OpenID Federation

Is it just for Christmas?

Phil Smart, Trust and Identity, Jisc.

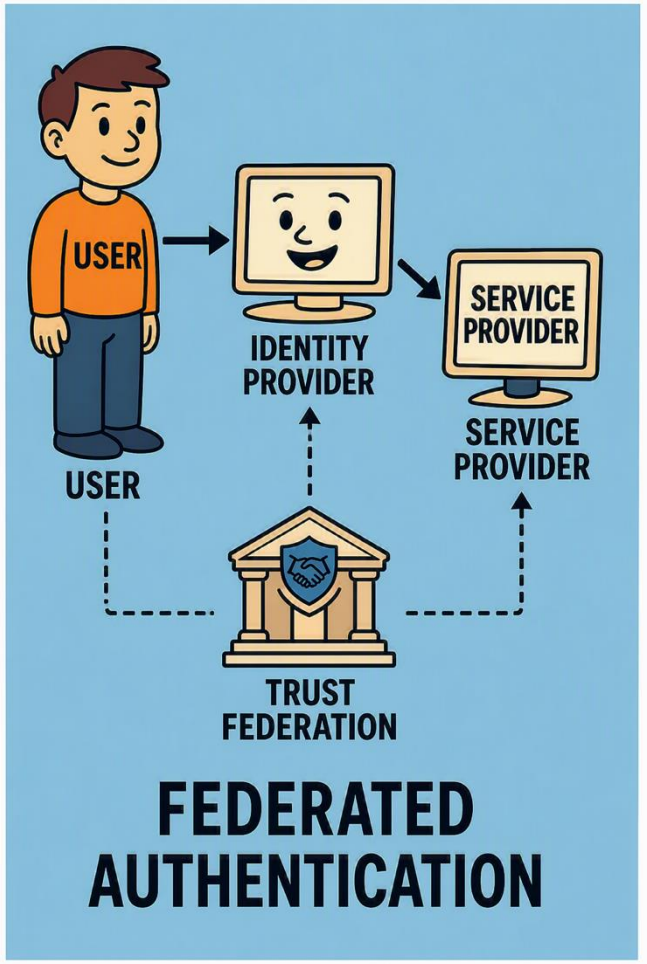
No...

Betteridge's law of headlines *is an adage that states: "Any headline that ends in a question mark can be answered by the word no." It is based on the assumption that if the publishers were confident that the answer was yes, they would have presented it as an assertion; by presenting it as a question, they are not accountable for whether it is correct or not.*

Some stronger words used, here: https://en.wikipedia.org/wiki/Betteridge%27s_law_of_headlines

Federation and Federated Identity?

- Services do **not** want responsibility for identity and credential management
- Services **want** trustworthy assertions about a user's affiliation (student, staff at university X), etc.
- Users want one login and one identity across many services: SingleSignOn (SSO)
- Therefore, authentication and identity are **delegated** to a **federated Identity Provider** (IdP).
- But if a Service allows somebody else to authenticate its users, why should it trust them?
  - *Bi-lateral*, I trust you, you trust me, thanks. (direct trust.)
  - *Multi-lateral*, trust is established using a **trusted third-party 'trust anchor'**; which validates and governs participating organizations



Components

- For bi-lateral, you need direct trust between the Identity Provider and Service Provider
- For multi-lateral federation, you need a **Trust Federation**
- A Single Sign-On (**SSO**) **authentication** protocol
  - Identifiers (who you are)
  - Attributes (allows fine grained authorization, amongst others)
- **Software** Implementations

Who Provides These Technologies/Frameworks

Trust Federation

Implementation

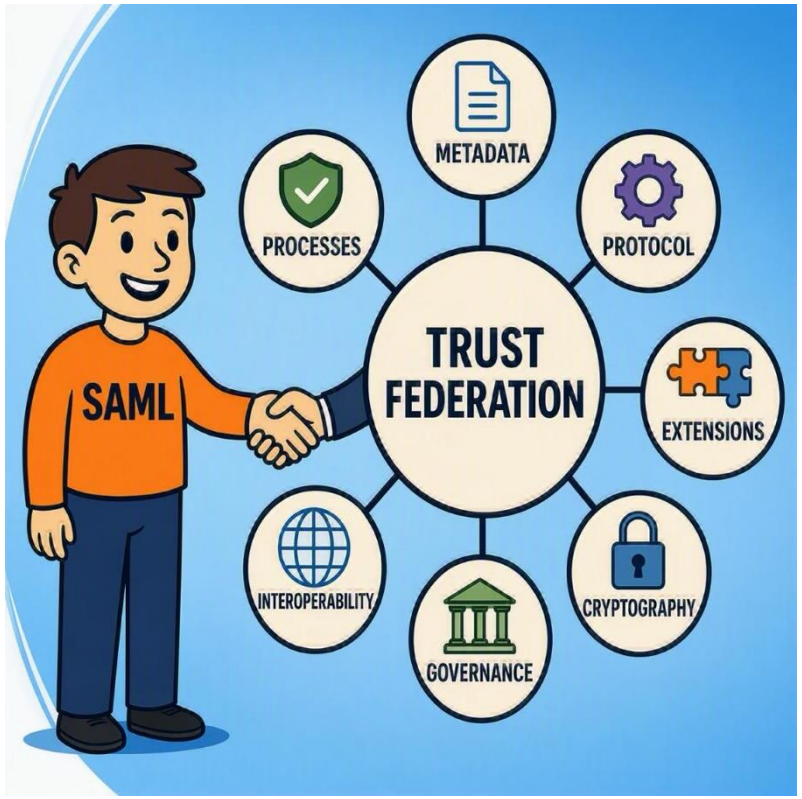
Standards

Application

Presentation

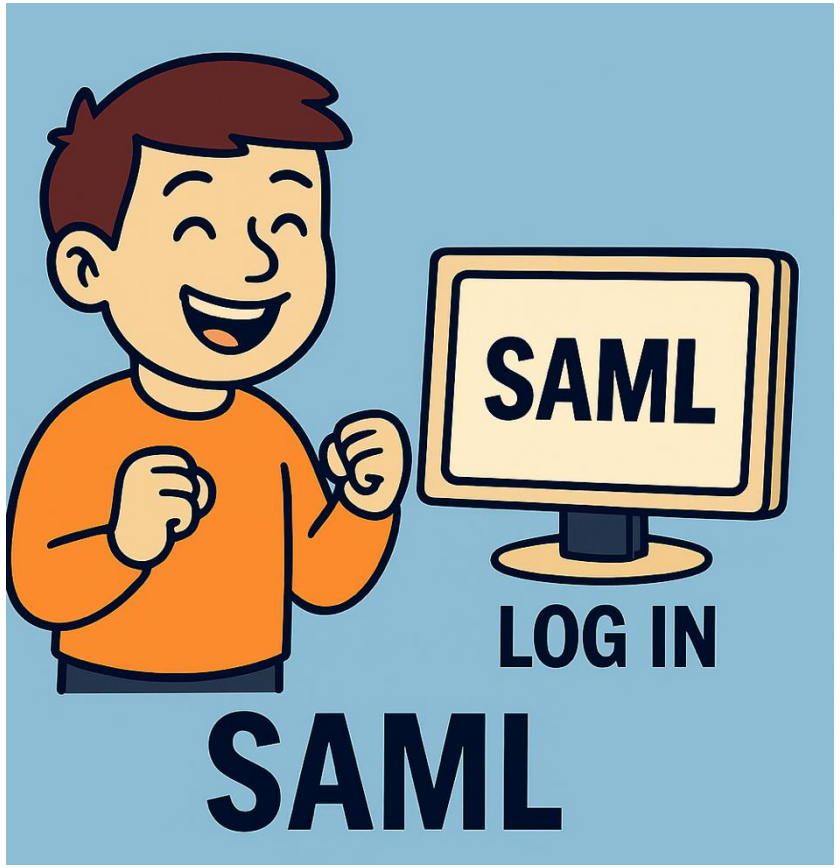
A Trust Federation: The UK federation

- National authentication infrastructure for library content existed before the UK federation…Athena -> Athens.
- Version 1.0 of the SAML protocol was standardised and published in 2002
- The UK federation developed from the SDSS federation using **SAML** as the core protocols and Shibboleth as the reference implementation
- Version 2.0 of the SAML protocol was standardised and published in 2005
- SDSS became the The UK federation in 2006!
- SAML does not natively define a complete federation trust model, so federations construct one using its building blocks
  - Indeed version 1.0 of SAML didn't even define metadata. Often, trust was based on X.509 path validation…see OpenID Federation
  - Once SAML metadata was defined, Federations turned to signed metadata aggregates.



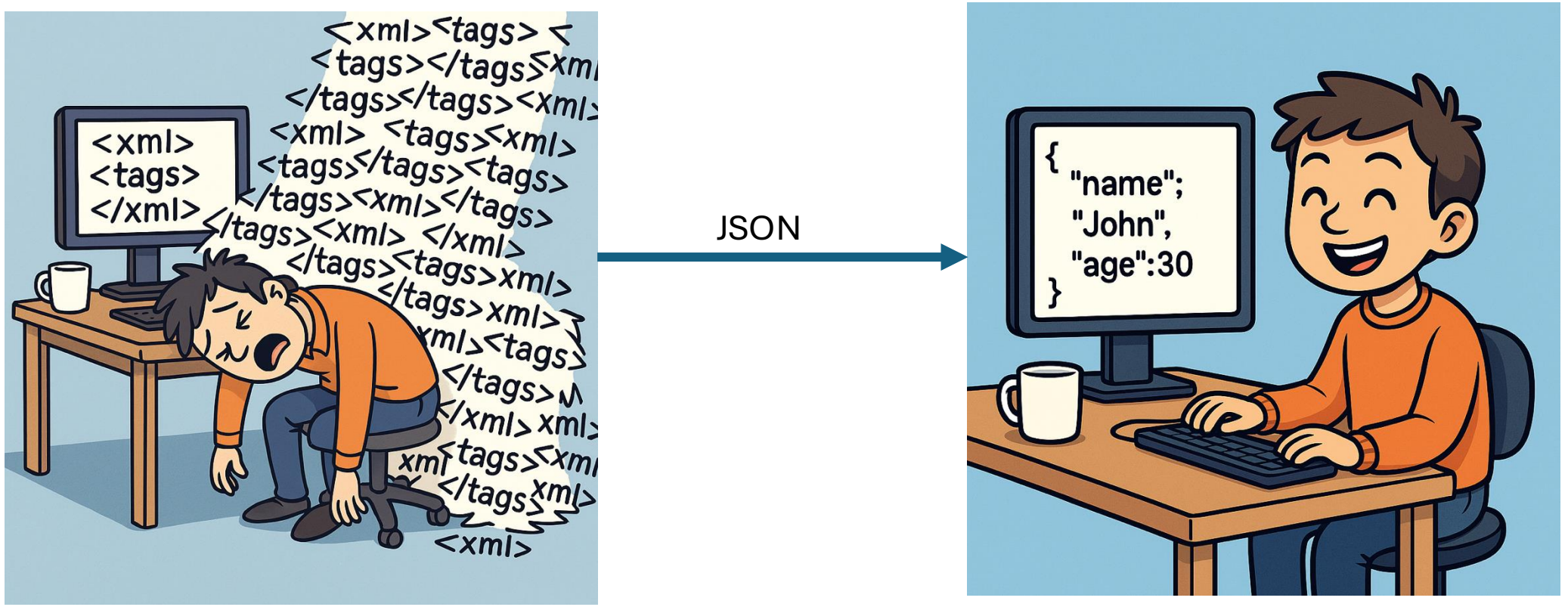
Using SAML for Federated Single Sign-On

- Research and Education were early pioneers of large-scale multi-lateral identity federation, creating global trust networks that continue to operate at significant scale today.
- SAML has provided robust and reliable Web SSO for over two decades.
  - Vulnerabilities mostly come from implementation, sometimes but less often the specification
    - For example, implementation issues around XML security
- So…*what is the point of this presentation*?
- SAML is dead?
  - No, but the SAML Technical Committee (SSTC) closed down.
  - Cryptography is changing? (Post Quantum Cryptography)
- There are other identity/authentication/authorization protocols that have emerged since SAML.
  - **OAuth 2.0**: a delegated authorization protocol for HTTP APIs
  - **OpenID Connect**: An identity layer on top of OAuth 2.0



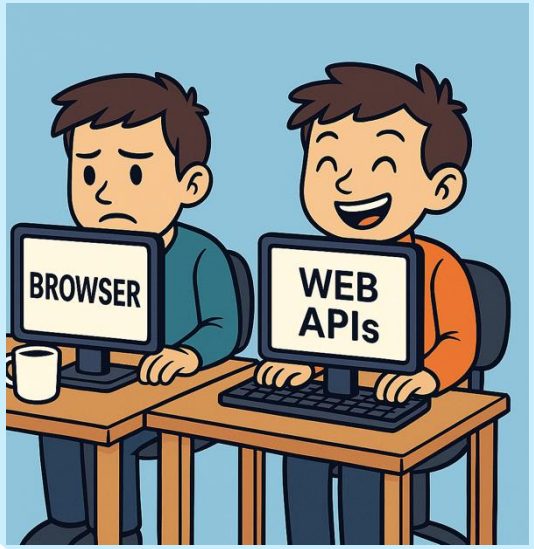
What's good about OAuth 2.0 and OpenID Connect?

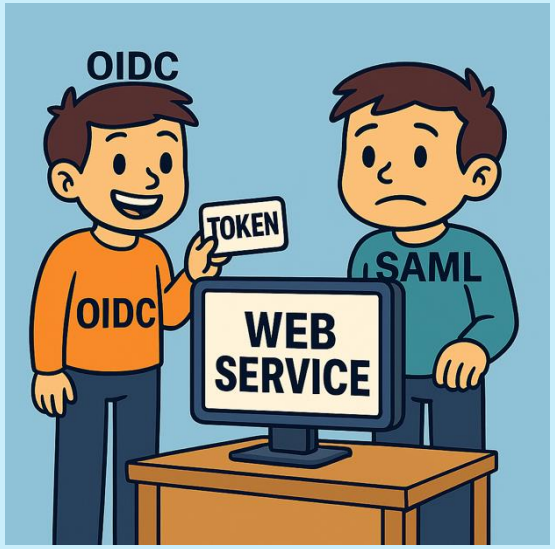
- It is JSON based, and **real people** *died* using XML (joke)
  - Although…XML security is hard to implement. JOSE based security is *perhaps* an improvement.



Why OAuth 2.0 and OpenID Connect?

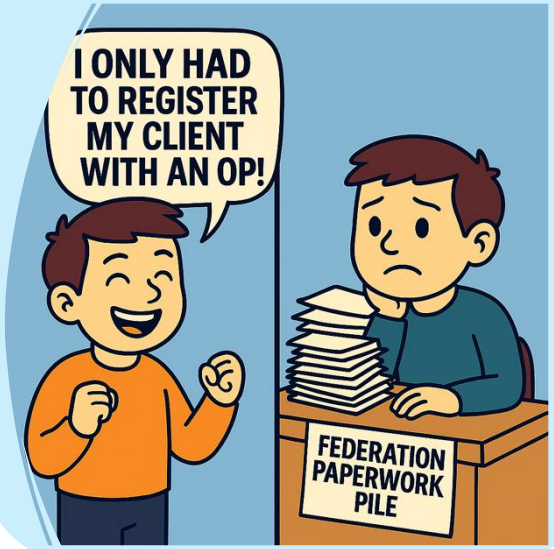
API, Mobile, and Web





- SAML found its fit in Web Browser SSO
  - RESTful (HTTP) APIs developed alongside SAML, not before
- OAuth/OpenID Connect designed to support machine to machine clients and stateless JWTs for RESTful APIs
- SAML provides authentication information, OpenID Connect and OAuth 2.0 are better at combining authorization with identity
  - Access tokens scoped to resources

Bilateral Federation



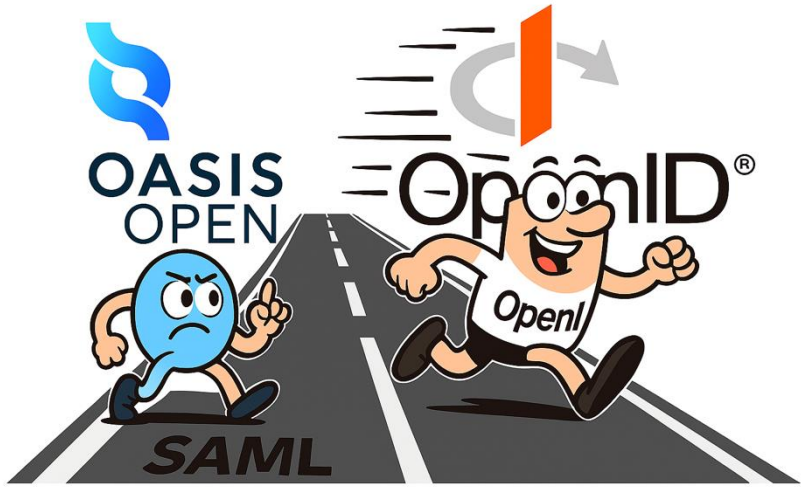
- It was never properly ‘federated’.
- This was a plus point for developers.
- Easier to register clients.

OpenID Federation?

- OAuth2.0 or OpenID Connect are not properly ‘federated’, being mostly based on bi-lateral (direct) trust relationships
- OpenID **Connect Federation**, Started by Roland Hedberg in 2016
  - Trying to achieve a first-class multi-lateral federation for OpenID Connect
- But, given we already had multi-lateral, large scale, production SAML federations
  - Nobody wanted or needed an OpenID **Connect** based federation
  - OpenID Connect 1.0 was still immature compared to SAML, not that well supported
  - OpenID Connect was favored for its simplicity, not federation complexities
- Then, around 2020-2023, it found its place in the OpenID Foundation as a multi-protocol federation model
  - And uses cases for trust in the digital wallet eco-system.

OpenID Foundation

- A Foundation founded in 2007.
- A non-profit open standards body developing identity and security specifications. For example:
  - **OpenID Connect**
  - **OpenID Federation**
  - Digital Credentials
  - Shared Signals
- They are one of the most active Identity groups on the Web, today.
- But some of their work builds on top of and alongside IETF protocols such as OAuth 2.0.



Changes/Benefits of OpenID Federation?

Dynamic federation topologies and trust establishment?

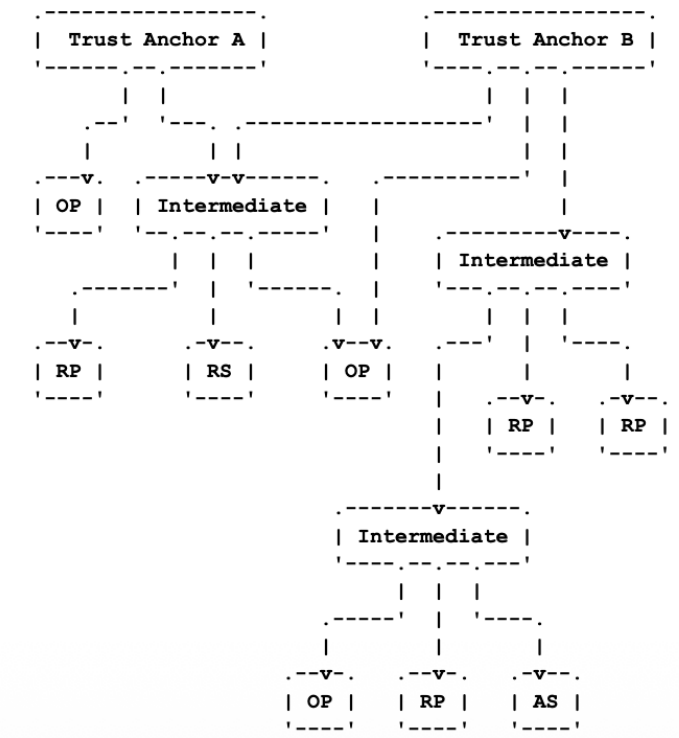
- Entities in multiple federations → Each with different governance and policy
- Federations in multiple federations → With different authentication assurances etc?

Federation operators set policies, and do not control all metadata

- In SAML we deal with entire Metadata → In OpenID Federation the entity still has control over metadata elements, subject to policy

A Third-Party multi-lateral trust model for identity protocols other than SAML e.g.

- OpenID Connect
- OAuth 2.0
- Digital Credentials



Jisc and OpenID Federation?

- We've been tracking OpenID Federation for many years
  - Since 2016…but with more interest in the last 3 years
- We've attended:
  - Conferences such as Internet2 Technology Exchange
  - OpenID Foundation Working Group calls
  - Software interoperability events e.g. in Stockholm in 2025.
- Jisc has explored the feasibility of implementing OpenID Federation.
  - OpenAthens has developed proof-of-concept implementations demonstrating compatibility with its Identity Provider (IdP) and Service Provider (SP) products.
- The UK federation contributes to the Shibboleth project, which has an active workstream integrating OpenID Federation into IdP and SP software.
- The UK federation and OpenAthens have deployed test infrastructure, including:
  - Federation-aware OpenID Providers such as the Shibboleth Identity Provider, and the OpenAthens PoC.
  - Federation-aware OpenID Relying Parties, such as OpenID Federation Forward Auth (OFFA).
  - Trust Anchor and Intermediate authority software, such as Lighthouse
- We have also become an early participant in the eduGAIN OpenID Federation Pilot.

The eduGAIN OpenID Federation Pilot

- eduGAIN is an inter-federation service that connects research and education federations around the word
  - currently based on SAML with over 10,000 Identity and Service Providers
- eduGAIN launched an OpenID Federation pilot in July 2025, intended to run through to July 2026
- Whilst version 1.0 (and 1.1) of the OpenID Federation protocol is agnostic to the underlying authentication protocol used, the pilot is focused on supporting federations built around OpenID Connect

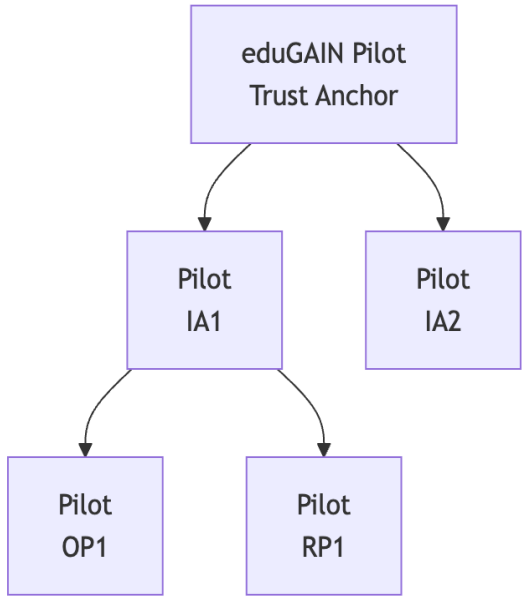
https://github.com/GEANT/edugain-oidf-pilot

Participants

Federation	Contact	Status	Trust Anchor
AAF	Russell Ianiello	Registered	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	Registered	https://ta-oidf-pilot-test.apps.canarie.ca
ArnesAAI	Tim Trojner Hlade		
DFN-AAI	Wolfgang Pempe	Registered	https://ia1.oidfed-pilot.aai.dfn.de
Haka	Sami Silen	Registered	https://testta1.oidfed.funet.fi/
eduid.hu	Czier Norbert	Registered	https://ta.eduid.hu
IDEM	Davide Vaghetti	Registered	https://ta-idem.aai-test.garr.it
Belnet Federation	Philip Brusten	Registered	https://icts-p-ccis-oidfed-pilot.cloud.icts.kuleuven.be
SURF	Harry Kodden	Registered	https://ta.poc2.dev.oidf.lab.surfconext.nl
InCommon	Nicole Roy Drew Capener		

eduGAIN Pilot Progress

- The pilot has laid a strong foundation for demonstrating the technical viability of an OpenID Federation
- The pilot has demonstrated that OpenID Federation-aware components are beginning to reach a level of maturity
  - OpenID Providers such as:
    - Shibboleth, SimpleSAMLphp
  - Relying Parties such as:
    - SimpleSAMLphp, OFFA, DjangoRP
  - Federation Tooling:
    - Lighthouse (GEANT)
    - Inmor (Sunet)
    - Tooling from Surf
- Test cases have been developed and technical policies have been tested



eduGAIN Pilot Remaining Challenges

- Key Management
  - Including key rollover
- Entity Categories
  - How to encode the Entity Attribute tags — used to describe important characteristics of Identity Providers and Service Providers — has not been tested
    - Trust Marks are proposed as the OpenID Federation equivalent, but definitions and adoption are still emerging.
- Trust Mark capabilities
  - Trust Marks can be verified, but how they drive attribute release, membership, and interoperability is largely untested.
- Scope Checking
  - OpenID Federation has no established equivalent to SAML scope checking, although Trust Marks are a likely solution.
  - Relying Party implementations must enforce scope validation to prevent identifier collisions and user impersonation.

eduGAIN Pilot Remaining Challenges

- Scaling
  - Building and validating trust chains PKI style, can require multiple lookups, policy evaluations, and intermediary checks.
  - Performance improvements through caching or resolvers can introduce stale data and make troubleshooting trust failures more difficult.
- Topologies:
  - OpenID Federation supports multiple Trust Anchors, intermediaries, and trust paths, unlike the simpler eduGAIN/SAML model.
  - Alternative trust paths (e.g. national-only vs eduGAIN participation, virtual organisations, direct eduGAIN membership) require additional design, testing, and operational effort.
- Productionalisation
  - Technology alone is not enough, a successful trust federation requires governance, security, support, onboarding, and operational processes.

What's Next?

- The eduGAIN Pilot will end (July 20206), but the infrastructure will remain for testing
  - Exploration of untested technical capabilities
  - Testing federation topologies and new ways of scaling federations
- Attention is starting to shift in eduGAIN from technical feasibility to federation policy, governance, and operational models.
  - Understanding how OpenID Federation maps to existing federation policies will be a major, long-term, area of work.
- Application of OpenID Federation to new use cases?
  - Digital Credentials
  - Straight OAuth 2.0 for HTTP API access.
- Improving levels of software maturity

And…

- Service Providers will need to change their federated authentication technology
- Identity Providers will need to support the new protocols
- Federations aren’t just for Christmas, they are for…