# eduGAIN OpenID Federation
## *Work in progress*

**Davide Vaghetti (GARR)**
*eduGAIN Service Owner*

Trust and Identity Infoshare for NRENs:
Wallets ( Virtual )

www.geant.org

# Agenda

- eduGAIN’s Overview
- OpenID Federation quick overview
- eduGAIN OpenID Federation
- OpenID Federation and the wallet ecosystem

# eduGAIN

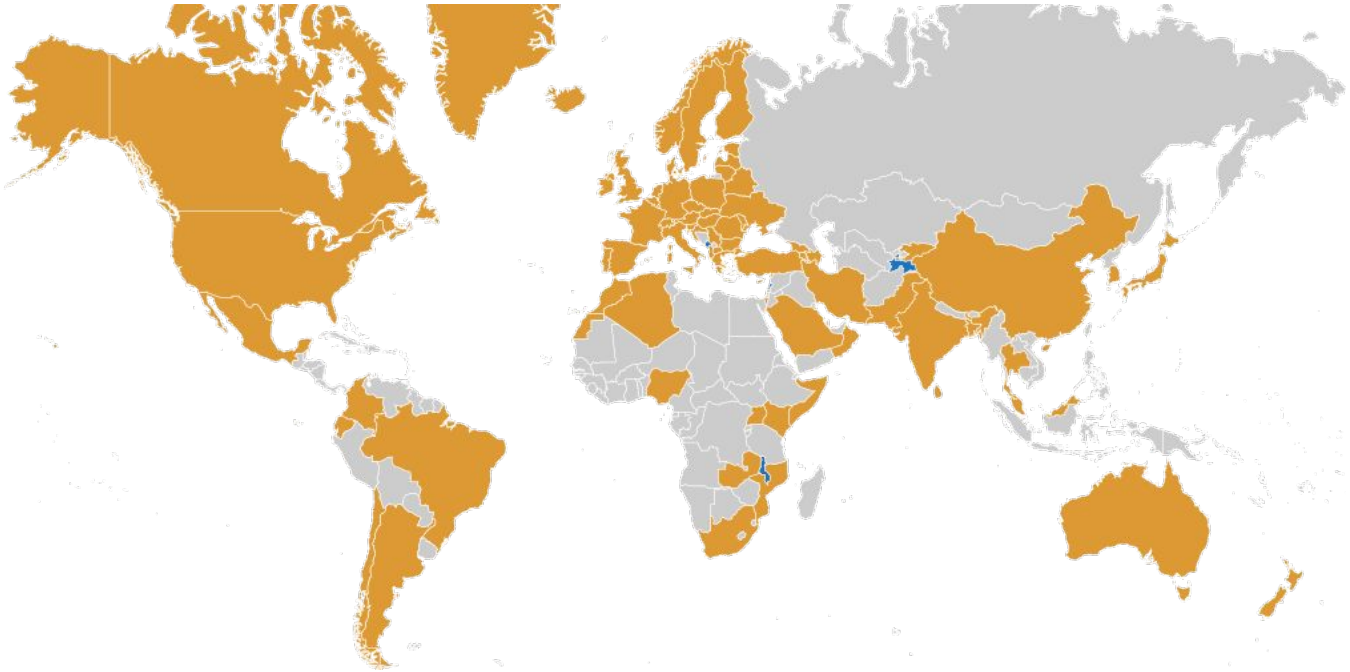
*"eduGAIN **interfederation service** connects identity federations around the world, simplifying **access** to content, services and resources for the **global** research and education community"*





GÉANT

# eduGAIN Global Coverage



**79** Federations

**9442** Entities

**5712** Identity Providers

**3749** Service Providers

*Last update September 7th 2024*

# eduGAIN Technological Profiles: SAML 2.0

**An open standard**

**Extremely successful and adopted**

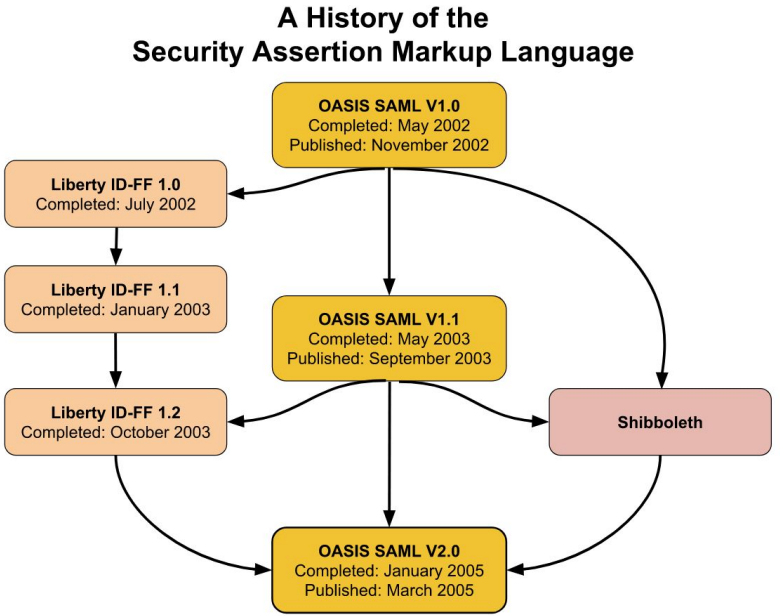
**87 R&E Federations + eduGAIN**

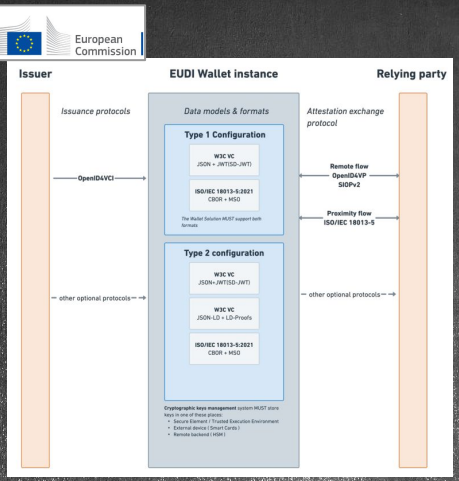
**Legacy Protocol: no new devs in the last 5 years**

**No support for Mobile App, REST/API flows, etc.**

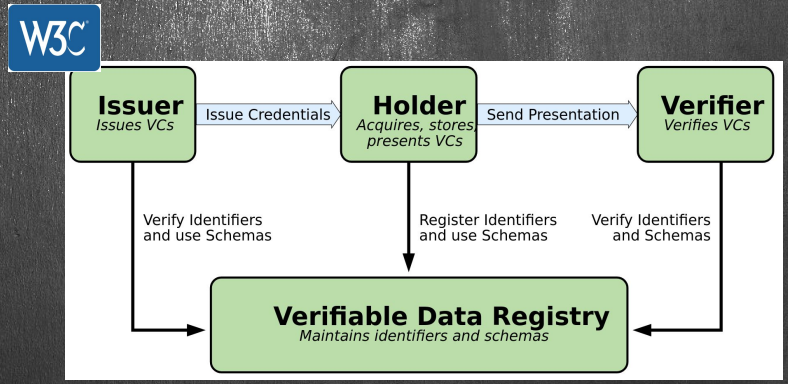
**Decentralized identity and Verifiable Credentials?**

**Post-quantum cryptography support?**










# OpenID Federation for eduGAIN

# OpenID Federation

OpenID® *An OpenID Foundation specification*

- Implementer Draft 38 of version 1.0 (published on Aug 19th)
- 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



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

# OpenID Federation 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*

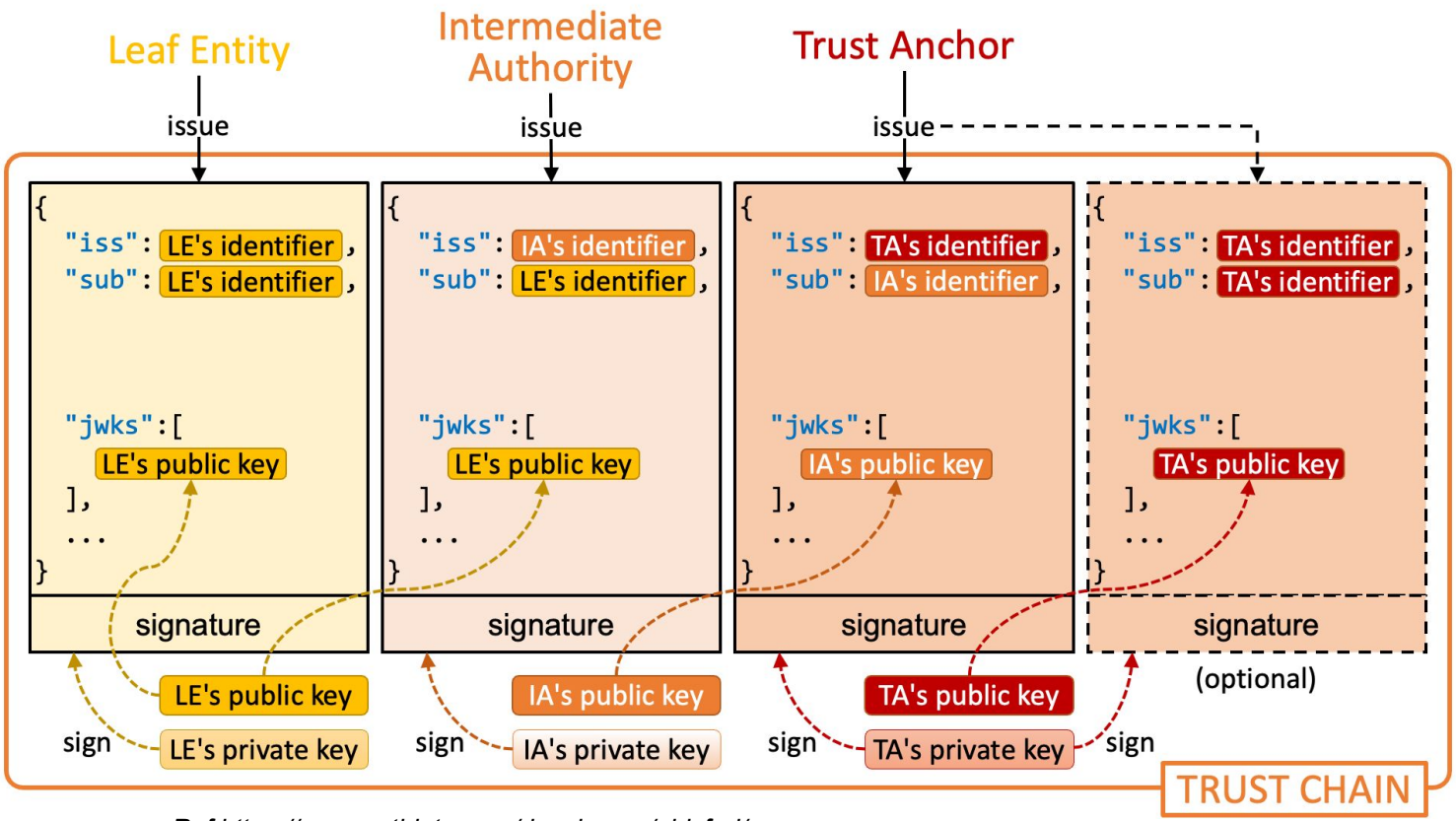
# OpenID Federation Entity Configuration

**Leaf's Entity Configuration**


```
{
  "alg": "ES256",
  "kid": "NFM1WUViUl",
  "typ": "application/entity-statement+jwt"
}
.
{
  "exp": 1649590602,
  "iat": 1649417862,
  "iss": "https://rp.example.org",
  "sub": "https://rp.example.org",
  "jwks": {"keys": [    {
                "kty": "EC",
                "kid": "NFM1WUViUl",
                "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



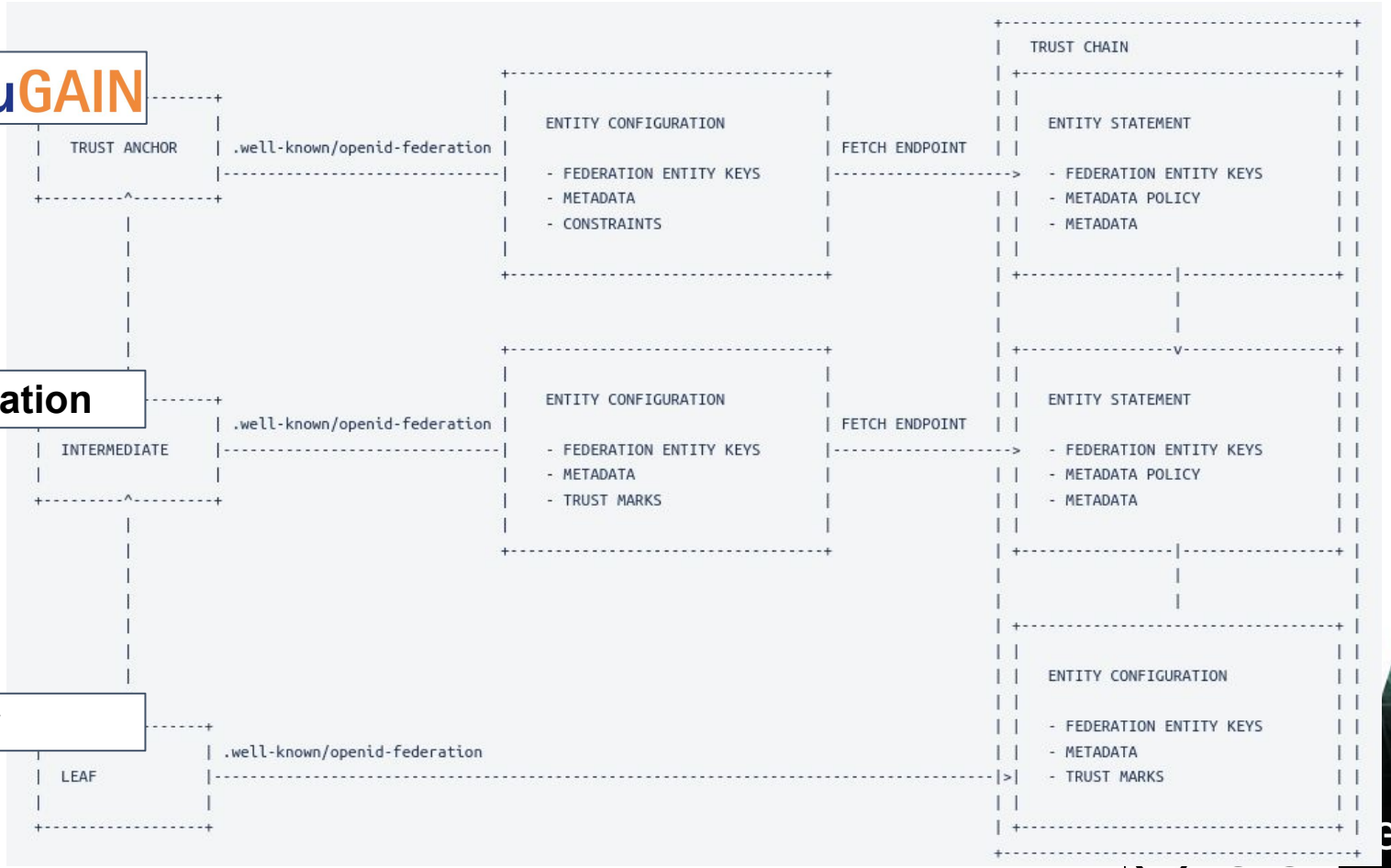

*Ref https://www.authlete.com/developers/oidcfed/*





GÉANT

# An eduGAIN OIDC Federation Trust Flow



# 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 Resolver
- **DRAFT** eduGAIN OpenID Federation Technological Profile

## WHO

- eduGAIN service and T&I Incubator
- Federation Operators
- RC AAIs
- Any interested party is welcome to join

## WHEN

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

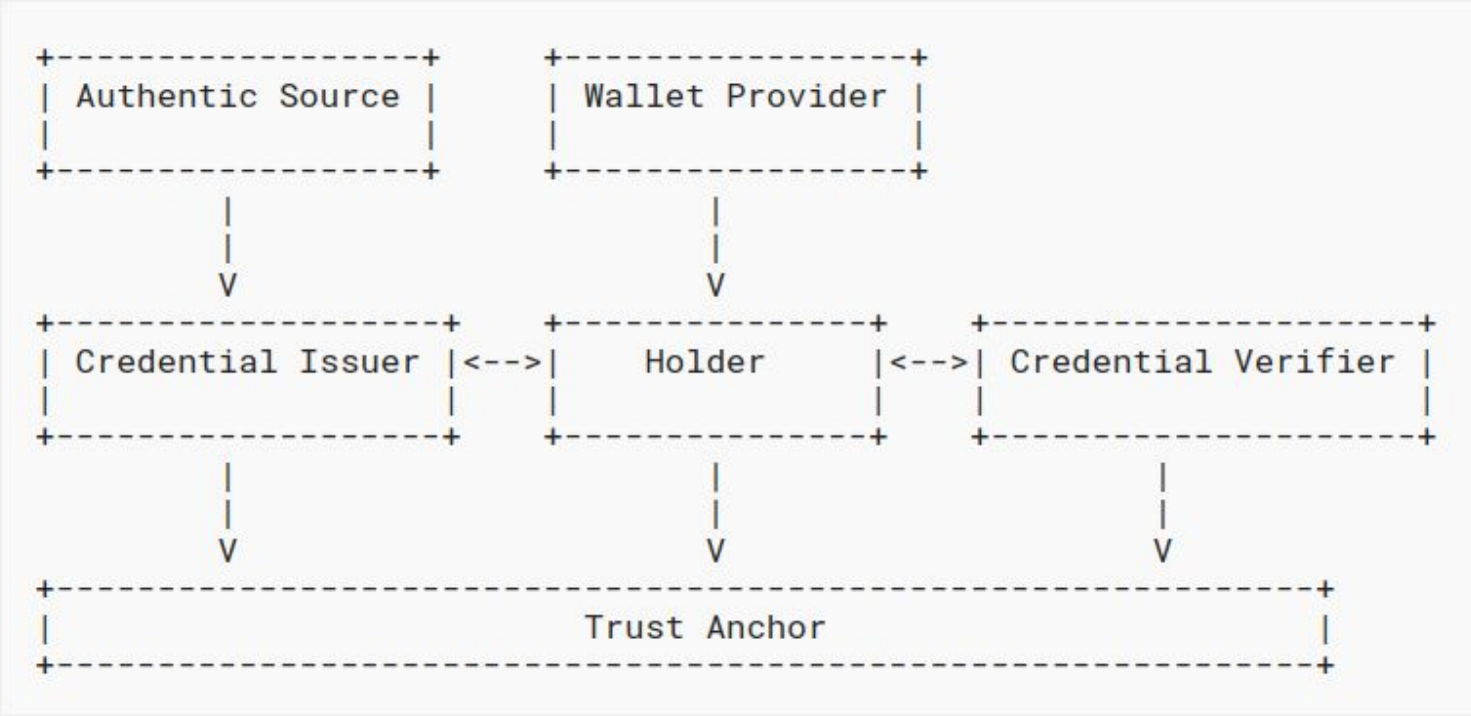
# The eduGAIN OpenID Connect Profile - work in progress

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

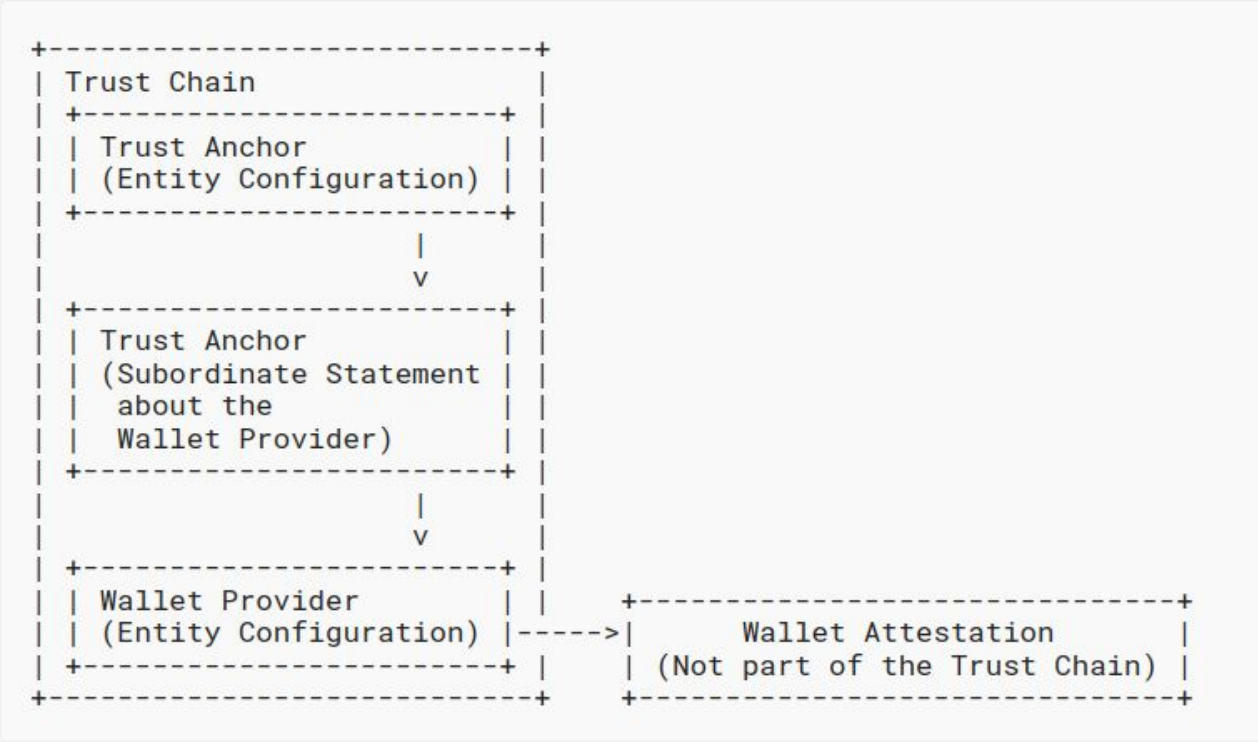
# OpenID Federation Wallet Architectures 1.0 - DRAFT






*https://peppelinux.github.io/federation-wallet/main.html*

# OpenID Federation Wallet Architectures 1.0 - DRAFT






*https://peppelinux.github.io/federation-wallet/main.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





GÉANT


# 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).