OIDFed topics: national federations and Discovery With SeamlessAccess

Mihály Héder
Niels van Dijk
Gabriel Zachmann
Diana Gudu
Kushal Das
Zacharias Törnblom
Bojhan Somers
Hylke Koers
Enrique Pérez
Andrijana Todosijevic

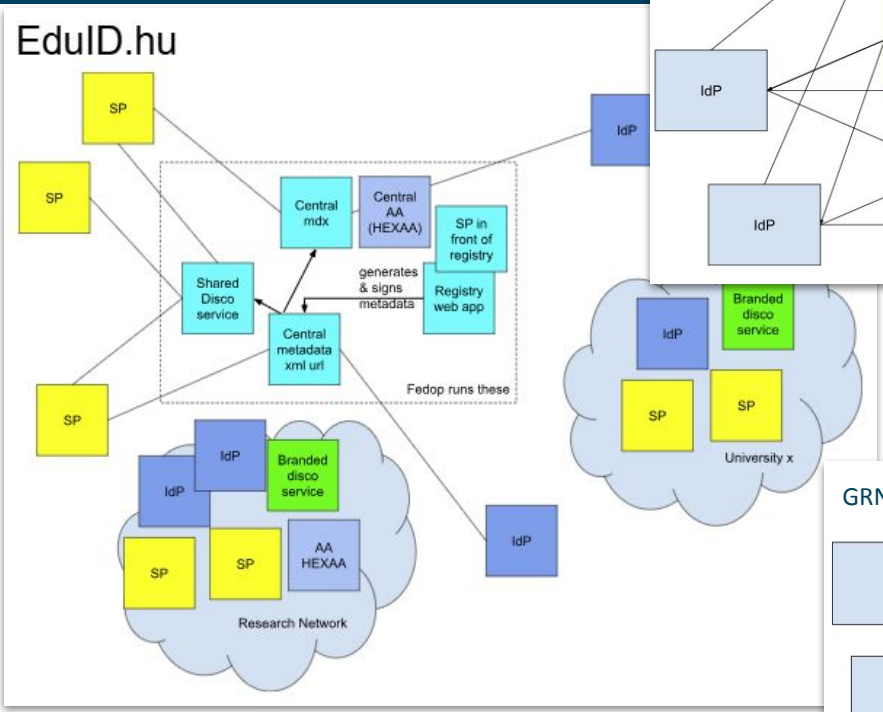
Motivation and initial idea

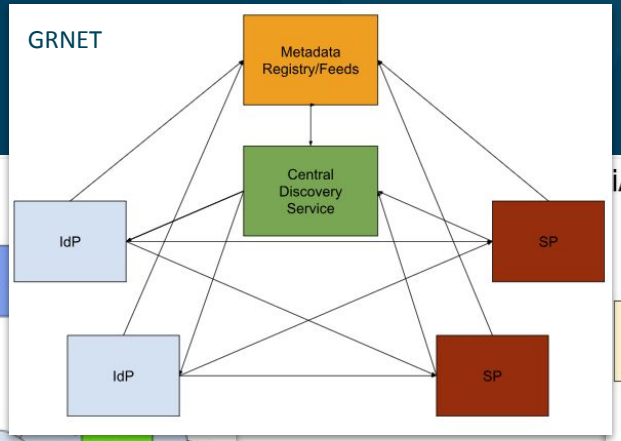
Simulate the migration from SAML Federations to OpenID Federation:

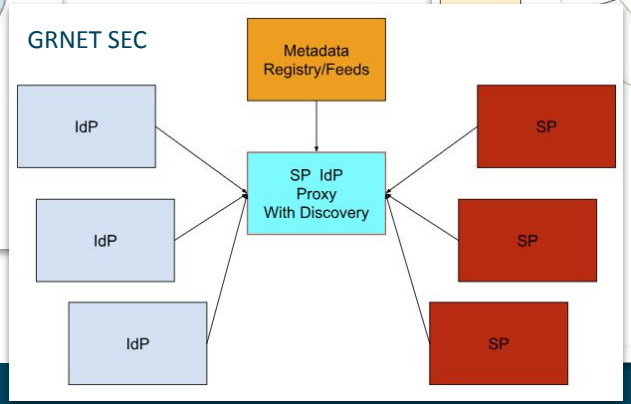
- Can FedOps replicate all functionalities that they already have in the SAML R&E Federations?
- Do the Federations have enough manpower to complete the process?
- Are all the tools ready?
- Are the necessary learning materials for FedOps available?

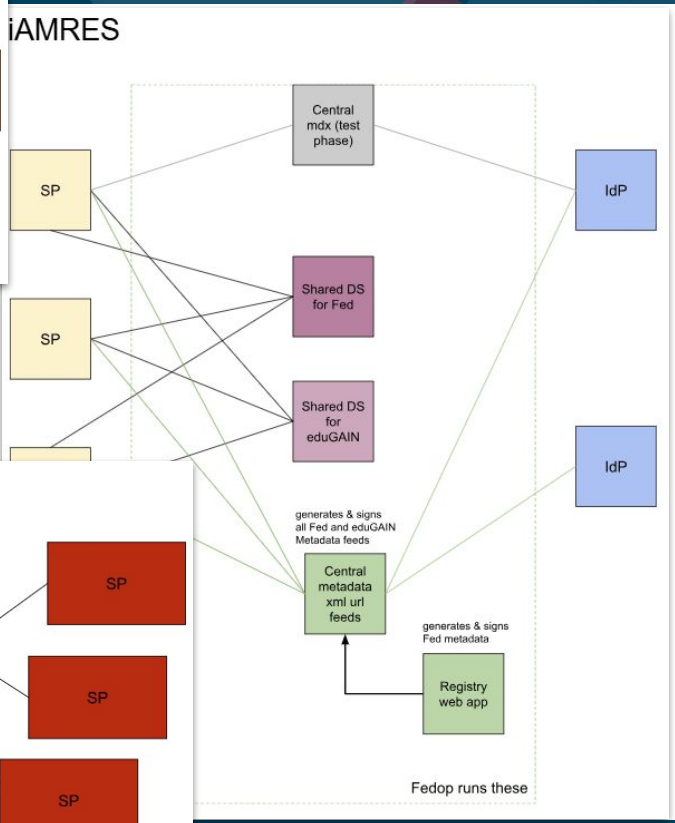
SAML Federation examples

GÉANT
Networks • Services • People









Identified gaps

- DS
- RPs
- Registry

- OpenID Federation R&E Testbed
- AuthMemCookie module for Apache
- DS with SeamlessAccess
- OFFA - Openid Federation Forward Auth

OpenID Federation R&E Testbed

Experimenting at scale

TRUST & IDENTITY INCUBATOR

Ongoing work wrt OpenID Federation

- Establish OID Federation profile for eduGAIN
- REFEDs OID Federation profiling (National Federation)
- Shibboleth and SimpleSamlPHP (OP ‘done’, RP planned)
- Incubator activities on discovery

> But how do we bring all of this together?

> And how do we test and validate our assumptions, preferably at scale?

> How do we enable federation engagement when we cannot overnight rollout OIDF?

TRUST & IDENTITY INCUBATOR

OpenID Federation R&E Testbed

- A “copy” of eduGAIN:
  - All trust relations exist
  - But **no** authentications can flow
- Includes Trust Anchors, OPs & RPs and Trustmarks as their equivalent exist in eduGAIN today
- Entities may be added or left out to study impact

Evaluate the impact of technical and policy decisions *before* we roll them into production

Broader engagement with OpenID Federation R&E Testbed

Provide working example of OIDFed implementation at scale

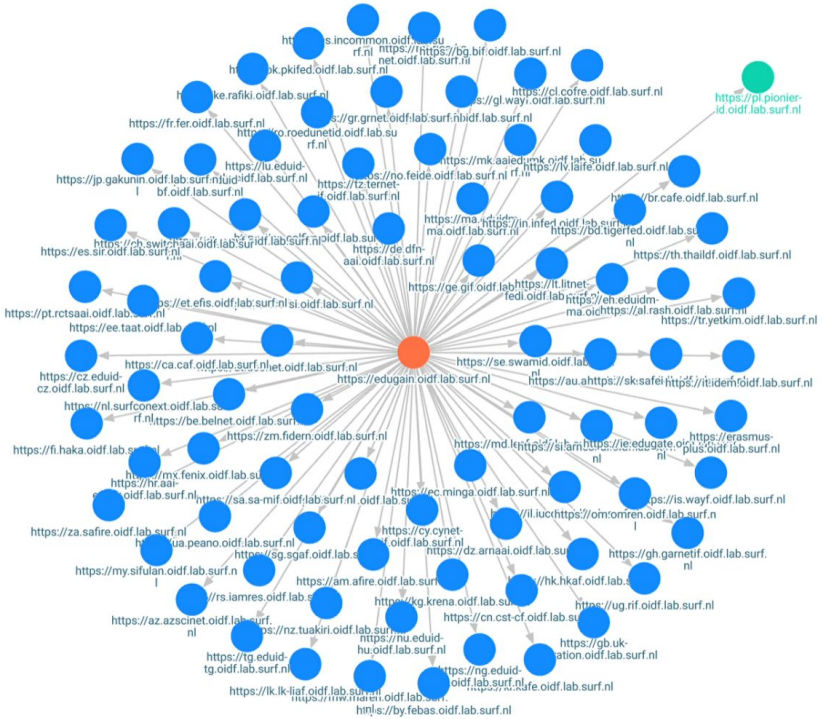
- Test with chain resolution
- OP and RP development
- Test Registry, TA, TMI and TMO tooling
- Discovery
- Interop testing
- Certification

OpenID Federation R&E Testbed - Technically

- Leverages go-oidfed (now: Lighthouse) (https://github.com/go-oidfed/lighthouse)
- Approx 120 dockers for TAs, TMIs, TMOs
- Approx 10k Leafs
- Test OPs and RPs

And a shoutout to HARICA's ACME implementation!

OpenID Federation R&E Testbed - Demo



TRUST & IDENTITY INCUBATOR

Findings so far

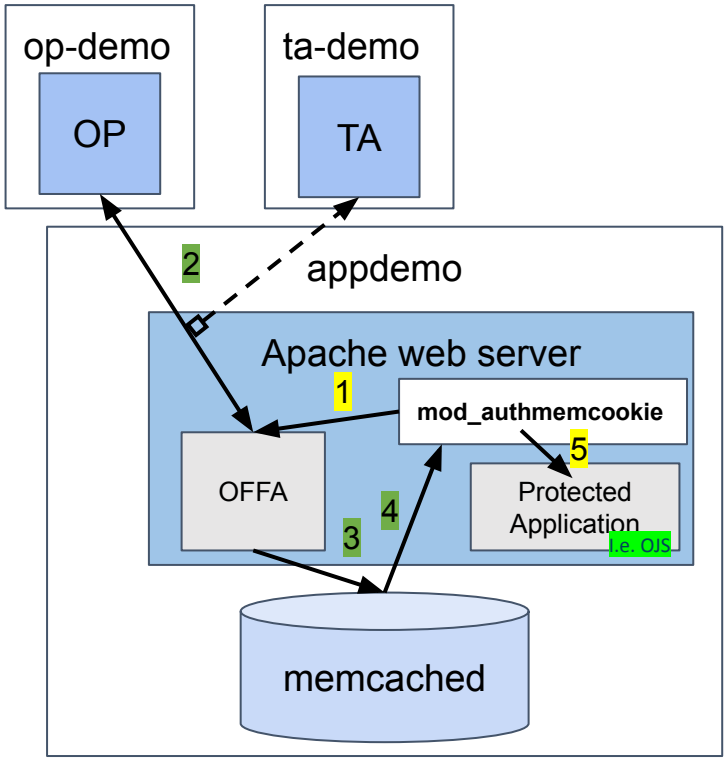
- Many things DO ‘translate’ pretty well - example
- Multi language support
- Several metadata elements we know from our SAML metadata cannot directly be represented:
  - Contacts
  - Shib MD Scope
  - Metadata registration statement

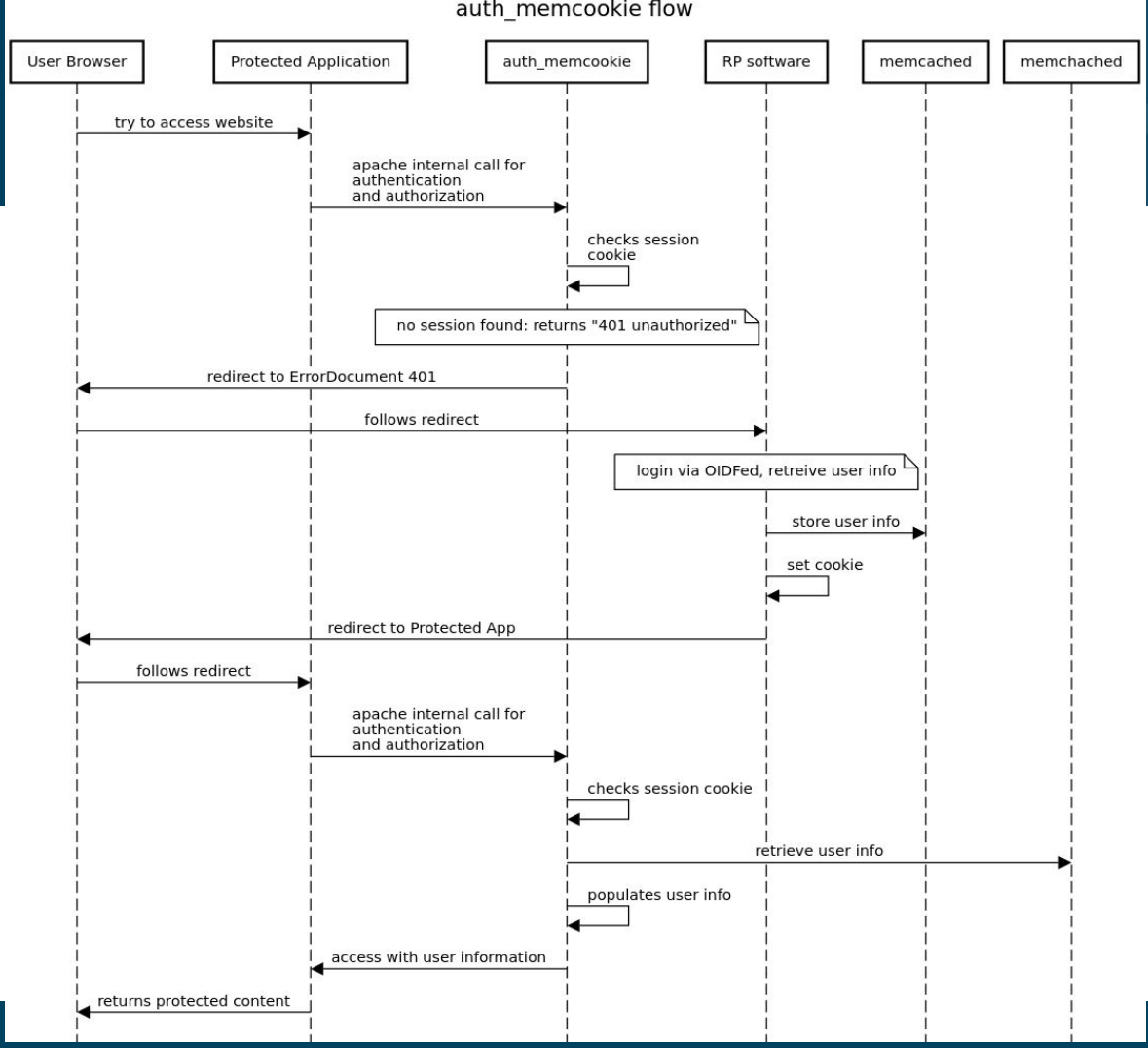
Dynamic trustmark for Shib MD Scope


```
{
    "trust_mark_type": "https://refeds.org/trustmarks/md_scope",
    "iss": "https://ta.federation.org",
    "sub": "https://leaf.institution.org/op",
    "iat": 1579621160,
    "ref": "https://refeds.org/trustmarks/md_scope/index.html",
    "mdscope": [
        "institution.org",
        "student.institution.org",
        "institution-businessschool.com"
    ]
}
```

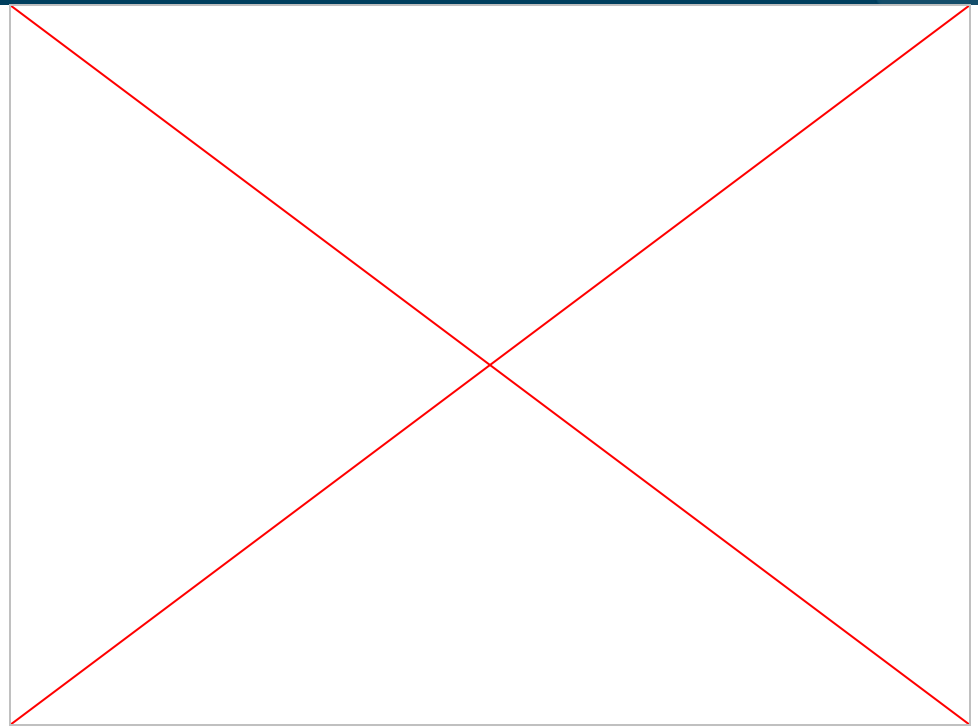
Apache module AuthMemCookie

Instant integration via Apache module AuthMemCookie

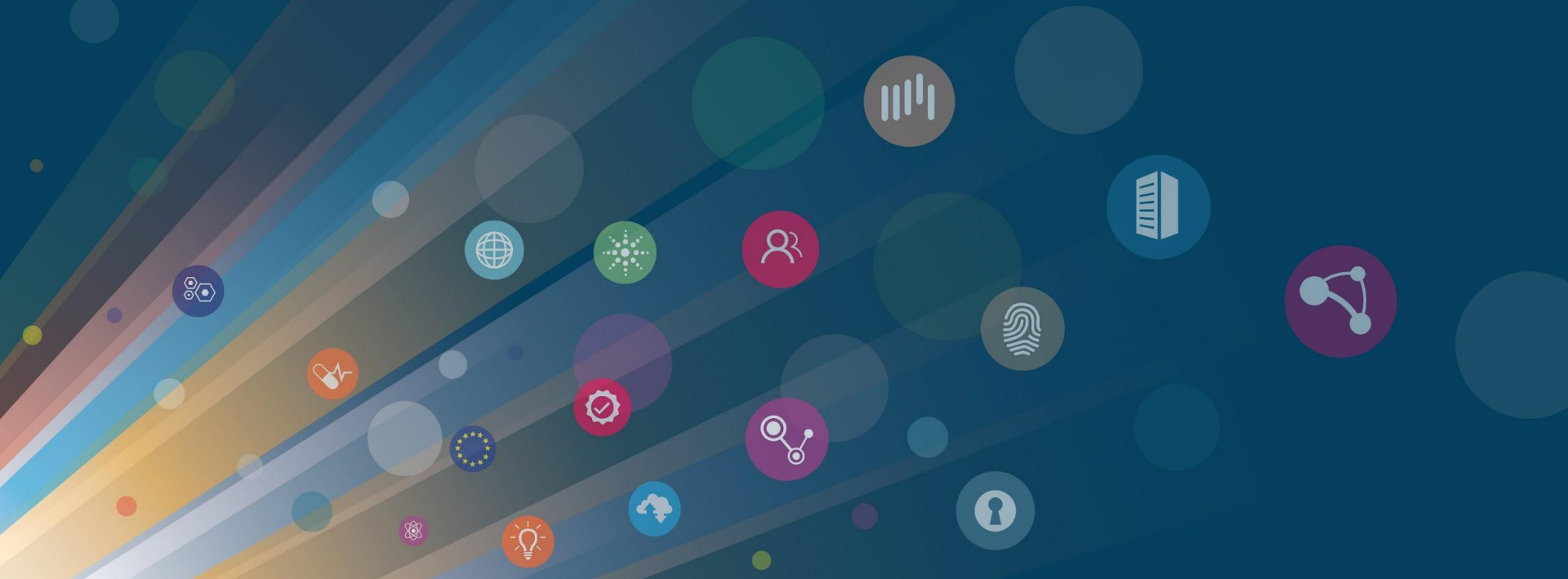




Instant integration via Apache module AuthMemCookie - Demo



SeamlessAccess with OIDFed Support



Goal

Integrate the SeamlessAccess with OpenID Federation:

- Show OIDC OPs the same way as SAML IdPs

Work Done

1. Investigate OpenID Federation discovery

Discovery Flow

2. Investigate OP listing methods, OIDFed Spec

Entity Collection endpoint

Propose additional metadata claims to the OpenID Federation specification

Work Done

3. Investigate SeamlessAccess architecture

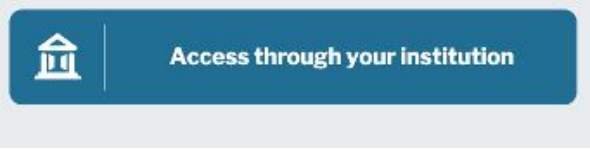
Identified points of integration:

- MDQ
- thiss-js

SeamlessAccess - introduction

SeamlessAccess

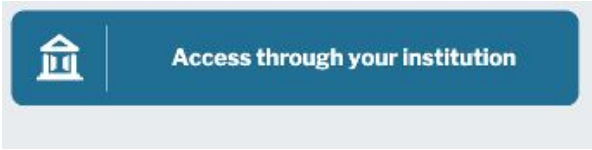
- Not-for-profit, collaborative initiative run by **GÉANT, Internet2, NISO**, and the **STM** Association
- Designed to foster a **more streamlined online access experience** when using scholarly collaboration tools, information resources, and shared research infrastructure.
- **Improving usability** of Federated Authentication



SeamlessAccess - introduction

Three key value elements:

1. **Consistent, recognizable UI**



Same button on different website
→ **recognition** and **trust**

SeamlessAccess - introduction

Three key value elements:

1. Consistent, recognizable UI
2. **Ability to remember the user's choice of institute across participating websites**

Pre-populated as much as possible

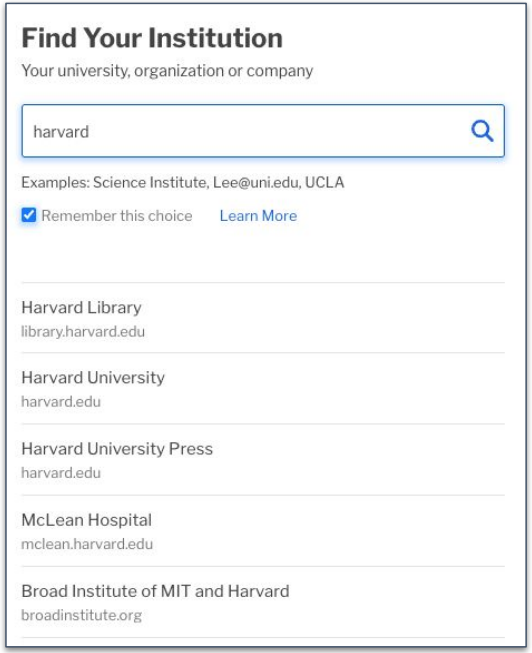
SeamlessAccess - introduction

SeamlessAccess

Three key value elements:

1. Consistent, recognizable UI
2. Ability to remember the user's choice of institute across participating websites
3. **Best-in-class IdP discovery service**

User-friendly way for users to **find their home institute**



SeamlessAccess - introduction

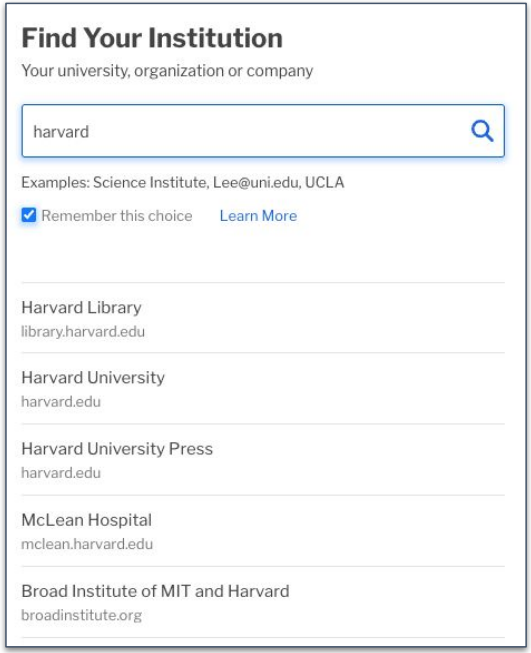
SeamlessAccess

Behind the scenes

- **Aggregate metadata** from eduGain, OpenAthens, NRENs
- MDQ

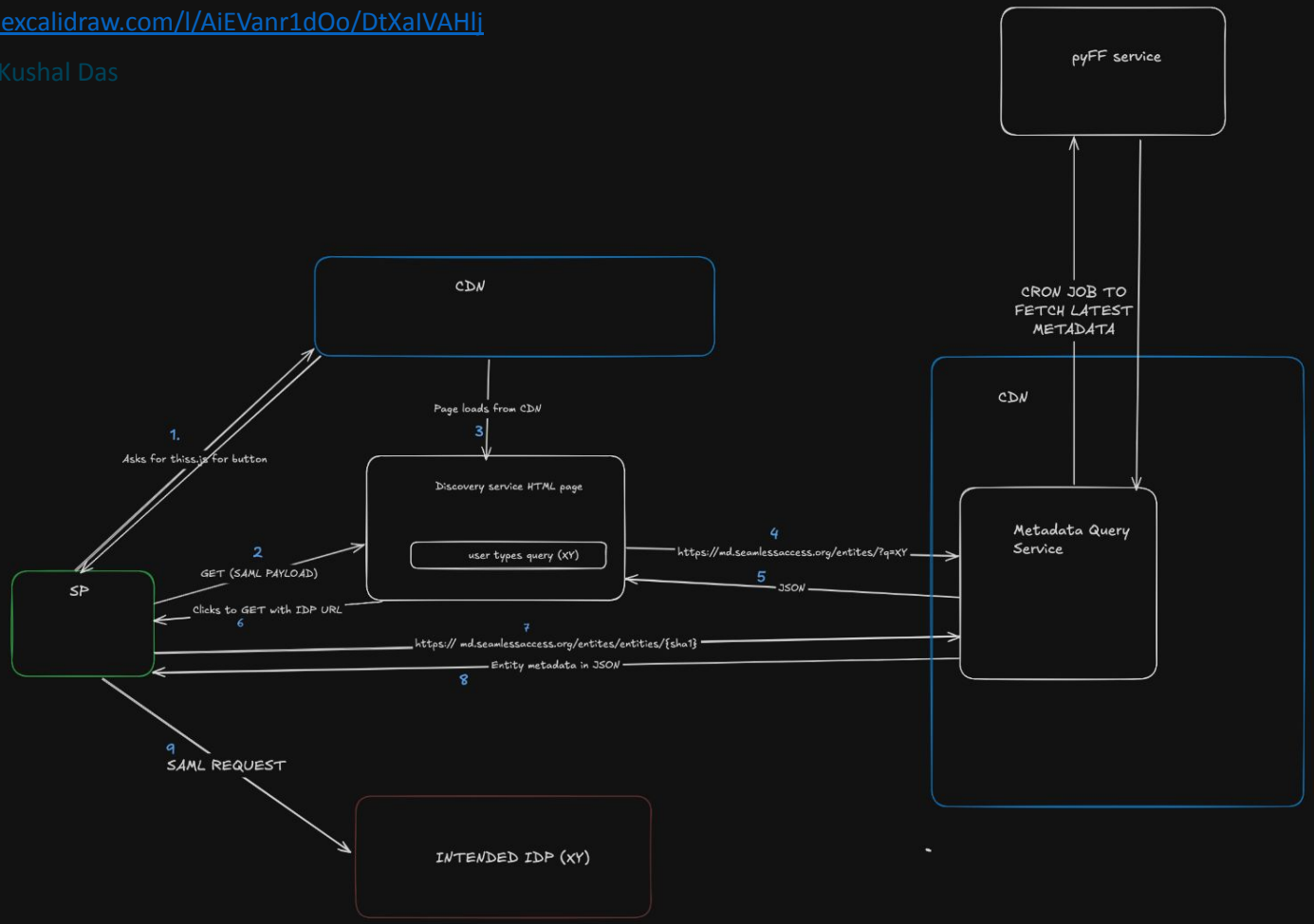
Under development: **customization** for Service Providers integration that use the discovery service:

- ‘Filtering out’ - ability to *remove* IdPs: live
- ‘Pinning’ - ability to prioritize IdPs: 2025Q4
- Co-branding: 2025Q4
- ‘Filtering in’ - ability to *add* IdPs: 2026Q1



https://app.excalidraw.com/l/AiEVanr1dOo/DtXaIVAHlj

courtesy of Kushal Das



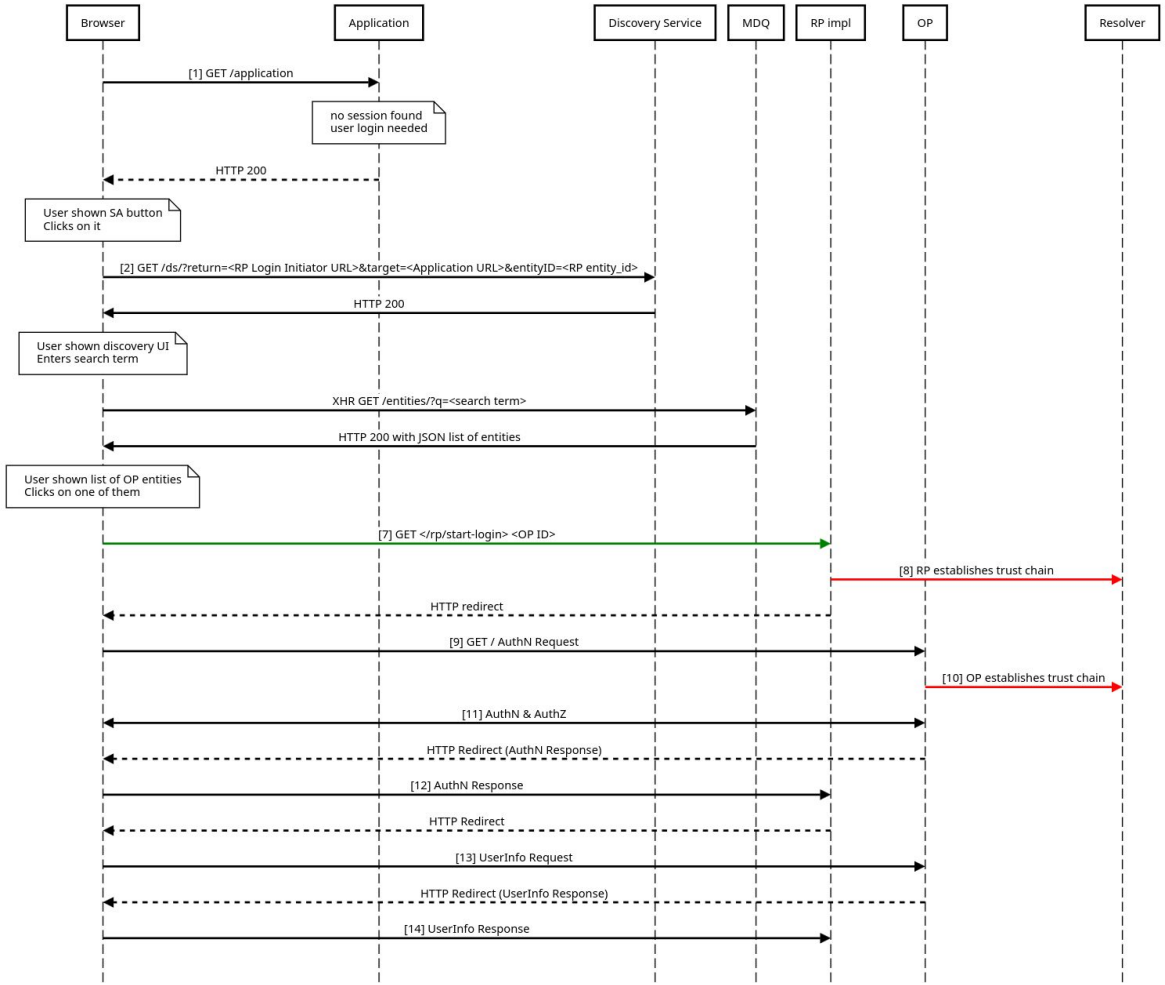
SeamlessAccess thiss-js changes

- SeamlessAccess uses an MDQ (metadata query) service to get the metadata of the OP's that are presented as choices to the end users of some RP that uses SeamlessAccess for discovery.
- Once the end user has chosen an OP, they are redirected to a *discovery response* endpoint of the RP, with the entity_id of the chosen OP as a query parameter, such that this endpoint knows how to initiate authentication of the the user using the chosen OP.

Differences between using SAML and Openid federations.

- The metadata served for SAML has a different JSON schema than that served for Openid. We have built a PoC MDQ server that serves Openid federation metadata, and also we have taught SeamlessAccess to understand both schemata.
- The query parameters that are accepted by the *discovery response* endpoints of SAML SP's and Openid RP's are different. We have taught SeamlessAccess to use one or the other set of query parameters depending on the metadata schema served by the configured MDQ service.

User logs in to Application with OID Federation - No persisted OP



Entity Collection Endpoint Specification

- Draft for an extension to the OpenID Federation specification
- Goal: Well-defined mechanism to obtain a filterable list of all(*) Entities in a federation
  - Primary intent: UI purposes, e.g. OP selection

(*) Not only direct subordinates

- Request: flexible filters
- Response: List of Entities with their UI related Claims
- Need for additional UI related Claims in the OIDFed spec
  - Submitted PR; accepted

- GitHub Repo: https://github.com/zachmann/openid-federation-entity-collection
- Issue Discussions: https://github.com/zachmann/openid-federation-entity-collection/issues
- Rendered Version: https://zachmann.github.io/openid-federation-entity-collection/main.html

Entity Collection Endpoint - Examples

Example Request

```
GET /collection?entity_type=openid_provider&
trust_mark_type=https://rp.refeds.org/sitfi&
trust_anchor=https://swamid.se HTTP/1.1
Host: openid.sunet.se
```

Example Response Entity Entry

```
{
  entity_id: https://fedop.example.com,
  entity_types: [
    federation_entity,
    openid_provider
  ],
  ui_infos: {
    openid_provider: {
      display_name: Example OP,
      keywords: [
        foo,
        bar
      ],
      logo_uri: https://fedop.example.com/static/img/logo.png,
      policy_uri: https://fedop.example.com/policy
    },
    federation_entity: {
      logo_uri: https://fedop.example.com/static/img/logo.png
    }
  }
}
```

OFFA - Openid Federation Forward Auth

- Enabling OpenID Federation SSO for “legacy” Services.
- Forward Authentication Service:
  - OFFA acts as a gatekeeper in front of services, handling authentication requests via a reverse proxy
  - Works with NGINX, Apache, Caddy
- Can also be used with the AuthMemCookie Apache Module
- Pass Userinfo to Service via HTTP Headers
- Easy to deploy with docker compose

- GitHub: https://github.com/go-oidfed/offa
- Documentation: https://go-oidfed.github.io/offa/
- Docker: https://hub.docker.com/r/oidfed/offa/tags
- Demo: https://hello.test.fedcloud.eu

Discovery with SeamlessAccess - Demo

GÉANT
Networks • Services • People

TRUST & IDENTITY
INCUBATOR

Future plans

- Continue our current work
- SimpleSamlPHP RP
- Apache_mod_oidfed
- Federation Registry API
  https://gitlab.software.geant.org/TI_Incubator/federation-admin-api
- Prepare the discovery elements for the community

Reach out to us!