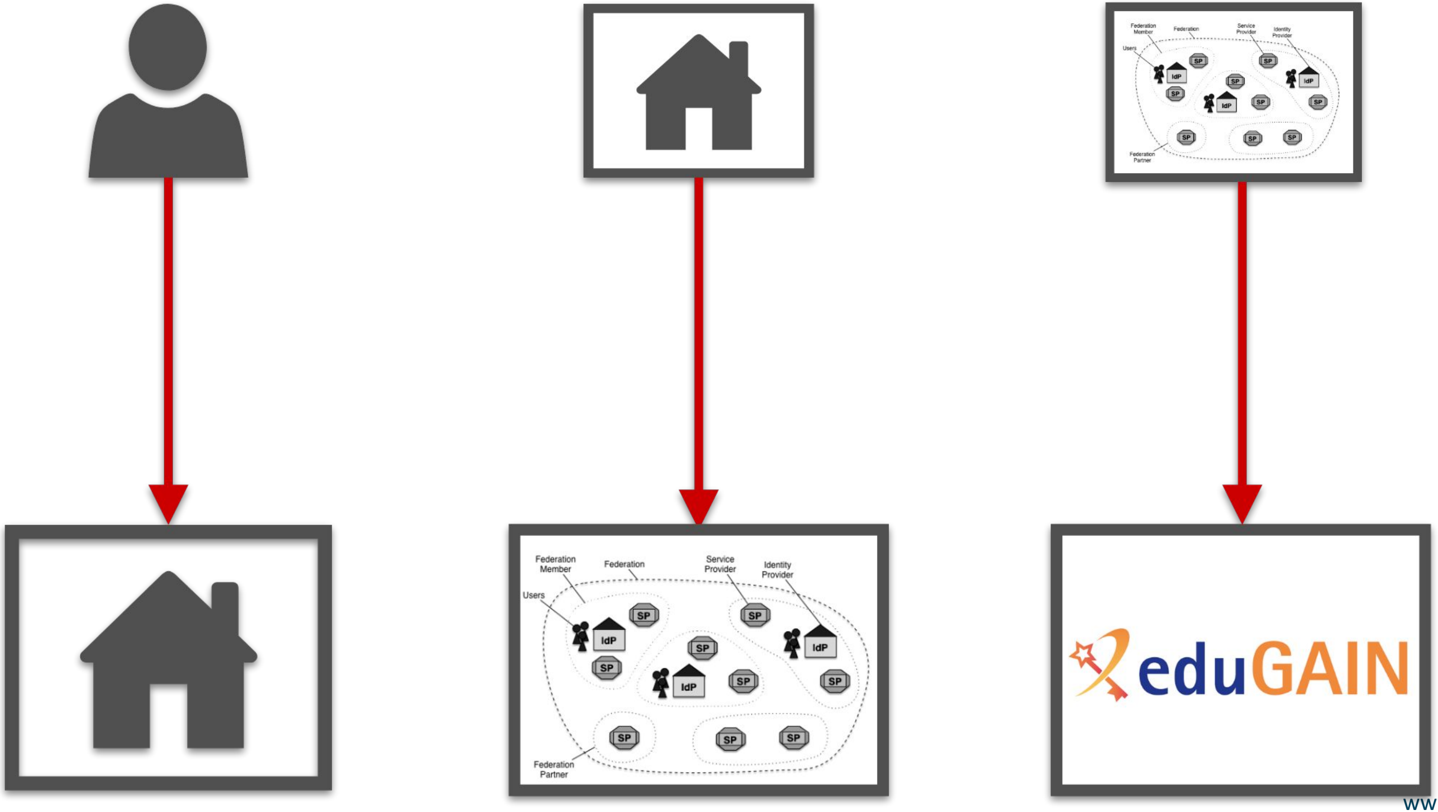
Policy requirements	Metadata Registration Practice Statement
Metadata Requirements	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0, SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0
Metadata Signing	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, SAML V2.0 Metadata Interoperability Profile Version 1.0
Metadata Publication	*Federations MUST provide their members with trustworthy SAML Metadata about eduGAIN Entities, signed with their own signing key [..]*
Participant requirements	*Produce and register a URL to the (participant) SAML Metadata export* *Register a signing certificate and an* `mdrpi:registrationAuthority`

ref https://technical.edugain.org/documents

eduGAIN SAML Metadata Creation and Distribution


Federation Downstream Metadata
Federation Upstream Metadata
Entity
Metadata Consumer
Service
Federation
Metadata Distribution System
Validation, Aggregation, Signing
Metadata getter
eduGAIN
Metadata getter
Validation, Aggregation, Signing
Metadata Distribution System
eduGAIN Metadata

eduGAIN Trust Flow

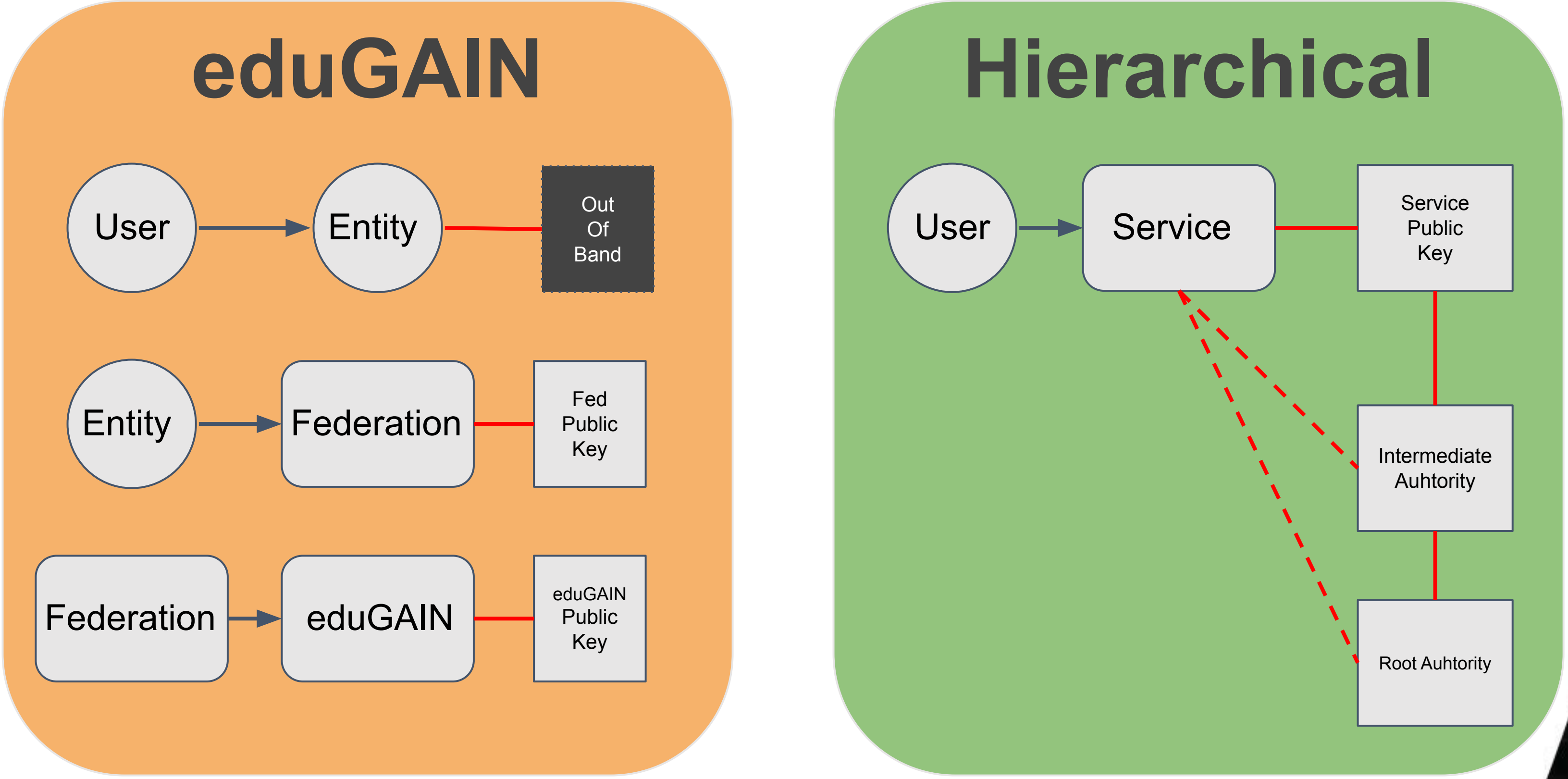


Users trust Home Organisation

HomeOrgs trust Federations

Federations trust eduGAIN

eduGAIN vs Hierarchical Trust Flow



www.geant.org

OpenID Federation

OpenID® *An OpenID Foundation specification*

- Implementer Draft 32 of version 1.0 (published on Dec 4th)
- A very comprehensive spec, more than 100 pages of flows, claims, endpoints, etc
- Reference implementations:python, java, golang, php
- Production implementations: Italian eGOV-ID (SPID/CIE)

ref https://openid.net/specs/openid-federation-1_0.html

R&E

OpenID Federation Authors

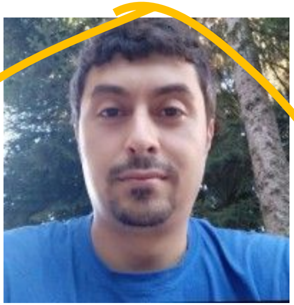
R. Hedberg,
Editor
independent

M.B. Jones
Self-Issued Consulting

A.Å. Solberg
Sikt

John Bradley

Yubico



G. De Marco
independent

V. Dzhuvinov
Connect2id

New and noteworthy

★ Native dynamic metadata publication and distribution.

★ Dynamic Relying Parties registration.

★ Federation transparency.

★ Federation intermediaries.

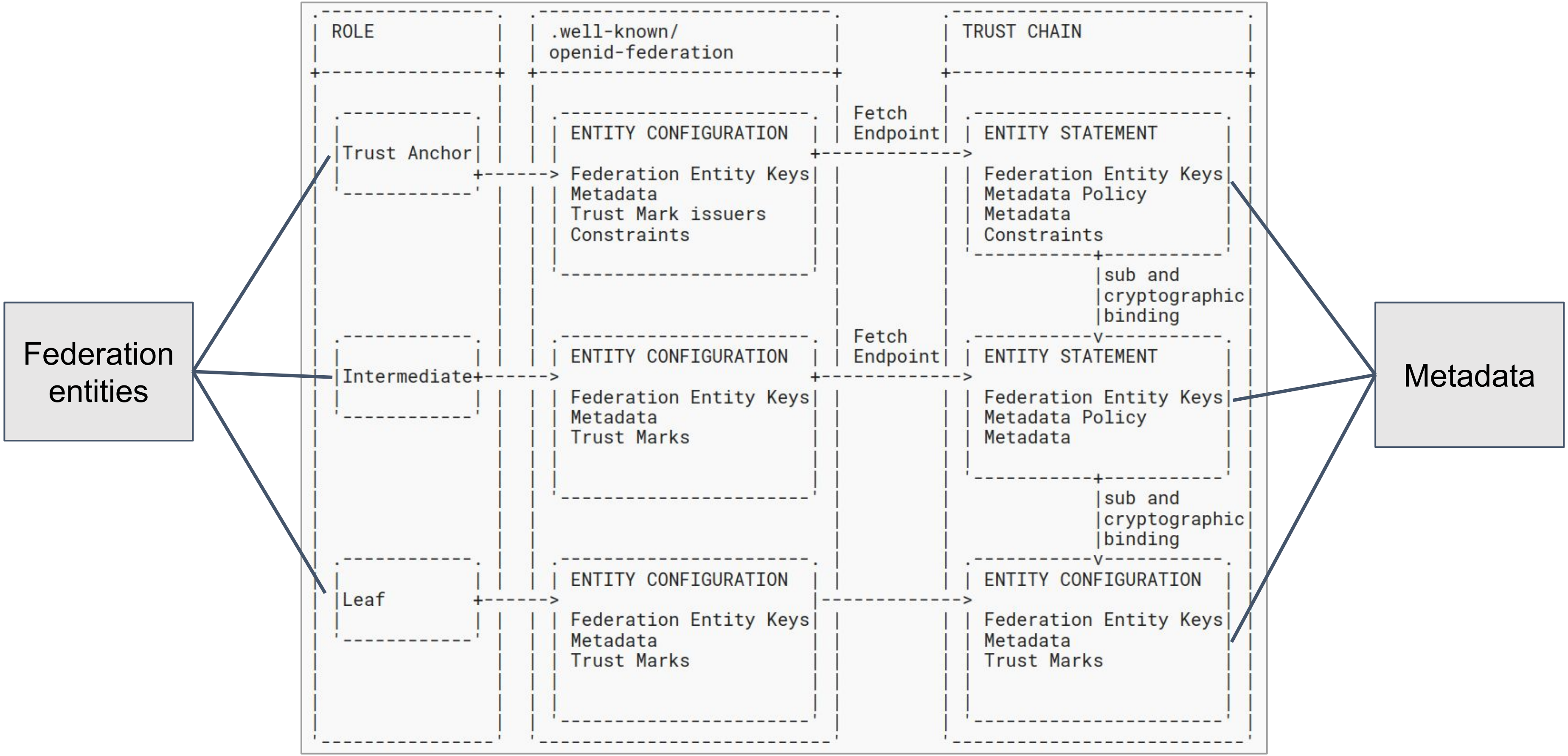
★ Inband metadata policy engine.

Lingo

Entity Statement	A signed JWT that contains the information needed for an Entity to participate in federation(s), including metadata about itself and policies that apply to other Entities that it is authoritative for.
Entity Configuration	An Entity Statement issued by an Entity about itself. It contains the Entity's signing keys and further data used to control the Trust Chain resolution process, such as authority hints.
Trust Anchor	An Entity that represents a trusted third party.
Intermediate (Entity)	An Entity that issues an Entity Statement appearing somewhere in between those issued by the Trust Anchor and the Leaf Entity in a Trust Chain
Leaf Entity	An Entity with no Subordinate Entities. Leaf Entities typically play a protocol role, such as an OpenID Connect Relying Party or OpenID Provider.
Trust Chain	A sequence of Entity Statements that represents a chain starting at a Leaf Entity and ending in a Trust Anchor.
Trust Mark	Statement of conformance to a well-scoped set of trust and/or interoperability requirements as determined by an accreditation authority.

Ref https://openid.net/specs/openid-federation-1_0.html#name-terminology

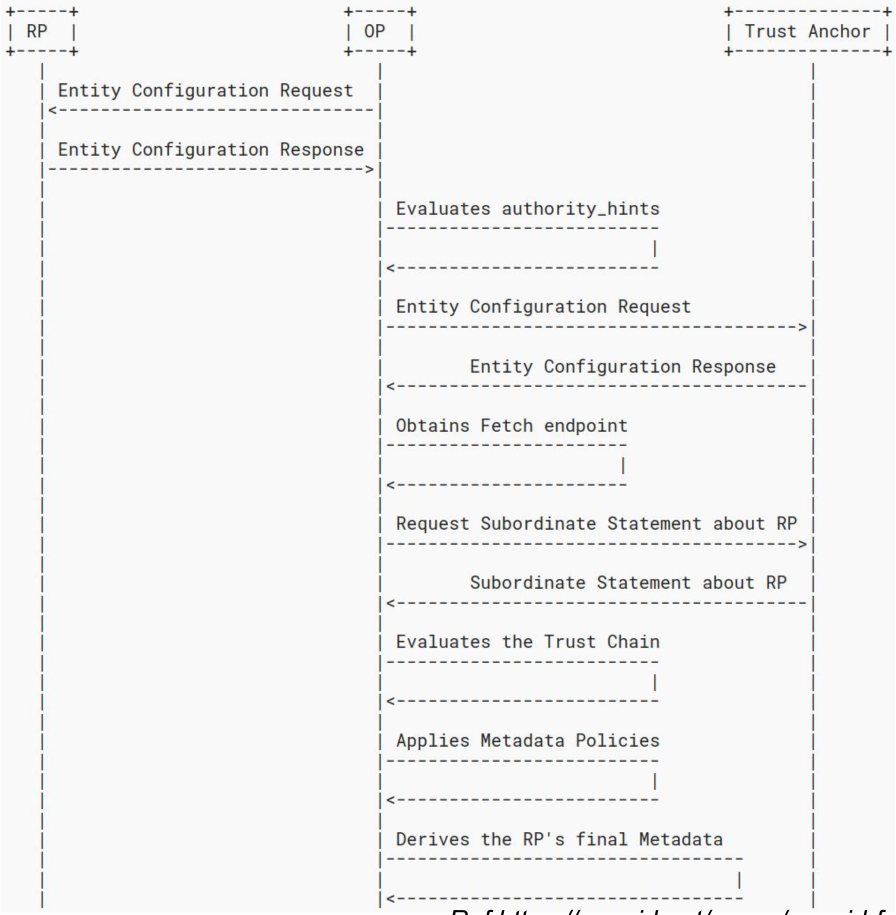
Trust Chain



```
.----------------.  .---------------------------.         .---------------------------.
| ROLE           |  | .well-known/              |         | TRUST CHAIN               |
|                |  | openid-federation         |         |                           |
+----------------+  +---------------------------+         +---------------------------+
|                |  |                           |         |                           |
| .------------. |  | .-----------------------. | Fetch   | .-----------------------. |
| |            | |  | | ENTITY CONFIGURATION  | | Endpoint| | ENTITY STATEMENT      | |
| |Trust Anchor| |  | |                       +-------------->                       | |
| |            +------> Federation Entity Keys| |         | | Federation Entity Keys| |
| '------------' |  | | Metadata              | |         | | Metadata Policy       | |
|                |  | | Trust Mark issuers    | |         | | Metadata              | |
|                |  | | Constraints           | |         | | Constraints           | |
|                |  | |                       | |         | '-----------+-----------' |
|                |  | '-----------------------' |         |             |sub and      |
|                |  |                           |         |             |cryptographic|
|                |  |                           |         |             |binding      |
| .------------. |  | .-----------------------. | Fetch   | .-----------v-----------. |
| |            | |  | | ENTITY CONFIGURATION  | | Endpoint| | ENTITY STATEMENT      | |
| |Intermediate+------>                       +-------------->                       | |
| |            | |  | | Federation Entity Keys| |         | | Federation Entity Keys| |
| '------------' |  | | Metadata              | |         | | Metadata Policy       | |
|                |  | | Trust Marks           | |         | | Metadata              | |
|                |  | |                       | |         | |                       | |
|                |  | |                       | |         | '-----------+-----------' |
|                |  | '-----------------------' |         |             |sub and      |
|                |  |                           |         |             |cryptographic|
|                |  |                           |         |             |binding      |
| .------------. |  | .-----------------------. |         | .-----------v-----------. |
| |            | |  | | ENTITY CONFIGURATION  | |         | | ENTITY CONFIGURATION  | |
| |Leaf        +------>                       |-------------->                       | |
| |            | |  | | Federation Entity Keys| |         | | Federation Entity Keys| |
| '------------' |  | | Metadata              | |         | | Metadata              | |
|                |  | | Trust Marks           | |         | | Trust Marks           | |
|                |  | |                       | |         | |                       | |
|                |  | |                       | |         | |                       | |
|                |  | '-----------------------' |         | '-----------------------' |
'----------------'  '---------------------------'         '---------------------------'
```

Ref https://openid.net/specs/openid-federation-1_0.html#name-trust-chain

Trust resolution



```
+-----+                         +-----+                             +--------------+
| RP  |                         | OP  |                             | Trust Anchor |
+-----+                         +-----+                             +--------------+
   |                               |                                        |
   | Entity Configuration Request  |                                        |
   |<------------------------------|                                        |
   |                               |                                        |
   | Entity Configuration Response |                                        |
   |------------------------------>|                                        |
   |                               |                                        |
   |                               | Evaluates authority_hints              |
   |                               |--------------------------              |
   |                               |                         |              |
   |                               |<-------------------------              |
   |                               |                                        |
   |                               | Entity Configuration Request           |
   |                               |--------------------------------------->|
   |                               |                                        |
   |                               |        Entity Configuration Response   |
   |                               |<---------------------------------------|
   |                               |                                        |
   |                               | Obtains Fetch endpoint                 |
   |                               |-----------------------                 |
   |                               |                      |                 |
   |                               |<----------------------                 |
   |                               |                                        |
   |                               | Request Subordinate Statement about RP |
   |                               |--------------------------------------->|
   |                               |                                        |
   |                               |        Subordinate Statement about RP  |
   |                               |<---------------------------------------|
   |                               |                                        |
   |                               | Evaluates the Trust Chain              |
   |                               |--------------------------              |
   |                               |                         |              |
   |                               |<-------------------------              |
   |                               |                                        |
   |                               | Applies Metadata Policies              |
   |                               |--------------------------              |
   |                               |                         |              |
   |                               |<-------------------------              |
   |                               |                                        |
   |                               | Derives the RP's final Metadata        |
   |                               |----------------------------------      |
   |                               |                                 |      |
   |                               |<----------------------------------     |
   |                               |                                        |
```

- *OP MUST have RP's Entity Identifier and a list of Entity Identifiers of Trust Anchors and their public signing keys.*
- *OP will first have to fetch sufficient Entity Statements to establish at least one chain of trust from the RP to one or more of the Trust Anchors.*
- *Then the OP MUST validate the Trust Chains independently.*
- *If there are multiple valid Trust Chains and if the application demands it, the OP MUST choose one to use.*

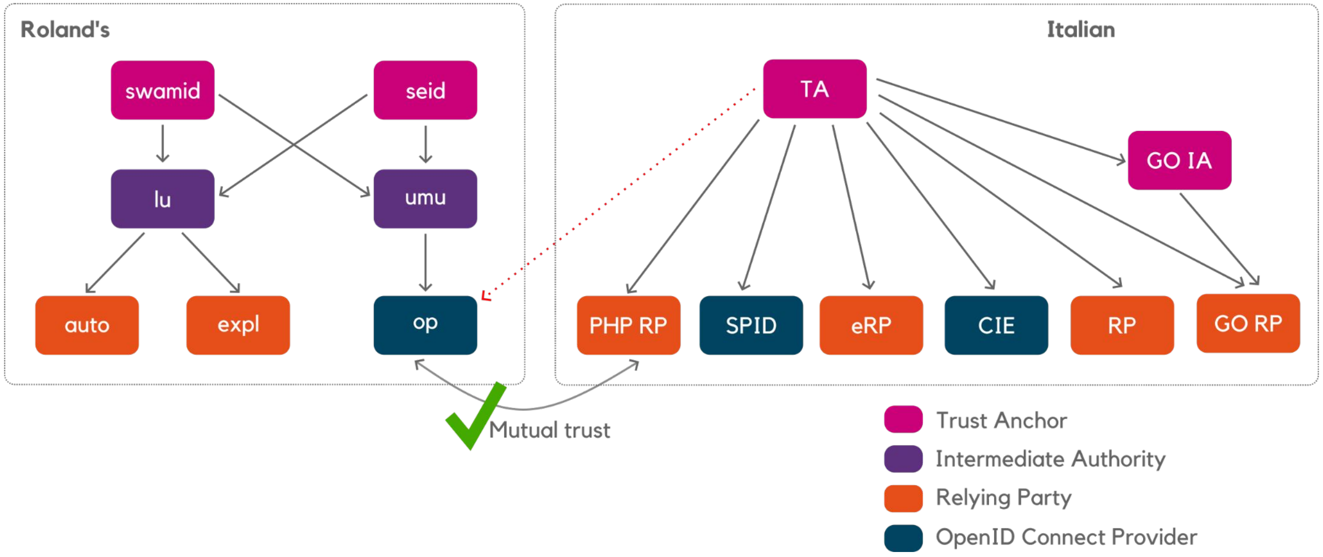
Ref https://openid.net/specs/openid-federation-1_0.html#name-resolving-the-trust-chain-a

How to get OpenID Federation in eduGAIN?

Leverage WP5 existing work!

TRUST & IDENTITY INCUBATOR

OIDCfed support on SimpleSAMLphp



ref https://wiki.geant.org/display/GWP5/OIDCfed+support+on+SimpleSAMLphp

eduGAIN OpenID Federation POC

Develop tools for federation operators

- **Trust Anchor**: RESTful web service that provides a root of trust for the federation.
- **Metadata parser and validator**: A metadata parser is a tool that can parse and validate entity metadata according to a defined schema.
- **Entity registry**: An entity registry is a database that stores entities HTTPs URL, their public keys and the Trust Marks issued for the entities.

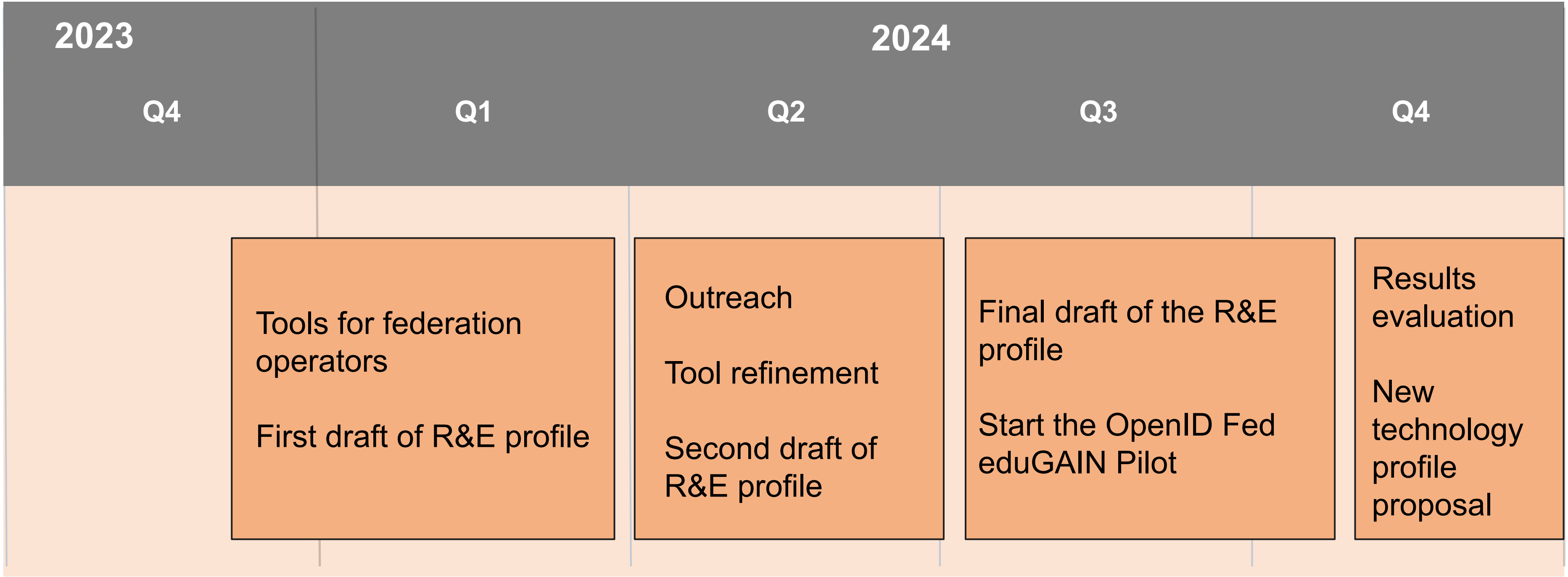
eduGAIN OpenID Federation POC

- Define an OpenID Federation implementation profile for National research and education networks and for eduGAIN.
- Refine the tools with an iterative approach and the collaboration of the eduGAIN and REFEDS community.
- Engage with the eduGAIN participants to set up an OpenID Federation based eduGAIN Pilot.
- Define a proposal for an additional Technology profile for eduGAIN.

eduGAIN OpenID Federation - Technology profile work in progress

- **General Architecture**: This document provides a general architecture for the trust model…
- **Federation**: This document discusses the role of OpenID Federation in the trust model...
- **OpenID Connect**: This document focuses on the use of OpenID Connect in the trust model...
- **Technical Rules, Policies and Constraints**: This document provides a detailed definition of the policies and artifacts in the trust model…

eduGAIN OpenID Federation POC



2023

2024

Q4

Q1

Q2

Q3

Q4

Tools for federation operators

First draft of R&E profile

Outreach

Tool refinement

Second draft of R&E profile

Final draft of the R&E profile

Start the OpenID Fed eduGAIN Pilot

Results evaluation

New technology profile proposal

Thank you

Any questions?

davide.vaghetti@garr.it

www.geant.org

The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).