Federated Identity Management

SWITCH

SWITCHaai Team
aai@switch.ch

Agenda

- What is Federated Identity Management?
- What is a Federation?
- The SWITCHaai Federation
- Interfederation

Evolution of Identity Management

- Stone Age
  Application maintains unique credential and identity information for each user locally

- Bronze Age
  Credentials are centralized (e.g. Kerberos, LDAP) but applications maintain all user identity information

- Iron Age
  Credentials and core identity information is centralized and application maintains only app-specific user data

Federated Identity

- Current mechanisms assume applications are within the same administrative domain
  - Adding an external user means creating an account in your IdM system. This could result in the new user having access to more than just the intended application.

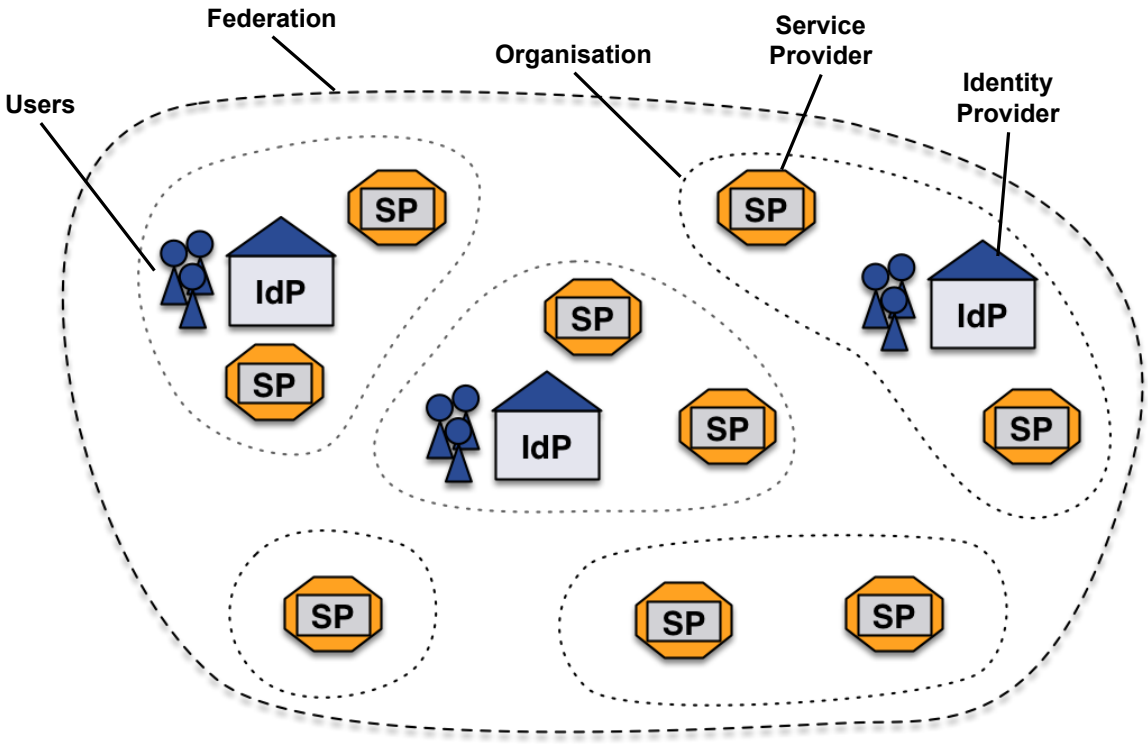
- Federated Identity Management (FIM) securely shares information managed at a users home organization with remote services.
  - Within FIM systems it doesn't matter if the service is in your administrative domain or another. It's all handled the same.

Federated Identity

- In Federated Identity Management:
  - **Authentication** (AuthN) takes place where the user is known
    - An **Identity Provider** (IdP) publishes authentication and identity information about its users
  - **Authorization** (AuthZ) happens on the service's side
    - A **Service Provider** (SP) relies on the AuthN at the IdP, consumes the information the IdP provided and makes it available to the application
  - An **entity** is a generic term for IdP or SP

- The first principle within federated identity management is the active protection of user information
  - Protect the user's credentials
    - only the IdP ever handles the credentials
  - Protect the user's personal data, including the identifier
    - a customized set of information gets released to each SP

Federated Identity Management



Benefits of Federated Identity Management

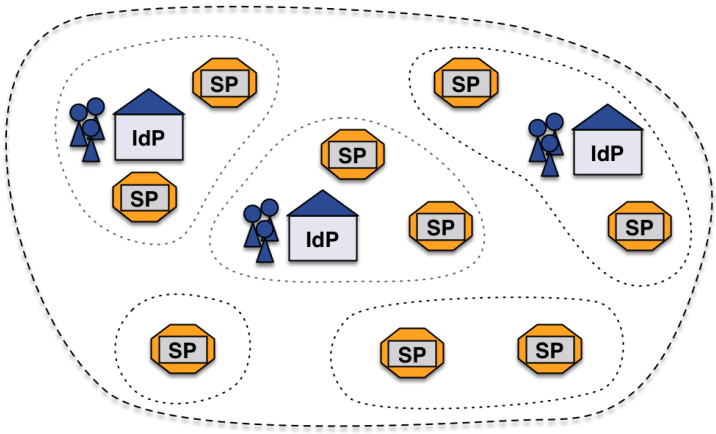
- Reduces work
  - Authentication-related calls to Penn State University's helpdesk dropped by 85% after they installed Shibboleth
- Provides current data
  - Studies of applications that maintain user data show that the majority of data is out of date. Are you "protecting" your app with stale data?
- Insulation from service compromises
  - With FIM data gets pushed to services as needed.
    An attacker can't get everyone's data on a compromised server.
- Minimize attack surface area
  - Only the IdP needs to be able to contact user data stores.
    All effort can be focused on securing this single connection instead of one (or more) connection per service.

Some other gains

- Users generally find the resulting single sign-on experience to be nicer than logging in numerous times.
- Usability-focused individuals like that the authentication process is consistent regardless of the service accessed.
- A properly maintained federation drastically simplifies the process of integrating new services.

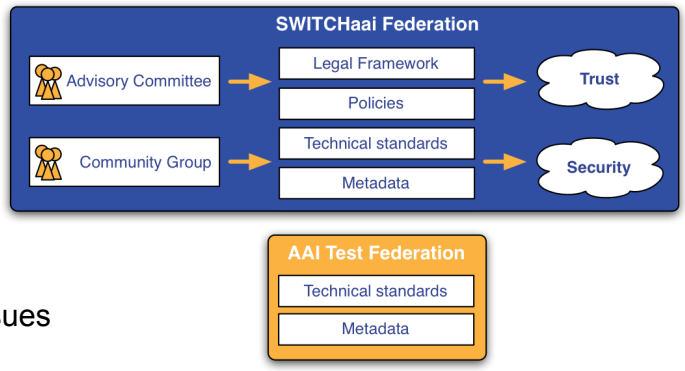
What is a Federation?

- A group of organizations running IdPs and SPs that agree on a common set of rules and standards
  - It's a label - to talk about such a collection of organizations
  - An organization may belong to more than one federation at a time
- The grouping can be on a regional level (e.g. SWITCHaai) or on a smaller scale (e.g. large campus)
- Note:
  IdPs and SPs 'know' nothing about federations



SWITCHaai (1)

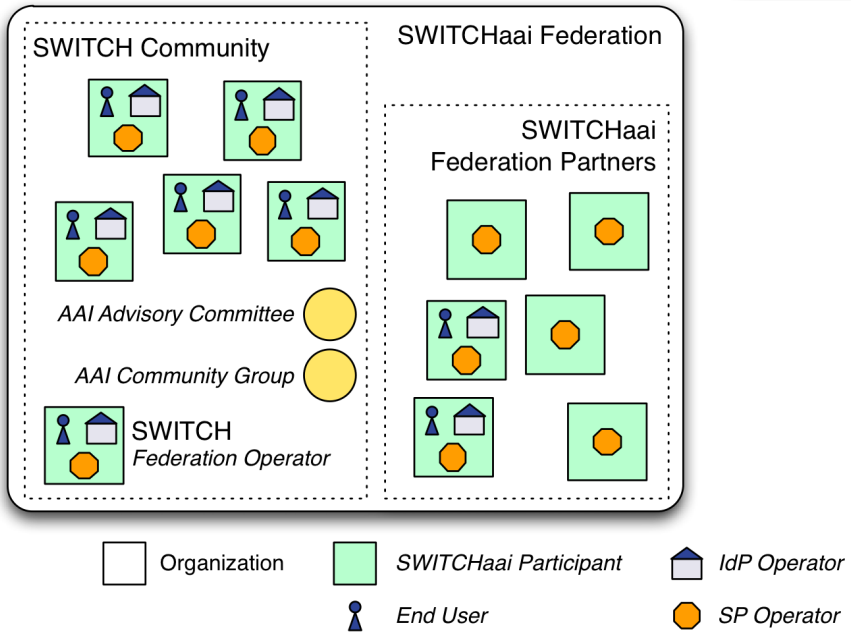
- SWITCH consults with two bodies
  - Advisory Committee deals with policies and legal framework
  - Community Group deals with technical/operational issues



- Two kinds of SWITCHaai Participants
  - **SWITCH Community**
    - Organisation fits the definition from the SWITCH Service Regulations
  - **SWITCHaai Federation Partner**
    - Organisation sponsored by a SWITCHaai Participant from the SWITCH Community

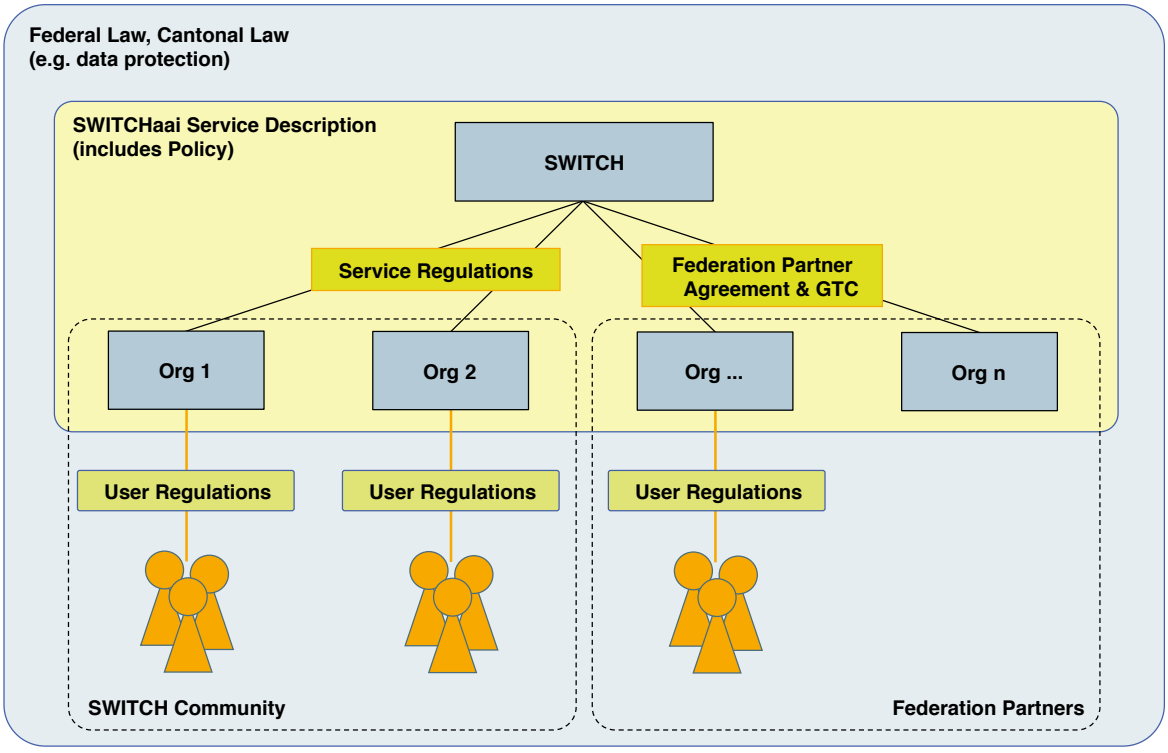
https://www.switch.ch/aai/about/federation/

SWITCHaai (2)



- SWITCH operates the SWITCHaai Federation
- AAI is a Basic Service for the SWITCH Community

SWITCHaai: The Legal Framework



SWITCHaai: Rules, Policies, & Agreements

- **SWITCHaai Service Description** (includes the Policy)
  concepts and rules for all entities in the federation
  https://www.switch.ch/aai/docs/SWITCHaai_Service_Description.pdf

- **SWITCHaai Federation Partner Agreement**
  legal contract between SWITCH and federation partner

- **Certificate Acceptance Policy**
  policy certificates accepted by the federation
  https://www.switch.ch/aai/support/certificate-acceptance.html

- **AAI Attribute Specification**
  minimum set of core and optional attributes supported by federation entities
  https://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf

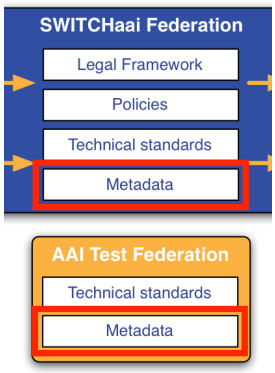
- **Best Current Practices for SWITCHaai service operations**
  Common practices for operating an IdP or SP
  https://www.switch.ch/aai/bcp

SWITCHaai: Services Provided

- Rules, policies and agreements https://www.switch.ch/aai/documents
- Guides: installation, configuration & migration https://www.switch.ch/aai/support
- Centralized Services https://www.switch.ch/aai/tools
  - Discovery Service
  - Resource Registry, the federation management Web App
  - Virtual Home Organization (VHO) & Guest Login
  - Attribute Viewer & AAI Demo
  - Group Management Tool (GMT)
- Call-in helpdesk and email support: aai@switch.ch
- uApprove Shibboleth IdP plugin for user consent
- AAI Test Federation
- Some application integration support
- Training

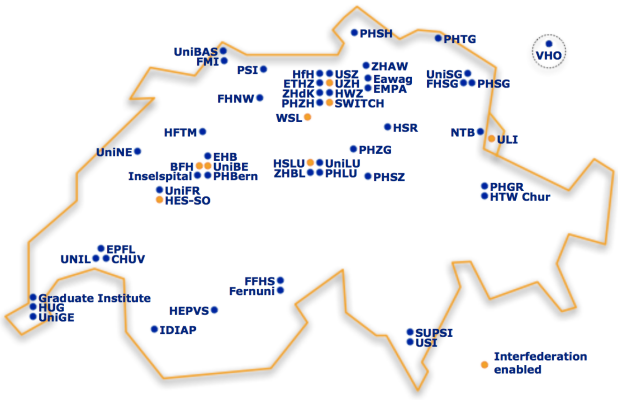
Federation Metadata

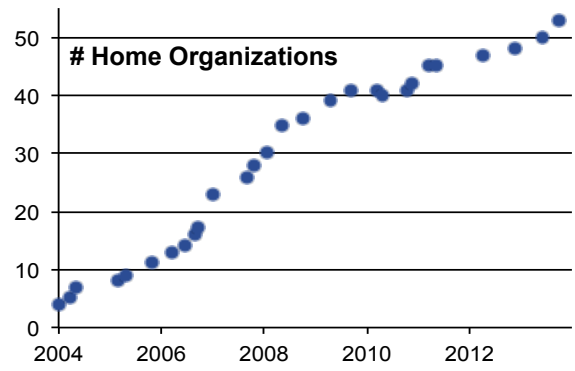
- An XML document that describes **every federation entity**
- Contains
  - Unique identifier for each entity known as the **entityID**
  - Endpoints where each entity can be contacted
  - Certificates used for signing and encrypting data
- May contain
  - Organization and person contact information
  - Information about which attributes an SP wants/needs
- Metadata is usually distributed by a public HTTP URL
  - The metadata should be digitally signed
  - Signature should be verified!
  - Bilateral metadata exchange scales very badly
- Metadata must be kept up to date, so that
  - new entities can interoperate with existing ones
  - old or revoked entities are blocked

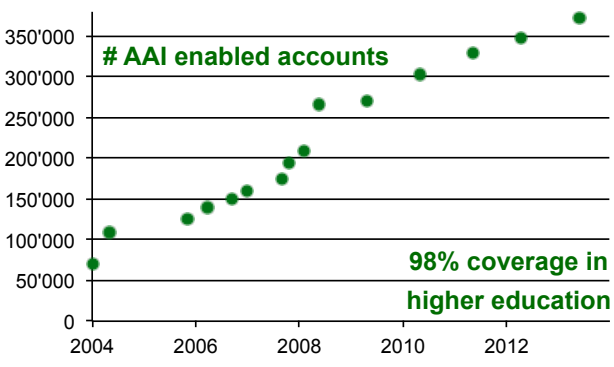


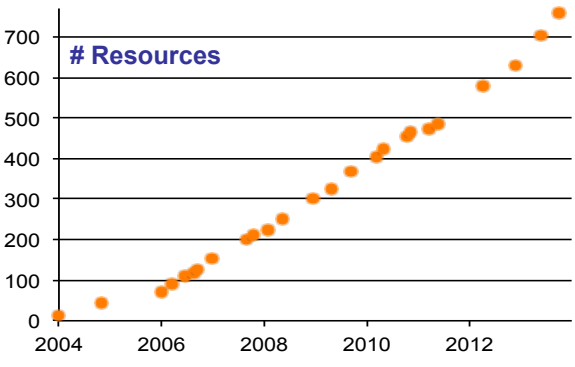
https://www.switch.ch/aai/metadata

SWITCHaai Federation Autumn 2013



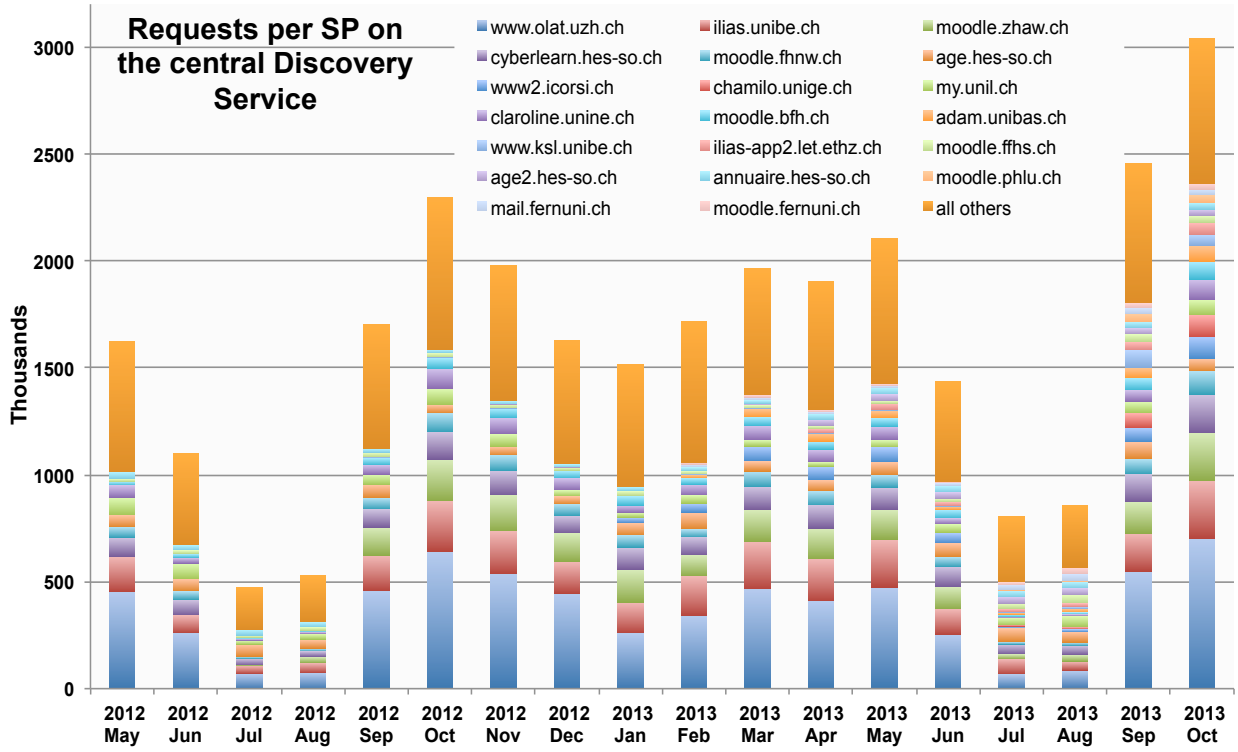






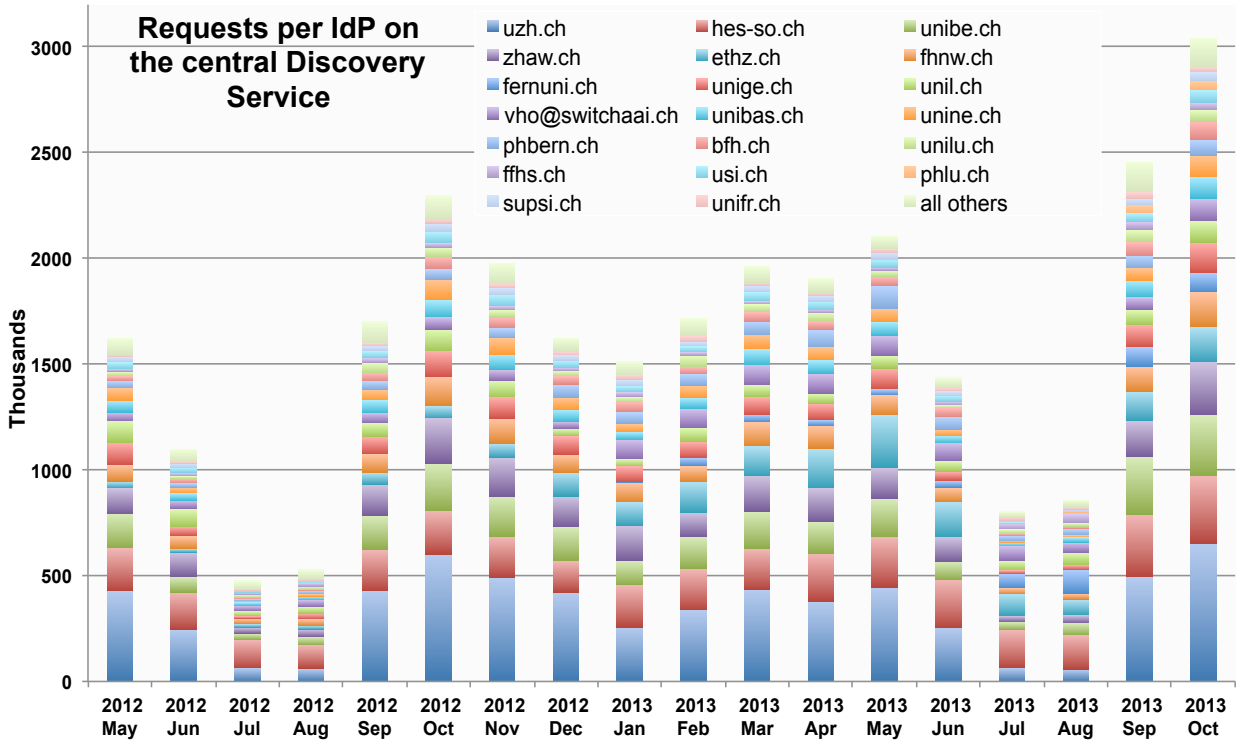
AAI User Authentication Requests

May 12 - Oct 13



AAI User Authentication Requests

May 12 - Oct 13



Interfederation

- Users get access to services from other federations
- eduGAIN is the GÉANT Interfederation Service
- See the 'Interfederation' presentation.

http://www.edugain.org
http://www.edugain.org/technical/status.php