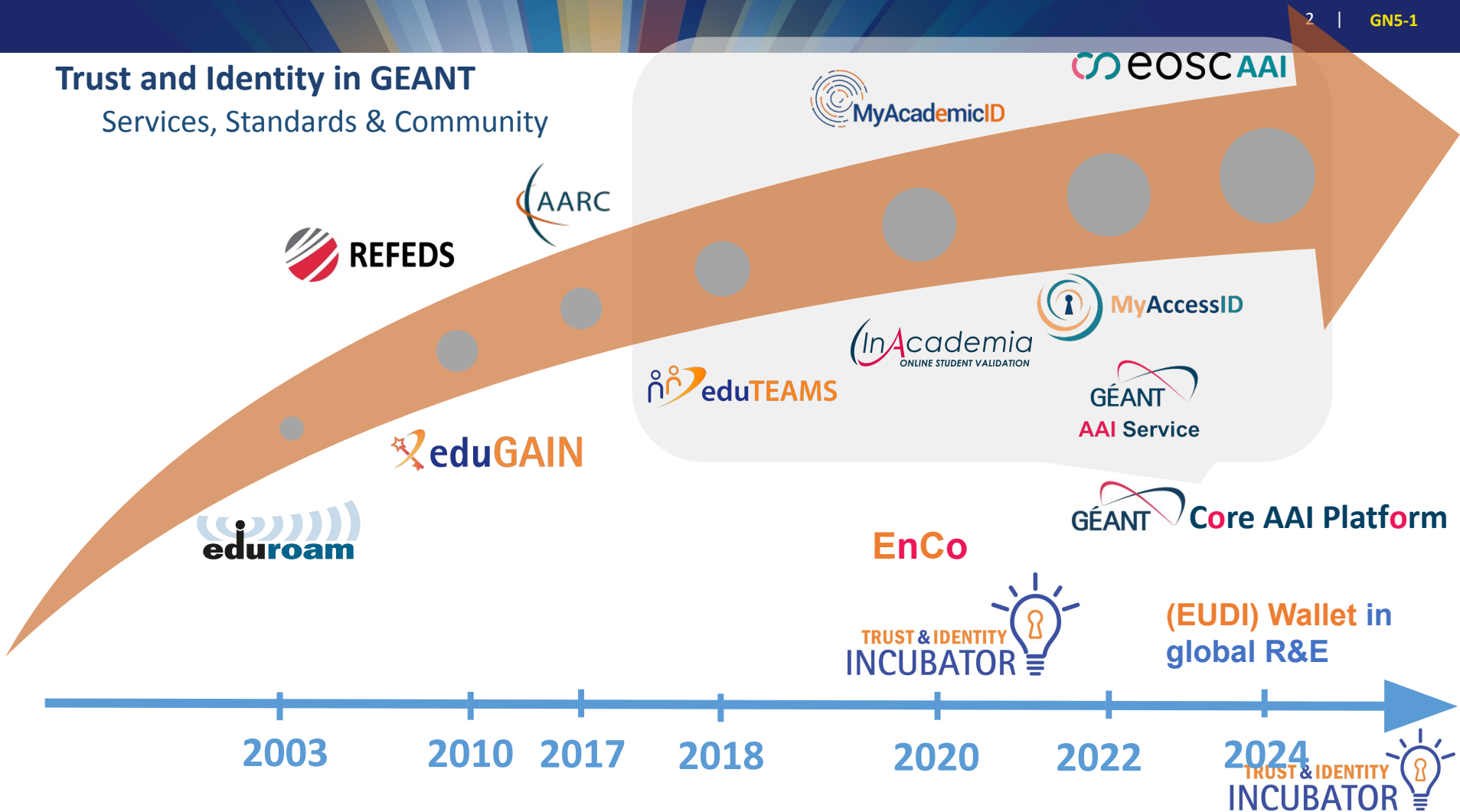
eduGAIN OID Federation Pilot

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

FIM4R - December 8, 2024

Trust and Identity in GEANT

Services, Standards & Community

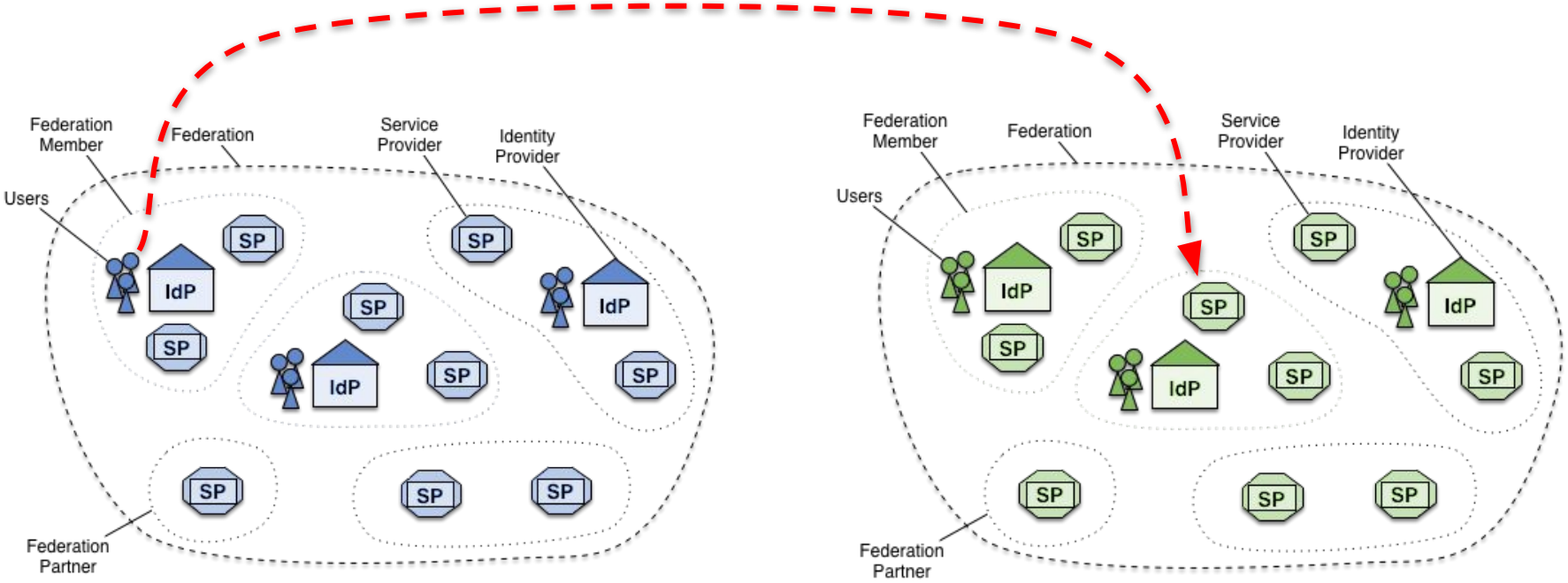


eduGAIN

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

TRUST & IDENTITY INCUBATOR

Inter-federated Access

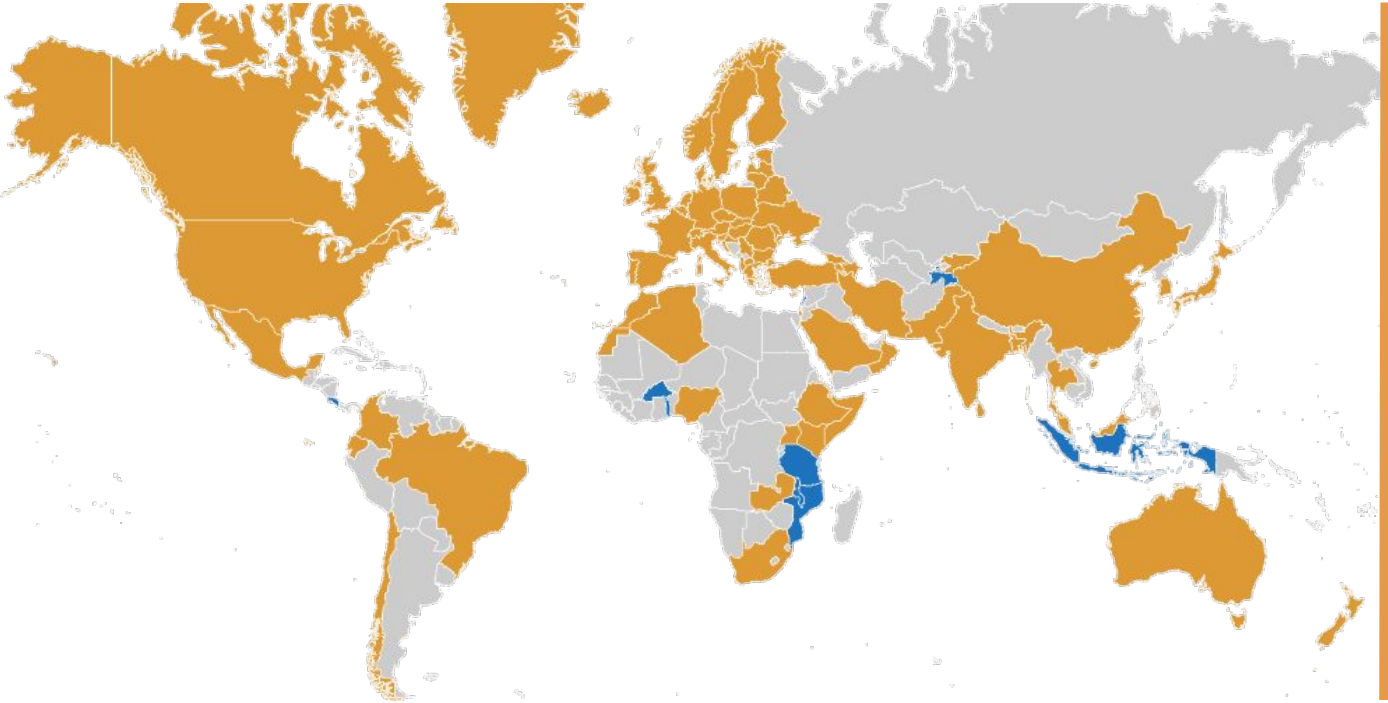


Federation Blue

Federation Green

TRUST & IDENTITY INCUBATOR

eduGAIN Global Coverage



78 Federations

9552 Entities

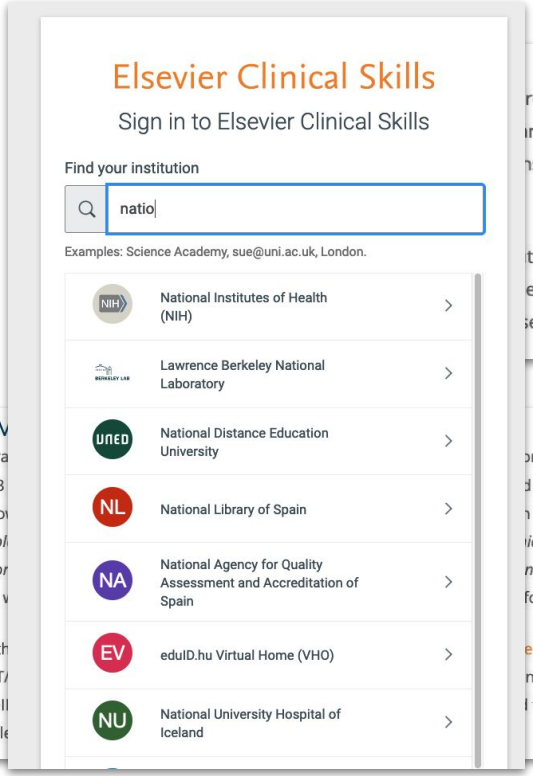
5775 Identity Providers

3795 Service Providers

Last update November 26th 2024

TRUST & IDENTITY INCUBATOR

What do we use it for?



rometer Gravitational-Wave Observatory, **LIGO**, comprises more than 1,500 scientists, all of whom
rds a single goal: to capture signs of gravitational waves and decode their meaning. The data
s 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
e their existing institutional identities to access data on remote systems and securely share results.

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 w

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

m 11 participating countries and around 3,000
d from mobility under Erasmus by 2017. The
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

TRUST & IDENTITY INCUBATOR

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

TRUST & IDENTITY INCUBATOR

eduGAIN Technological Profiles: SAML 2.0

An open standard

Extremely successful and adopted

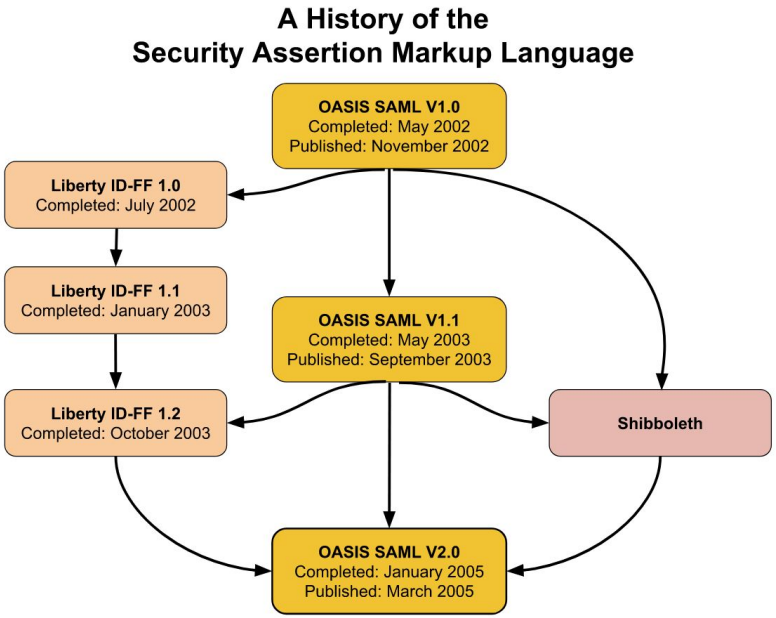
87 R&E Federations + eduGAIN

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?



Davide Vaghetti - GARR - davide.vaghetti@garr.it

TRUST & IDENTITY INCUBATOR

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 AAIs
- Any other interested stakeholder

WHEN

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

TRUST & IDENTITY INCUBATOR

OpenID Federation

OpenID® *An OpenID Foundation specification*

- Implementer Draft 40 of version 1.0 (published on Oct 24th 2024)
- 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), Authlete, Findynet, Radimian, Connect2ID …

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

OpenID Federation Lingo

Subordinate Statement	A signed JWT that contains the information including public cryptographic material, metadata 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 a Subordinate 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

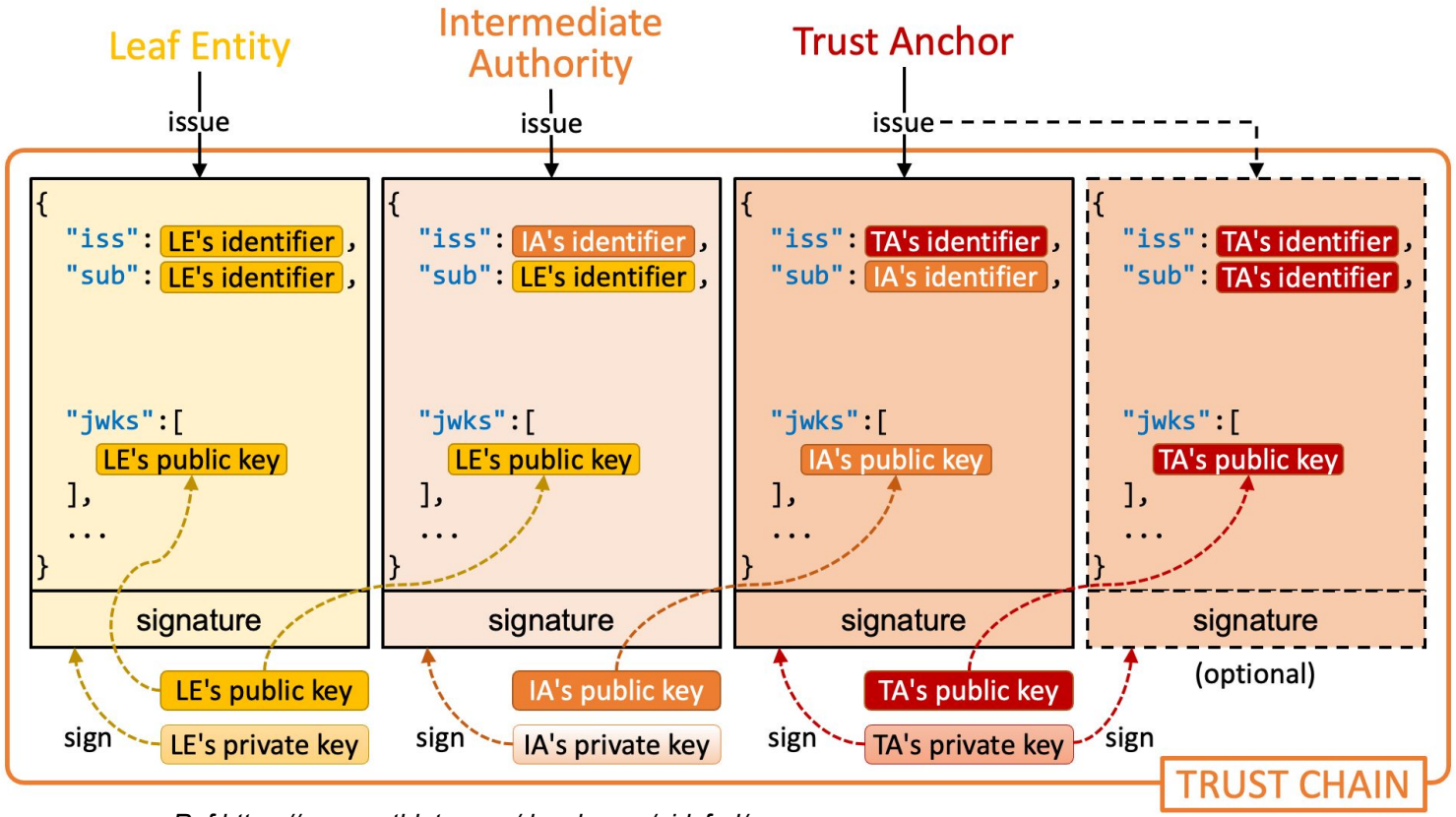
OpenID Federation Entity Configuration

Leaf's Entity Configuration


```
{
  "alg": "ES256",
  "kid": "NFM1WUViUI",
  "typ": "application/entity-statement+jwt"
}
.
{
  "exp": 1649590602,
  "iat": 1649417862,
  "iss": "https://rp.example.org",
  "sub": "https://rp.example.org",
  "jwks": {"keys": [    {
                "kty": "EC",
                "kid": "NFM1WUViUI",
                "crv": "P-256",
                "x": " … ",
                "y": " … "
  }]},
  "metadata": {
        "openid_relying_party": { … },
        "openid_credential_issuer": { … },
        "oauth_authorization_server": { … }
  },
  "trust_marks": [{
                "id": "https://fw.example.it/tm/1",
                "trust_mark": "eyJh …"
  }],
  "authority_hints": ["https://ta.example.org"]
}
```

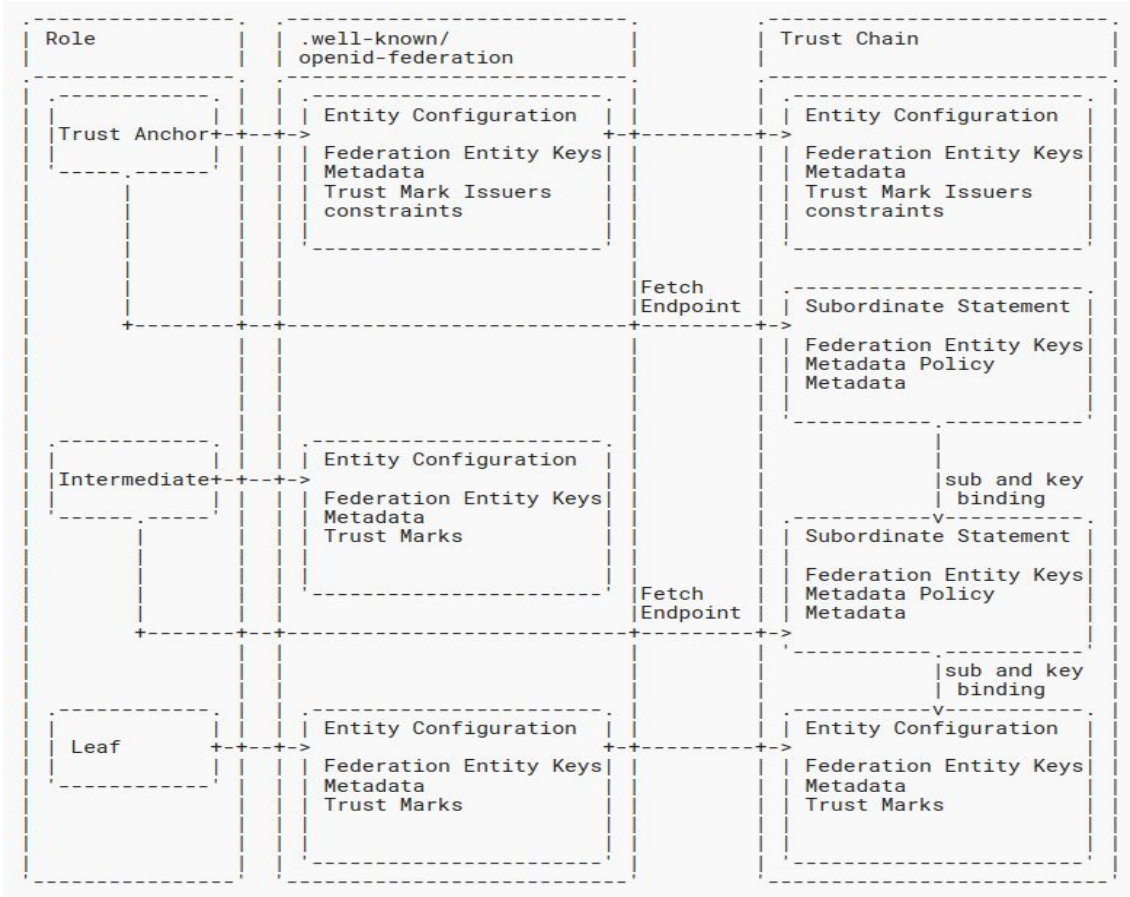

1. Self Signed JWT
2. Federation JWKs in the payload top level
3. Multiple Metadata (with their JWKS)
4. Trust Marks, compliance assertions to particular profiles
5. Authority hints, indicating the immediate Superior Entities that has registered this Entity and can "say something about it"

Trust Chain



Ref https://www.authlete.com/developers/oidcfed/

An eduGAIN OIDC Federation Trust Flow



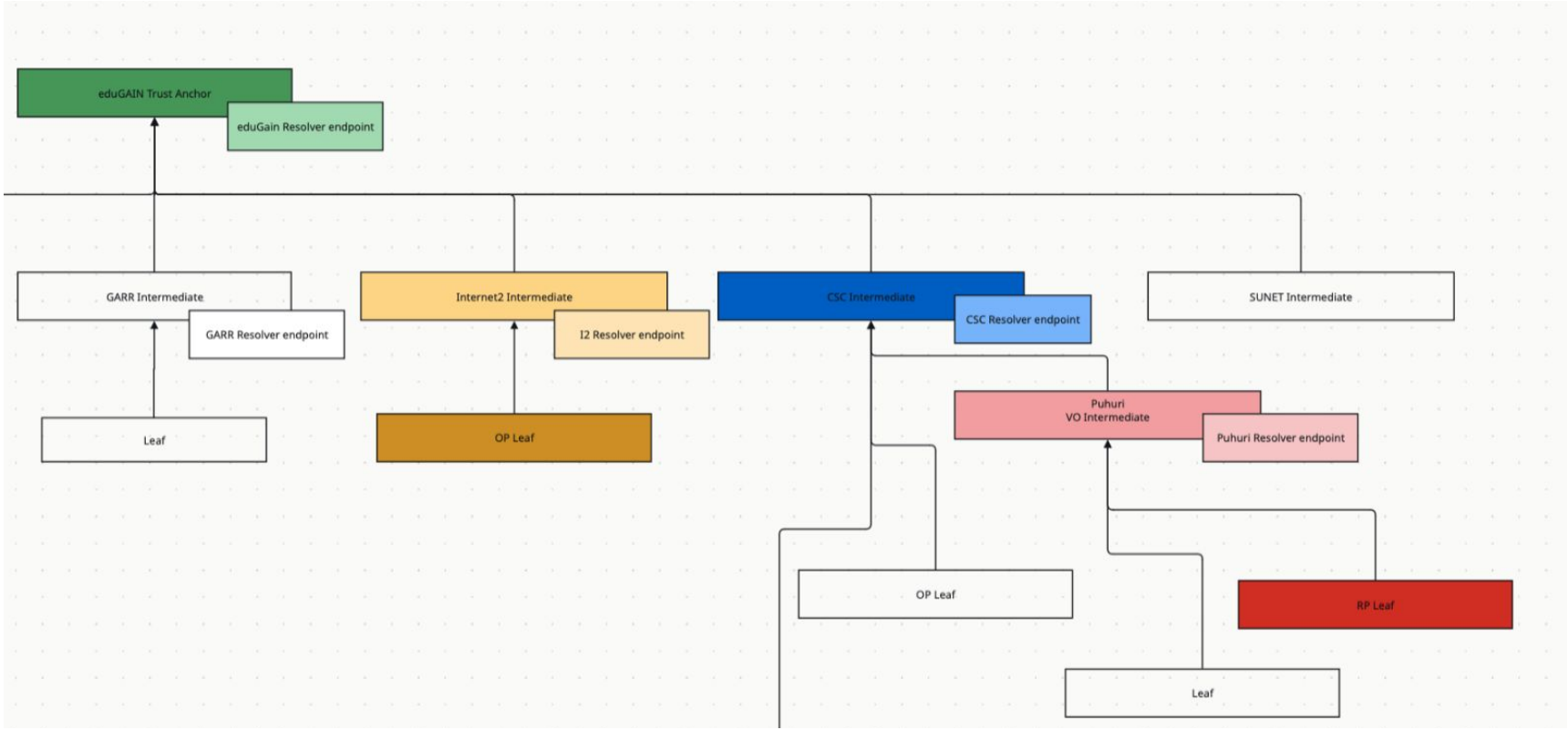
Federation

Entity

Davide Vaghetti - GARR - davide.vaghetti@garr.it

TRUST & IDENTITY INCUBATOR

eduGAIN OpenID Federation Trust model



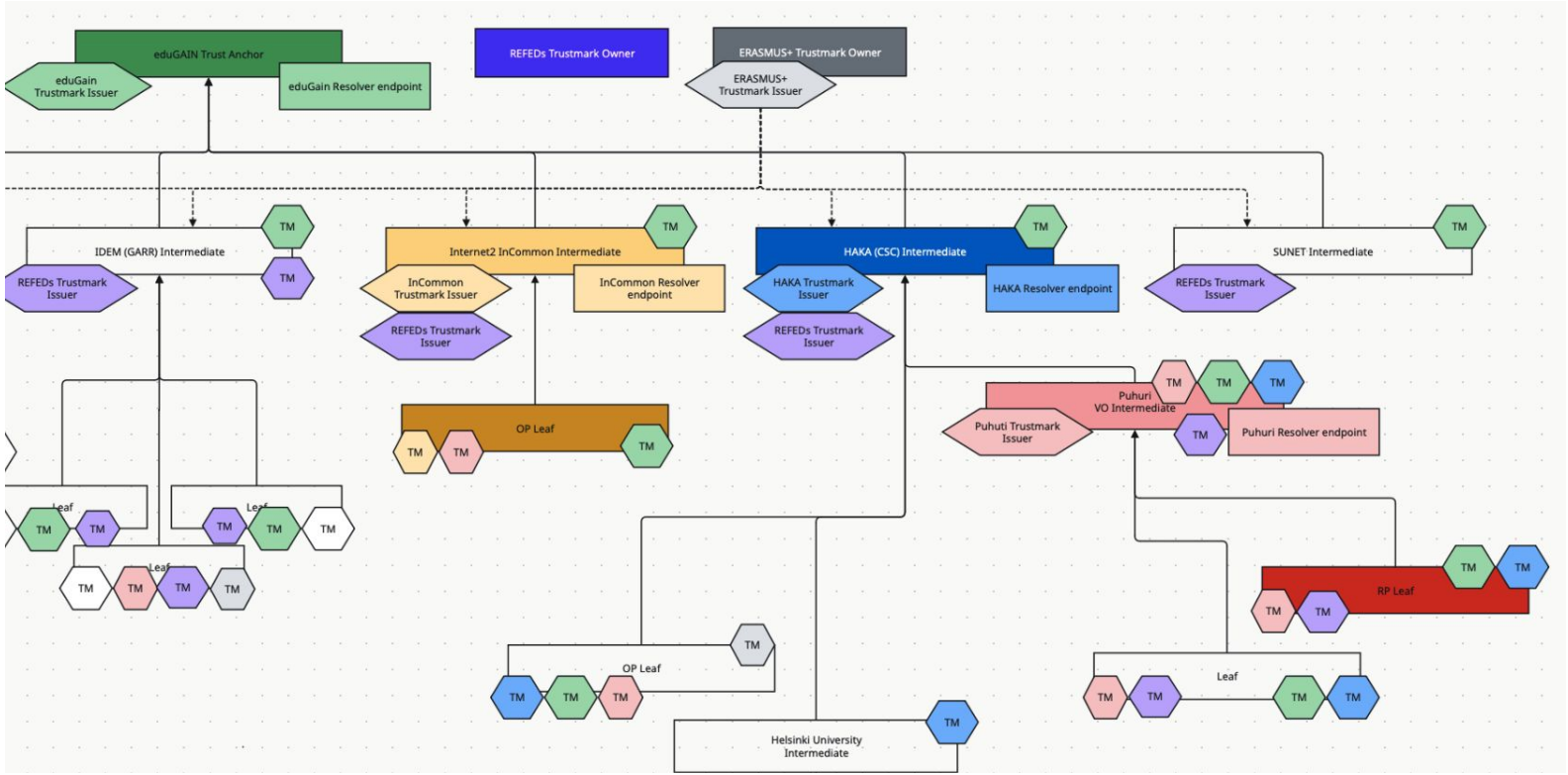
The eduGAIN OpenID Connect Profile - work in progress

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**

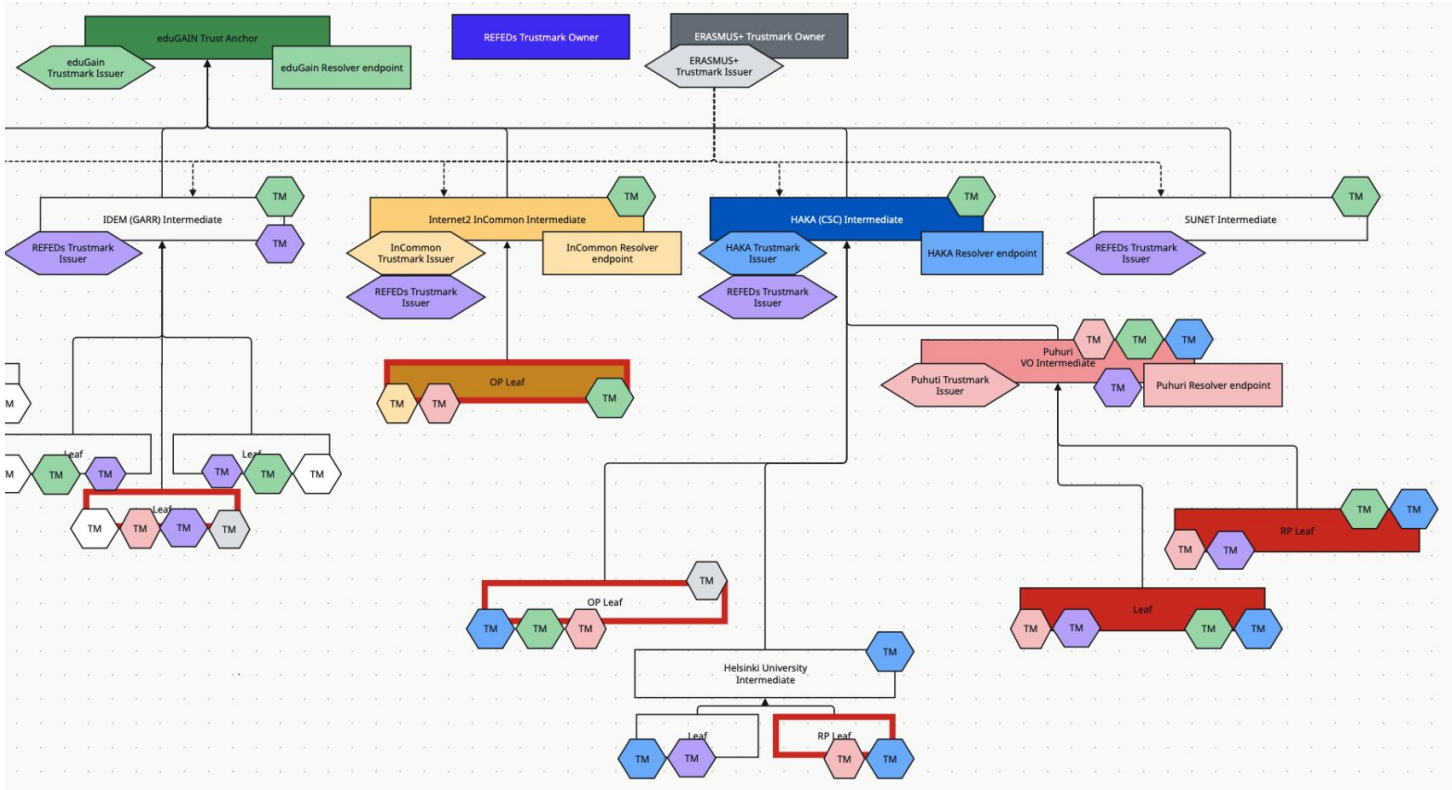
ENTITY RESOLUTION is provided by a resolver endpoint at federation and inter-federation level that provides metadata about entities

Trust hierarchy ‘remix’ using Trustmarks



TRUST & IDENTITY INCUBATOR

Trust hierarchy ‘remix’ using Trustmarks



TRUST & IDENTITY INCUBATOR

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 T&cubatorI Inc 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!)

OpenID Federation Wallet Architectures
DRAFT

OpenID Federation Wallet Architectures 1.0 - DRAFT

```
+------------------+     +-----------------+
| Authentic Source |     | Wallet Provider |
|                  |     |                 |
+------------------+     +-----------------+
         |                        |
         |                        |
         V                        V
+-------------------+    +---------------+    +---------------------+
| Credential Issuer |<-->|    Holder     |<-->| Credential Verifier |
|                   |    |               |    |                     |
+-------------------+    +---------------+    +---------------------+
         |                        |                      |
         |                        |                      |
         V                        V                      V
+-------------------------------------------------------------+
|                         Trust Anchor                        |
+-------------------------------------------------------------+
```

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

OpenID Federation Wallet Architectures 1.0 - DRAFT

```
+----------------------------+
| Trust Chain                |
| +------------------------+ |
| | Trust Anchor           | |
| | (Entity Configuration) | |
| +------------------------+ |
|                     |      |
|                     v      |
| +------------------------+ |
| | Trust Anchor           | |
| | (Subordinate Statement | |
| |  about the             | |
| |  Wallet Provider)      | |
| +------------------------+ |
|                     |      |
|                     v      |
| +------------------------+ |
| | Wallet Provider        | |    +--------------------------------+
| | (Entity Configuration) |------>|      Wallet Attestation        |
| +------------------------+ |    | (Not part of the Trust Chain) |
+----------------------------+    +--------------------------------+
```

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

OpenID Specifications around Verifiable Credentials

OpenID4VCI – OpenID for Verifiable Credentials - draft 14

https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

OpenID4VP – OpenID for Verifiable Presentations - draft 21

https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

SIOPv2 – Self-issued OpenID Provider v2 - draft 13

https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

DCP-HAIP – Digital Credential Protocols High Assurance Interoperability Profile - draft 00

https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0-00.html

UserInfo-VC - UserInfo Verifiable Credentials - draft 00

https://openid.net/specs/openid-connect-userinfo-vc-1_0.html

DCP-SecTrust - Digital Credential Protocols Security and Trust - draft

https://openid.github.io/OpenID4VC_SecTrust/draft-oid4vc-security-and-trust.html

OpenID for Verifiable Presentations over BLE - draft 00

https://openid.net/specs/openid-4-verifiable-presentations-over-ble-1_0.html

Thank You

Niels van Dijk, niels.vandijk@surf.nl

Davide Vaghetti, davide.vaghetti@garr.it

www.geant.org

Co-funded by
the European Union