Federated Identity Management

SWITCH

Thomas Lenggenhager
aai@switch.ch

SWITCHaai Introduction Course
Bern, 1. March 2013

Overview

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

Federated Identity

- Older mechanisms assume applications are within the same administrative domain
  - Adding a user from outside means creating an account within your IdM system. This could result in the new user having access to more than just the intended application.
  - *Simple technical solutions based on domain cookies*

- 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.
  - *More advanced technical solutions required!* ➔ *SAML2*

SAML = Security Assertion Markup Language

Federated Identity (2)

- In Federated Identity Management:
  - 

    Identity Providers (IdP) asserts authentication and identity information about users
  - 

    Service Providers (SP) check and consume this information for authorization and makes it available to an application
  - An IdP or SP is generically known as an **entity**

- 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 credential
  - Protect the user's identity information, including identifier
    - customized set of information released to each SP

What does FIM do for me?

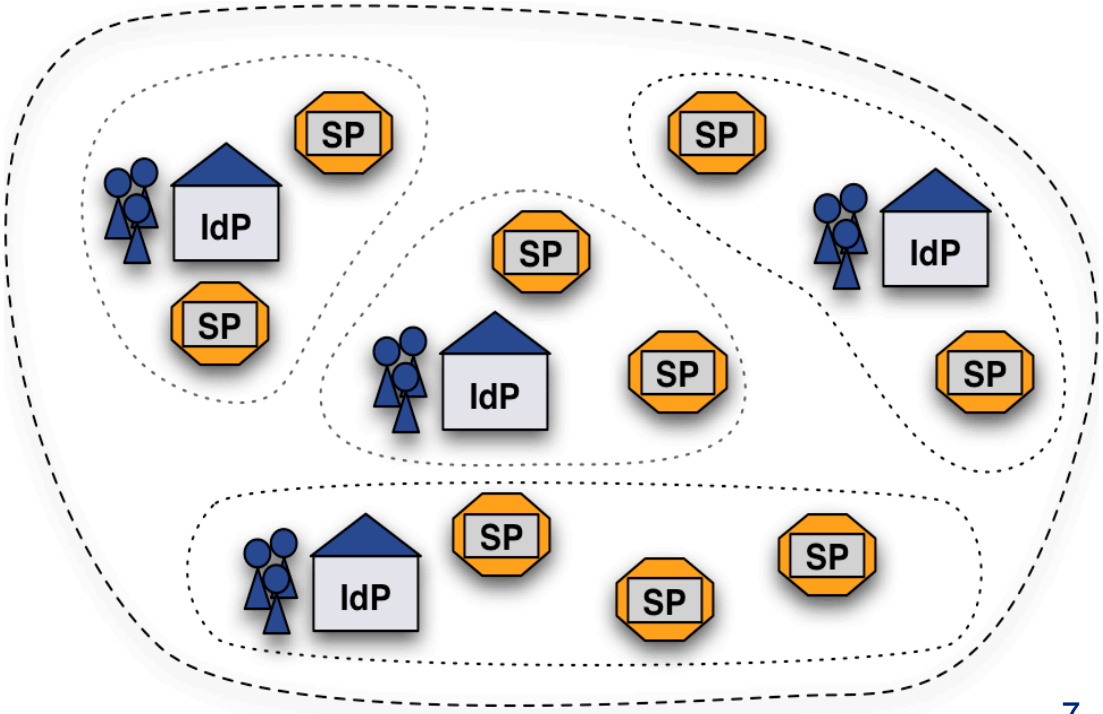
- Reduces work
  - Authentication-related calls to Penn State University's helpdesk dropped by 85% after they installed Shibboleth
- Provides current data
  - Studies of applications that maintain user data show that the majority of data is out of date. Are you "protecting" your app with stale data?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

Some other gains

- Users generally find the resulting single sign-on experience to be nicer than logging in numerous times.
- Consistent authentication process regardless of the service accessed. Usability-focused individuals like that .
- 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
  - 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)
- IdPs and SPs "know" nothing about federations They read metadata!



What are these rules of which you speak?

- Technical Interoperability
  - Supported protocols
  - User authentication mechanisms
  - User attribute specifications
  - Accepted X.509 server certificates
- Legal Interoperability
  - Membership agreement or contract
  - Federation operation policies
  - Requirements on identity management practices
- Others
  - Common/best operational practices

http://switch.ch/aai/bcp

What does a Federation do?

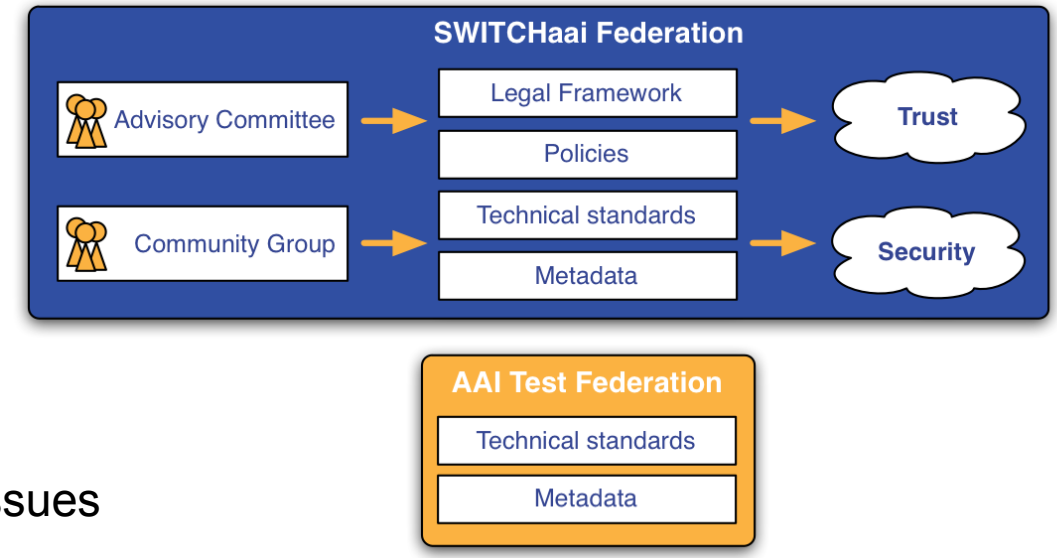
- At a minimum a federation maintains the list of which IdPs and SPs are in the federation
- Most federations also
  - define agreements, rules, and policies
  - provide some user support (documentation, email list, etc.)
  - operate a central discovery service and test infrastructure
- Some federations
  - provide self-service tools for managing IdP and SP data
  - provide application integration support
  - host or help with outsourced IdPs http://switch.ch/aai/idp-hosting
  - provide tools for managing "guest" users http://switch.ch/aai/vho
  - develop custom tools for the community

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
  - Bilateral metadata exchange scales very badly
- Metadata must be kept up to date so that
  - New entities can work with existing ones
  - Old, or revoked, entities are blocked

SWITCHaai Federation (1)

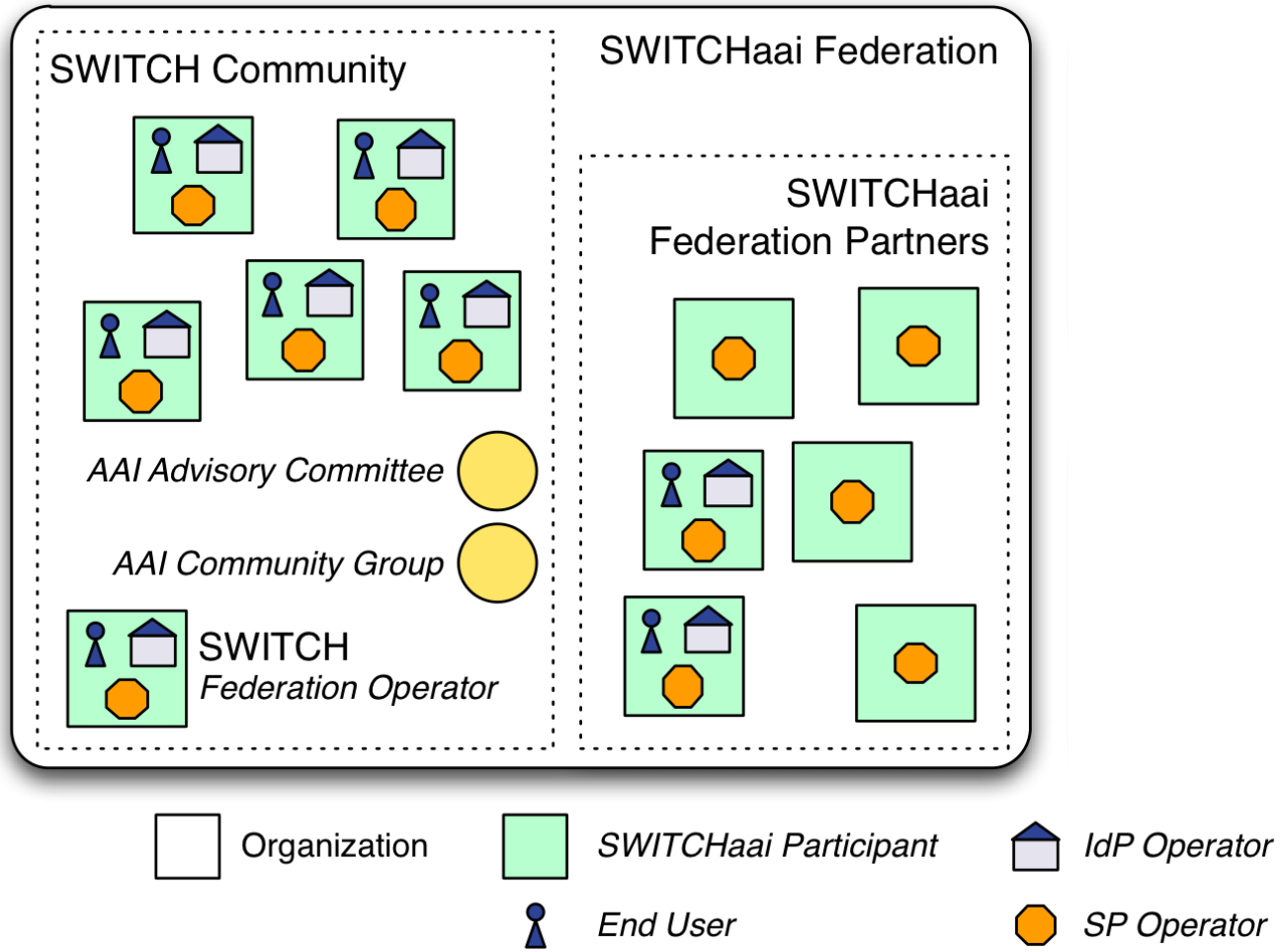
- SWITCH consults with two bodies
  - Advisory Committee deals with policies and legal framework
  - Community Group deals with technical/operational issues



- Two classes of SWITCHaai Participants
  - SWITCH Community
    - Organization fits the definition from the SWITCH Service Regulations
  - Federation Partner
    - Organization sponsored by a SWITCHaai Participant from the SWITCH Community

http://switch.ch/aai/about/federation/

SWITCHaai Federation (2)



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

SWITCHaai: Rules, Policies, & Agreements

- SWITCHaai Service Description (includes the Policy)
  concepts and rules for all entities in the federation

  http://switch.ch/aai/docs/SWITCHaai_Service_Description.pdf

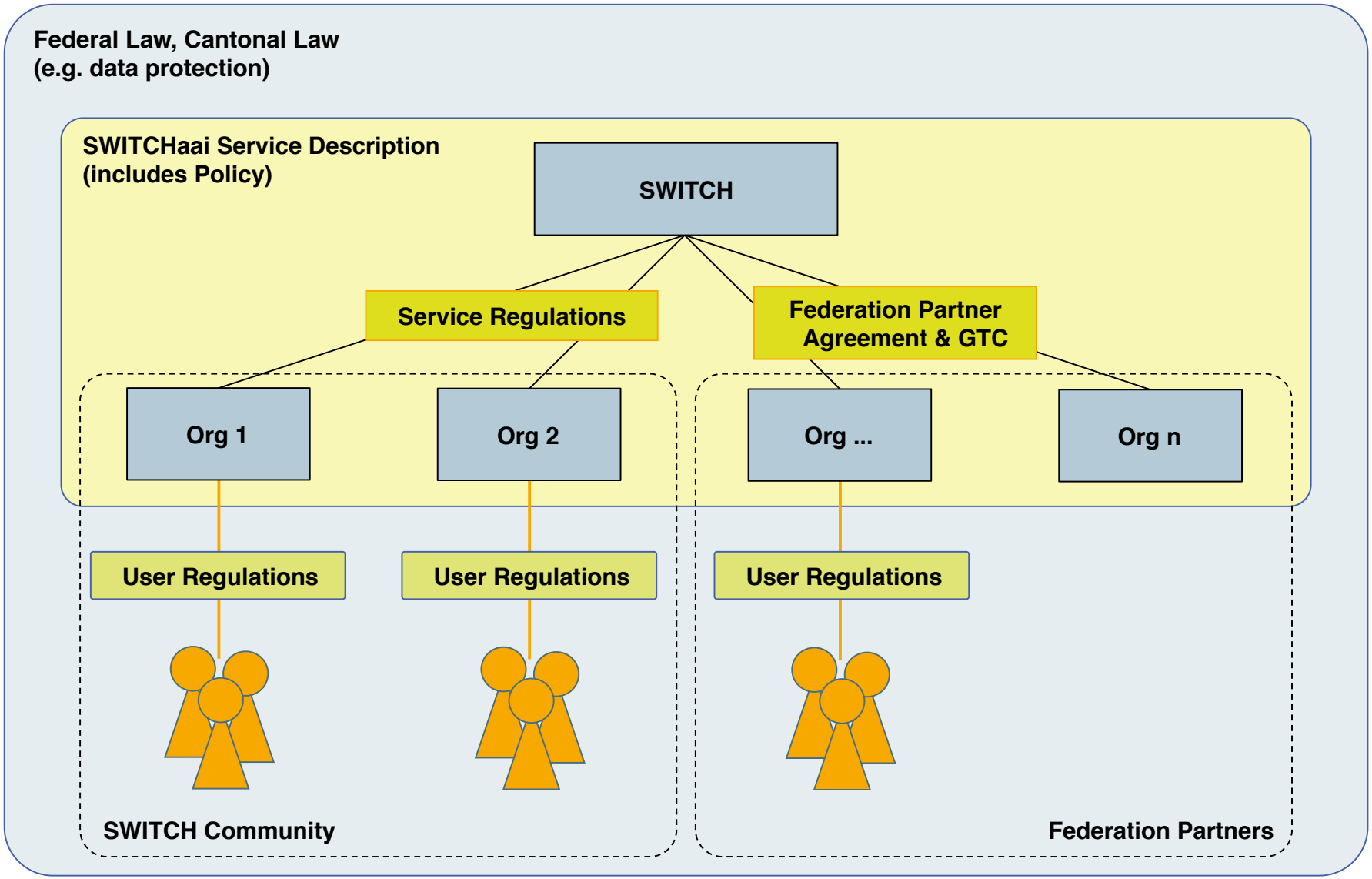
- Federation Partner Agreement
  legal contract between SWITCH and federation partner

- Certificate Acceptance Policy
  policy certificates accepted by the federation

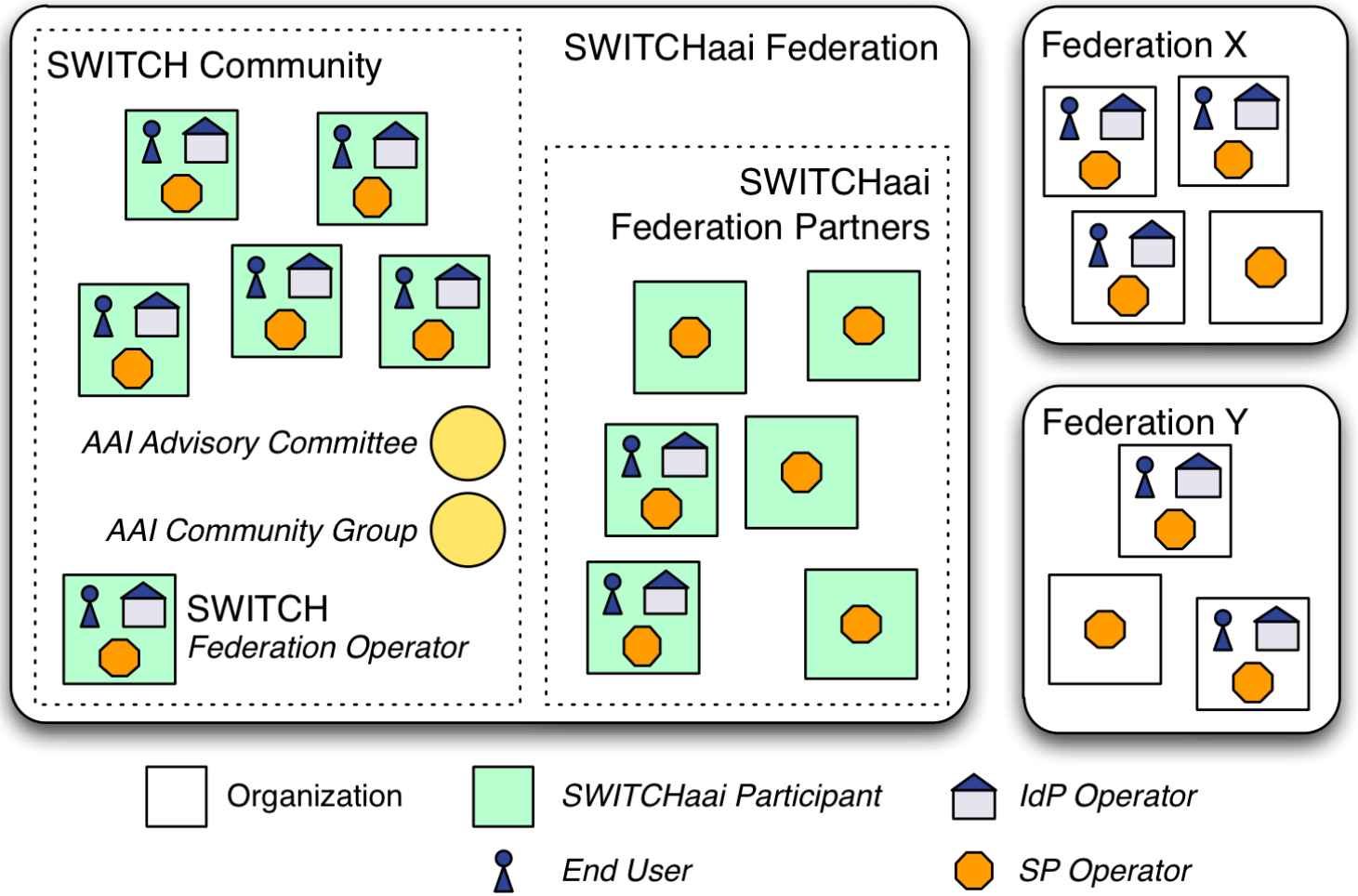
- AAI Attribute Specification
  minimum set of core and optional attributes supported by federation entities

  http://switch.ch/aai/docs/AAI_Attr_Specs.pdf

SWITCHaai: The Legal Framework



SWITCHaai & Interfederation



http://switch.ch/aai/interfederation

Conclusions

- Federated Identity Management
  - provides scalable, protected access to services
    also in other administrative domains
  - supports data protection by releasing only personal data
    as required by the SP
  - separates responsibilities for authentication and authorization
  - is based on a set of rules and guidelines to support trust