

WORK
SHOP
GARR
2024

NET
MAKERS

eduGAIN OpenID Federation Pilot

Davide Vagheti

GARR

Agenda

eduGAIN's Overview

OpenID Federation quick overview

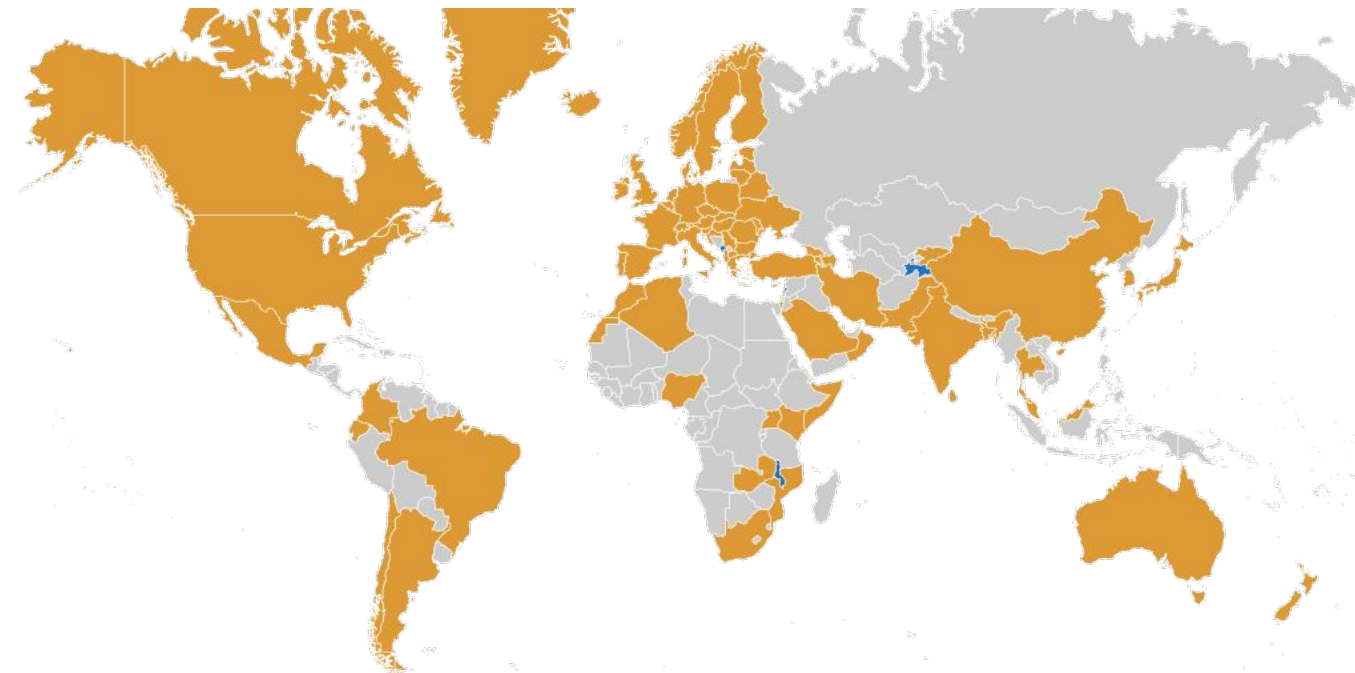
eduGAIN OpenID Federation

OpenID Federation and the wallet ecosystem



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

eduGAIN Global Coverage



80 Federations

9536 Entities

5754 Identity Providers

3800 Service Providers

Last update November 6th 2024

eduGAIN Technological Profiles: SAML 2.0

An open standard

Extremely successful and adopted

87 R&E Federations + eduGAIN

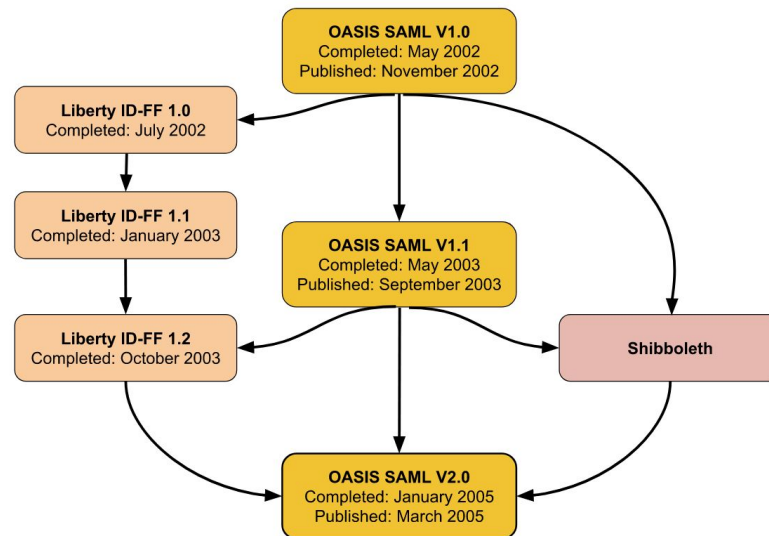
Legacy Protocol: no new devs in the last 5 years

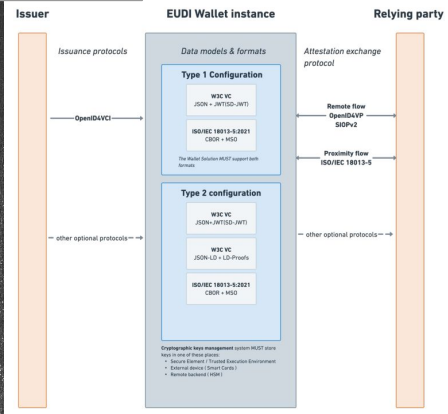
No support for Mobile App, REST/API flows, etc.

Decentralized identity and Verifiable Credentials?

Post-quantum cryptography support?

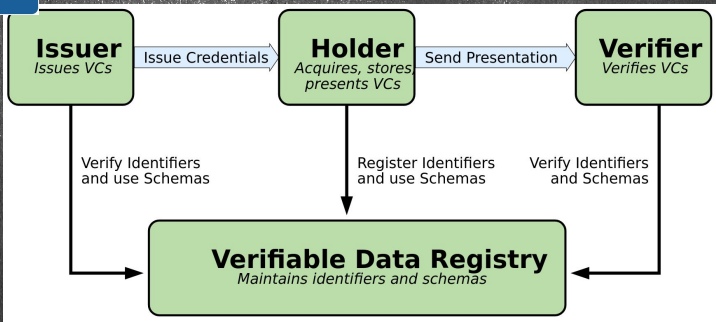
A History of the Security Assertion Markup Language





```
{
  "iss": "https://rp.umu.se",
  "sub": "https://rp.umu.se",
  "iat": 1516239022,
  "exp": 1516298022,
  "metadata": {
    "openid_relying_party": {
      "application_type": "web",
      "redirect_uris": [
        "https://rp.umu.se/rp/callback"
      ],
      "grant_types": [
        "authorization_code",
        "implicit"
      ],
      "jwks_uri": "https://rp.umu.se/static/jwks.json"
    }
  },
  "jwks": {
    "keys": [
      {
        "kid": "key1",
        "kty": "RSA",
        "use": "sig",
        "e": "AOAB",
        "n": "pnXB0ueEAnUug6wez9J_..."
      }
    ]
  },
  "authority_hints": [
    "https://Federation.umu.se"
  ]
}
```

OpenID Federation



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

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

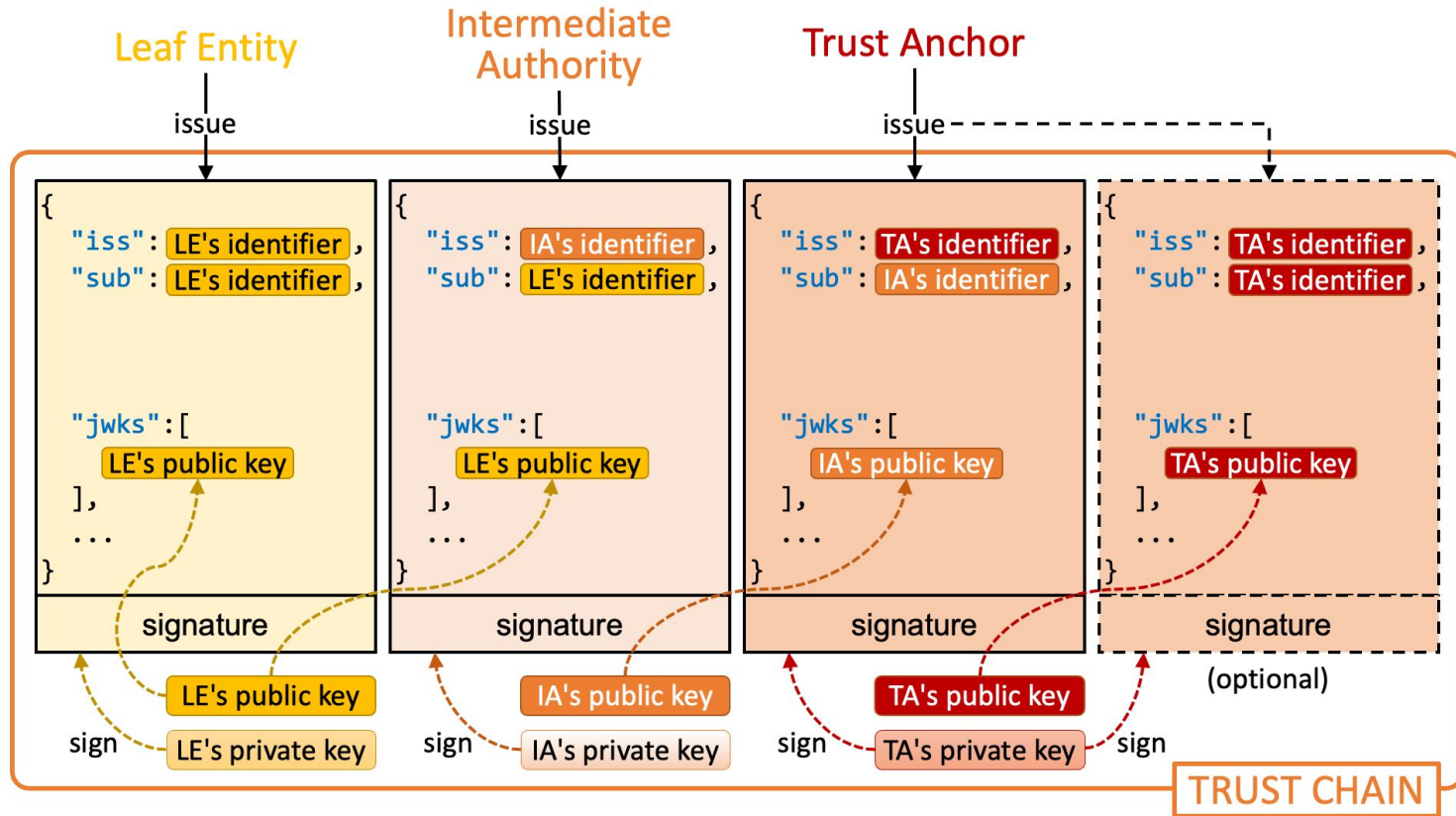
OpenID Federation Entity Configuration

Leaf's Entity Configuration

```
{
  "alg": "ES256",
  "kid": "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/>

WORK
SHOP
GARR
2024

NET
MAKERS

eduGAIN OpenID Federation Pilot overview

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

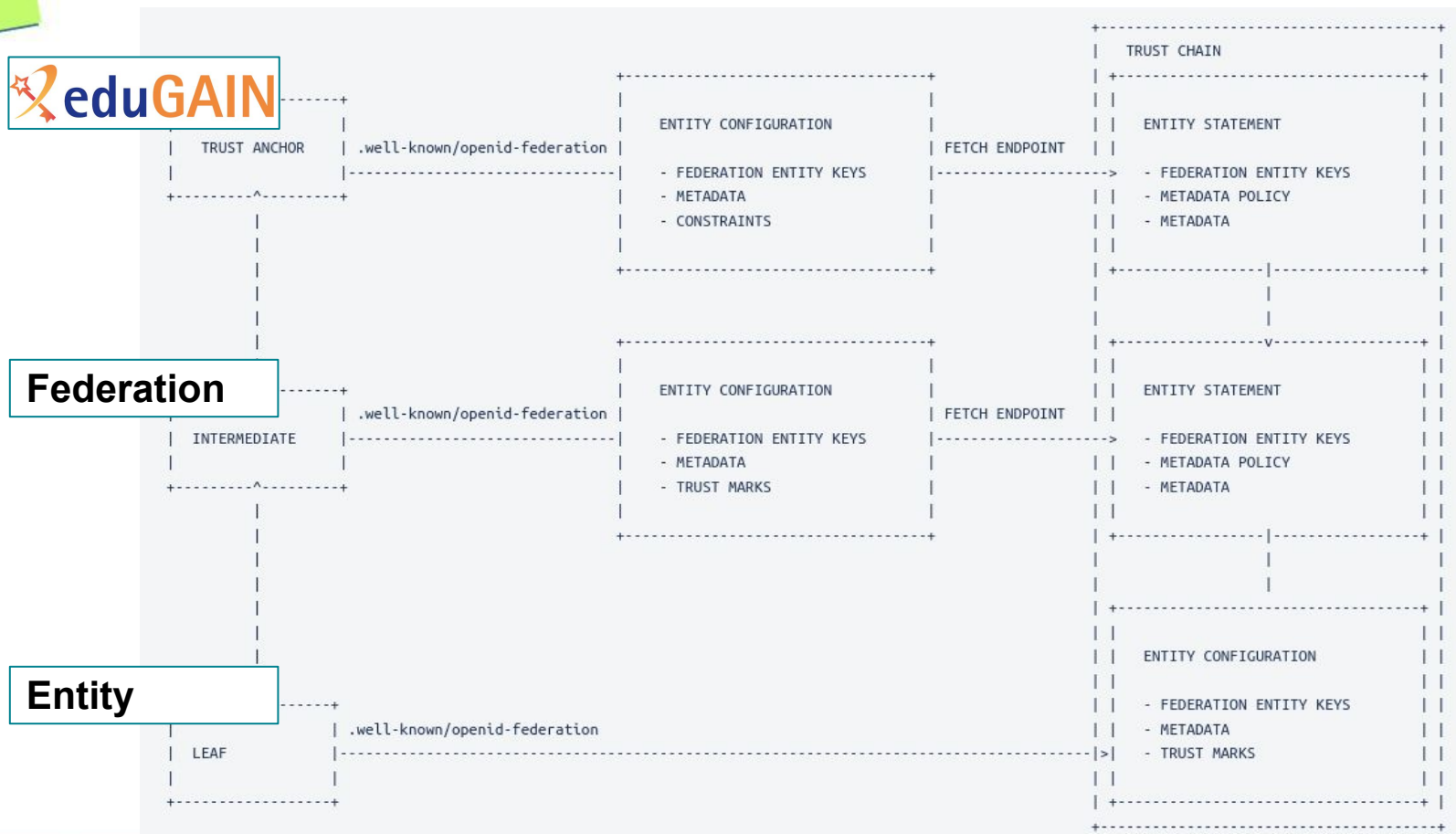
- eduGAIN service and T&I Incubator
- Federation Operators
- RC AAls
- OPs/RPs implementers are welcome



WHEN

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

An eduGAIN OIDC Federation Trust Flow



The eduGAIN OpenID Connect Profile



TRUST is based on trust chains with eduGAIN as Trust Anchor



ENTITY VALIDATION is based the eduGAIN Trust Mark.



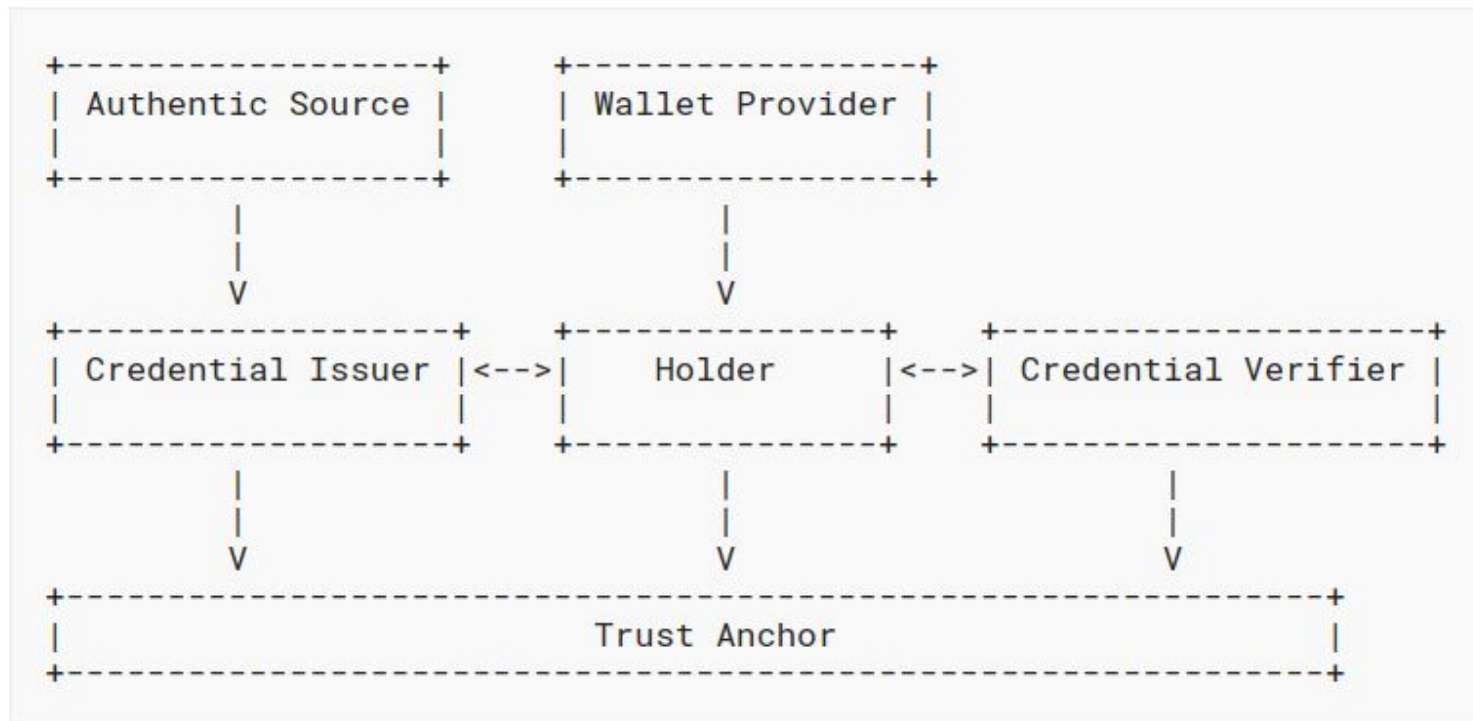
ENTITY RESOLUTION is provided by a resolver endpoint

WORK
SHOP
GARR
2024

NET
MAKERS

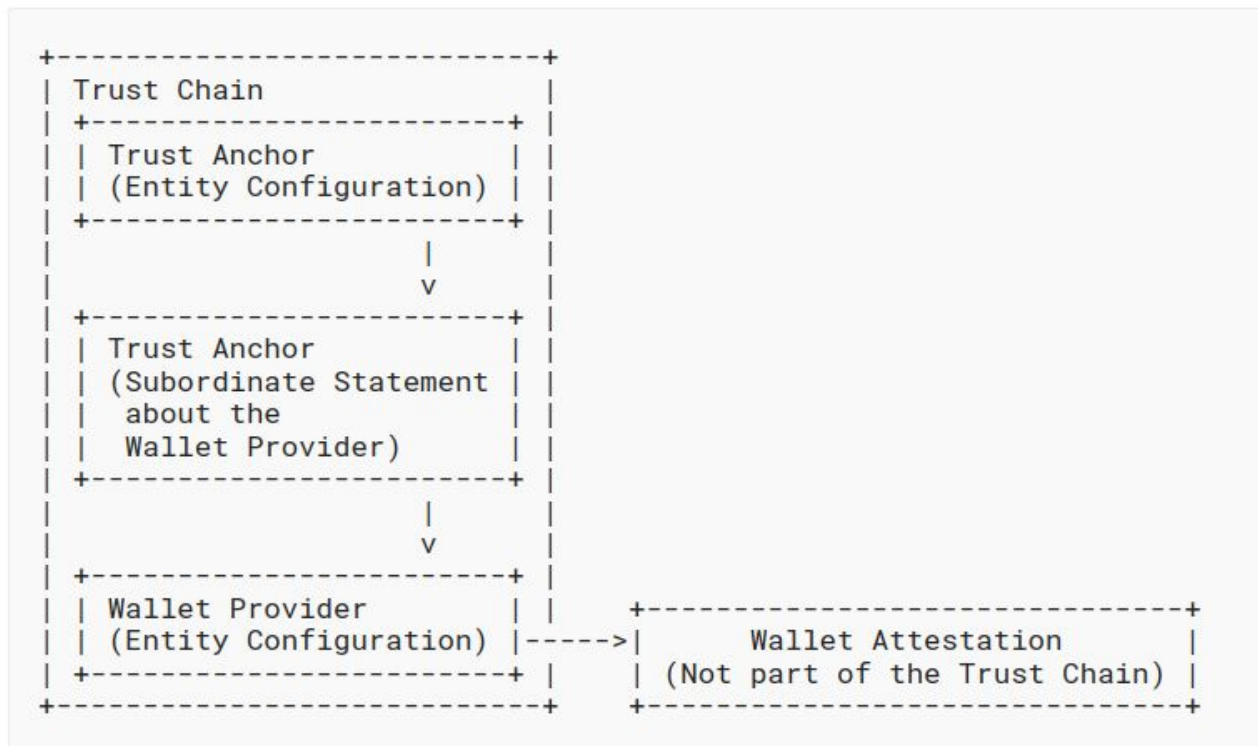
OpenID Federation Wallet Architectures DRAFT

OpenID Federation Wallet Architectures 1.0 – DRAFT



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

OpenID Federation Wallet Architectures 1.0 – DRAFT



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

WORK
SHOP
GARR
2024

NET
MAKERS

Thanks

Davide Vagheti

GARR