The Administrative Task

SWITCHaai Interfederation Access Declaration

SWITCH

Thomas Lenggenhager
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

Overview

- The steps required to interfederate

- SWITCHaai Interfederation Access Declaration

- What's to consider for IdPs?

- What's to consider for SPs?

The Steps Required to Interfederate

1) Once per SWITCHaai Participant from the SWITCH Community a signature is required

2) Thereafter, SWITCH sets the 'flag' in the Resource Registry for that institution

3) Now, the IdP and SP administrators can opt-in for interfederation provided;

   - they first adapt their IdP and SP configurations according to the new "Enabling Interfederation Support" guides
   - the IdP administrator installs and configures uApprove to support user consent
   - Finally the administrator can click the checkbox in the Resource Registry!

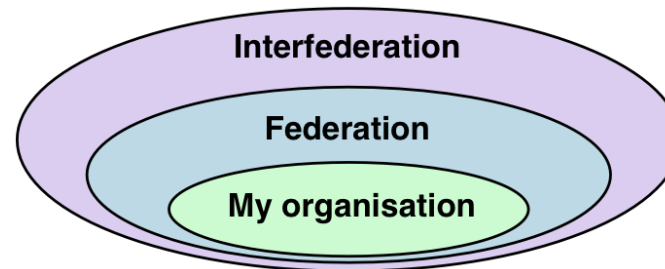| Interfederation	
Interfederation	☑ Enable interfederation for this Home Organisation Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources.

http://www.switch.ch/aai/interfederation

SWITCHaai Interfederation Access Declaration

- The Interfederation Access Declaration needs to be signed to assert:

  1) the institution is aware of the additional data protection requirements when releasing personal data beyond SWITCHaai participants.

  2) the institution acknowledges that it is liable for the actions of its End Users according to the "Service Regulations for Services by SWITCH" and the "SWITCHaai Service Description"

  3) that the IdP supports user consent (uApprove module)

  4) the SPs adhere to the "Code of Conduct" (CoC) and implement a privacy statement along the CoC-criterias

http://www.switch.ch/aai/interfederation

What's to consider for IdPs?

- ## Release of personal information to foreign SPs

  - Install and activate User Consent for attribute release (uApprove) (required for interfederation, optional in SWITCHaai)

  - Check and update your "Default Attribute Release Policy" in the RR

    - To whom to release what by default?

  - Constantly review the necessity of specific Attribute Policy Rules

What's to consider for SPs?

- Not every SP needs to interfederate!
  You should have a good reason

- Who shall be allowed to use my service?
  - Users from IdPs from
    - My Organization
    - SWITCHaai Federation
    - Interfederation
    - or my own selective set of IdPs

- Which attributes does my service **really** require?
  - Be as restrictive as possible
  - Check what IdPs might be able to provide