REFEDs PORE Working Group Meetup at TIIME2025

Introduction

The REFEDs PORE Working Group Meetup at TIIME2025 intends to provide a first f2f meetup for federation operators and other relevant stakeholders to discuss an Open ID Federation (OIDFed) profile for *national* identity federation in research and education. While we have been very successful in deploying SAML based identity federations, this protocol now no longer has formal governance. Also OpenID Connect (OIDC) is rising in usage in our sector. Finally, novel technologies like wallets heavily depend on OpenID based protocols. Hence identity federations need to start thinking about how we may work towards adoption of a new federation technology which may support these new protocols. At this point in time, OIDFed looks like the only reasonable alternative, in terms of openness, standardisation, scalability and flexibility.

Our SAML federations have grown out of national initiatives in the past 20 or so years. This has led to many very successful deployments, large scale adoption and a very vibrant and knowledgeable community. The national scope of these activities has however also led to choices in policy and deployment which yielded several challenges when we wanted to interconnect these national solutions into an international framework. We also learned that research (and increasingly also education) have requirements for trust frameworks that can more easily span across countries and sectors.

As a community we have grown tremendously over the years in our understanding of what it means to build and operate identity federations. The challenge before us is to come up with a new way of describing our trust relations, using the OIDFed protocol, taking into account the use cases of our institutions and researchers. And while we need to act locally, we will have to think globally.

Meeting Agenda: https://edu.nl/v4vkm

Gabriel’s Slides:
https://docs.google.com/presentation/d/1ZH6nyBGvPeFprdB9i_Aw53QxxkB2k4nDTqO6BhMIcnE/edit?usp=sharing

Tools

Giuseppe De Marco’s OpenID Federation Browser:
https://github.com/italia/openid-federation-browser
Live demo: https://italia.github.io/openid-federation-browser/main/

Setting the scene

The meeting is not about discussing the how and why of OIDFed itself. It is of course possible we discover challenges or even gaps in the standard wrt our requirements.

The meeting is also *not* about learning the basics of the OIDFed specification and its concepts. Please do prepare before joining!

Here are some resources which may help:

- https://darutk.medium.com/oidc-federation-c2840622dc8f
- https://www.authlete.com/developers/oidcfed/
- https://connect2id.com/learn/openid-federation
- Gabriel's Slides: https://docs.google.com/presentation/d/1ZH6nyBGvPeFprdB9i_Aw53QxxkB2k4nDTqO6BhMIcnE/edit?usp=sharing
-

It also does not hurt to read the actual specification, although I admit it is a bit lengthy ;)
https://openid.net/specs/openid-federation-1_0.html

The session will include a OIDFed introduction, however, please take that as a way to confirm your understanding, not as the way to learn about the concepts for the first time.

It is unlikely we will be able to get a profile done in just one day. However, we may get to a better joint understanding of how we may use OIDFed to fulfill some commonly defined requirements. This may then serve as a basis for further work in the WG.

To facilitate the process I have defined 4 thematic areas

Homework - virtual post-its

As ***a homework exercise*** I am kindly asking all of you to provide **max 3 of your most critical** functional or technical requirements you (representing your organisation) may for each of these topics in the tables below. This will allow us to zoom-in inti specific areas of the specification

If somebody else provided the same requirement already, please *do* duplicate, as requirements will be discussed in order of relevance.

I will aggregate the requirements before the session and will try to make sure we timebox each topic so we actually do touch on all topics.

Participants

Name	Email
Niels van Dijk	niels.vandijk@surf.nl
Gabriel Zachmann	gabriel.zachmann@kit.edu
Peter Gietz	p.gietz@daasi.de
Albert Wu	awu@internet2.edu
Stefan Liström	steli@sunet.se
Björn Mattsson	bjorn@sunet.se
Pål Axelsson	pax@sunet.se
Sascha Hoppler	sascha.hoppler@switch.ch
Gyöngyi Horváth	gyongyi.horvath@geant.org
Wolfgang Pempe	pempe@dfn.de
Francisca Martin-Vergara	fmarver@uma.es
Phil Smart	philip.smart@jisc.ac.uk
Henri Mikkonen	henri.mikkonen@nimbleidm.com
Jon Agland	jon.agland+oidc@jisc.ac.uk
Peter Molnar	molnarp@niif.hu
Christoph Graf	christoph.graf@switch.ch
Jens Jensen	jens.jensen@stfc.ac.uk j.jensen.ral@gmail.com
Mario Di Lorenzo	mario.dilorenzo@garr.it
Drew Capener	drew@omnibond.com
Mads Freek Petersen	freek@wayf.dk
Nicole Roy	nroy@internet2.edu
Scott Koranda	skoranda@illinois.edu
Zacharias Törnblom	zacharias@sunet.se
Davide Vaghetti	davide.vaghetti@garr.it
Alan Buxey	alan.buxey@myunidays.com

Federation Operator perspective

Client registration

https://openid.net/specs/openid-federation-1_0.html#section-12
Please note this is NOT the same as registration of a federation member!

Name	Requirement
Niels	1 Support Automatic Client Registration
	2 Provide Trust Chain in the Request
	3 Benefit of Explicit registration?
Nicole	1 Support automatic client registration
	2
	3

Minimum support automatic client registration, scenarios for explicit registration (discourage use, think naughty SAML bi-lateral one-sided/SPs?). Client libraries, may not be possible.

RPs and OPs will still need to register with a federation (Trust Anchor) on a policy basis, but technical automatic client registration possible.

Think about adding how we add ADFS toolkit currently?

Note that during the discussion, SSH via SAML ECP did come up, proving again that any higher ed and research meeting will always result in at least one discussion of SSH over SAML via ECP.

Entity Configuration (metadata) signing and issuance

https://openid.net/specs/openid-federation-1_0.html#section-3
https://openid.net/specs/openid-federation-1_0.html#section-5
https://openid.net/specs/openid-federation-1_0.html#section-8

Name	Requirement
Niels	1 Admin/technical/Contact data and security contact data need to be added
	2
	3
Switch	1 stay compatible with existing SAML world content-wise (unless we deprecate specific elements in both worlds)
	2
	3
Nicole	1 Balancing metadata policy: Minimal requirements for trust, without too much complexity of policy
	2 Very little policy at the eduGAIN level, only the basics
	3 Most of the policy at the national federation level (but national fed ops should make it as simple as possible, too)
Davide	registration authority and scopes (attribute qualifiers?)

Federations already have well defined “paper” trust fabric e.g. https://www.ukfederation.org.uk/content/Documents/FederationContacts, we shouldn’t re-invent the wheel (or part of the wheel)?

Do we need a shibmd:Scope-like 6.2.2 “Naming Constraints” policy thingy that enables us to restrict asserted claim values?

Use of max_path_length to prevent malicious policies/trust chains that could be used to do denial-of-service attacks?

Shared use of resolvers?

Might reduce metadata replication time.

Key handling

https://openid.net/specs/openid-federation-1_0.html#section-11

Name	Requirement
Niels	1 Trust chain exp 1 day?
	2 Entity Config and key rollover 1 day?
	3
Switch	1 ensure end-to-end trust propagation of 1-2 days
	2 follow emerging good practices
	3
Nicole	1 Balancing trust chain security with the metadata re-signing complexity/burden and trust chain caching (how long should a trust chain be valid?)
	2 How frequently should key rollover happen at various levels?
	3 Which crypto algorithms do we need to support (and which do we need to require support for) at the beginning?

We need to delve deeper into resolver response signing as a potential resource use issue: Each response must be signed on-demand. Do we need to use a lightweight signing algorithm like ED25519 for this? Is there something else that needs to be done to accommodate this?

Is there a scaling of HSM usage currently from thousands per day (batch signing of metadata), to millions per day for resolver or trust path usage?

Trust path evaluation

https://openid.net/specs/openid-federation-1_0.html#section-4
https://openid.net/specs/openid-federation-1_0.html#section-10

Name	Requirement
Niels	1 Provide resolver at TA level to take care of heavy lifting for all Entities which are sub
	2
	3
Switch	1 Should each "national" federation provide its own TA for requests not passing borders?
	2
	3
Nicole	1 Federation-hosted metadata policy application and trust chain resolution
	2 Should each "national" federation provide its own TA for requests not passing borders?
	3 Should each "national" federation provide an intermediate which is actually the one that signs? A la CA intermediates? This may help with future change-management needs.

Certification suite? ← YES! THIS is needed (Nicole)

Concern about logic encapsulated in existing federations, and what is happening in SAML feds currently (Example: XML Canonicalization differences which cause hash function discrepancies and thus different signatures for the same metadata) , and whether rules applied at registration easier?

LUNCH at 12.30?

Resolvers

https://openid.net/specs/openid-federation-1_0.html#section-8.3

Name	Requirement
Niels	1 Every TA/Intermediate MUST provide a resolver (but it may not need to run one, just like DNS this may be distributed)
	2 Resolver takes care of heavy lifting on behalf of Fed members
	3
Switch	1 do the heavy-lifting for its member RPs
	2 make it easy for external RPs to trust our members (diploma use case or whatever)
	3
Nicole	1 Every TA/intermediate MUST provide a resolver (but it may not need to run one, like DNS this may be distributed)
	2 Resolver takes care of heavy lifting on behalf of fed members
	3 It’s not just about resolution, it’s also about applying metadata policy, trustmarks and trustmark trust evaluation, etc. Should these functions be separate microservices?
Jon	Can I mention the name clash with people who will be used to “attribute resolver” in Shibboleth? (never written revolver by mistake 😹)

First place of mutual trust and can resolve the chain?

Need functionality of good caching? Each federation may not actually have a resolver, and share technical capability between NRENs

LUNCH AT 12:30!!!

Trust Marks & Trust Mark Issuers

https://openid.net/specs/openid-federation-1_0.html#section-7

Name	Requirement
Wolfgang P. (DFN)	1 Unified process(es) for onboarding Trust Mark issuers
	2
	3
Niels	1 Do we standardize TM semantics?
	2 If edugain and VO membership is based on TMs does it help (RPs) to have a TM for Fed membership also?
	3
Switch	1 That's the real fun bit! Probably a good moment to look into emerging X-sectorial governance models like Ayra
	2 Standardise TM semantics
Nicole	1 How do we prevent trust mark “sprawl” from radically increasing complexity and trust path resolution resource use?
	2 Where do trust mark issuers sit in the TA hierarchy? At the eduGAIN level? National fed level? Some of both? Other? A separate intermediate somewheres(s)?
	3 Trust mark resolution/validation as-a-service at a federation level
	4 How do we handle self-issued trustmarks like REFEDS R&S for OPs?

(OP) Discovery

LIke we do it in SAML federations, this is *not* about the OpenID Connect Discovery protocol

Name	Requirement
Switch	1 How do the RPs learn which OPs exist in order to offer the user a useful choice?
	2
	3
Nicole	1 Providing a richer subset of OP metadata (similar to the existing Shibboleth embedded discovery service discovery json feed) at a federation level.
	2 Every TA and intermediate MUST supply discovery feed
	3 RPs MAY provide their own discovery feed
	4 Discovery services MUST accept a discovery feed parameter

Organisation Registration

Note this is NOT “federation_registration_endpoint“, which is an OP capability.
How organisational entities get registered at the TA/Intermediate is out of scope for the specification, so we can/must lay out the rules for this, and perhaps also the protocol.

Name	Requirement
Wolfgang P. (DFN)	1 Common playbook (mandatory for federations in eduGAIN) for onboarding Intermediates?
	2
	3
Niels	1 Can we separate administrative from technical registration so it does not matter if an org registers 1 or more OPs and RPs
	2
	3
Switch	1 keep our organisational onboarding processes, this is rather protocol agnostic (contractual)
	2 offer a choice of protocols for the technical onboarding
Nicole	1 Onboarding using existing TA/FO processes
	2 eduGAIN requirements must be met by national TAs/FOs
	3 If delegation is present, intermediate onboarding may be its own “thing”

OP perspective

How do we onboard/migrate our institutions?

Name	Requirement
Wolfgang P. (DFN)	1 Mitigation of technical issues when transferring an IdP’s Entity ID to its OIDFed counterpart (Entity Identifier -> iss/Issuer)
	2
	3
Switch	1 Let the SAML participants continue as is with feature freeze
	2 make it attractive and easy to join with OIDC or to migrate to it
	3 the new opportunities to own constituency
Nicole	1 Let SAML participants continue with feature freeze
	2 Make it attractive and easy to join/migrate to use of OIDC - all of our community’s SAML implementations should add support for OIDF
	3 Migration is “opportunistic” until it becomes an emergency/necessary to shut down SAML (example: Quantum Cryptocalypse)
	4 (Sorry about adding a 4th) What about an Implementation profile for OPs to enable things like trustmark-based functionality like claims release/ACR-execution/etc?

Supporting software

https://openid.net/developers/openid-federation-implementations/

Name	Requirement
Nicole	1 We need a diversity of FO software as we have now: Python, Java, Ruby, PHP, etc… Maybe switch one or more of these to Rust/Go? Who knows
	2 All of our community's federating software (SSP, Shib, Identity Python) needs to support OIDF
	3 We will need new functionality we haven't had before, like trust chain compliation/resolution and policy rules engine software, microservices. Much of this stuff will need to be deployed in a "cloud-native" manner to achieve the performance, availability and scaling needed
	1
	2
	3

RP perspective

How do we onboard/migrate our institutions?

Name	Requirement
Niels	1 How can we make OID fed as simple as possible for the RPs - resolver - automation - discovery (service)
	2 How can we offer a migration path from SAML -> OIDC+OIDFed can we persist identifiers between SAML and OIDC+OIDFed?
	3
Switch	1 How to make it as simple for RPs to do federation stuff?
	2 How to enable RPs to profit from interfederation opportunities?
	3 How to enable RPs to interact with other parties from eID world or elsewhere?
Nicole	1 Opportunistic… until it becomes an emergency (Cryptocalypse)
	2 All our software needs to support SxS migration
	3 All our business processes at the FO/eduGAIN levels need to support SxS migration, but we will need localised migration “campaigns” including education, support services, hand-holding, appropriate software, more education, marketing, etc.
	4 (Sorry for adding a 4th) What about an Implementation profile for OPs to enable things like trustmark-based functionality like claims release/ACR-execution/etc?

Supporting software

https://openid.net/developers/openid-federation-implementations/

Name	Requirement
Niels	1 We are seriously lacking RP software I think
	2
	3
Switch	1 Do we have some hope to get something useful from the eID world?
	2
	3
Nicole	1 Would be nice to get some buy-in from at least one major cloud vendor like Microsoft
	2
	3