

GÉANT Project Symposium 2023

MONTPELLIER, FRANCE

12 - 14 December

symposium.geant.org



Co-funded by
the European Union



GÉANT Project Symposium 2023



A new identity federation standard

December 13th 2023

Davide Vagheti (GARR)
eduGAIN Service Owner
WP5

symposium.geant.org



Co-funded by
the European Union





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.

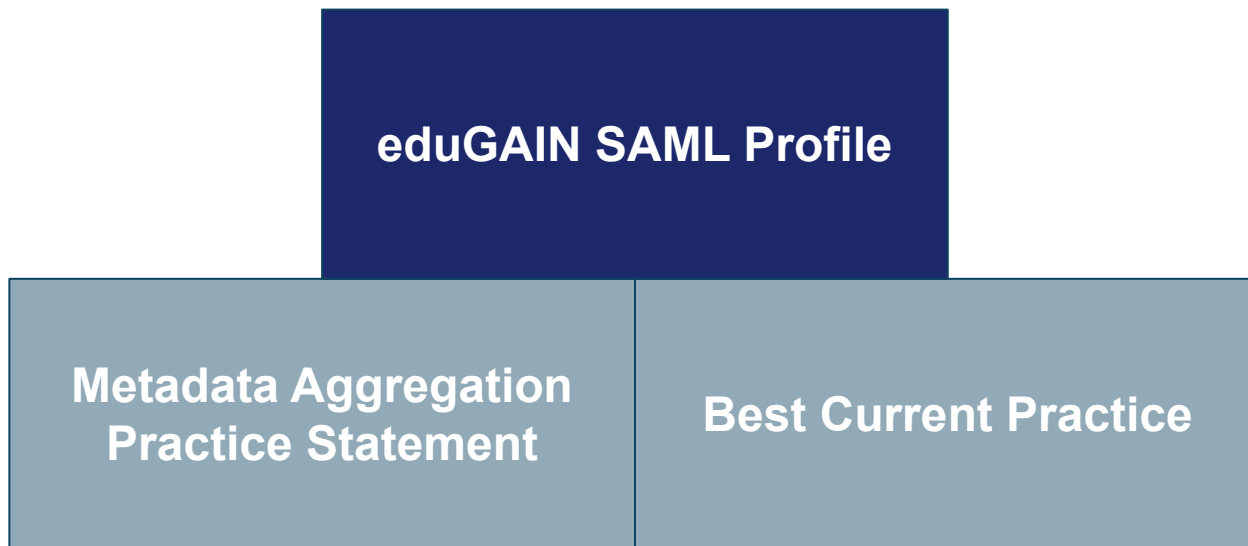


In **Q2 2024** we will start an eduGAIN OpenID Federation pilot.



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

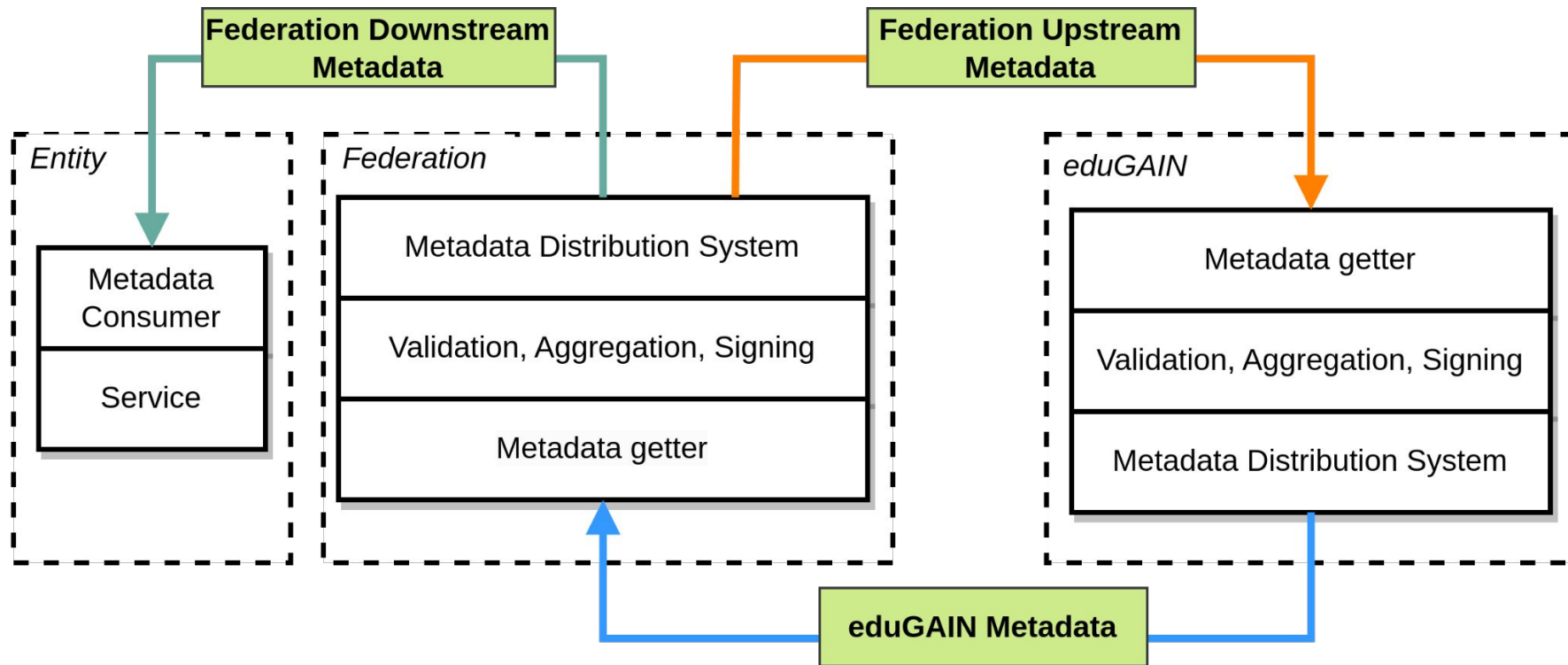
- eduGAIN and Identity Federations are based on SAML 2.0
 - eduGAIN SAML Technological Profile
 - eduGAIN Trust flow
- OpenID Federation
- The eduGAIN OpenID Federation POC

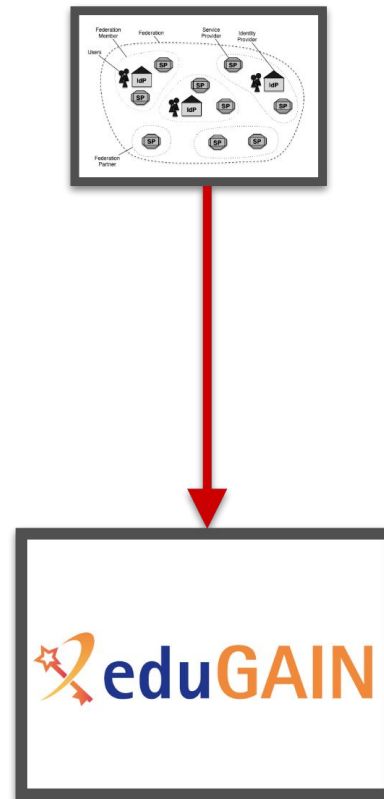
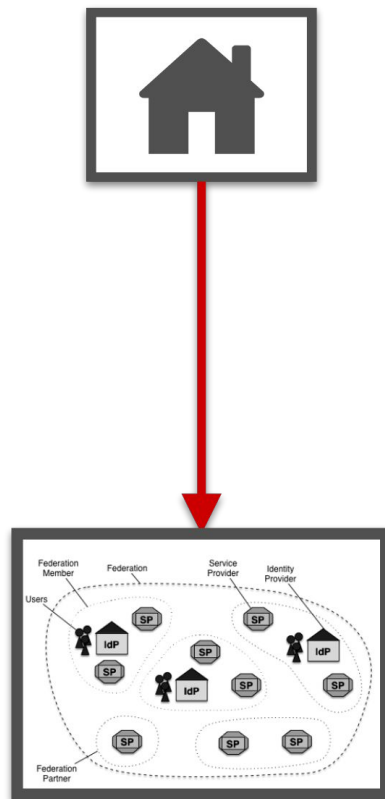
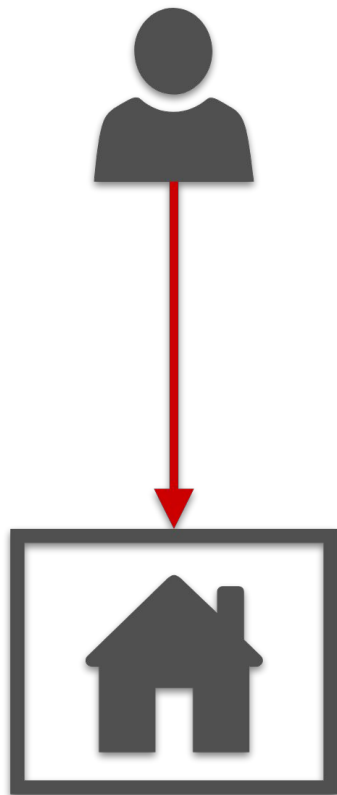


ref <https://technical.edugain.org/documents>

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	<i>Federations MUST provide their members with trustworthy SAML Metadata about eduGAIN Entities, signed with their own signing key [..]</i>
Participant requirements	<i>Produce and register a URL to the (participant) SAML Metadata export</i> <i>Register a signing certificate and an <code>mdrpi:registrationAuthority</code></i>

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





Users trust Home Organisation

HomeOrg/Providers trust Federations

Federations trust eduGAIN

Do users trust eduGAIN?

Do users even know eduGAIN?

 OpenID® *An OpenID Foundation specification*

Implementer Draft 32 of version 1.0 (published on Dec 4th)



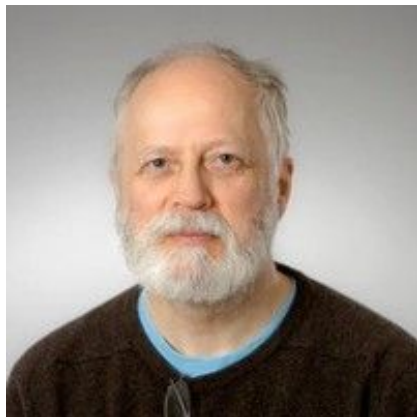
A very comprehensive spec, more than 100 pages of flows, claims, endpoints, etc



Reference implementations: python, java, golang, php



Production implementations: Italian eGOV-ID (SPID/CIE)



R. Hedberg,
Editor
independent



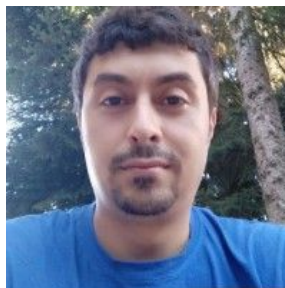
M.B. Jones
Self-Issued Consulting



A.Å. Solberg
Sikt



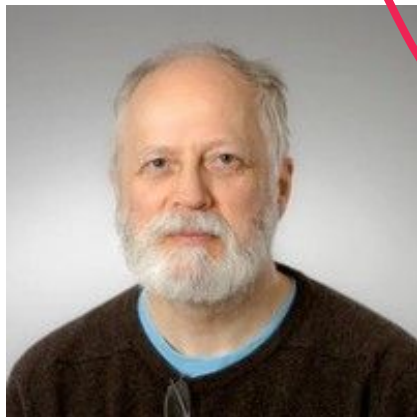
John Bradley
Yubico



G. De Marco
independent



V. Dzhuminov
Connect2id



R. Hedberg,
Editor
independent



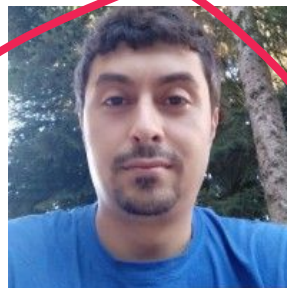
M.B. Jones
Self-Issued Consulting



A.Å. Solberg
Sikt



John Bradley
Yubico



G. De Marco
independent

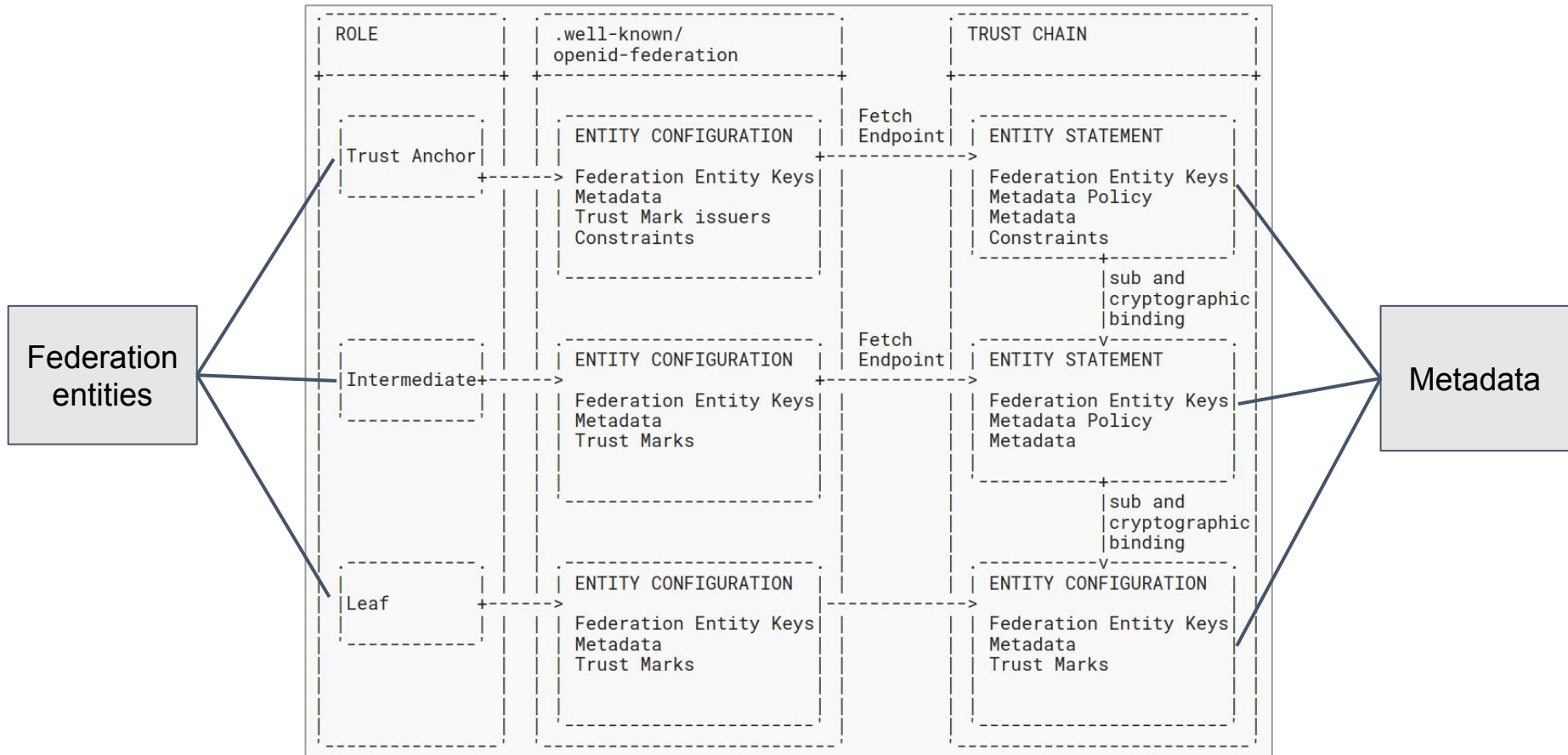


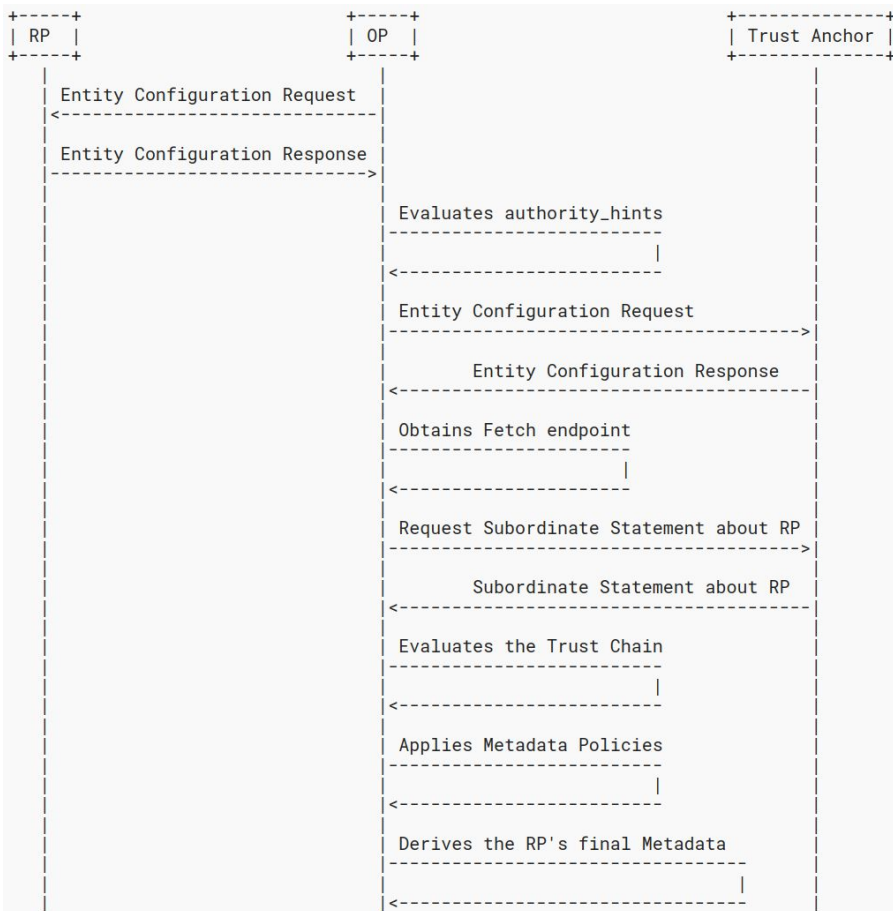
V. Dzhuvinov
Connect2id

- ★ Native dynamic metadata publication and distribution.
- ★ Dynamic Relying Parties registration.
- ★ Federation transparency.
- ★ Federation intermediaries.
- ★ Inband metadata policy engine.

A large, stylized, white, 3D-effect word "NEW" is oriented vertically on the right side of the slide. The letters are bold and have a slight shadow, giving them a three-dimensional appearance. The word is slanted slightly to the right.

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.





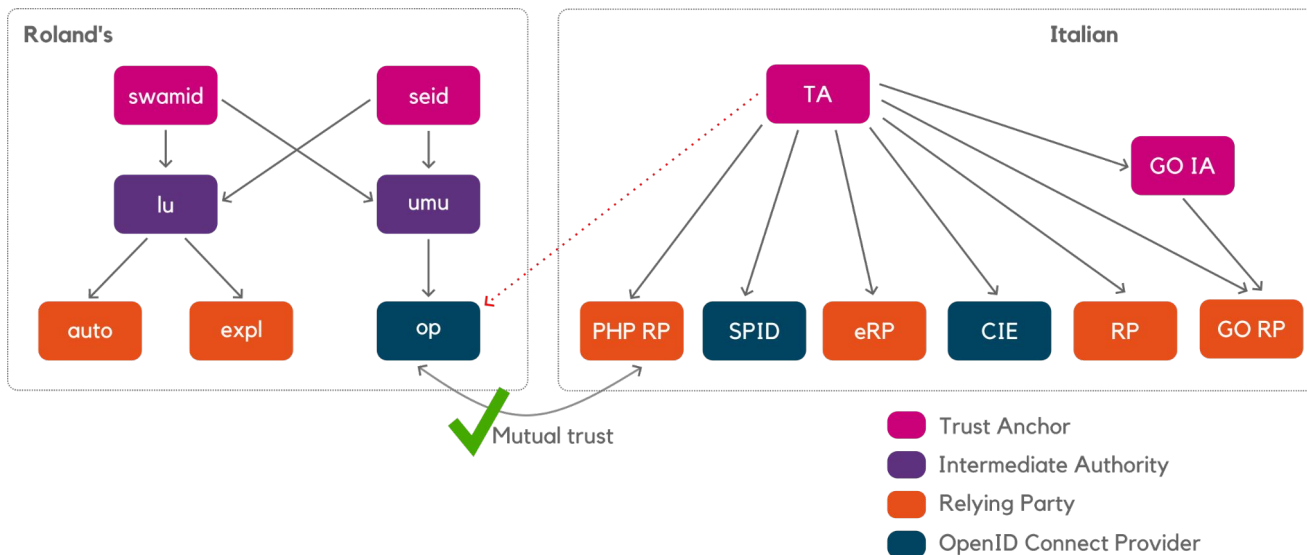
Ref https://openid.net/specs/openid-federation-1_0.html#name-resolving-the-trust-chain-a

- *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.*

How to get OpenID Federation in eduGAIN?



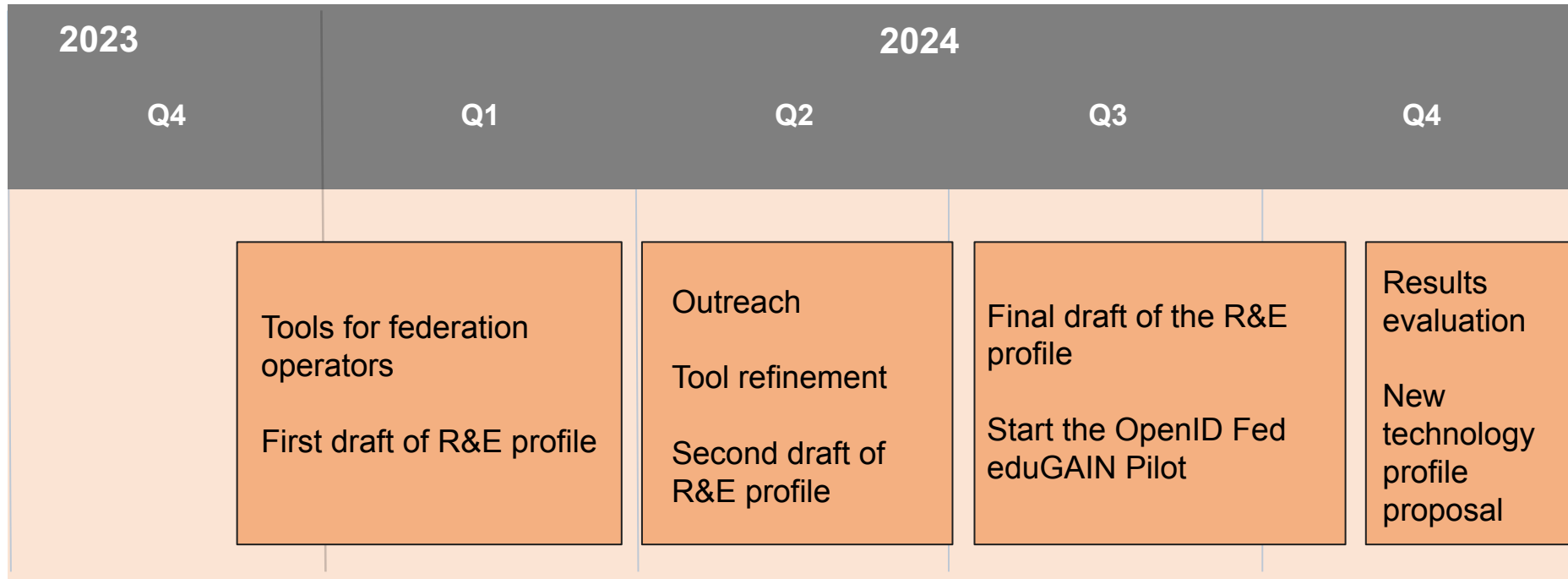
OIDCfed support on SimpleSAMLphp



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.

- 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.





Please leave your comments and feedback on the eduGAIN OpenID Federation POC plan!

<https://u.garr.it/edugainofedpoc>

Thank you

Any questions

symposium.geant.org



Co-funded by
the European Union

