November 17th 2025

Participants:

- Davide Vaghetti (GARR)
- Matthew Slowe (UKfed/Jisc)
- Harry Kodden (SURF)
- Henri Mikkonen (CSC)
- Nicole Harris (GÉANT)
- Wolfgang Pempe (DFN)
- Calogero Costa (GARR)
- Pål Axelsson (Sunet)
- Björn Mattsson (Sunet)
- Tom Vitez (CANARIE)
- Sami Silén (CSC/Haka)
- Gabriel Zachmann (KIT)
- Rob Smith (JISC)
- Norbert Czier (Pro-M/eduid.hu)
- Esmeralda Pires (FCCN)

Notes:

- test/use cases:
    - Harry: mostly concerned about RP tests and federation, need to add an inter-federation view as well.
    - Nicole: adding a why column to the tests tables would help understanding what we are trying to achieve and where this test or requirement is coming from.
    - Davide:
        - Add already defined requirements for TA to dependencies table
        - Add a TA04 scenario with multiple intermediates
        - Add normative language (MUST/SHOULD/RECOMMENDED) to expected results
    - Nicole: TA should filter out trust chain resolution queries by the eduGAIN trustmark.
    - Pal/Davide: multiple resolve endpoints support
    - Henri: Shib OP does support multiple resolve endpoints (sort of chain resolution) and results can be filtered by trust marks.
    - Gabriel: OFFA supports trust marks, resolve endpoint is chosen by the entity evaluating the configured TAs.
    - Phil: we could have multiple resolve endpoints per federation, as a local one and international one (plus the eduGAIN one).
    - Phil: endpoint authentication for clients should be discussed in the profile.
    - Harry: will add some specific tests for the OP part.
    - Gabriel: the OpenID Federation specification will get a final round of comments before moving to final review for approval.

November 3rd 2025

Participants:

- Davide Vaghetti (GARR)
- Gabriel Zachmann (KIT)
- Esmeralda Pires (FCCN)
- João Guerreiro (FCCN)
- Phil Smart (UKfed/Jisc)
- Matthew Slowe (UKfed/Jisc)
- Pal Axelsson (SUNET)
- Björn Mattsson(SUNET)
- Nicole Harris (GEANT)
- Niels Van Diek (SURF)
- Henri Mikkonen (CSC)
- Harry Kodden (SURF
- Norbert Czier (Pro-M/eduid.hu)
- Halil Adem (GRNET)
- Marc Thomas (DFN-CERT)
- Waldo Fouche (AAF)

Notes:

- Use cases:
  - Federation and inter-federation use cases has been contributed by UKf, check https://docs.google.com/document/d/1u6WTONRukCUQIo1_aGVonTSMJo2K-PTXL6dRQQYgIXY/edit?tab=t.b7iy7ib8eojq
  - eduGAIN Pilot OP1 details for running tests: https://docs.google.com/document/d/1u6WTONRukCUQIo1_aGVonTSMJo2K-PTXL6dRQQYgIXY/edit?tab=t.t7wzb5nxeegh
  - We need a formal approach to define tests.

- Phil: Side service to enable vanilla OIDC RP proposed at TIIME 2025. Any news on that?
- Niels: There are currently a number of projects in the incubator to have RPs for SSP, Apache and nginx modules.
- Pal: Shibboleth SP is going to support OIDF as well in the future.

- Niels: At TIIME unconference on Friday after the event we are going to host an OpenID Federation workshop.

- Action:
  - move actual tests proposal to github, assign a reference number/code to each test.
  - openid federation conformance testing expanding
  - eduGAIN Profile testing

October 20th 2025

Participants:

- Davide Vaghetti (GARR)
- Björn Mattsson (Sunet)
- Pål Axelsson (Sunet)
- Gabriel Zachmann (KIT)
- Tom Vitez (CANARIE)
- Emerald Pires(FCCN)
- Robert Smith(Jisc)
- Nicole Harris (GEANT)
- Calogero Costa (GARR)
- Tim Trojner Hlade (ARNES)
- João Guerreiro (FCCN)
- Sami Silén (CSC/Haka)
- Phil Smart (Jisc/UK Federation)
- Henri Mikkonen (CSC/Haka/Shibboleth)

Notes

- Phil: allowed_entities constraint, JISC is interested in implementing it.
    - Gabriel: current constraints cannot limit the type of entity so that you cannot turn the entity into a TA/Intermediate because the federation type cannot be ruled out.
    - Current implementation allows limiting the number of entities that can be trusted behind a certain node.
- Phil: JISC would like to test also OAuth2 entities, is this something possible in the pilot?
    - Are the current implementations of OP able to work as AS as well?
    - +1 to support OAuth2 use cases, but currently missing tools.
- Current set of use cases proposed (part1):
    - OpenID Federation Explicit Registration use case 1: Federation selected RP to Pilot OP1 and Pilot OP2.
    - OpenID Federation Automatic Registration use case 1: Federation selected RP to Pilot OP1 and Pilot OP2.
    - OpenID Federation Explicit Registration use case 2: Pilot RP1 and Pilot RP2 to a selected Federation OP.
    - OpenID Federation Automatic Registration use case 2: Pilot RP1 and Pilot RP2 to a selected Federation OP.
- Agreed to share the list of use cases with all the participants and define a common set of use cases to be run.
- Resolver/TA separation:

    - Jisc is working on implementing it in the current pilot infrastructure
    - Gabriel is also further developing the resolver function with more resolver strategies, aggressive caching and further enhancement.
- Rust based implementation of TA/IA from SUNET is close to being ready for testing.
- OIDF enabled RP implementations (other than Offa):
    - SSP coming from incubator in the next months (7 months)
    - Shib SP dev team also plan to work on OIDF enabled RP (to be scheduled)
- AAF started the TA registration process.

September 22nd 2025

Participants

- Davide Vaghetti (GARR)
- Pål Axelsson (Sunet)
- Wolfgang Pempe (DFN)
- Björn Mattsson (Sunet)
- Harry Kodden (SURF)
- Halil Adem (GRNET)
- Gabriel Zachmann (KIT)
- Marc Thomas (DFN-CERT)
- Benjamin Lojack (DFN-CERT)
- Calogero Costa (GARR)
- Tim Trojner Hlade (ARNES)
- Niels van Dijk (SURF)
- Henri Mikkonen (CSC/Haka/Shibboleth)
- Sami Silén (CSC/Haka)
- Waldo Fouche (Australian Access Federation)
- Matthew Slowe (Jisc/UK Federation)
- Phil Smart (Jisc/UK Federation)
- João Guerreiro (FCCN)

Notes

Resolve endpoints update (Lighthouse)

- (Gabriel) POC for separating the resolver endpoint from the TA in lighthouse:
- (Matthew) Vanilla (not separated) Lighthouse seems to sustain high rate of requests on the resolve endpoint
- (Niels) Some of lighthouse ops are realtime, but we should rely as much as possible on caching, as simple as HTTP caching
- (Gabriel) lighthouse does some internal caching on the resolve endpoint, a possible strategy is to pre-calculate trust chains so that the cache will be already filled up for the desired TAs.

- (Niels) Incubator Sprint demo with 1 hour of OIDfed stuff:
  https://events.geant.org/event/1946/
  25 Sept 2025 17:00 → 18:00
  OIDFed topics: national federations and Discovery With SeamlessAccess_
- (Henry) Shibboleth has an initial implementation of a local cache
- (Phil) UKf will share load tests results
- (Niels) Probably not a good idea at this stage to spend too much time on optimization of the resolve endpoint

Metadata policy

- (Niels) `metadata_policy` or metadata policy?
- (Pål) we should pay attention to the difference between policy and the technical implementation.
- (Matthew) How to prevent an entity from presenting itself as an RP and then transforming itself into a TA/Intermediate and let in other entities. Can an eduGAIN trust mark prevent this?
- (Gabriel) A way to enforce this is using the `constraints` claim.
- (Matthew) Organization Name matching the legal name
- (Pål)
- Some talk about the current flat list of contacts and our requirements for different contact types e.g. security contacts.
- (From the chat) “Leveraging REFEDs specifications in OpenID Federation federation and OpenID Fed based wallet ecosystem"
  https://wiki.geant.org/spaces/GWP5/pages/694812853/Leveraging+REFEDs+specifications+in+OpenID+Federation+federation+and+OpenID+Fed+based+wallet+ecosystem
- (Niels) Lots of talk about what national federations are doing, but perhaps less so about what eduGAIN needs. However, the national federations feed into eduGAIN, and it would be nice if the national federations work in similar ways this time around.
- (Pål)
- (Wolfgang) This is a good chance to get things coordinated and started together. Agree on the same policies and similar things.

September 8th 2025

Participants

- Gabriel Zachmann (KIT)
- Harry Kodden (SURF)
- Björn Mattsson (SUNET/SWAMID)
- Pål Axelsson (SUNET/SWAMID)
- Henri Mikkonen (CSC/Haka/Shibboleth)
- Niels van Dijk (SURF)
- Tim Trojner (ARNES)
- Wolfgang Pempe (DFN / DFN-AAI)
- Calogero Costa (GARR)
- Tom Vitez (CANARIE)

- Phil Smart (Jisc)
- Matthew Slowe [foo] (UK federation / Jisc)
- Esmeralda Pires (FCCN)
- João Guerreiro (FCCN)
- Norbert Czier (Pro-M/eduid.hu)

Notes

Agenda:

1. Review requirements
2. Metadata policy
3. Schedule (interfed) tests
4. Availability/protection of resolver endpoints
5. If we have time left:
    - OIDF testbed https://testbed.oidf.lab.surf.nl/
    - Future integration options with HSM (Hardware Security Module) [jisc]

Review requirements

Davide discusses the requirements as listed

Remarks:

- Davide: *Contacts* - We want them to be more complex, like we have in SAML (Admin/tech/Security etc) - Niels will look up proposal made by GN Incubator
- Matthew: other implementations available for IA/TA?
    - Participants are using Lighthouse for their TA and Intermediates.
    - In progress : SUNET is developing their own implementation in RUST,
    - SURF is going to test the Sphereon implementation (https://github.com/Sphereon-Opensource/OpenID-Federation)
- Niels: add multilingual support to metadata claims for Intermediates/TA. Example from Leaf entity config with multi language support


```
display_name:                "University of Fribourg"
display_name#en:             "University of Fribourg"
client_name:                 "University of Fribourg"
client_name#en:              "University of Fribourg"
display_name#de:             "Universität Freiburg"
display_name#fr:             "Université de Fribourg"
client_name#de:              "Universität Freiburg"
client_name#fr:              "Université de Fribourg"
logo_uri:                    "
description#de:              "Universität Freiburg"
description:                 "University of Fribourg"
description#en:              "University of Fribourg"
description#fr:              "Université de Fribourg"
organization_name:           "unifr.ch"
organization_name#en:        "unifr.ch"
organization_uri#de:         "http://www.unifr.ch/"
organization_uri:            "http://www.unifr.ch/"
organization_uri#en:         "http://www.unifr.ch/"
organization_uri#fr:         "http://www.unifr.ch/"
```


-

Other libraries & products
https://openid.net/developers/openid-federation-implementations/

Resolve endpoint
We think we need this to make the work for SPs less
Matthew: live metadata resolution could be an intensive computational task, need to understand the volume and impact --- client authentication can be a strategy to enhance security
Gabriel: client authentication was an item discussed at the time of development of the incubator TA implementation (currently lighthouse) --- they came to the conclusion that caching is the real answer
Niels: as we already do for SAML and other services, we can and should implement caching and precomputed metadata resolution strategies.

Matthew:

- Noting that this is similar to MDQ but the resource required may be higher
- How can we (as a FedOp) protect our resources from unacceptable request load while maintaining access to the resolver endpoint for legitimate clients?
- Discussion about client authentication (allowed in spec but could be hard)
- Discussion about moving the resolver endpoint off the TA to somewhere else (can deploy Lighthouse *again* with a different mode)
- Need to consider the ideal caching heuristics to balance security (freshness) against resources (stale data)
- Action: Load test the Resolver endpoint to see how much of a problem this might actually be
- Matthew and Phil to separate Resolver from other TA components and test it under load etc.