eduGAIN OpenID Federation Pilot

Davide Vaghetti (GARR)

5 November 2025 - Rome, Workshop GARR 2025

OpenID Federation: why

R&E Identity Federations and **eduGAIN** are based on **SAML 2.0, but SAML 2.0 is a legacy protocol.**

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 protocol..

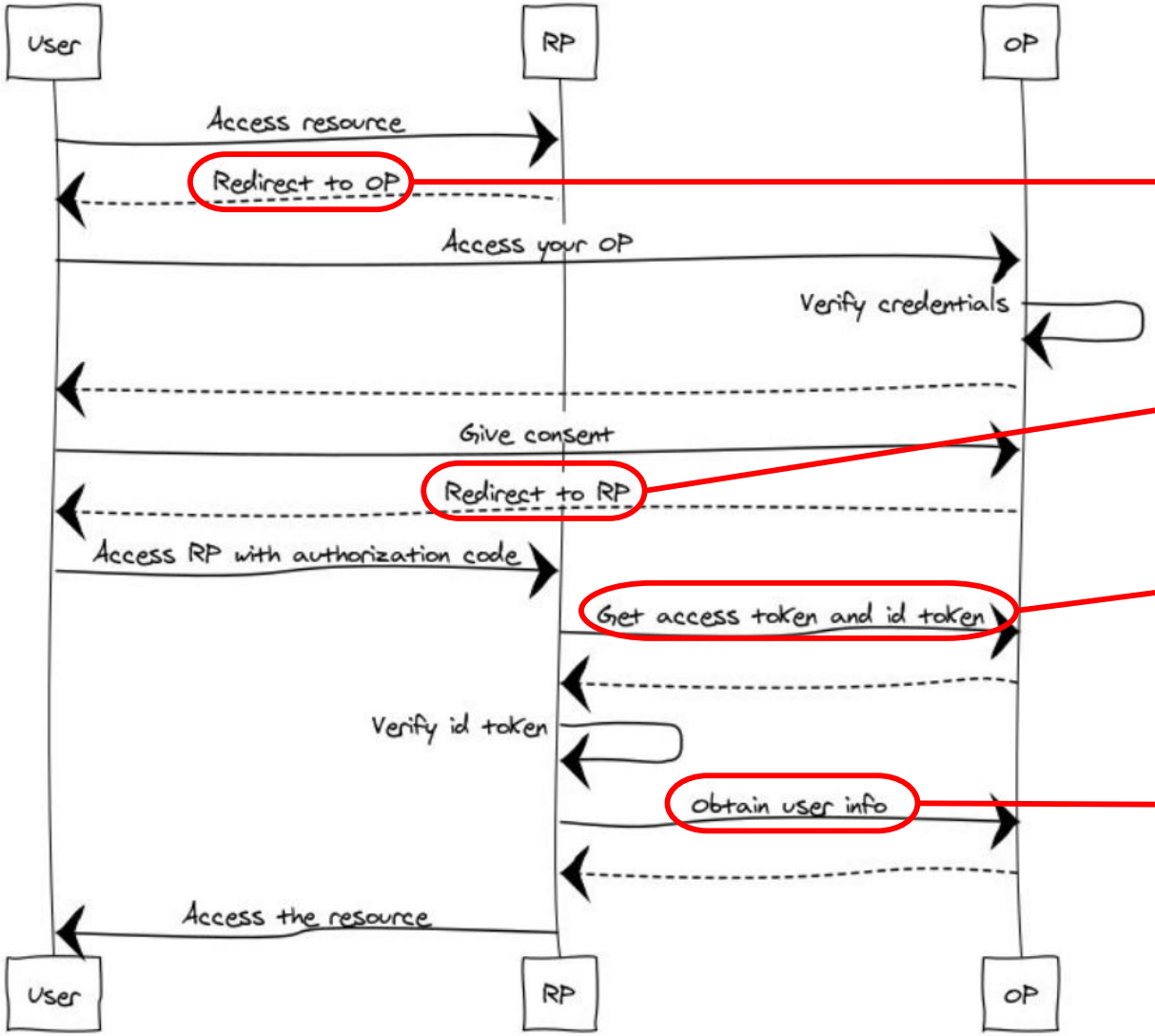
OpenID Federation is also currently being tested as one of the trust framework for the EUID Wallet.

The eduGAIN Service and the T&I Incubator run a Proof of Concept activity to develop tools to build OpenID Federations for Reseach and Education.

OpenID Federation bits and pieces

OpenID Federation: the problem space

*OP and RP need to know and **trust** information about each other*



The RP redirect the user to the OP's **authorization_endpoint**

The OP redirect the user to the RP's **redirect_uri**

The RP exchange the code for an access_token at the **token_endpoint** (and authenticate…)

The RP requests user claims at the OP's **userinfo_endpoint**

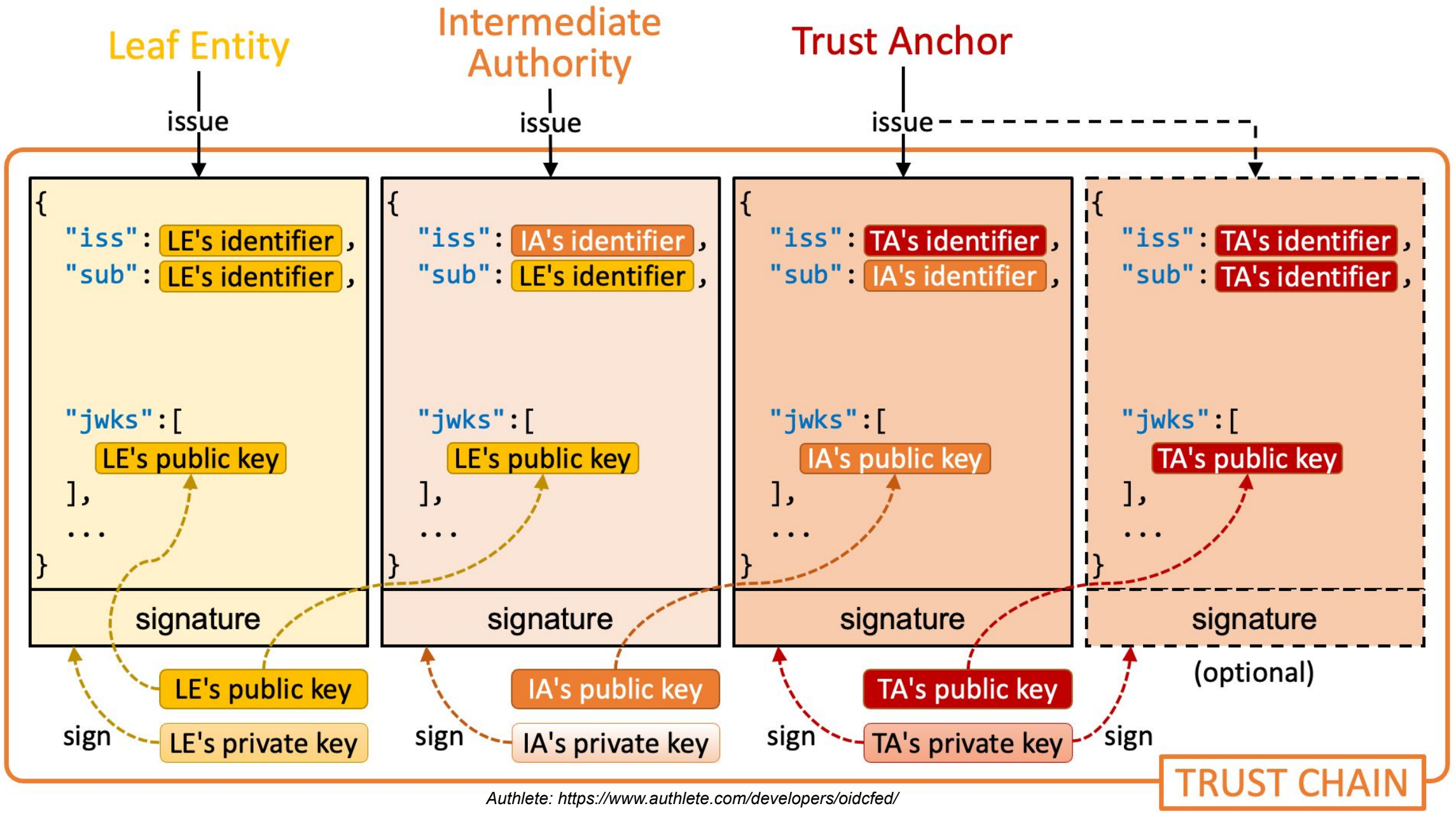
OpenID Federation: what

- **A Trust Framework for Federations**: Defines a way to establish and manage trust between organizations.
- **Hierarchical Trust Model**: Trust flows through chains of signed JSON Web Token (like PKI).
- **Signed Metadata Distribution**: All critical configuration data (endpoints, keys, capabilities, policies) is published as signed JSON metadata statements that are fetched and validated from federation's entities.

OpenID Federation: what

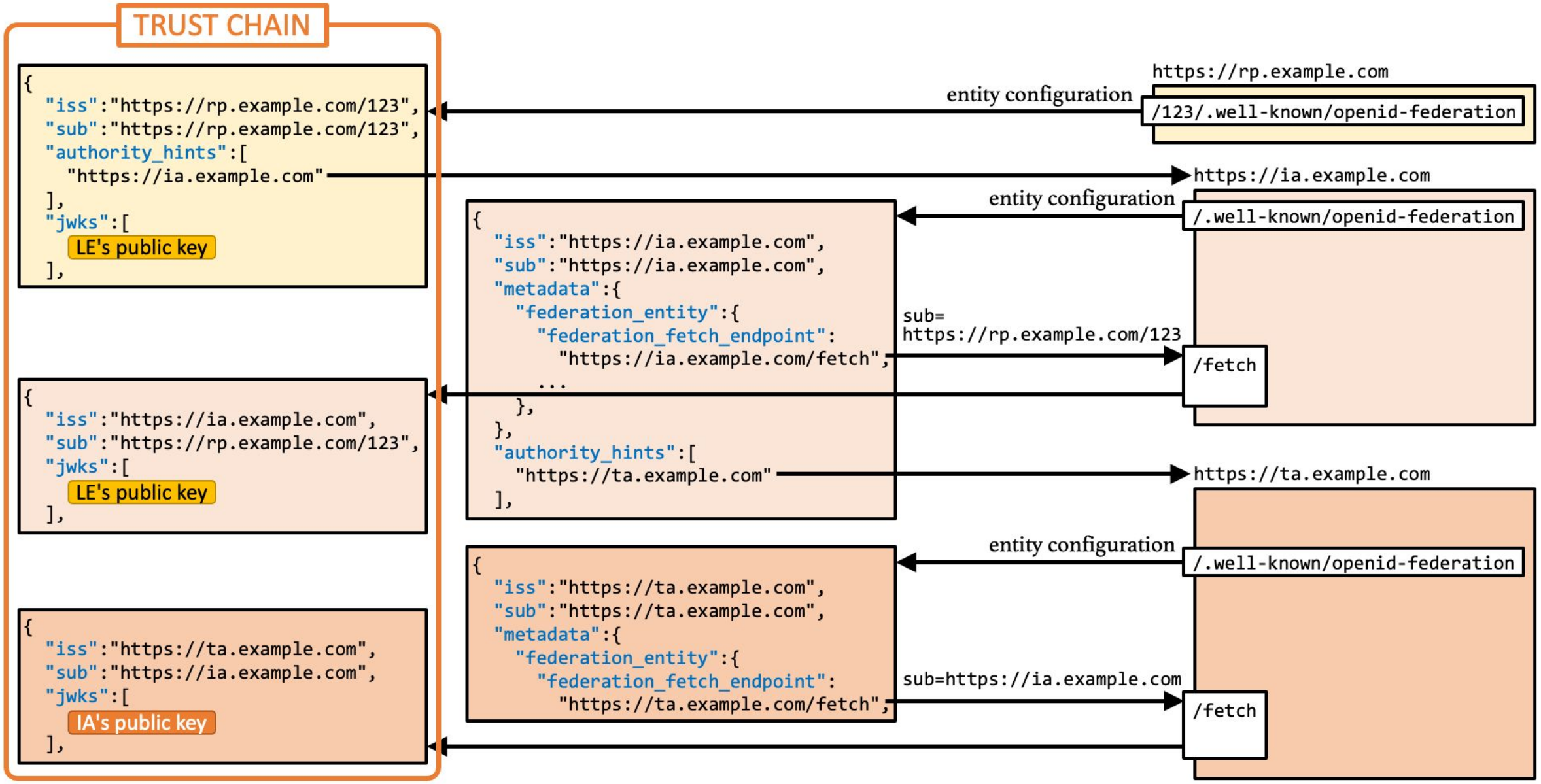
OIDF Element	Description	SAML 2.0 equivalent
Entity Statement	A signed JWT that contains the information needed for an Entity to participate in federation(s).	**Metadata**
Trust Anchor	An Entity that represents a trusted third party.	**A Federation**
Intermediate Authority	An Entity that issues an Entity Statement appearing somewhere in between those issued by the Trust Anchor and the subject of a Trust Chain.	**N/A ~ A federation in the context of eduGAIN**
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.	**An IdP or an SP**
Trust Chain	A sequence of Entity Statements that represents a chain starting at a Leaf Entity and ending in a Trust Anchor.	**N/A - SAML Trust Chain has only one level**
Trust Mark	Statement of conformance to a well-scoped set of trust and/or interoperability requirements as determined by an accreditation authority.	**N/A**
Resolver	An endpoint that provides Resolved Metadata and Trust Marks to another Entity.	**Metadata Distribution Service (Aggregate or Dynamic/MDQ)**

OpenID Federation: Trust Chain



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

OpenID Federation: Trust Chain Resolution



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

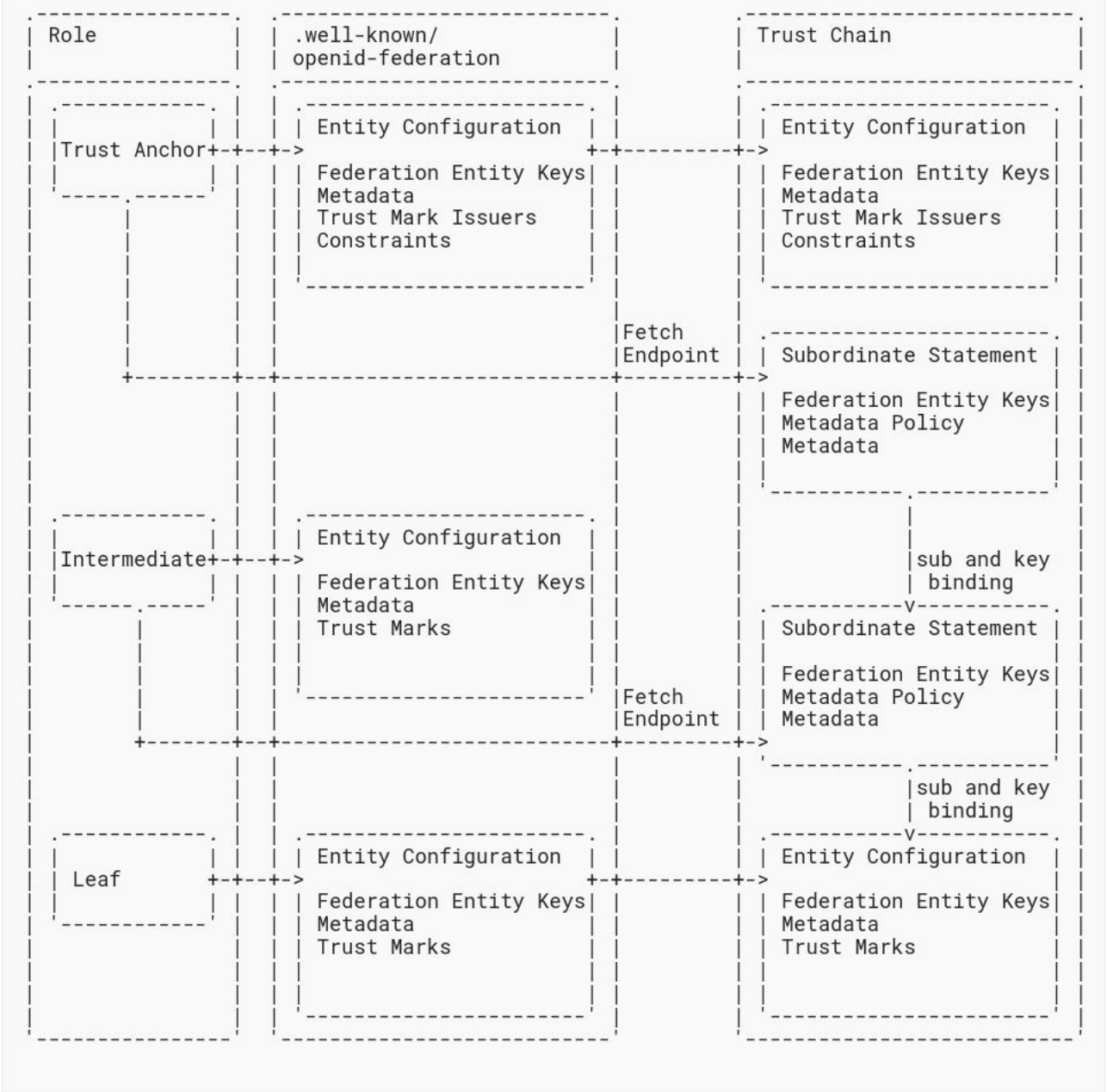
eduGAIN OpenID Federation profile principles

GN5-2

Principle 1

Principle 1: The eduGAIN federation has one defined mechanism to establish trust among all the participants.

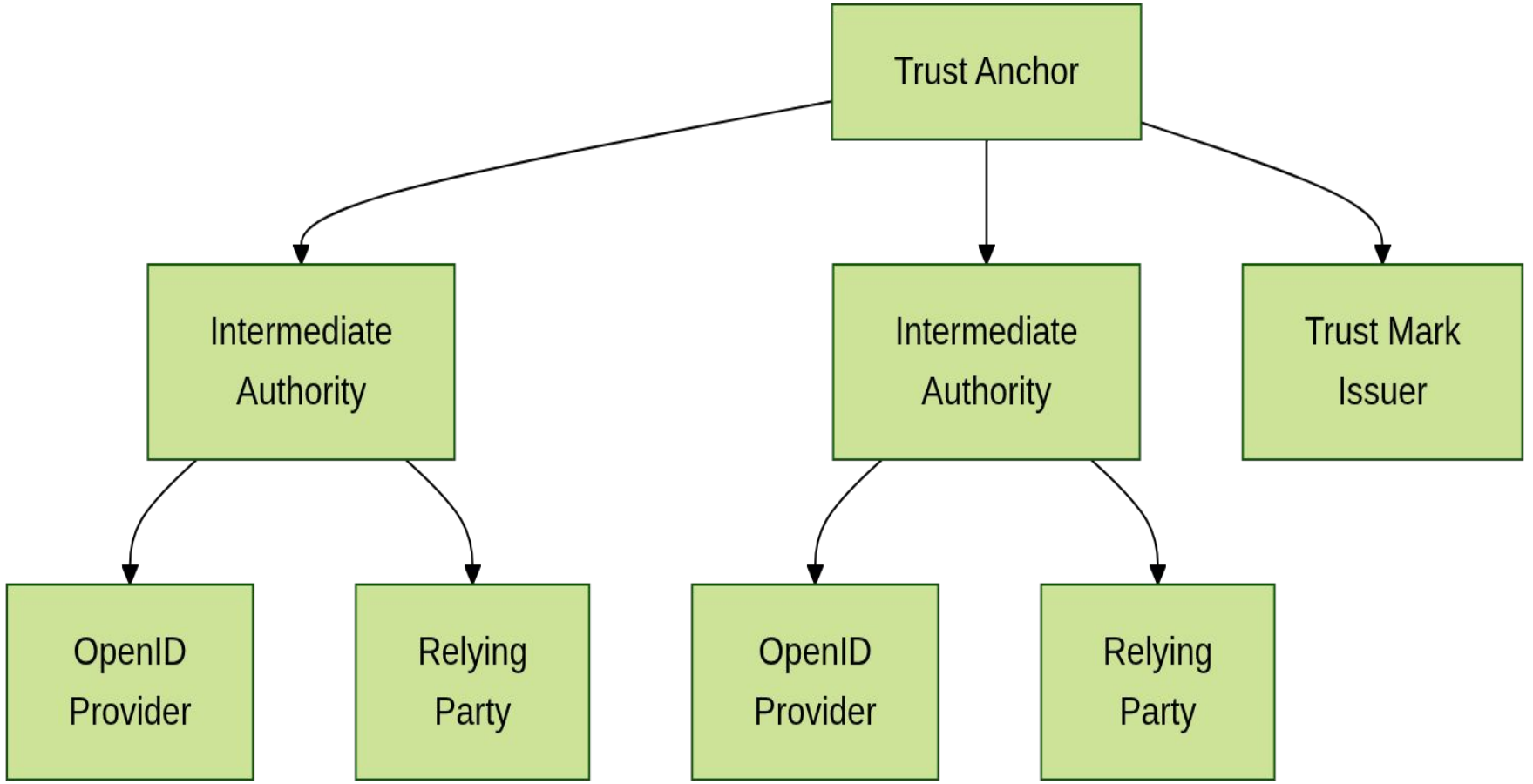
Requirement: Trust Chains is the basic technical trust of the federation.



Principle 2

Principle 2: eduGAIN is a federation of federations, end organisations cannot join eduGAIN directly.

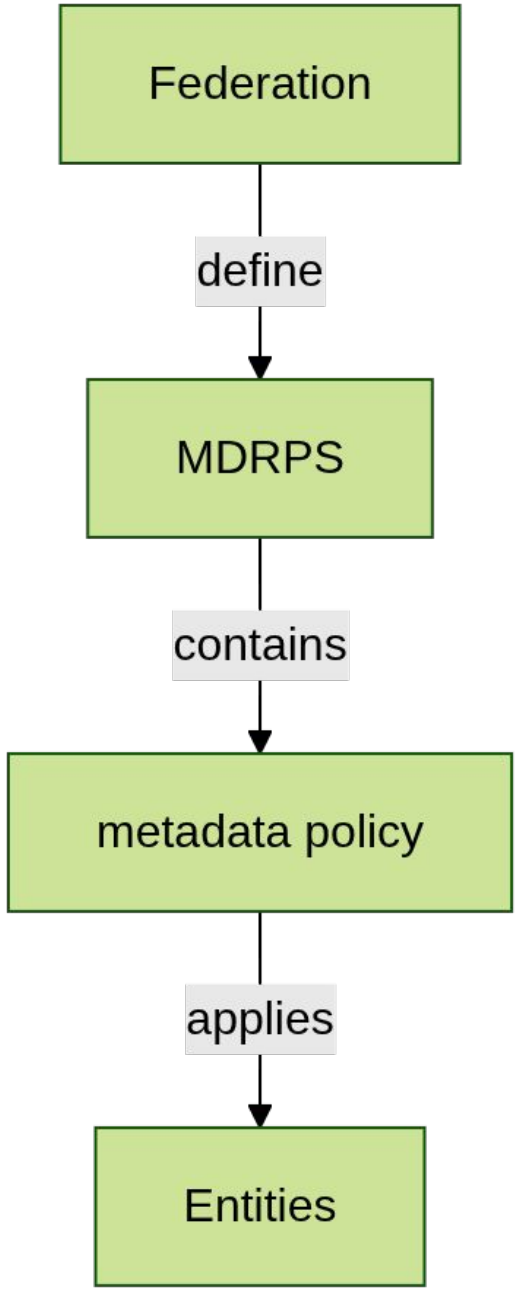
Requirement: All Immediate Subordinate Entities to the eduGAIN Trust Anchor MUST have the federation_entity entity type, such as Intermediate Authorities and Trust Mark Issuers.



Principle 3

Principle 3: eduGAIN is a federation of federations and it builds on the layer of local trust already provided by the federation.

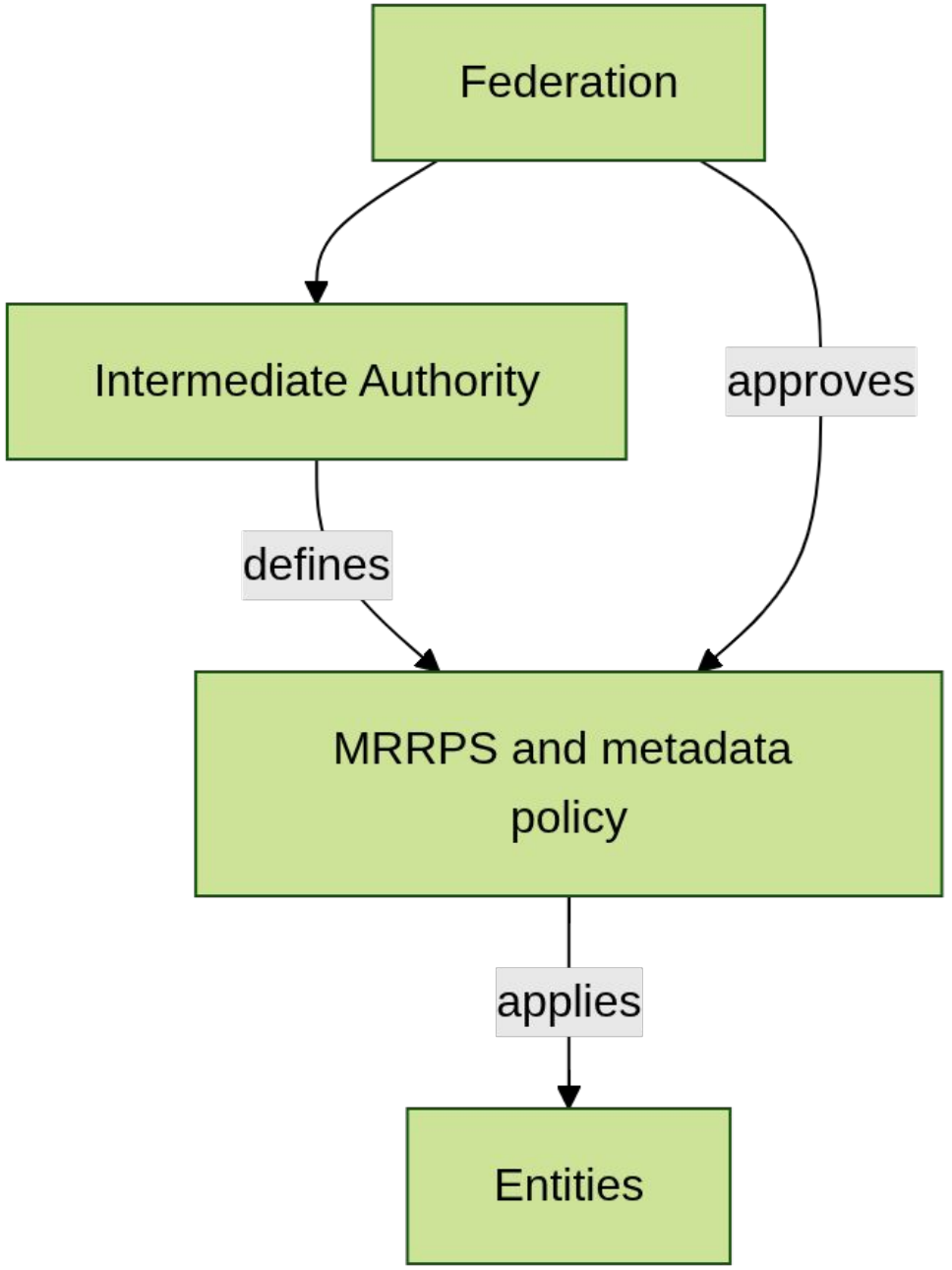
Requirement: An Immediate Subordinate Entity to the eduGAIN Trust Anchor MUST be a Trust Anchor for its subordinates and be operated by a federation operator. MUST provide a Metadata Registration Practice Statement (MDRPS). The MDRPS must contain metadata policies, including a description of trust chain constraints for subordinates.



Principle 4

Principle 4: Federations MAY admit Intermediate Authorities as subordinates and let them register their own entities provided that they can support the federation requirements.

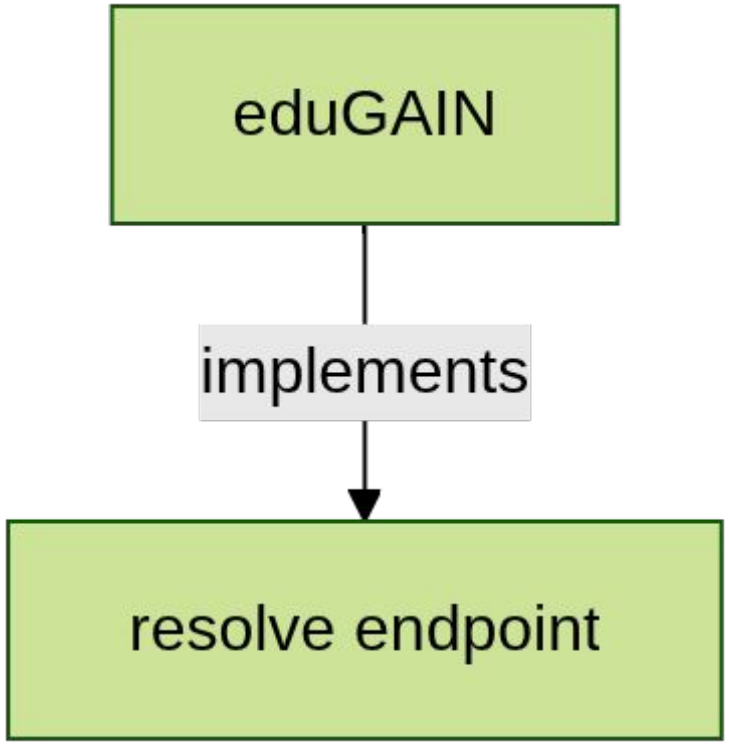
Requirement: Intermediate Authorities subordinate to a federations MUST provide a Metadata Registration Practice Statement. The MDRPS MUST contain metadata policies, including a description of trust chain constraints for subordinates, and MUST be apprroved by the federation.

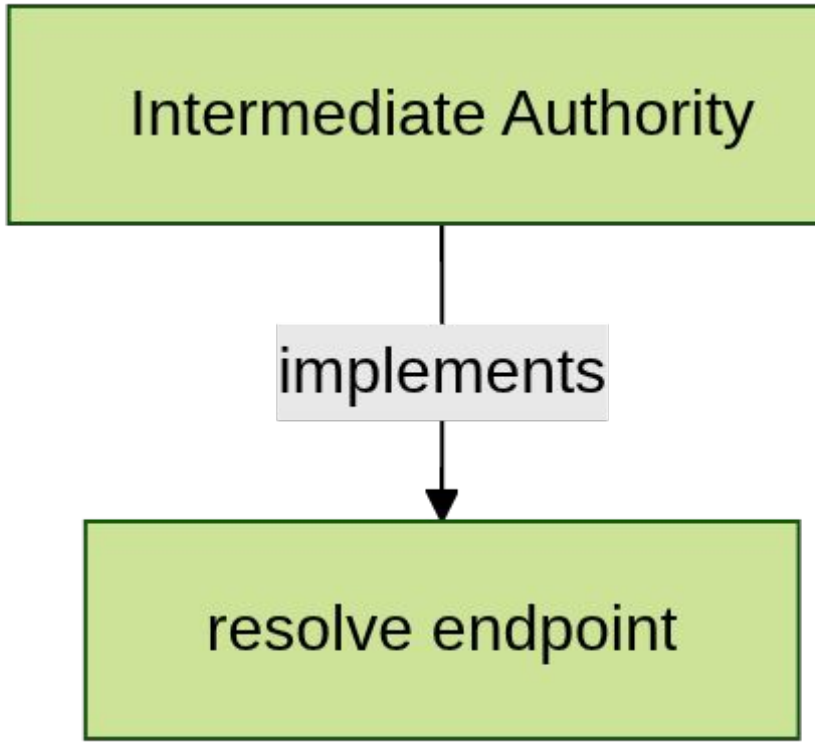


Principle 5

Principle 5: All the eduGAIN entities MUST be discoverable and their trust resolvable to the eduGAIN Trust Anchor.

Requirement: eduGAIN and Intermediate Authorities subordinate to the eduGAIN TA MUST provide a resolve endpoint.

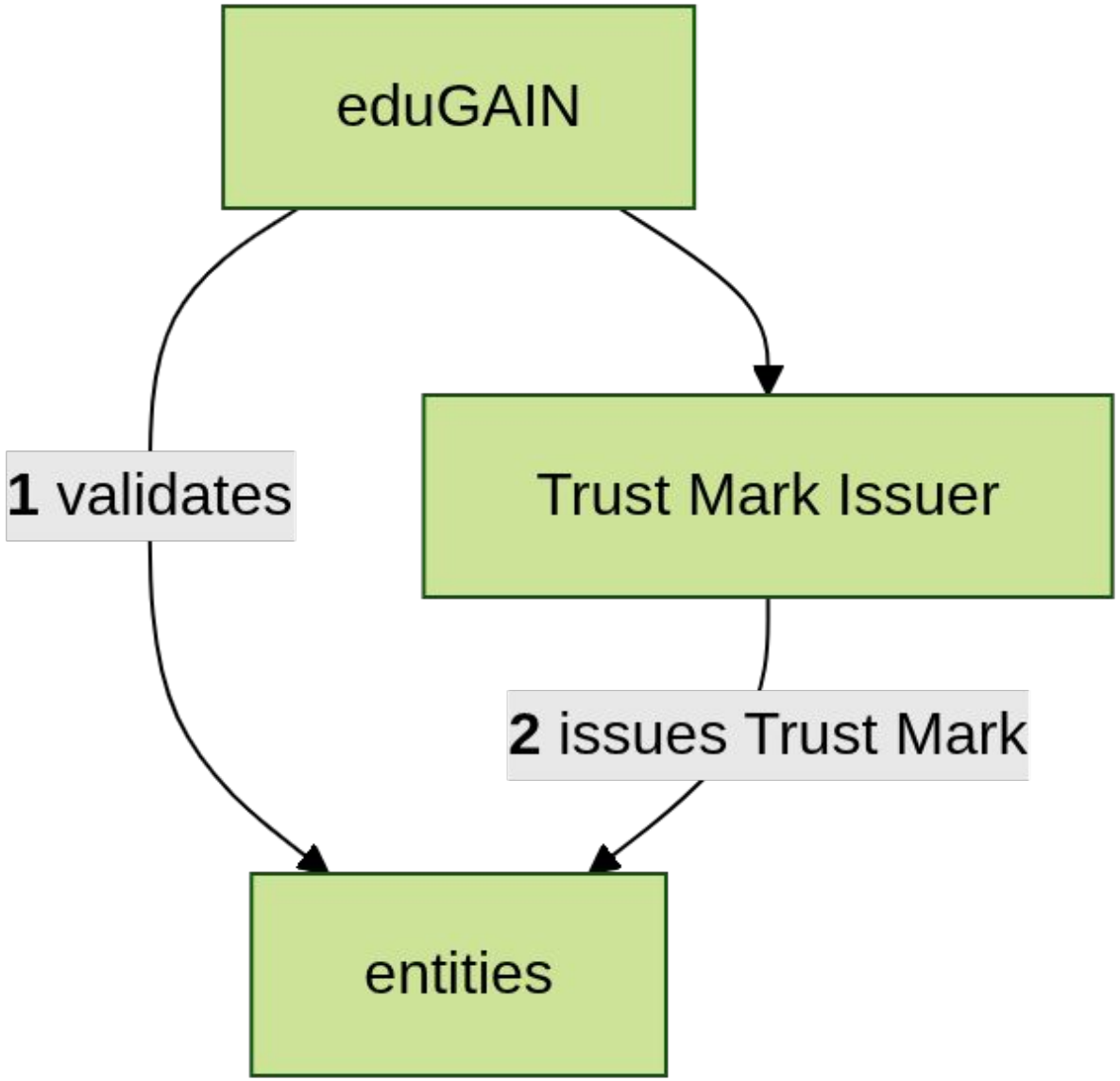




Principle 6

Principle 6: End entities that have eduGAIN as Trust Anchor must be validated against the eduGAIN OpenID Federation Profile. Additional validation is required to support other profiles, specifications and trust frameworks.

Requirement: Trust Marks convey trust information about the eduGAIN OpenID Federation profile and other profiles, specifications and trust frameworks.



eduGAIN OpenID Federation Pilot details

GN5-2

eduGAIN OpenID Federation Pilot

WHY

- Support OIDC and OAuth 2.0 in eduGAIN
- Provide an alternative to SAML

HOW

- OpenID Fed set up kit based on T&I Incubator Resolver
- **Define an** eduGAIN OpenID Federation Technological Profile

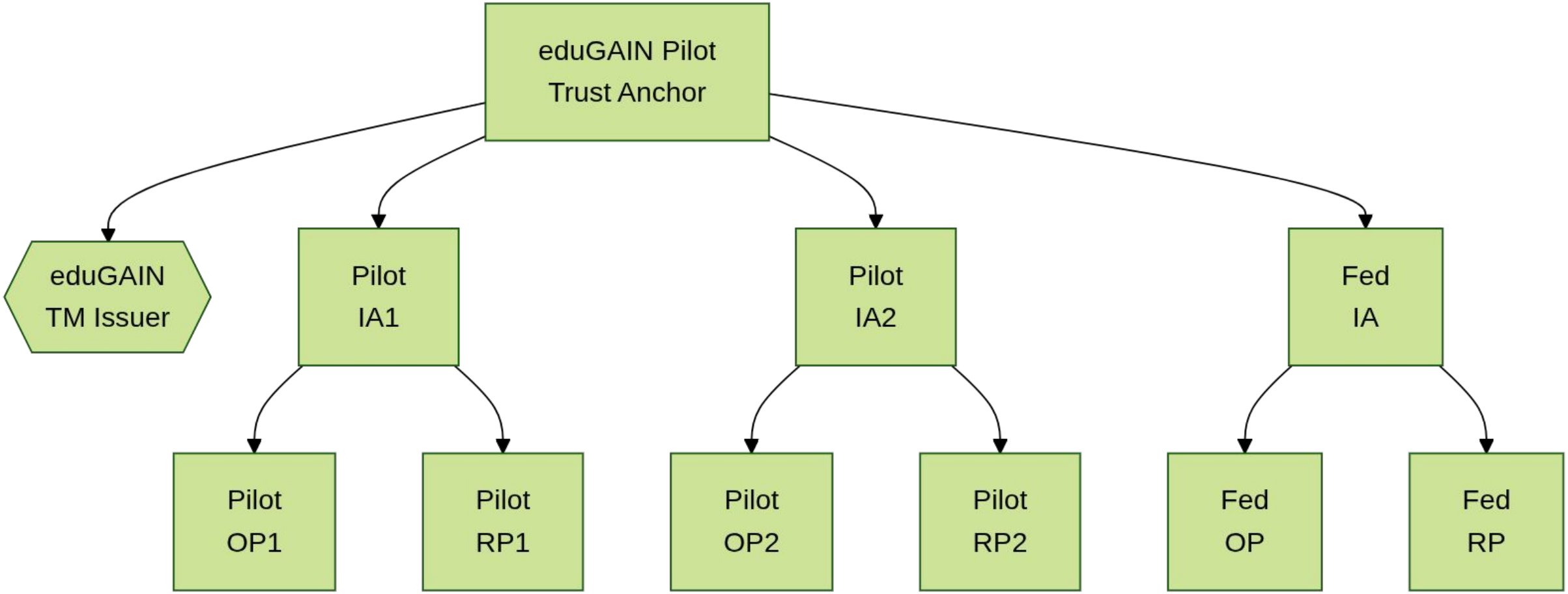
WHO

- eduGAIN service
- T&I Incubator
- Federation Operators

WHEN

- June 30th 2025
- 12 Months
- Biweekly calls

eduGAIN OpenID Federation Pilot: Infrastructure



KNOWHOW

- Have an overall comprehension of the OpenID Federation (OIDF) specification.
- Have working knowledge of OpenID Connect (OIDC) Providers and Relying Parties.
- Have a working knowledge of the current eduGAIN SAML Technological Profile.

OpenID Federation Specification

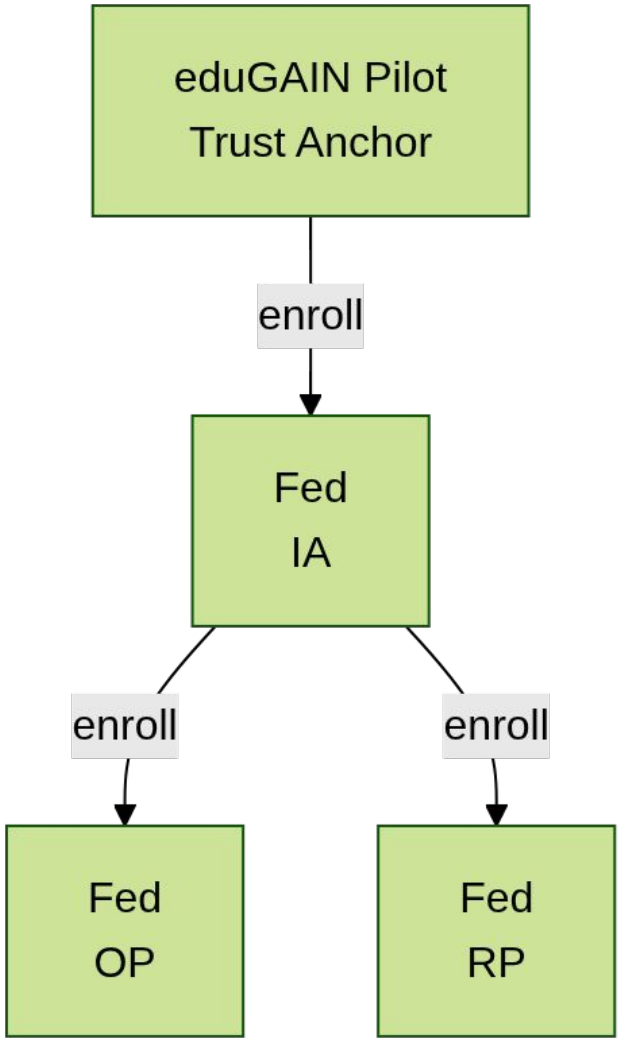
OpenID Connect Provider

OpenID Connect Relying Party

eduGAIN SAML Profile

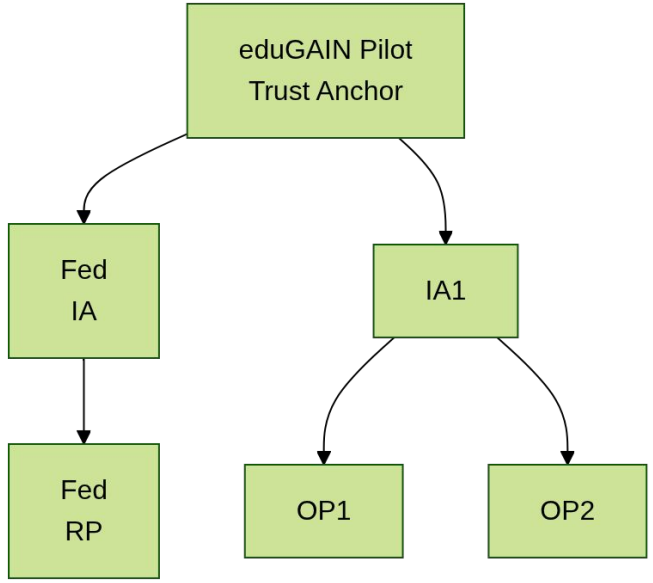
DevOps - part 1

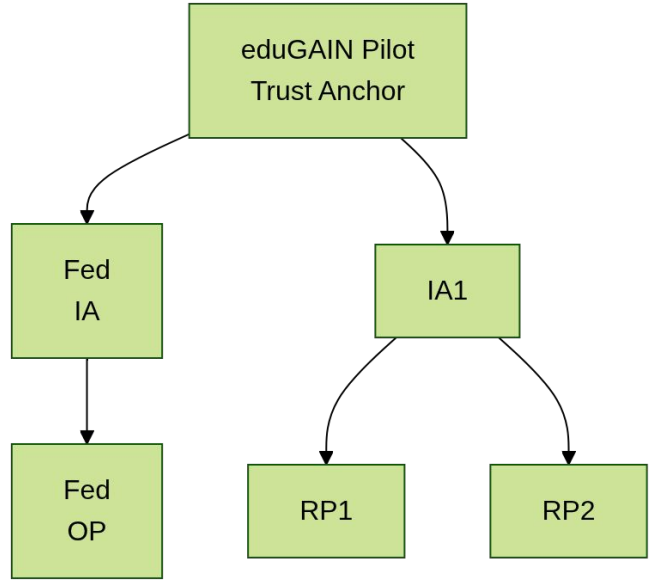
1. Set up a TA for their own federation, connect it as a subordinate (IA) to the eduGAIN TA.
2. Define a metadata policy.
3. Set up at least a test OIDF enabled OIDC Provider and connect it as a subordinate to the IA.
4. Set up at least a test OIDF enabled OIDC Relying party and connect it as a subordinate to the IA.



Use Cases - part 1

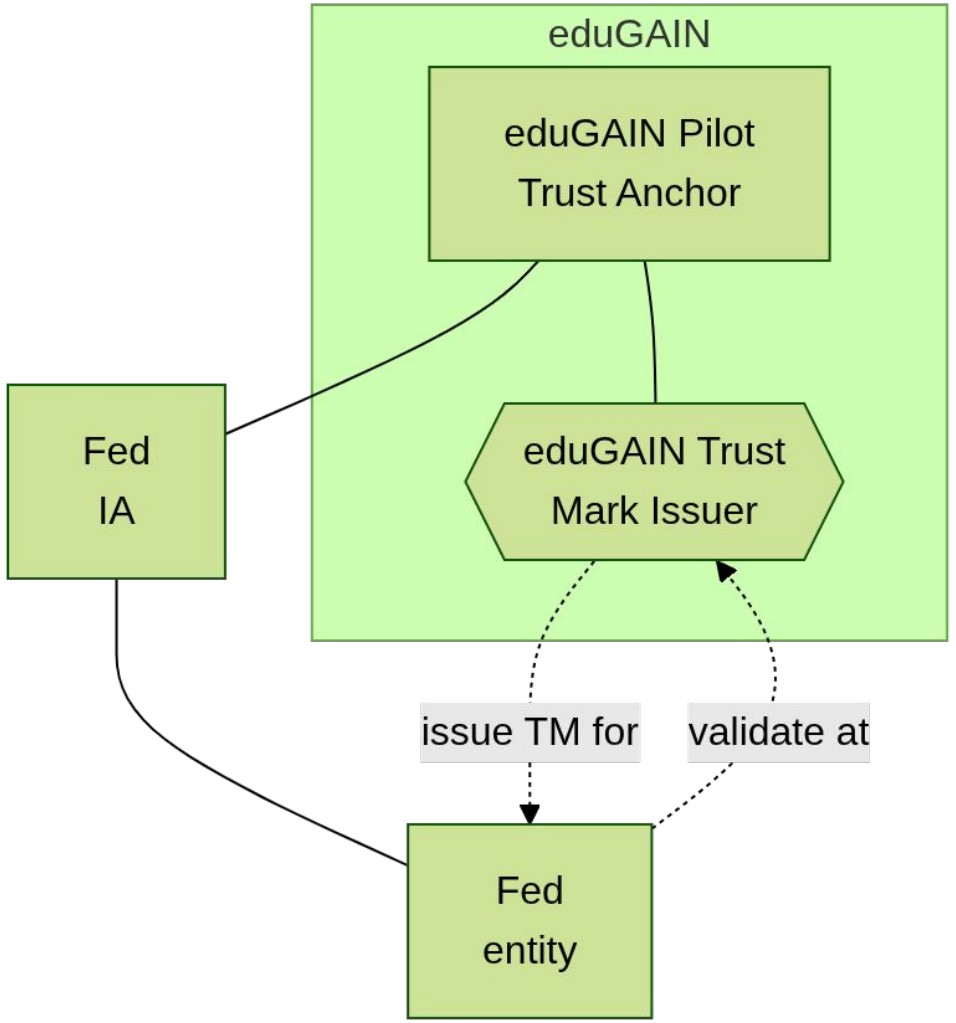
1. OpenID Federation Explicit Registration use case 1: Federation selected RP to Pilot OP1 and Pilot OP2.
2. OpenID Federation Automatic Registration use case 1: Federation selected RP to Pilot OP1 and Pilot OP2.
3. OpenID Federation Explicit Registration use case 2: Pilot RP1 and Pilot RP2 to a selected Federation OP.
4. OpenID Federation Automatic Registration use case 2: Pilot RP1 and Pilot RP2 to a selected Federation OP.





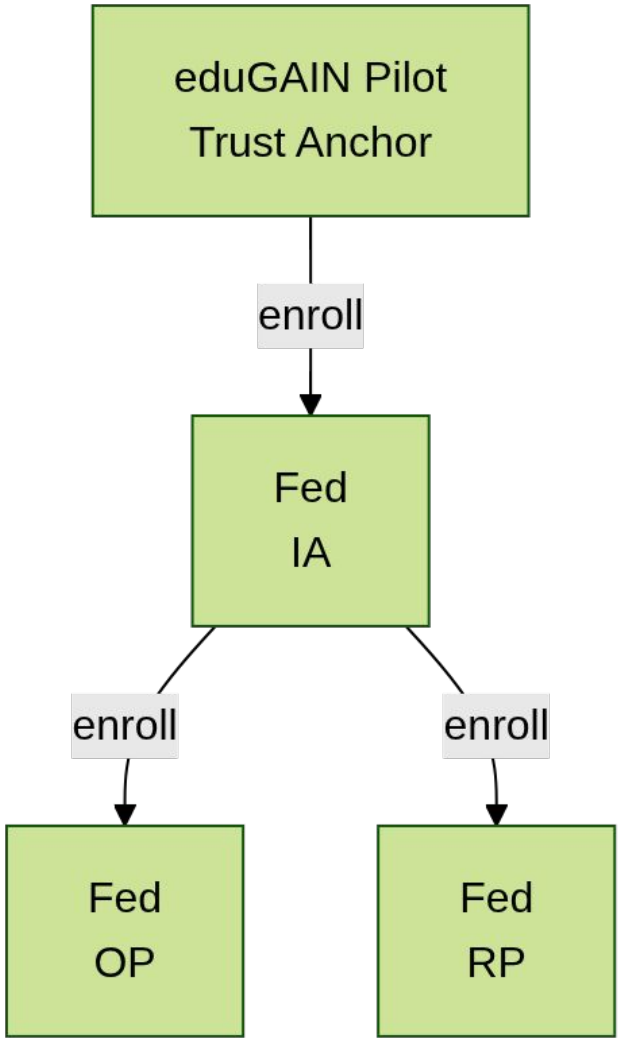
Use Cases - part 2

1. Validate entities to be “exported” to eduGAIN at the provided eduGAIN Trust Mark Issuer validator.
2. Retrieve the issued eduGAIN Trust Mark and refer to it in the entities’ statements.
3. Repeat **use cases - part 1** with Trust Marks.



DevOps - part 2

1. Define a Trust Mark for the Federation.
2. Set up a Trust Mark Issuer for the federation, connect it as a subordinate to the Federation Intermediate Authority.
3. Issue Trust Marks to the Federation's Entities.



Profile work

1. Provide feedback on the basic principles for the eduGAIN OpenID Federation Profile.
2. Participate in the definition of the eduGAIN OpenID Technological Profile.
3. Provides requirements and constraints.
4. Work with the eduGAIN CSIRT and the Federations' security community to define **security considerations** for the eduGAIN OpenID Federation profile.

https://wiki.geant.org/display/eduGAIN/eduGAIN+Technical+Profiles+Working+Group

eduGAIN OpenID Federation Pilot - Status

GN5-2

eduGAIN OpenID Federation Pilot: Participants

Federation	Representative	Status	Trust Anchor
AAF	Russell Ianiello	In Progress	https://ta.dev.aaf.edu.au
UK Federation	Phil Smart	Registered	https://ta.pilot.ukfederation.org.uk
SWAMID	Björn Mattsson	Registered	https://oidf-dco-poc-ta-1.swamid.se
RCTSaai	Esmeralda Pires	Registered	https://ta-fccn.qua.rctsaai.pt
CAF	Tom Vitez		
ArnesAAI	Tim Trojner Hlade		
DFN-AAI	Wolfgang Pempe	Registered	https://ia1.oidfed-pilot.aai.dfn.de
Haka	Sami Silen		
eduid.hu	Czier Norbert	Registered	https://ta.eduid.hu
IDEM	Davide Vaghetti	In progress	

eduGAIN OIDF Pilot on https://italia.github.io/openid-federation-browser/main/

eduGAIN OpenID Federation Pilot: wiki page

https://wiki.geant.org/x/c4DrPw

Pilot Participation

Pilot participation is reserved to current eduGAIN Participants as listed on the eduGAIN Members page, https://technical.edugain.org/status. eduGAIN delegates and deputies can nominate or acknowledge the participation of anyone on their behalf. Here you can find information on how to su
entities requirements and technical information: ht

Participation requests

Requests for participation should be sent by the eduGAIN delegate or deputy to support@edugain.org with the following content:

- eduGAIN Participant name.
- The Entity Identifier of the Federation Trust Anchor.
- The Federation Trust Anchor public key in PEM format can be communicated in one of the following way:

signing is enabled with trusted (CAB/Forum) certificates, or
B/Forum) certificates and pointing to the Federation Trust Anchor
part of the URL is expected to insist on a domain in the remit of

Federations set up

The eduGAIN pilot team will process each request with the following process:

1. Verify that the request is complete and the PEM key is valid.
2. Query the configuration endpoint to obtain the Entity Configuration of the Federation Trust Anchor. The configuration endpoint is determined by concatenating the string `/.well-known/openid-federation` to the Entity Identifier.
3. Verify that the Entity Configuration is signed with the same key communicated in the request.
4. Verify that the federation signing key contained in the Entity Configuration is the same key communicated in the request.
5. Verify that the Federation Trust Anchor is compliant with all the requirements listed above.
6. If everything is ok, add the Federation Trust Anchor as a subordinate of the eduGAIN OIDF Pilot Trust Anchor.
7. Communicate to the requester that all is good and they've been officially on boarded to the pilot.

eduGAIN OpenID Federation Pilot: Participants meetings

https://wiki.geant.org/x/c4DrPw

- Every other Monday 14:00 PM CET/CEST (full meeting schedule on the wiki page)
- Meeting Notes
  - https://docs.google.com/document/d/1eiigmnxUF6mmueaedCq6fSKeSOKtyoscw5EZoTHEOBM
- Participants mailing list:
  - https://lists.geant.org/sympa/info/edugain-oidf-pilot

eduGAIN OpenID Federation Pilot: github repository

https://github.com/GEANT/edugain-oidf-pilot

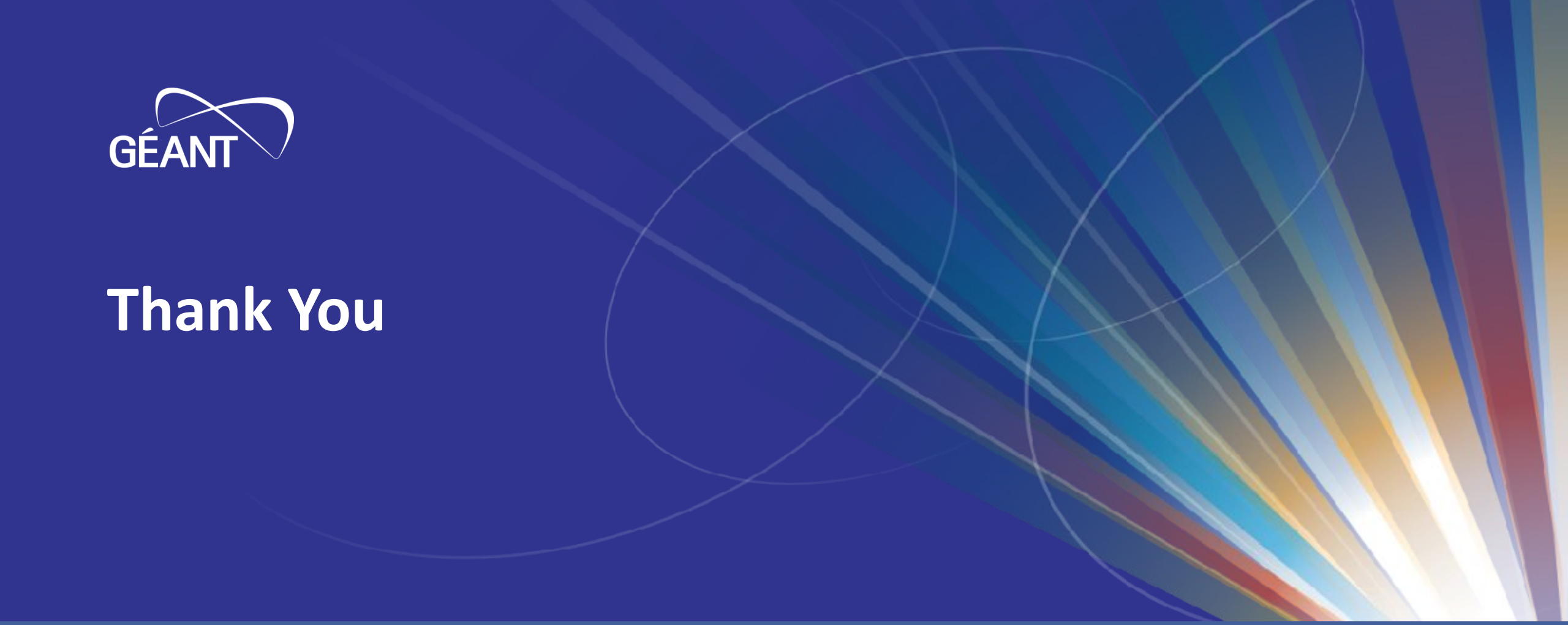
- Trust Anchors requirements
- Docker set up and configuration:
  - eduGAIN Trust Anchor
  - eduGAIN Intermediate 1 and 2
  - eduGAIN RP1

eduGAIN Pilot Entities Configurations

Here you can find some example Entity Configurations provided by the current eduGAIN OpenID Federation Pilot entities.

- eduGAIN OpenID Federation Pilot Trust Anchor - https://ta.oidf-pilot.edugain.org


```
{
  "exp": 1752246223.7172408,
  "iat": 1752159823.7172408,
  "iss": "https://ta.oidf-pilot.edugain.org",
  "jwks": {
    "keys": [
      {
        "alg": "ES256",
        "crv": "P-256",
        "kid": "xcXdyJ2_7cOd05QIqfpdrb3j5-mYFw8dqdcqzEh0lUw",
        "kty": "EC",
        "use": "sig",
        "x": "hh5u_VrRXLaXNAdZX2CQWNAXFqgDCYhYGY1y1qbx9Q8",
        "y": "qNPeoZOuVv-I6e-oUt9imwV6TSt-ymTaaW2Mrlgo0JQ"
      }
    ]
  },
  "lighthouse_version": "0.5.1",
  "metadata": {
    "federation_entity": {
      "contacts": [
        "support@edugain.org"
      ],
      "display_name": "eduGAIN OIDF Pilot Trust Anchor",
      "federation_enroll_endpoint": "https://ta.oidf-pilot.edugain.
      "federation_fetch_endpoint": "https://ta.oidf-pilot.edugain.o
      "federation_list_endpoint": "https://ta.oidf-pilot.edugain.or
      "federation_resolve_endpoint": "https://ta.oidf-pilot.edugain
      "organization_name": "eduGAIN",
      "organization_uri": "https://edugain.org"
    }
  },
  "sub": "https://ta.oidf-pilot.edugain.org"
}
```



Thank You

www.geant.org

Co-funded by
the European Union