New Challenges with Interfederation SPs?

Interfederation unites various cultures

SWITCH

SWITCHaai Team
aai@switch.ch

Goals

- Get an idea of why access to an interfederated SP might fail differently than in SWITCHaai
- Understand what is different regarding
  - Opt-in vs. opt-out
  - Metadata
  - Discovery Service
  - Attributes
- Know whom to contact and where to get help

Interfederation Rollout: Opt-in vs. Opt-out

- Opt-in
  - IdPs and SPs decide when they are ready to interfederate
    - Once the configuration is up-to-date
      - Interfederation Metadata gets loaded
      - IdP: Additional attributes, user consent
      - SP: Discovery Service, attribute mapping, access rules
  - ⊖ Slow process
  - ⊕ Entities unlikely to cause interoperability problems

- Opt-out
  - Federation announces a flag day for enabling interfederation
    - IdPs and SPs need to opt-out before
      - if they do not want to participate
      - if they are not yet ready
  - ⊕ Quick adoption
  - ⊖ More likely that entities cause problems, unless they opted-out before the flag day

Three Examples

1) UK Data Archive
   http://www.data-archive.ac.uk
2) FUNET FileSender
   https://filesender.funet.fi
3) WISEflow
   https://europe.wiseflow.net

What is wrong in these examples?

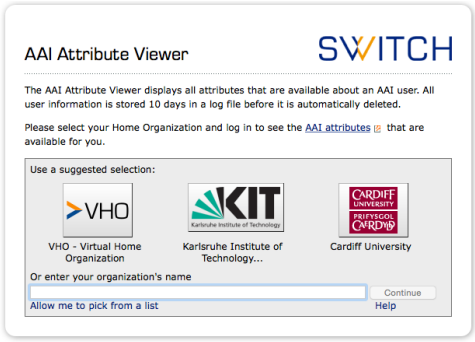
1) Unclear use of terminology at the SP to know whether interfederation is supported or not
   Central discovery service of the UK Federation lists all interfederated IdPs, even when the service did opt-out
2) eduGAIN shown as an option, but no IdPs available that are interfederated via eduGAIN
3) eduGAIN is not available as an option to pick from, despite the SP is published to eduGAIN

Metadata

<meta><data>

- Interfederated IdPs and SPs need additional metadata
  - SWITCHaai entities configure an additional metadata source signed with the same trust anchor.
  - 'Opt-out federations' integrate all entities into a single metadata file.
- Propagation speed of metadata changes
  - In SWITCHaai: two hours
  - For interfederation: one to a few days
- Possible issue
  - SP does not load interfederation metadata
    - SP does not know the IdP and fails.

Discovery Service (DS)



- Within SWITCHaai, users easily find their IdP
- An SP needs a DS that knows the appropriate set of IdPs
  - An interfederation enabled SP registered in SWITCHaai needs to deploy a DS that includes interfederation
  - E.g. in the UK Federation the central DS lists always all interfederated IdPs, also for SPs that did opt-out
    - That can result in such an error message at your IdP: **Shibboleth SSO profile is not configured for relying party https://sp.example.org/shibboleth-sp**

Attributes

- Missing attributes cause interoperation problems
  - Check SP's attribute requirements in the Resource Registry
  - Verify that attributes were released (in IdP's `audit.log`)
    - If NO: check your IdP's attribute release policy
    - If YES
      - Were all required attributes released?
        - If YES: SP has to check it out why it fails
        - If NO: review your attribute release policy

- Another issue:
  - An SP failed because it was not able to decrypt the SAML assertion that included the attribute values.
    The SP's federation used only signed but not encrypted SAML assertions, so that problem was not discovered earlier

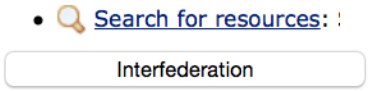
Exploring interfederated entities

- Is a university's IdP or an SP already interfederated?
  - go to: https://technical.edugain.org/status.php
  - pick the country where the entity might be registered
  - under 'Metadata URL' click on 'validate this metadata set', then on 'show entities list'
- or search it in the **eduGAIN List of Entities**
  - go to: https://technical.edugain.org/entities.php
- or try the **Is Federated Checker**
  - go to: https://wiki.edugain.org/isFederatedCheck/
  - provide email addresses or domain names

- Additional web pages of interest
  - Which interfederated SPs are committed to the GEANT Data Protection Code of Conduct (CoCo)?
    - go to: http://monitor.edugain.org/coco/
  - **REFEDS Metadata Explorer Tool** (MET)
    - go to: https://met.refeds.org/

Troubleshooting interfederated entities

- Find an SP in the Resource Registry
  - go to: https://rr.aai.switch.ch/
  - pick 'Search for resources'
  - pick 'interfederation'



- or search it in the metadata file 😀
  - `/opt/shibboleth-idp/metadata/metadata.interfederation-sps.xml`

- Contact the SWITCHaai Team

  ➔`aai@switch.ch`