



eduGAIN OpenID Federation Pilot

Davide Vaghetti (GARR)

June 18th 2025, GN5-2 WP5 Infoshare

Public (PU)

GN5-2



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.



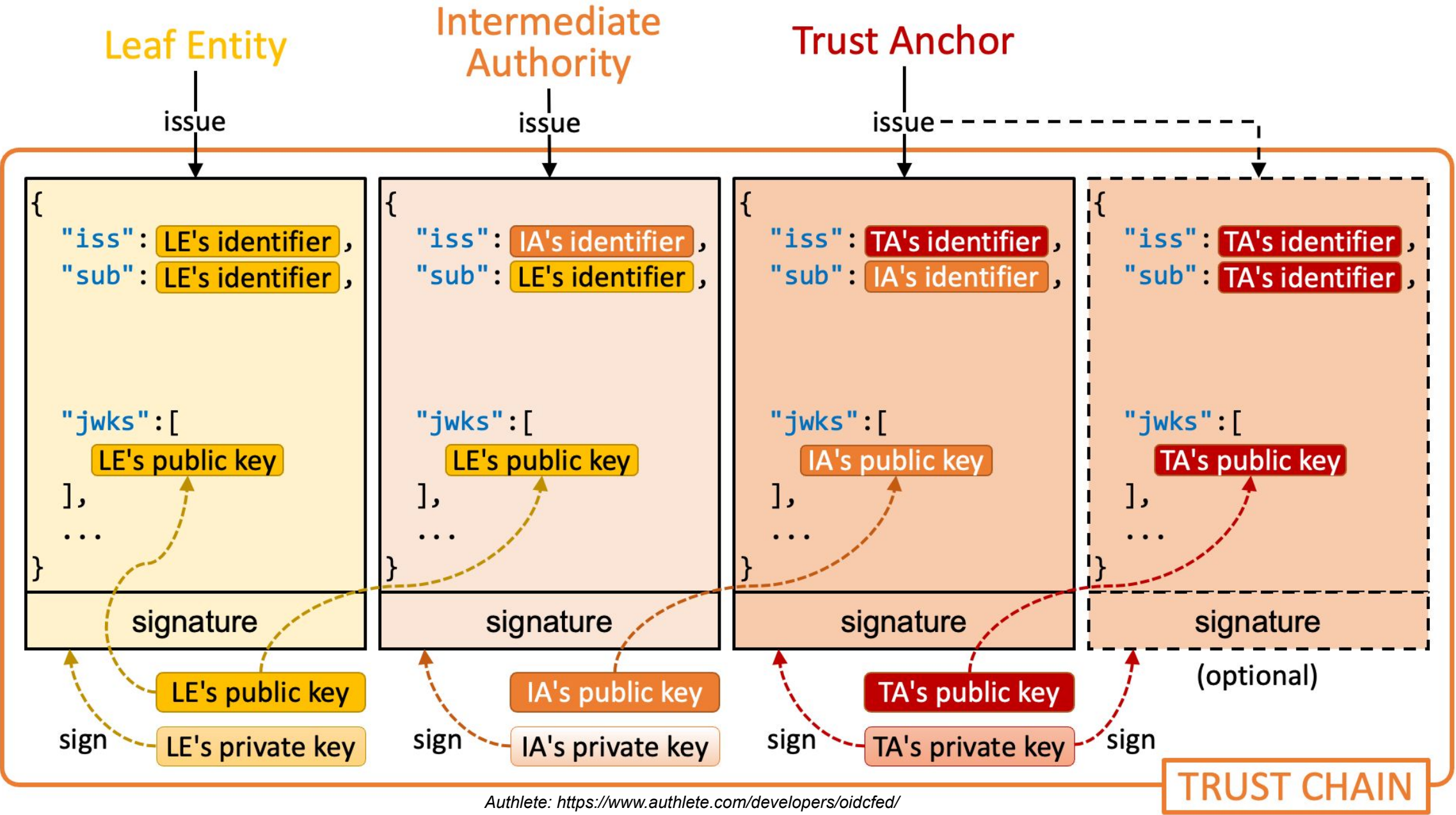
The eduGAIN Service and the T&I Incubator run a Proof of Concept activity to develop tools to build OpenID Federations for Research and Education.

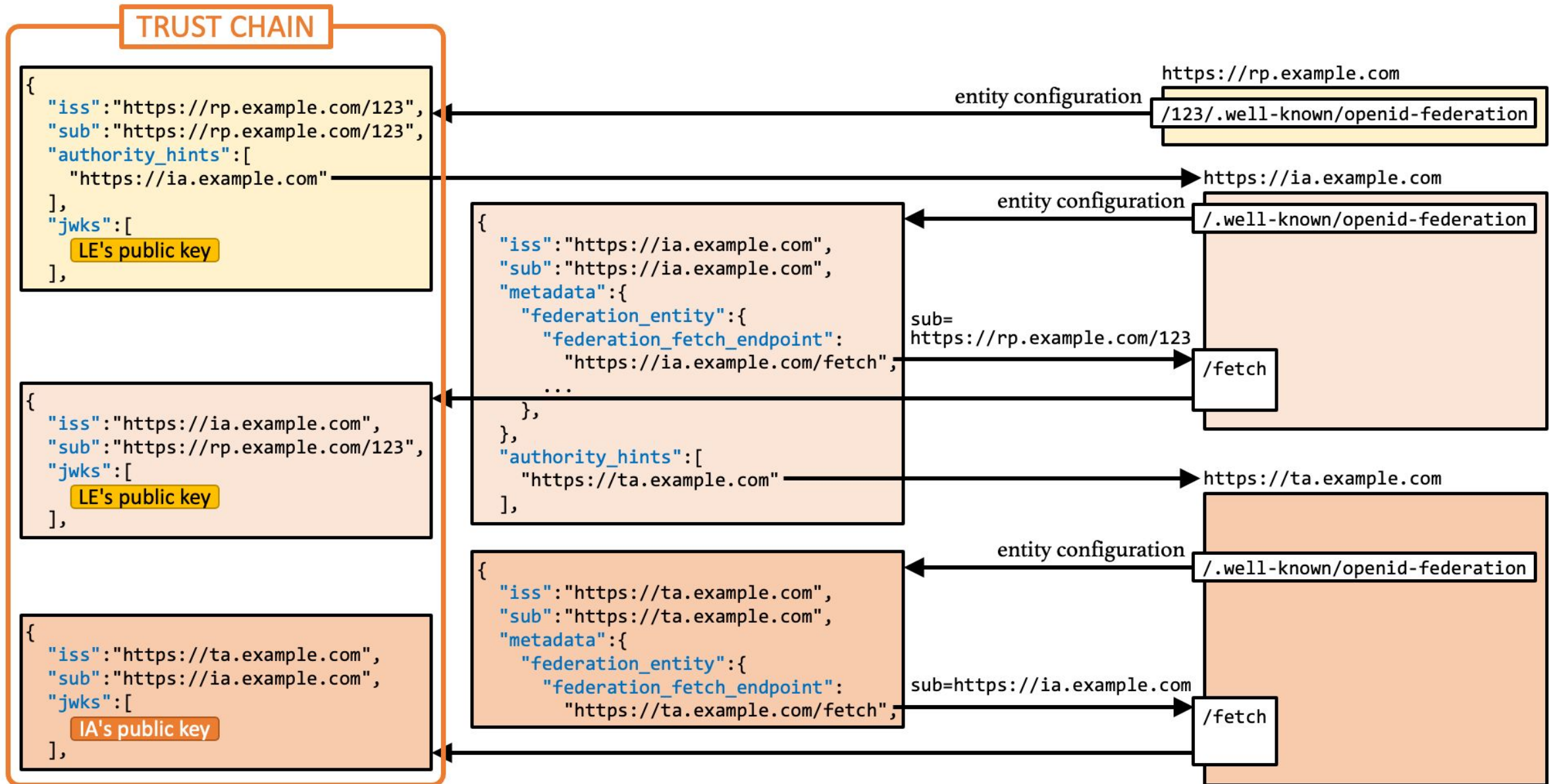
OpenID Federation bits and pieces

- **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.

| | |
|------------------------|--|
| 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. |
| Trust Anchor | An Entity that represents a trusted third party. |
| 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. |
| 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. |
| Resolver | An endpoint that provides Resolved Metadata and Trust Marks to another Entity. |

| | |
|------------------------|---|
| Entity Statement | Metadata |
| Trust Anchor | A Federation or an Inter Federation (eduGAIN) |
| Intermediate Authority | N/A ~ A federation in the context of eduGAIN. |
| Leaf Entity | An IdP or an RP. |
| Trust Chain | N/A ~ current eduGAIN and federations have only one level of trust (one signature). |
| Trust Mark | N/A |
| Resolver | An MDQ Service |





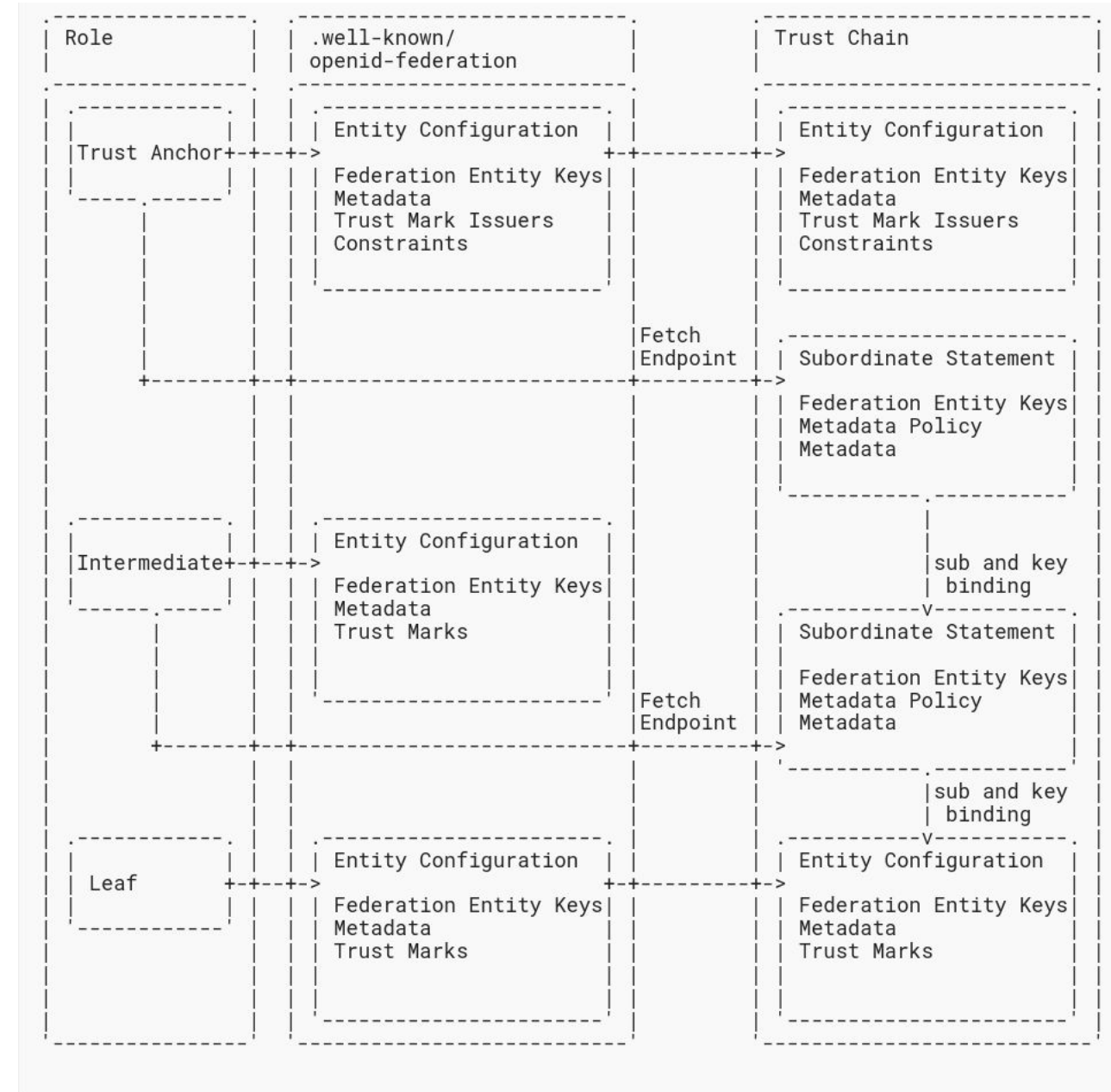


eduGAIN OpenID Federation profile principles

Principle 1

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

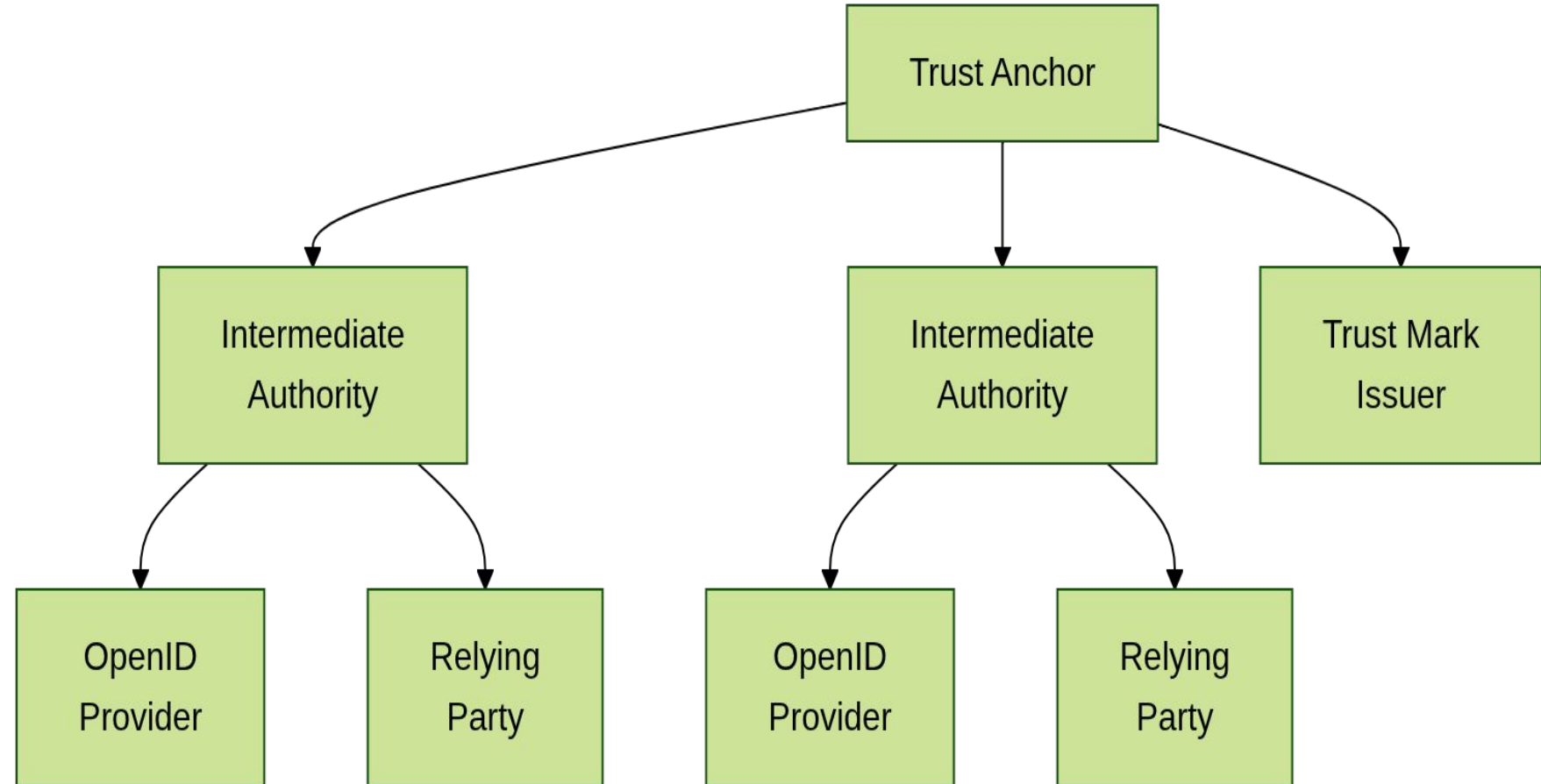
Requirement: Trust Chains is the basic technical trust of the federation.



Principle 2

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

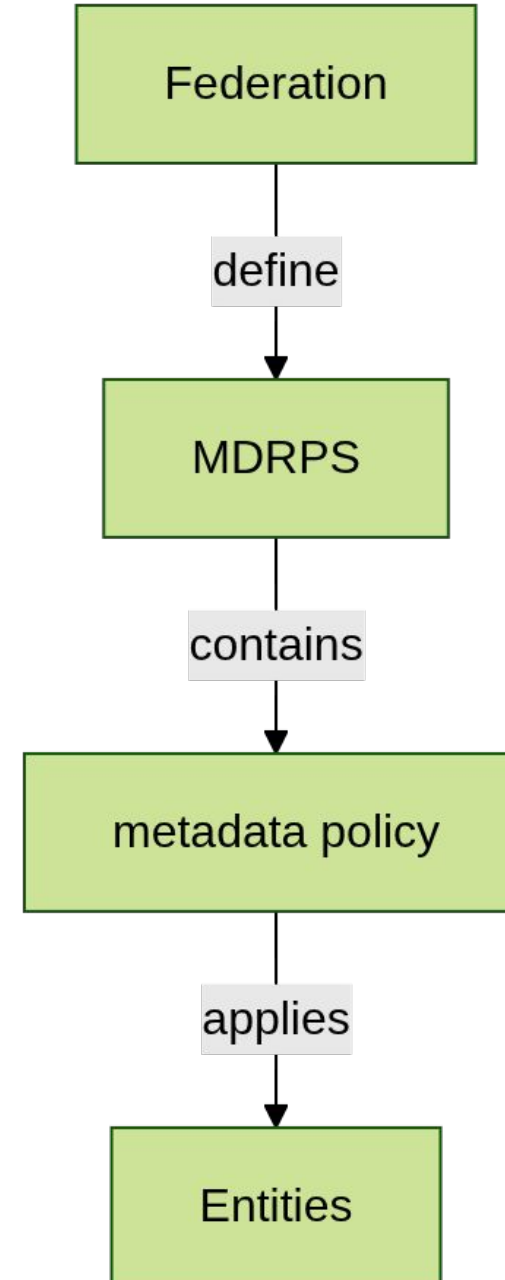
Requirement: All Immediate Subordinate Entities to the eduGAIN Trust Anchor MUST have the federation_entity entity type, such as Intermediate Authorities and Trust Mark Issuers.



Principle 3

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

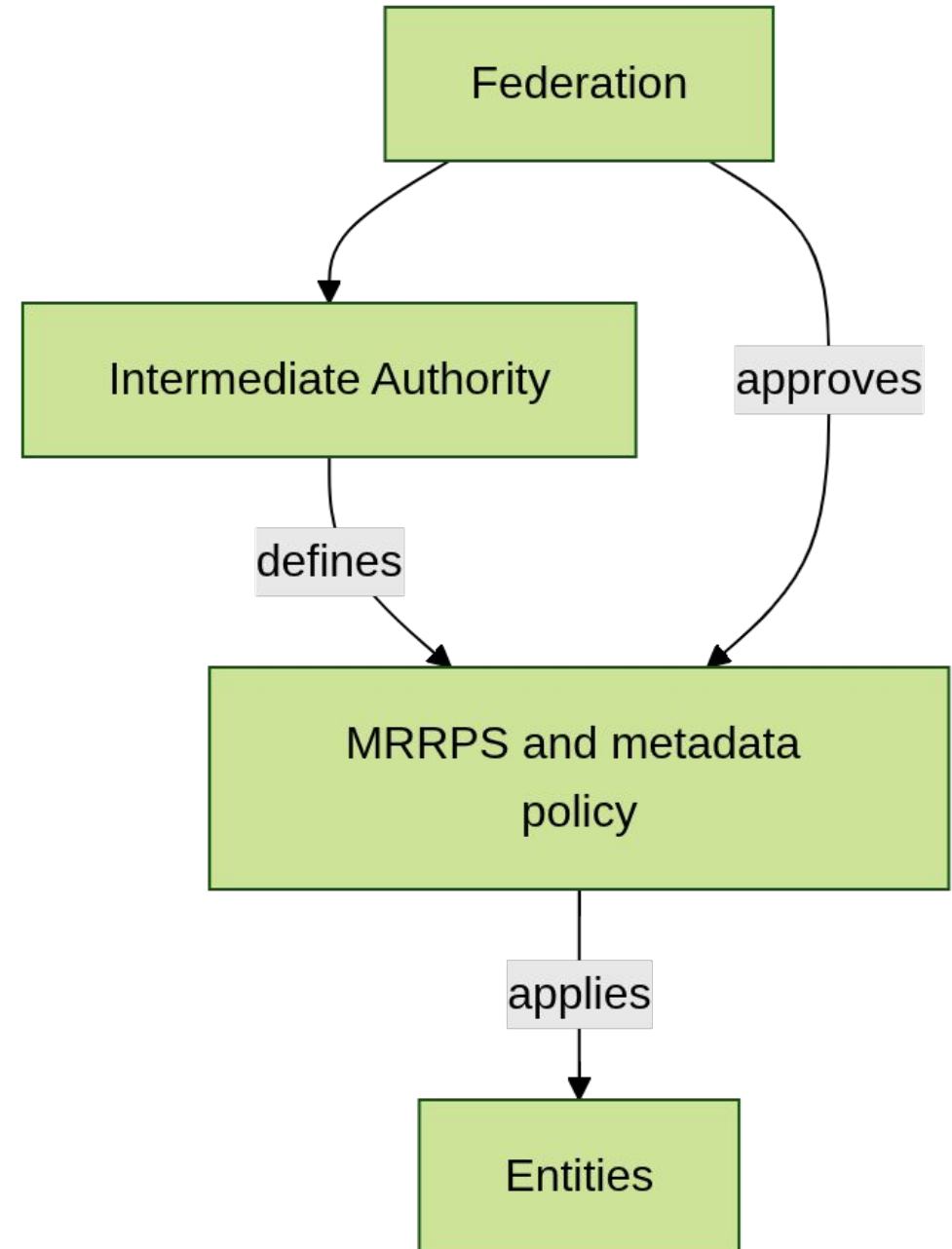
Requirement: An Immediate Subordinate Entity to the eduGAIN Trust Anchor MUST be a Trust Anchor for its subordinates and be operated by a federation operator. MUST provide a Metadata Registration Practice Statement (MDRPS). The MDRPS must contain metadata policies, including a description of trust chain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

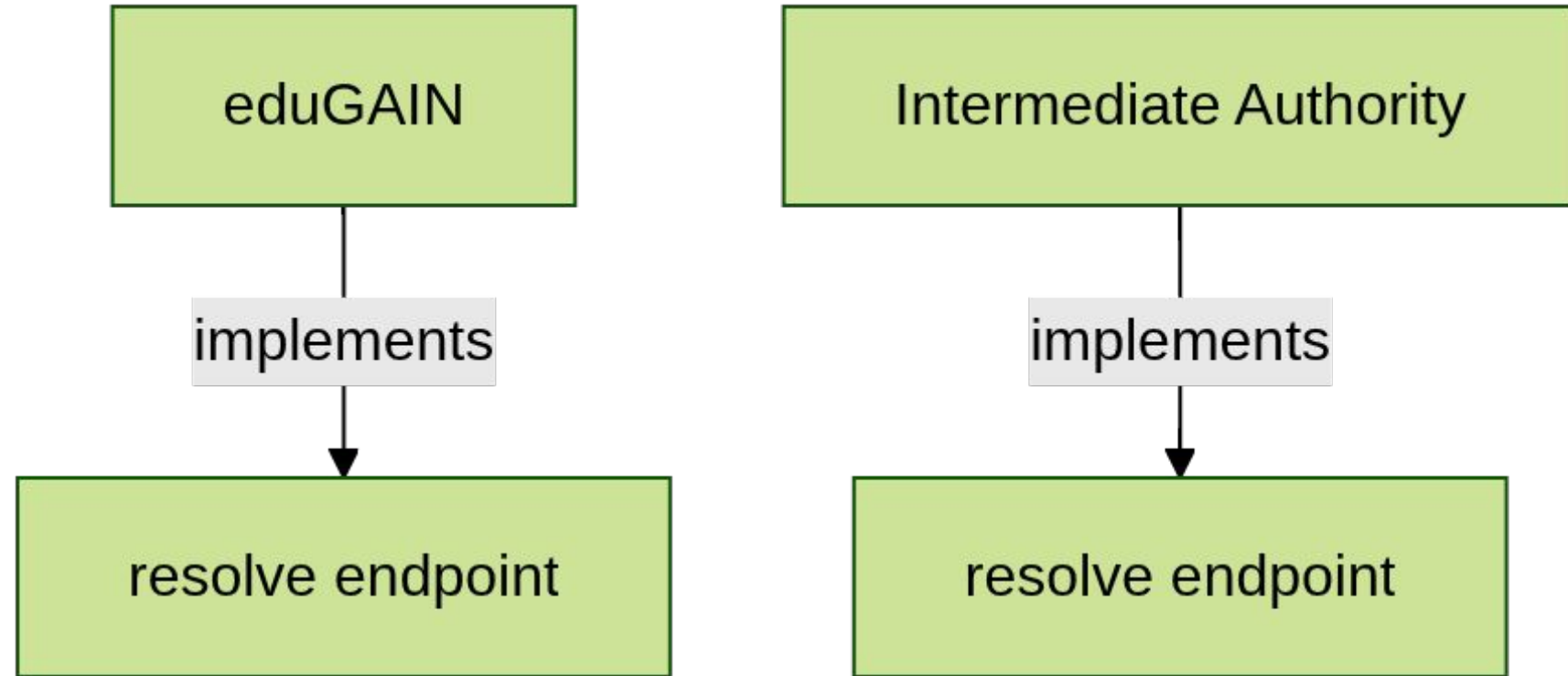
Requirement: Intermediate Authorities subordinate to a federations MUST provide a Metadata Registration Practice Statement. The MDRPS MUST contain metadata policies, including a description of trust chain constraints for subordinates, and MUST be approved by the federation.



Principle 5

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

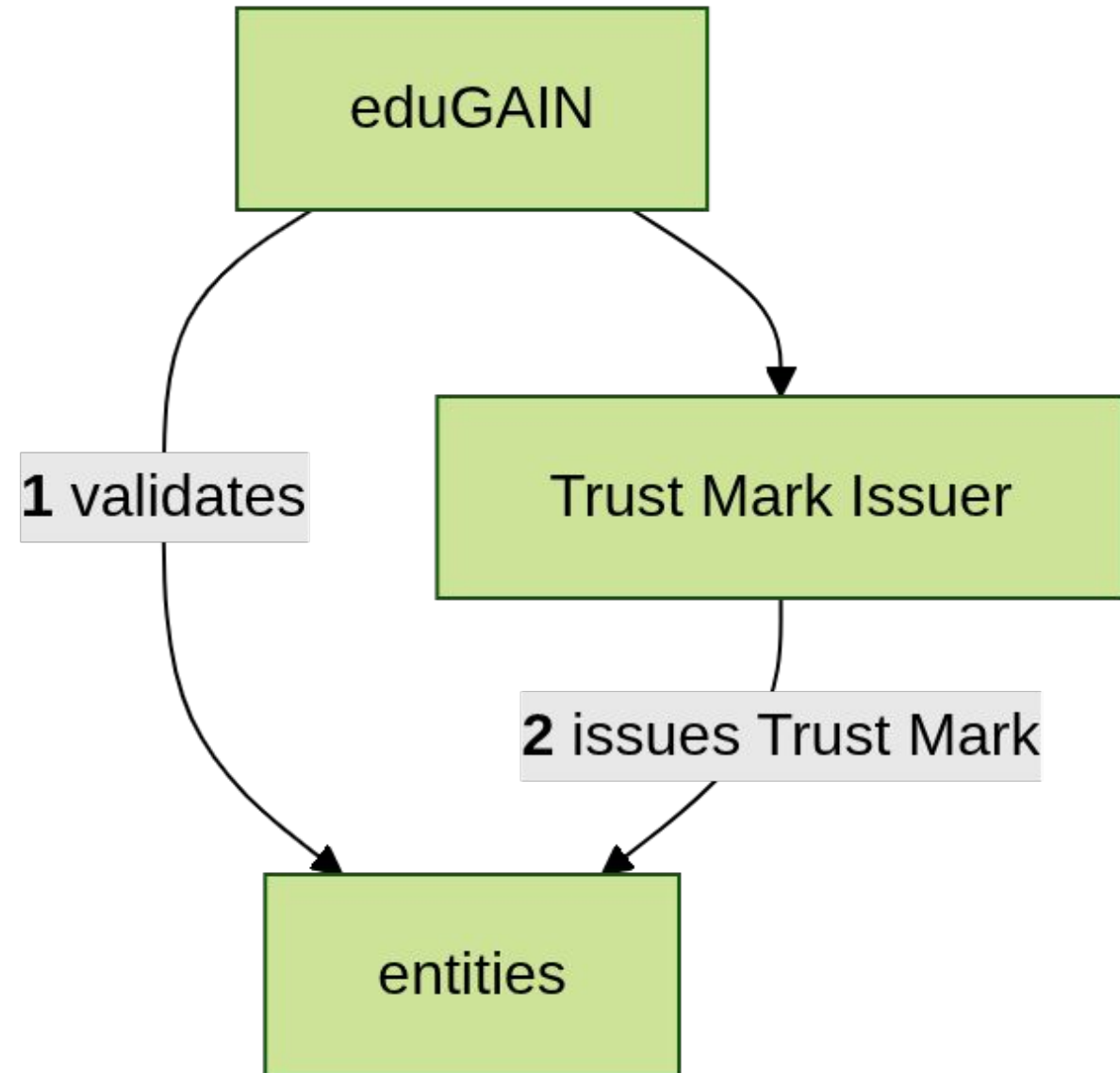
Requirement: eduGAIN and Intermediate Authorities subordinate to the eduGAIN TA MUST provide a resolve endpoint.



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



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



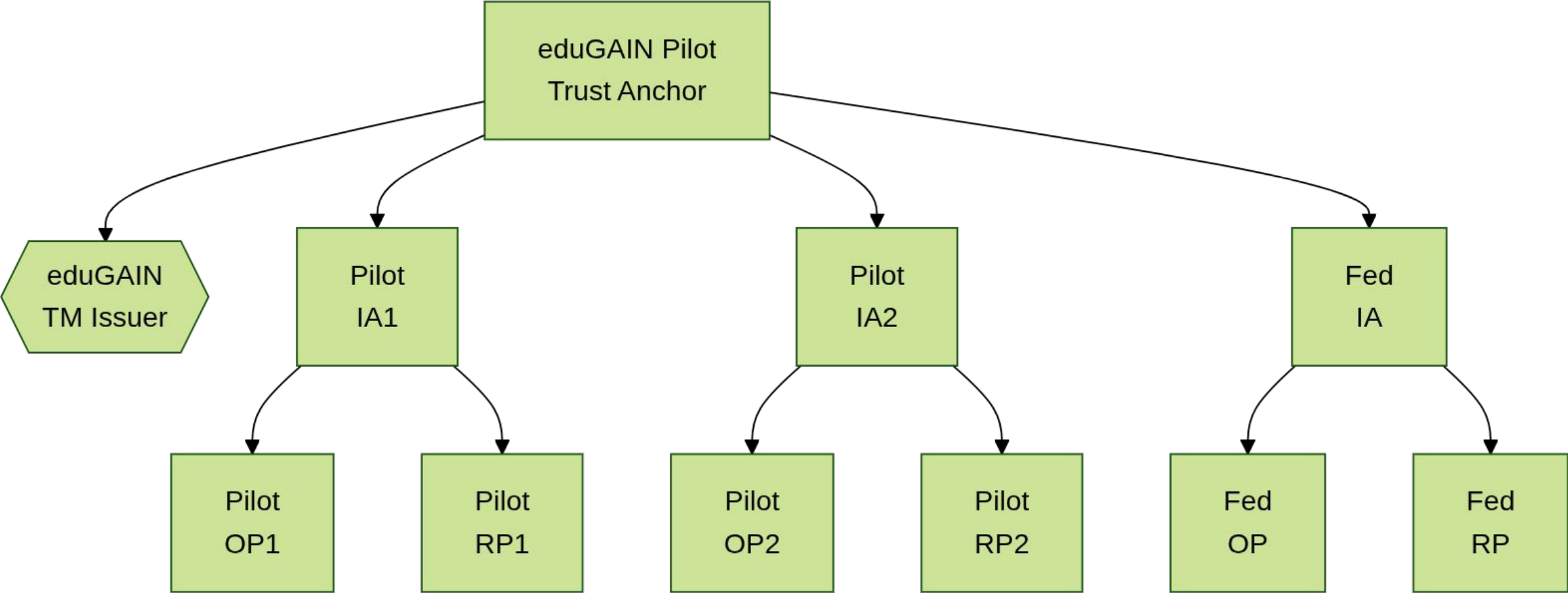
WHO

- eduGAIN service
- T&I Incubator
- Federation Operators



WHEN

- June 30th 2025
- 12 Months
- Biweekly calls





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

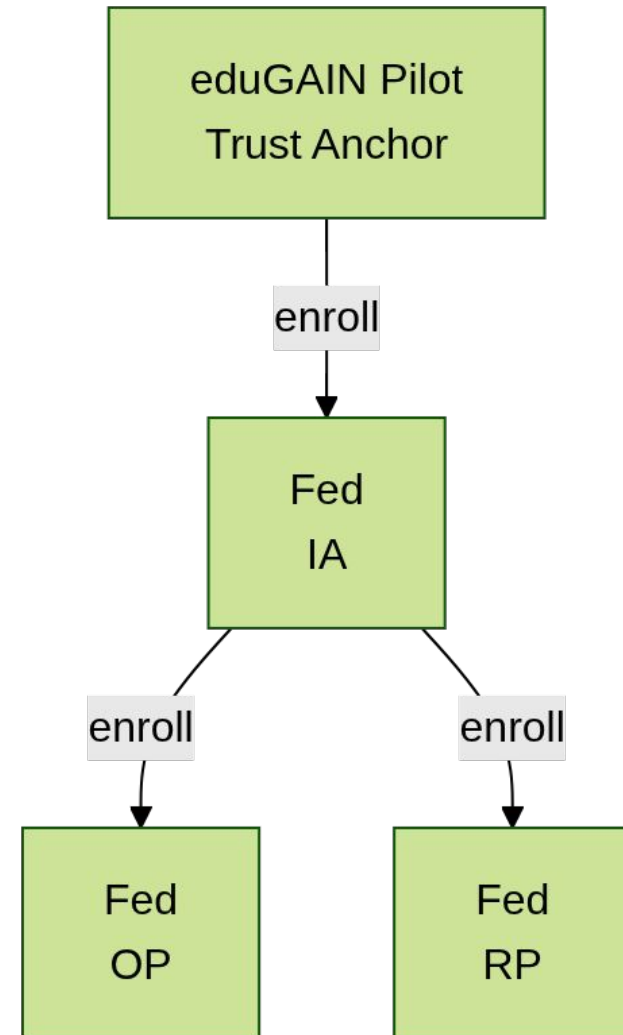
OpenID Connect Relying
Party

eduGAIN SAML Profile



DevOps - part 1

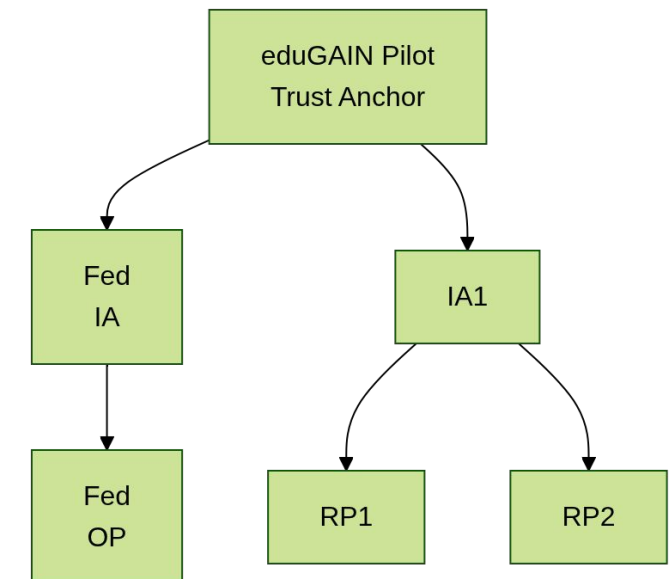
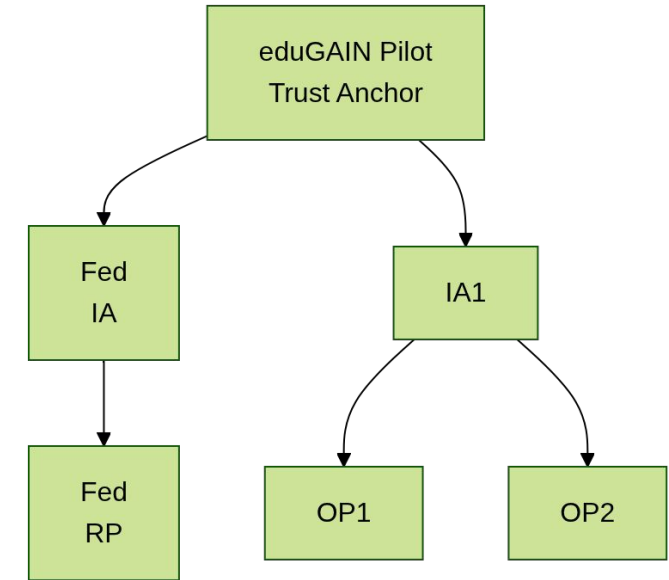
1. Set up a TA for their own federation, connect it as a subordinate (IA) to the eduGAIN TA.
2. Define a metadata policy.
3. Set up at least a test OIDF enabled OIDC Provider and connect it as a subordinate to the IA.
4. Set up at least a test OIDF enabled OIDC Relying party and connect it as a subordinate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





Use Cases - part 1

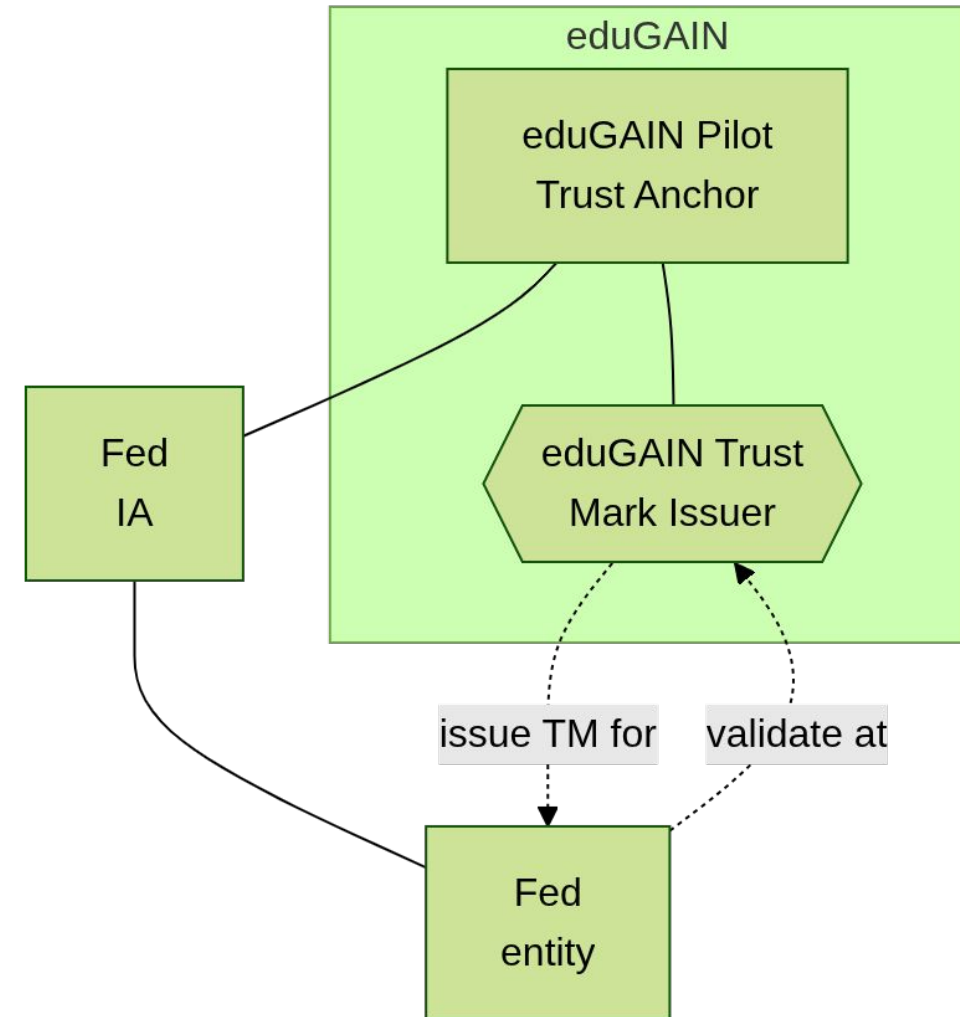
1. OpenID Federation Explicit
Registration use case 1: Federation selected RP to Pilot OP1 and Pilot OP2.
2. OpenID Federation Automatic
Registration use case 1: Federation selected RP to Pilot OP1 and Pilot OP2.
3. OpenID Federation Explicit
Registration use case 2: Pilot RP1 and Pilot RP2 to a selected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





Use Cases - part 2

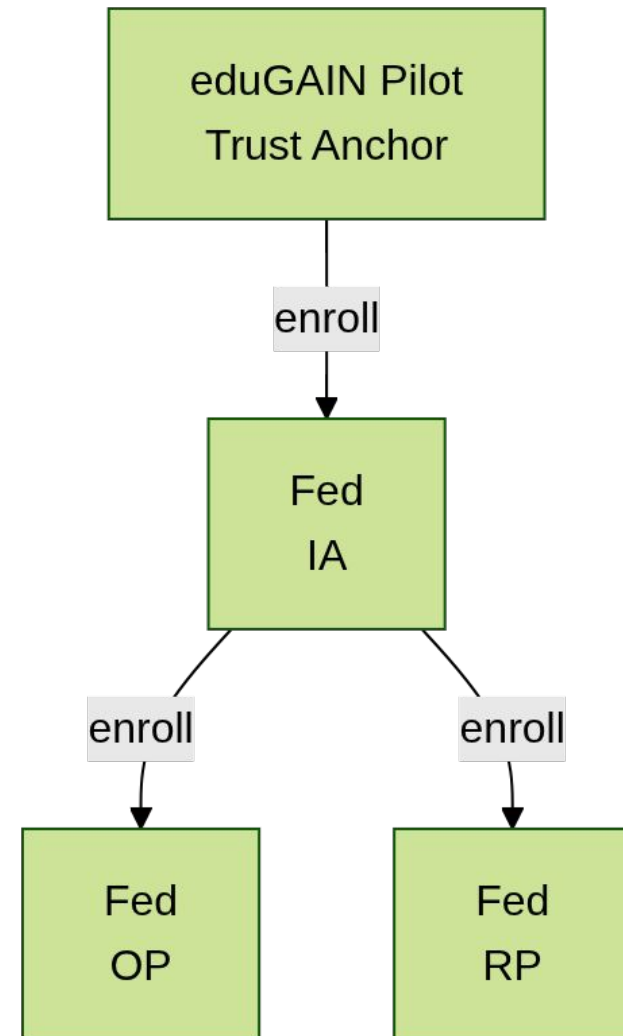
1. Validate entities to be “exported” to eduGAIN at the provided eduGAIN Trust Mark Issuer validator.
2. Retrieve the issued eduGAIN Trust Mark and refer to it in the entities’ statements.
3. Repeat **use cases - part 1** with Trust Marks.





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>

- June 23rd 2025 - eduGAIN OIDF Pilot space on the eduGAIN wiki.
- June 30th 2025 - eduGAIN OIDF Pilot github repository:
 - All the scripts and docker images used to set up the pilot infrastructure and entities will be provided.
- June 30th 2025 - Official eduGAIN OIDF Pilot start: write to support@edugain.org to join the pilot.
- Biweekly call to assess the ongoing work.



Thank You

www.geant.org



Co-funded by
the European Union