eduGAIN OpenID Federation

Davide Vaghetti (GARR)

eduGAIN Service Owner

Giuseppe De Marco (Independent)

OpenID Federation Co-Author

tnc24

RENDEZVOUS À RENNES

Rennes, France | 10-14 JUNE 2024

Co-funded by
the European Union

GÉANT

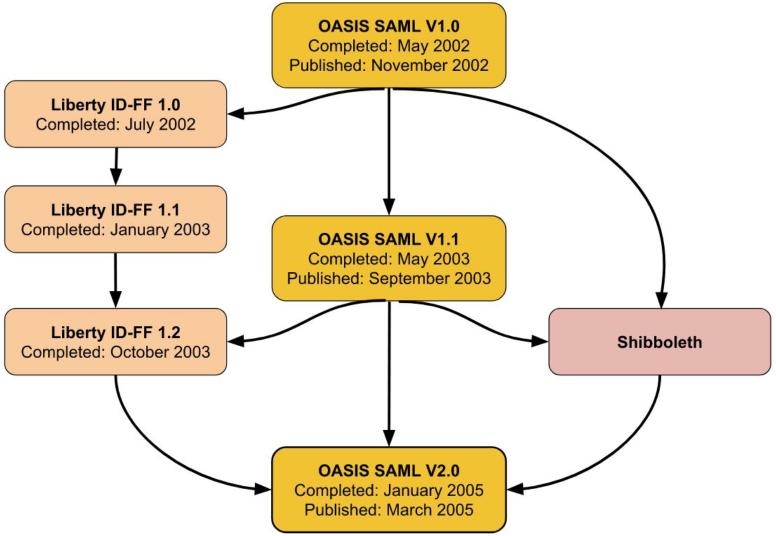
Why OpenID Federation?

R&E Federations are based on SAML 2.0

SAML 2.0:

- An open standard
- Extremely successful and adopted
- It has several implementations
- 87 R&E Federations + eduGAIN
- Used everyday by millions of users

A History of the Security Assertion Markup Language



OASIS SAML V1.0
Completed: May 2002
Published: November 2002

Liberty ID-FF 1.0
Completed: July 2002

Liberty ID-FF 1.1
Completed: January 2003

OASIS SAML V1.1
Completed: May 2003
Published: September 2003

Liberty ID-FF 1.2
Completed: October 2003

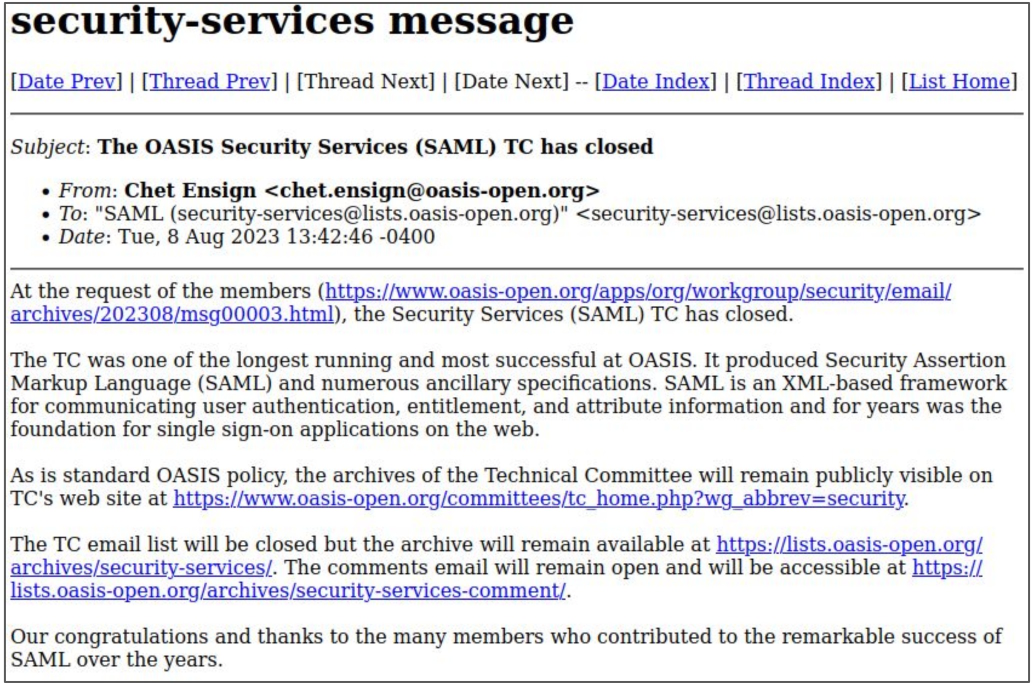
Shibboleth

OASIS SAML V2.0
Completed: January 2005
Published: March 2005

Trscavo, CC BY-SA 4.0

SAML 2.0 is a legacy protocol

- OASIS Security Services Technical Committee closed last year.
- Last specification dates back to 2019.



security-services message

[Date Prev] | [Thread Prev] | [Thread Next] | [Date Next] -- [Date Index] | [Thread Index] | [List Home]

Subject: **The OASIS Security Services (SAML) TC has closed**

- *From*: **Chet Ensign <chet.ensign@oasis-open.org>**
- *To*: "SAML (security-services@lists.oasis-open.org)" <security-services@lists.oasis-open.org>
- *Date*: Tue, 8 Aug 2023 13:42:46 -0400

At the request of the members (https://www.oasis-open.org/apps/org/workgroup/security/email/archives/202308/msg00003.html), the Security Services (SAML) TC has closed.

The TC was one of the longest running and most successful at OASIS. It produced Security Assertion Markup Language (SAML) and numerous ancillary specifications. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information and for years was the foundation for single sign-on applications on the web.

As is standard OASIS policy, the archives of the Technical Committee will remain publicly visible on TC's web site at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

The TC email list will be closed but the archive will remain available at https://lists.oasis-open.org/archives/security-services/. The comments email will remain open and will be accessible at https://lists.oasis-open.org/archives/security-services-comment/.

Our congratulations and thanks to the many members who contributed to the remarkable success of SAML over the years.

Source https://lists.oasis-open.org/archives/security-services/202308/msg00004.html

Won’t (ever?) get supported in SAML 2.0

- Mobile App.
- REST-like/API based authentication flows.
- FedCM (Federated Credential Management).
- Decentralized identity and Verifiable Credentials.
- Post-quantum cryptography support.

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service [..] on behalf of a resource owner [RFC 6749]

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User [..] in an interoperable and REST-like manner.

[openid-connect-core-1_0]

OAuth 2.0 and OpenID Federation

- Current industry standards for Authorization and Authentication.
- Mobile friendly and API (REST-like) friendly.
- JSON Web Token.
- Actively supported by the developer community.
- Very lively standards.
- DID and VC support.

OpenID Federation Overview

What is OpenID Federation

OpenID Federation is:

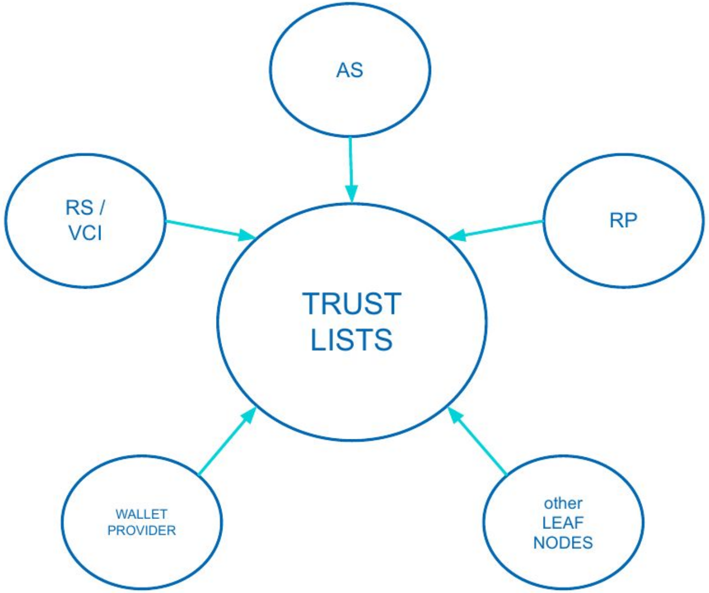
- a **technical specification** that shows us how to **evaluate the Trust from a technical perspective**.
- a technology that shows us **how to build trust infrastructures**.
- an advanced system for **securely establishing the interoperability** of participants.

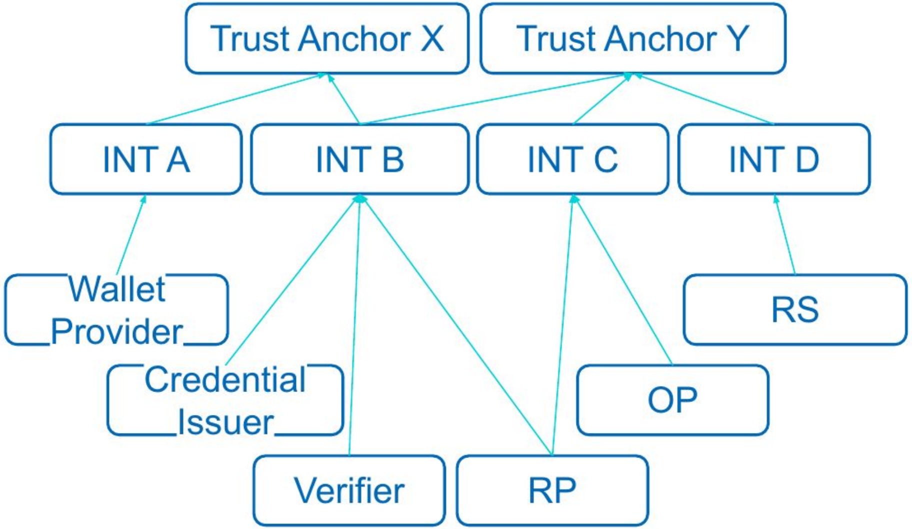
OpenID Federation Defines How to …

Build a **trust infrastructure that scales**:

a. **distributed** over multiple participants
b. **hierarchical**, a single ecosystem or federation is one ecosystem, one Federation
c. **decentralized**:
    i. The Federation Authority has Intermediates
    ii. participants can join in multiple ecosystems and multiple federation without configuration changes

Flat vs. Distributed and Hierarchical





OpenID Federation Defines How to …

Build a **trust infrastructure** that gives freedom to its participants.

a. participants can publish their metadata on their own and **join in multiple ecosystems with a single deployment**

b. a single .well-known endpoint (Entity Configuration) can carry **multiple metadata for multiple specific roles/protocol** (Client, RP, OP, AS, RS, Wallet Provider …)

c. **custom protocol specific metadata are possible**, not limited to OpenID and OAuth 2.0 only.

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"]
}
```

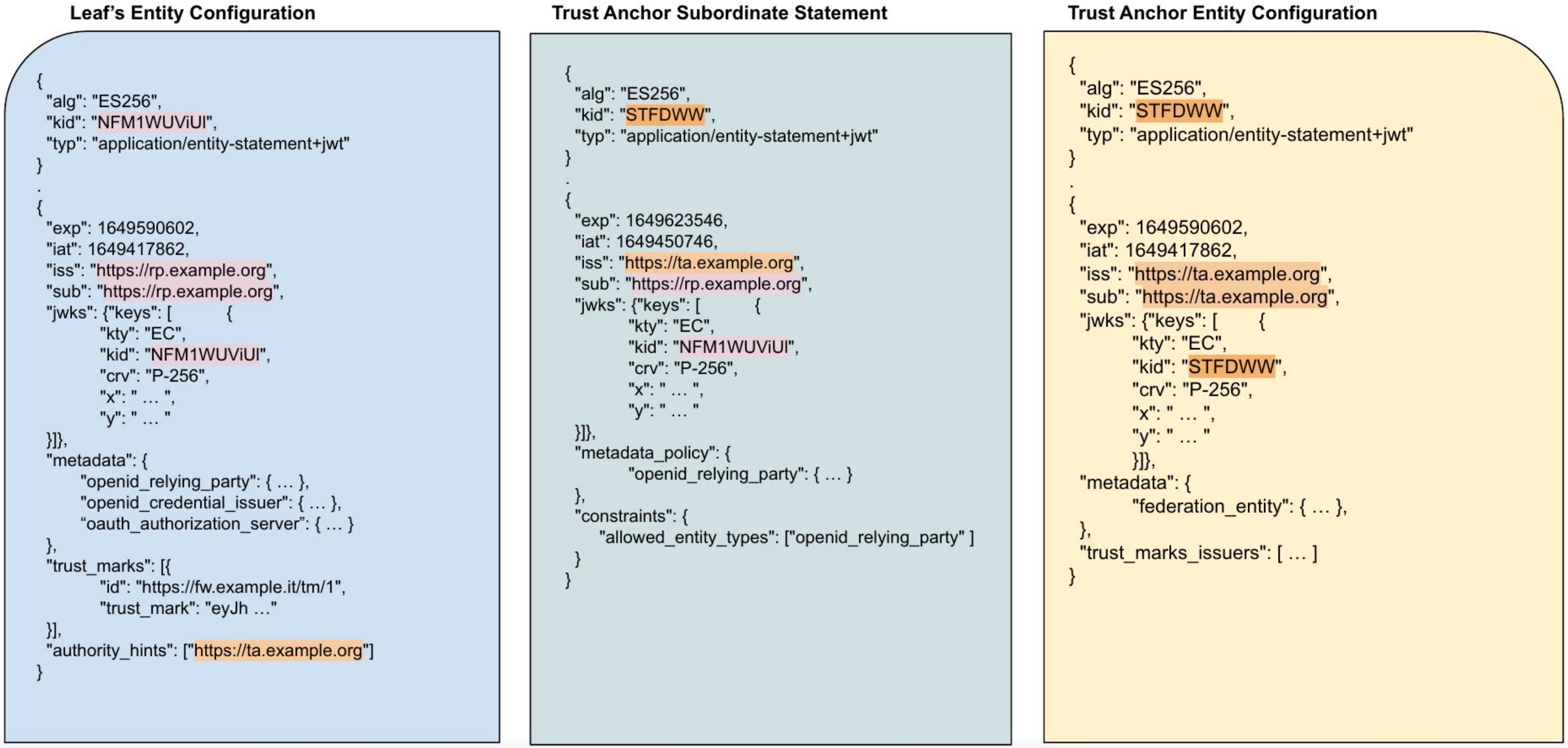
1. Self Signed JWT
2. Federation JWKs in the payload top level
3. Multiple Metadata (with their JWKS)
4. Trust Marks, compliance assertions to particular profiles
5. Authority hints, indicating the immediate Superior Entities that has registered this Entity and can “say something about it”

OpenID Federation Defines How to …

Assess the compliance of participants in an ecosystem with shared rules.

a. Verify whether a participant is still active within the ecosystem (**revocation**).
b. Verify whether a participant supports specific protocols, such as OpenID, OAuth 2.0, others, and **if it is trusted when using that protocol**.
c. Verify whether a participant is **compliant to specific profiles** (es: security profiles, custom profiles)

OpenID Federation Trust Chain



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"]
}
```

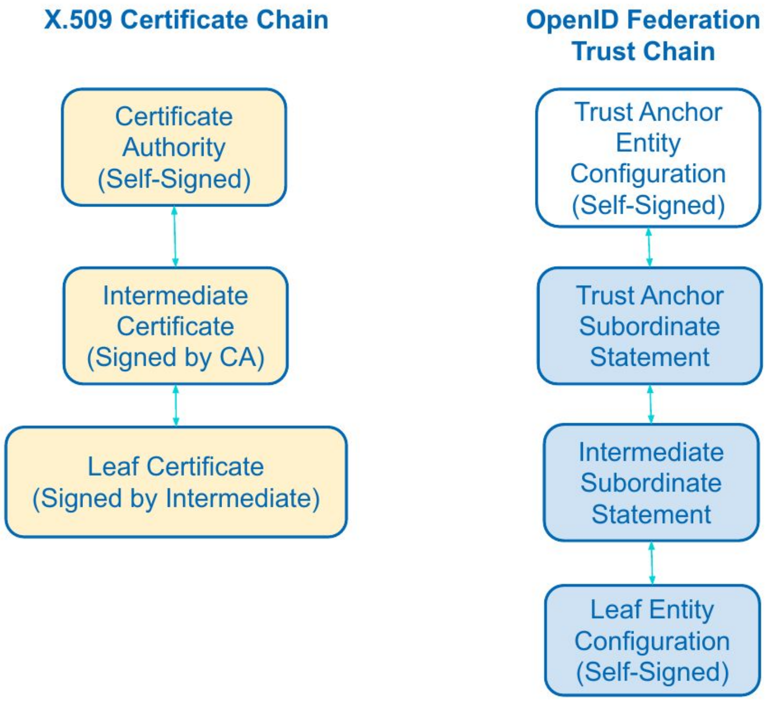
Trust Anchor Subordinate Statement

```
{
  "alg": "ES256",
  "kid": "STFDWW",
  "typ": "application/entity-statement+jwt"
}
.
{
  "exp": 1649623546,
  "iat": 1649450746,
  "iss": "https://ta.example.org",
  "sub": "https://rp.example.org",
  "jwks": {"keys": [          {
           "kty": "EC",
           "kid": "NFM1WUViUI",
           "crv": "P-256",
           "x": " … ",
           "y": " … "
  }]},
  "metadata_policy": {
           "openid_relying_party": { … }
  },
  "constraints": {
      "allowed_entity_types": ["openid_relying_party" ]
  }
}
```

Trust Anchor Entity Configuration

```
{
  "alg": "ES256",
  "kid": "STFDWW",
  "typ": "application/entity-statement+jwt"
}
.
{
  "exp": 1649590602,
  "iat": 1649417862,
  "iss": "https://ta.example.org",
  "sub": "https://ta.example.org",
  "jwks": {"keys": [       {
           "kty": "EC",
           "kid": "STFDWW",
           "crv": "P-256",
           "x": " … ",
           "y": " … "
           }]},
  "metadata": {
           "federation_entity": { … },
  },
  "trust_marks_issuers": [ … ]
}
```

Establishing Technical Trust


X.509 Certificate Chain
Certificate Authority (Self-Signed)
Intermediate Certificate (Signed by CA)
Leaf Certificate (Signed by Intermediate)
OpenID Federation Trust Chain
Trust Anchor Entity Configuration (Self-Signed)
Trust Anchor Subordinate Statement
Intermediate Subordinate Statement
Leaf Entity Configuration (Self-Signed)

Technical trust encompasses security, reliability, and integrity of entities, demonstrating a commitment to security standards and shared rules.

Each entry is linked to the next through the issuer and the subject identifier and cryptographic material.

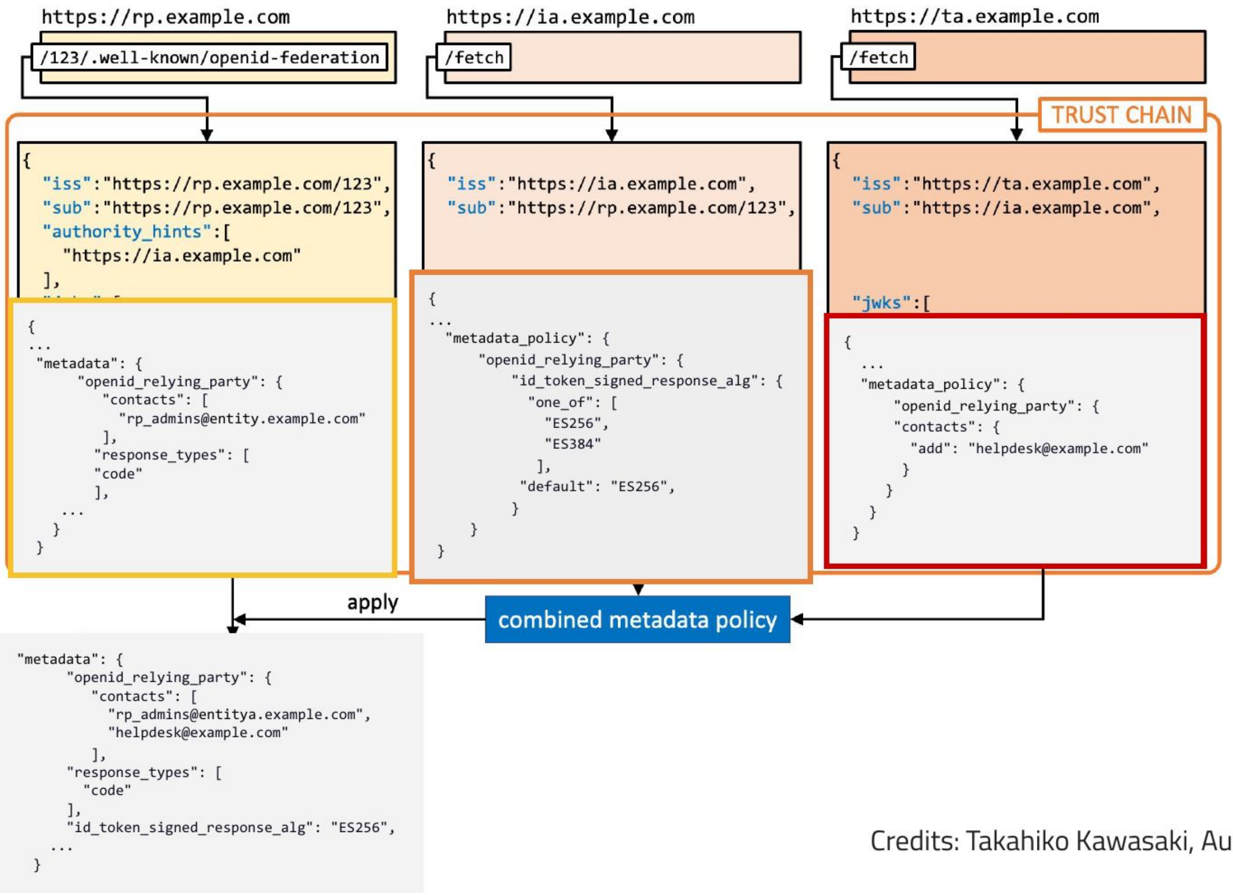
Attributes and cryptographic bindings helps in validating the signature of the subordinate entry in the chain.

By only having the Trust Anchor cryptographic public key is possible to verify the entire chain.

X.509-based PKI and OpenID Federation

	X.509	OpenID Federation
Born	1988	2016
Format	ASN.1/DER	JWT
RESTful API	–	Yes
Revocations	CRL, OCSP	Using the RESTful API
Attestation artifact	Public key certificate	Entity Statement (ES)
Attestation content	1 Subject Identifier 1 Public Key	1 Subject Identifier (HTTPs URL) N Public Keys Protocol Specific Capabilities Grants
Chain name	Certificate chain	Trust Chain
Chain payload	Identity, Public key, constraints, custom extensions.	Identity, Public key**S**, constraints, several **protocol specific metadata**, customizable **Trust Marks**, **policies** (**X.509 certificates too!**).
Cryptographic Keys specialized per scope	–	Federation Keys != Protocol specific keys

Build A Trust Chain And Fetch Metadata, Policies Included!



```
{
  "iss":"https://rp.example.com/123",
  "sub":"https://rp.example.com/123",
  "authority_hints":[
    "https://ia.example.com"
  ],
```

```
{
 ...
  "metadata": {
       "openid_relying_party": {
          "contacts": [
            "rp_admins@entity.example.com"
          ],
         "response_types": [
         "code"
         ],
       ...
     }
  }
```

```
{
  "iss":"https://ia.example.com",
  "sub":"https://rp.example.com/123",
```

```
{
...
  "metadata_policy": {
      "openid_relying_party": {
          "id_token_signed_response_alg": {
            "one_of": [
              "ES256",
              "ES384"
             ],
           "default": "ES256",
          }
      }
 }
```

```
{
  "iss":"https://ta.example.com",
  "sub":"https://ia.example.com",


  "jwks":[
```

```
{
  ...
  "metadata_policy": {
      "openid_relying_party": {
      "contacts": {
        "add": "helpdesk@example.com"
        }
      }
    }
 }
```

```
"metadata": {
      "openid_relying_party": {
         "contacts": [
           "rp_admins@entitya.example.com",
           "helpdesk@example.com"
         ],
      "response_types": [
        "code"
      ],
      "id_token_signed_response_alg": "ES256",
    ...
  }
```

Giuseppe De Marco

Credits: Takahiko Kawasaki, Authlete (source)

eduGAIN OpenID Federation Profile

eduGAIN OpenID Federation Profile

OpenID4RS General Architecture

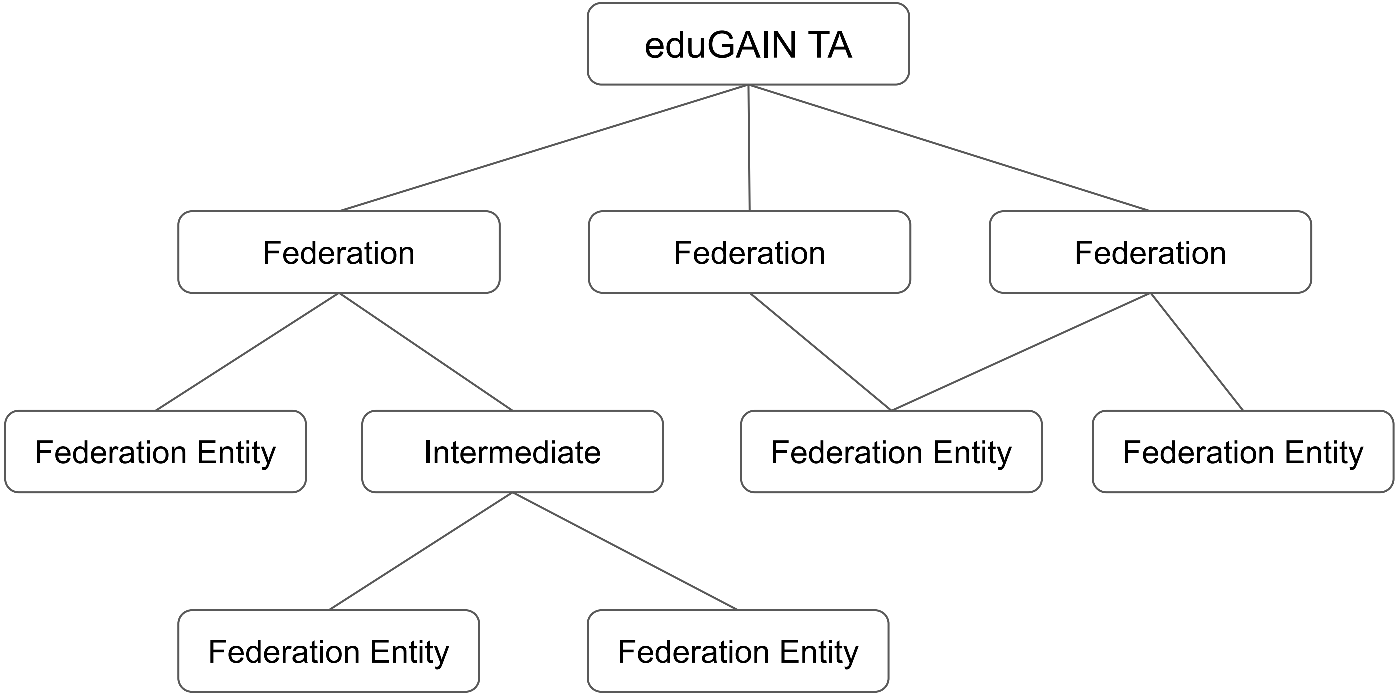
OpenID4RS Federation

OpenID4RS Connect

OpenID4RS Technical Rules, Policies and Constraints

https://github.com/GEANT/edugain-openidfed

An eduGAIN OpenID Federation Topology



eduGAIN OpenID Federation POC

eduGAIN OpenID Federation POC

TRUST & IDENTITY INCUBATOR

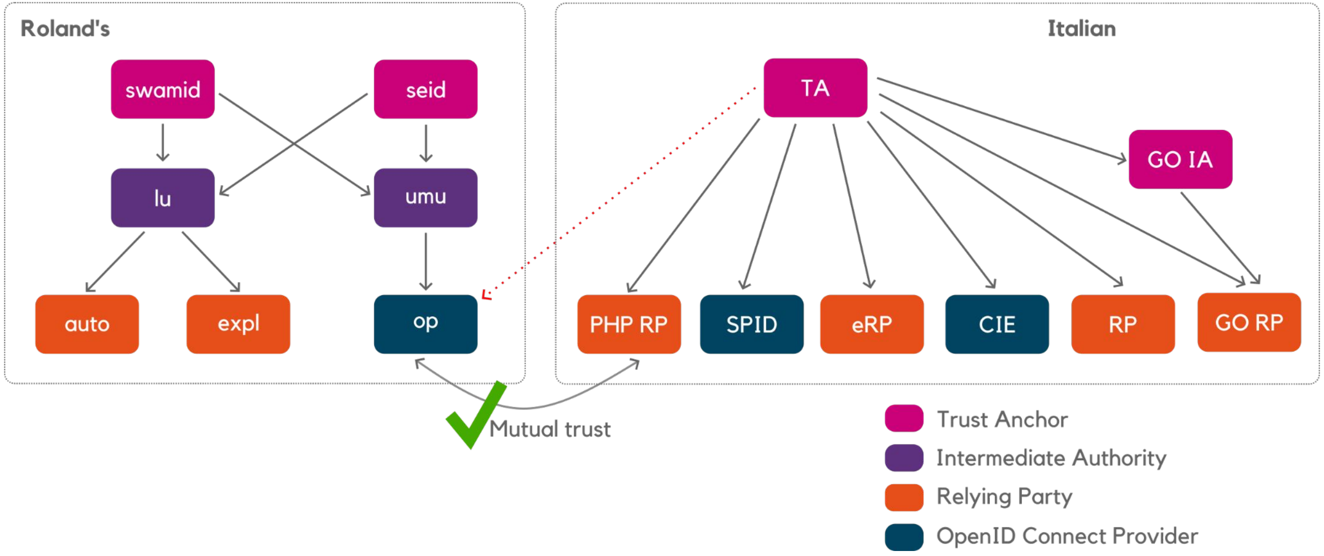
- *Sharing existing experience and providing a sparring partner to the eduGAIN PoC team*
- *Contribute to standards and policy development for eduGAIN and national federations (upon request by the eduGAIn PoC team)*
- *Developing or further enhancing software tools, including, but not limited to:*
  - *Contribute to existing software development for the eduGAIN PoC*
  - *Build/Productise a (scalable) resolver which can be deployed by fedops and eduGAIN*
  - *Further improve visualisation and reporting tooling*
  - *Further improve Go based OP/RP*

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

Leverage GEANT Project GN5-1 WP5 existing work and expertise

TRUST & IDENTITY INCUBATOR

OIDCfed support on SimpleSAMLphp



https://wiki.geant.org/display/GWP5/OIDCfed+support+on+SimpleSAMLphp

Implement OpenID Federation into SimpleSAMLphp and Shibboleth IdP

Related to the above eduGAIN OpenID Federation Pilot, we would like to add OpenID Federation capabiliteis to commonly used software in our ecosystem. This activity will complete the work on implementing OpenID Federation into SimpleSAMLphp, as well as start with an implementation for Shibboleth IdP.

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

Contributors to eduGAIN POC and OpenID Federation Incubator activities

Giuseppe De Marco, Independent

Roland Hedberg, Independent

Niels van Dijk, SURF

Michael Schmidt, LRZ

Gabriel Zachmann, KIT

Diana Gudu, KIT

Martin van Es, Independent

eduGAIN OpenID Federation Pilot

Stay Tuned!

eduGAIN OpenID Federation Pilot will start in September 2024

https://edugain.slack.com/archives/CF3C7BAR5

support@edugain.org

Thank you

Any questions?

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

tnc24
RENDEZVOUS À RENNES
Rennes, France | 10-14 JUNE 2024

Co-funded by
the European Union

GÉANT