

FIM with SWITCHaai



SWITCH

Serving Swiss Universities

andres.aeschlimann@switch.ch

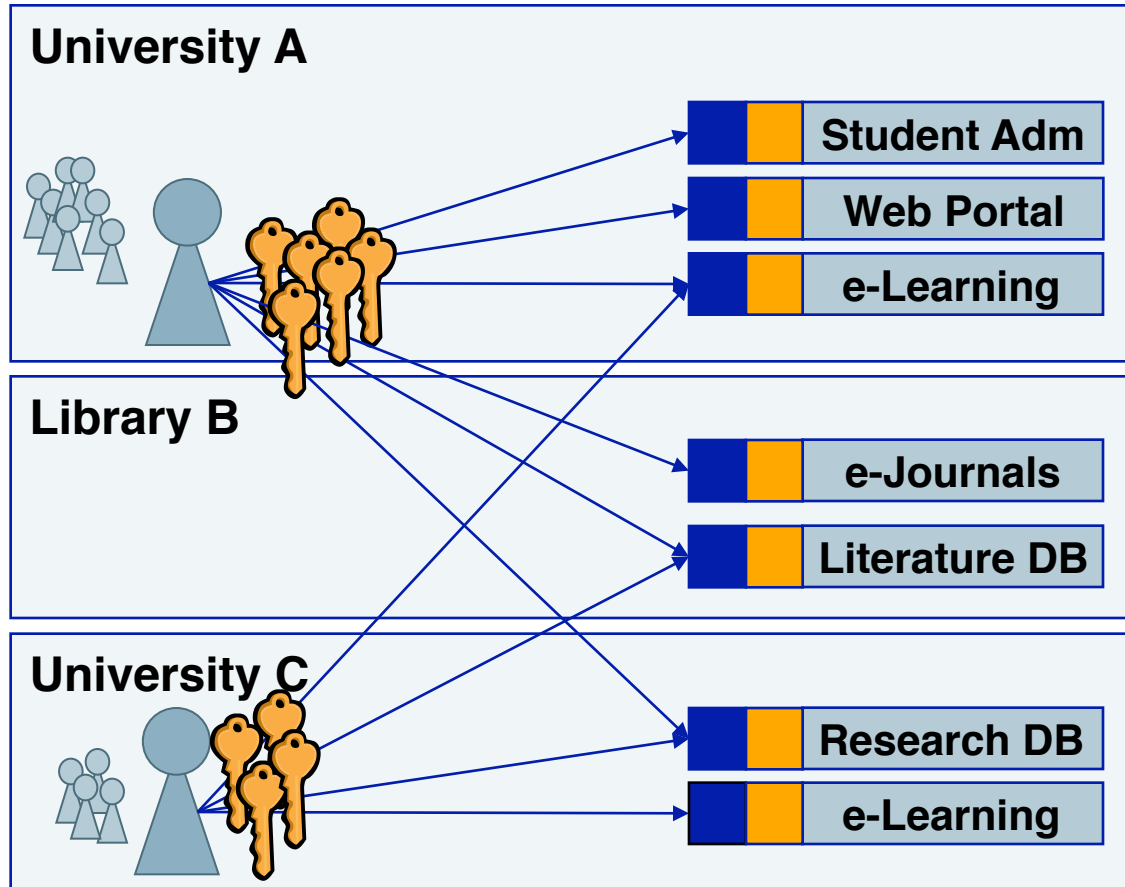


11.3.2013

Content

- Introduction to SWITCHaai
- Components
 - Resource Registry
 - Ensuring compliance
 - Attribute Aggregation
- Interfederation

Without AAI



- Tedious user registration at all resources
- Unreliable and outdated user data at resources
- Different login processes
- Many different passwords
- Many resources not protected due to difficulties
- Often IP-based authorization
- Costly implementation of inter-institutional access

User Administration
Authentication

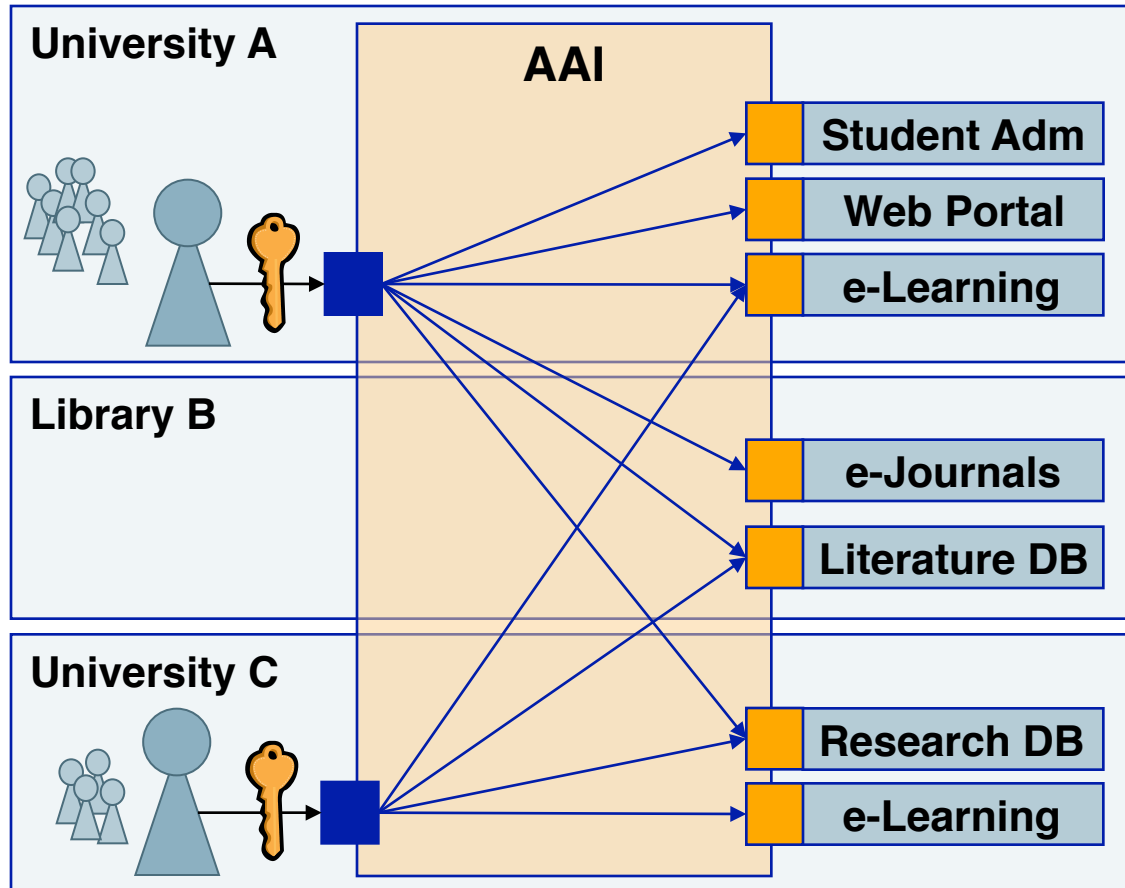
Authorization

Resource



Credentials

With AAI



- No user registration and user data maintenance at resource needed
- Single login process for the users
- Many new resources available for the users
- Authorization independent of location
- Efficient implementation of inter-institutional access

User Administration
Authentication

Authorization

Resource



Terminology



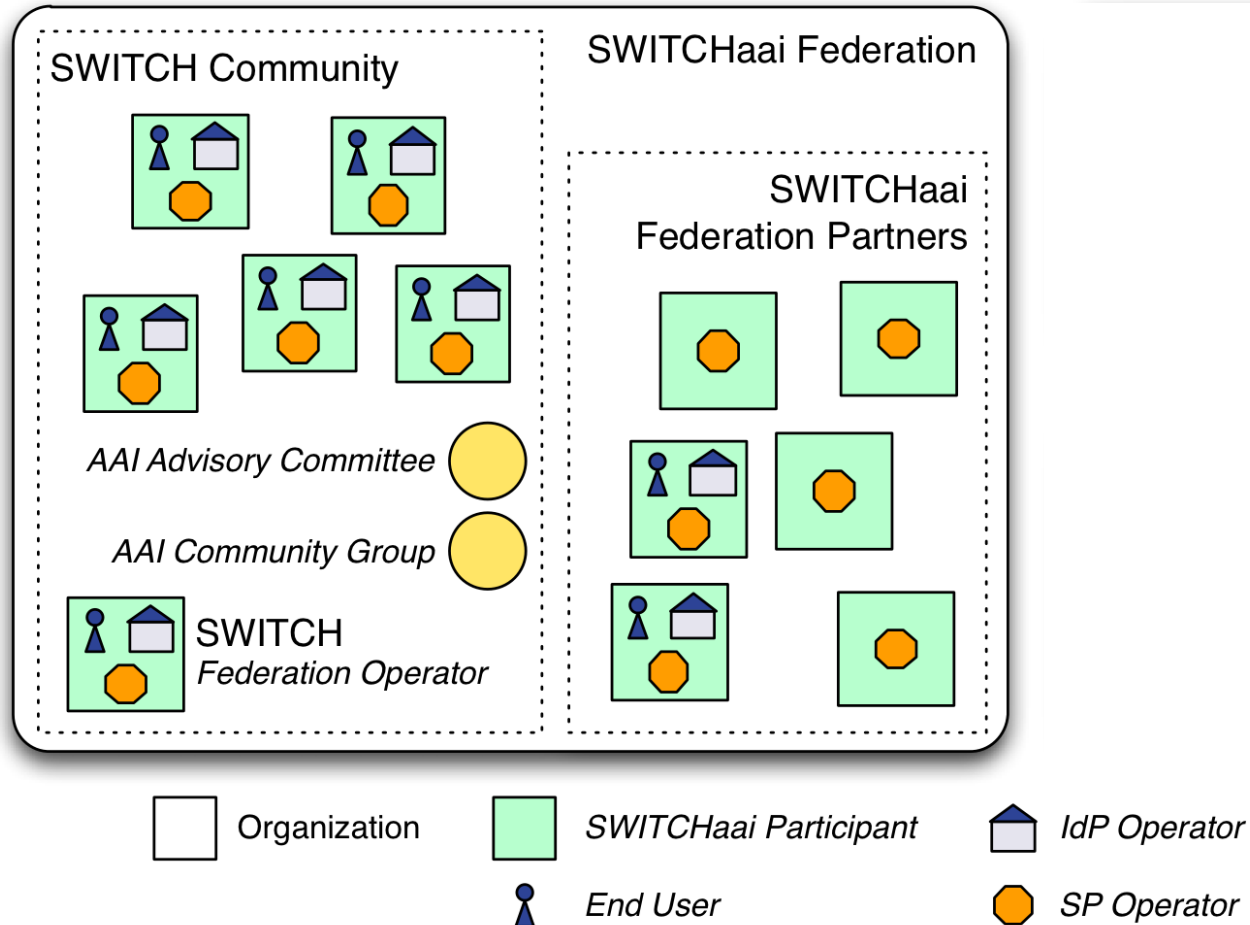
- Home Organisation
Operates a SAML Identity Provider (IdP) that authenticates a user and asserts identity information about this user in form of SAML assertions



- Resource
Consists of a SAML Service Provider (SP) that protects one or more web-applications by enforcing authentication.

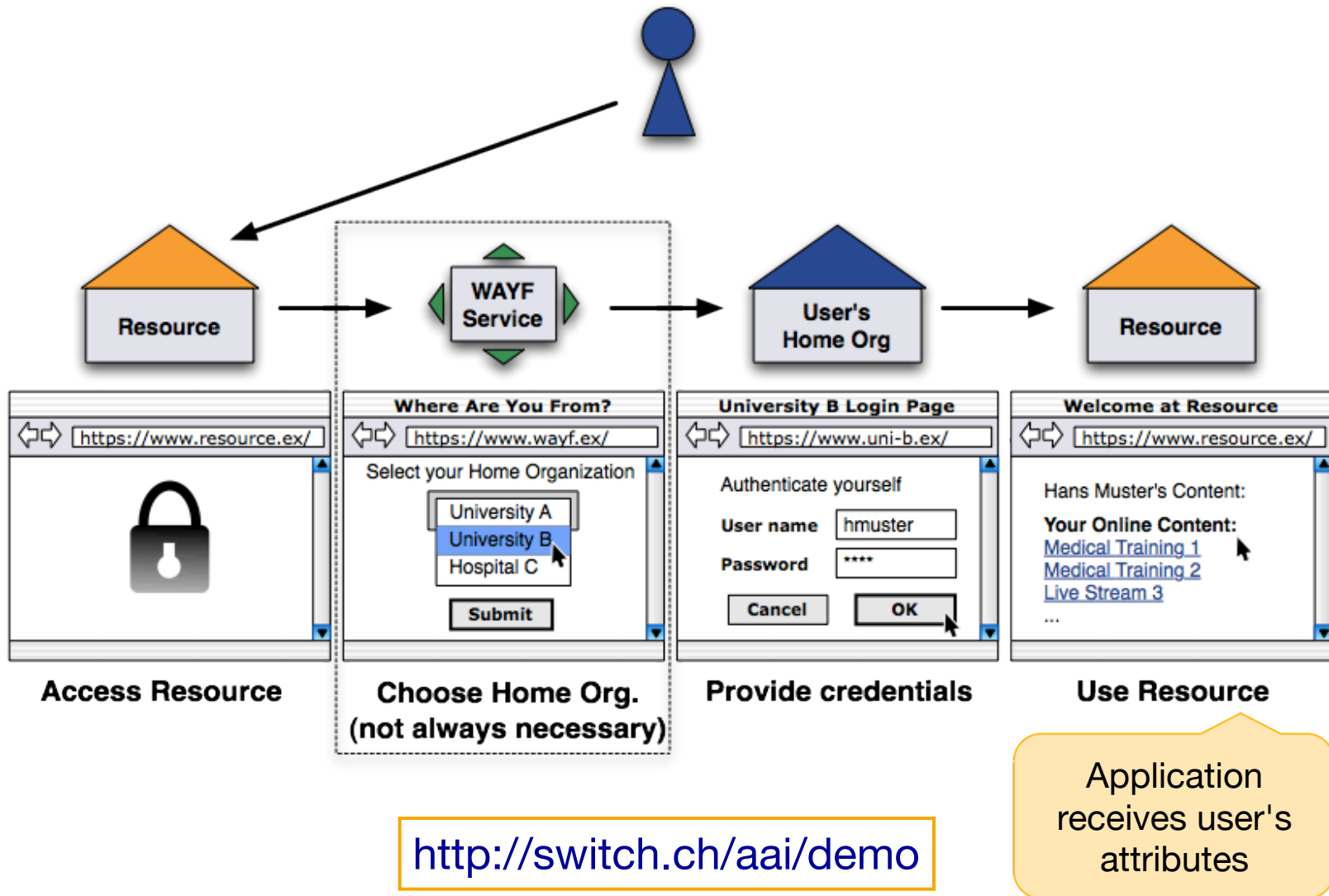
SAML = Security Assertion Markup Language

The SWITCHaai Federation



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

AAI Login as seen by a User



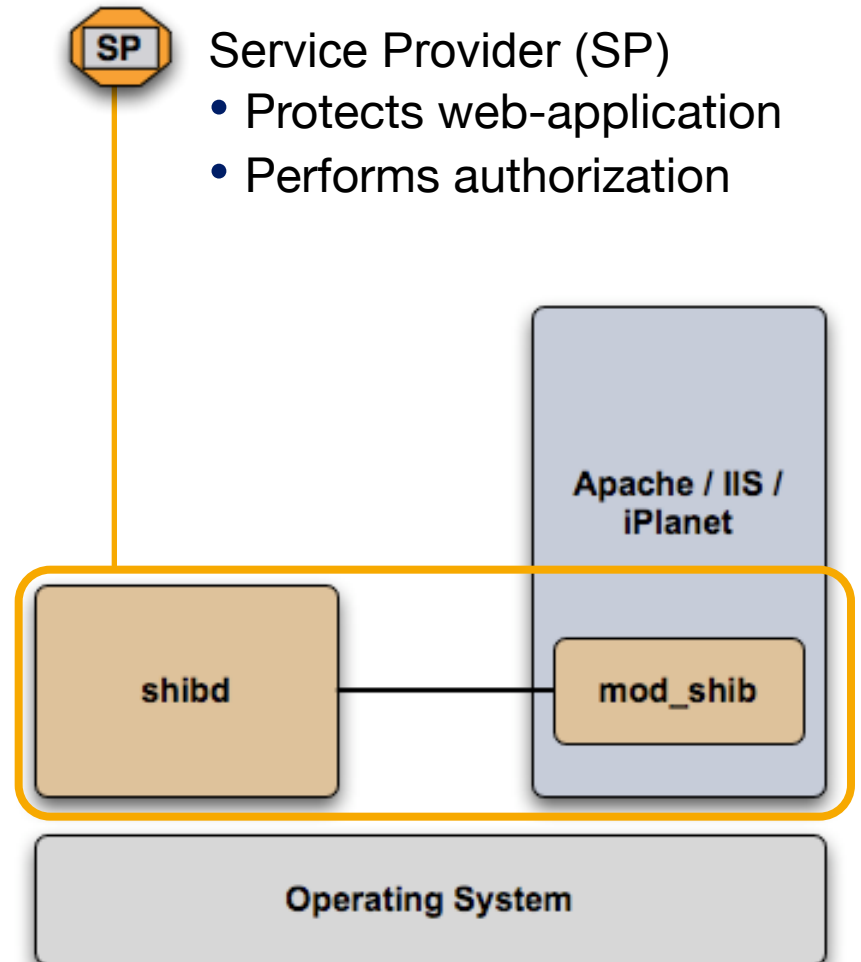
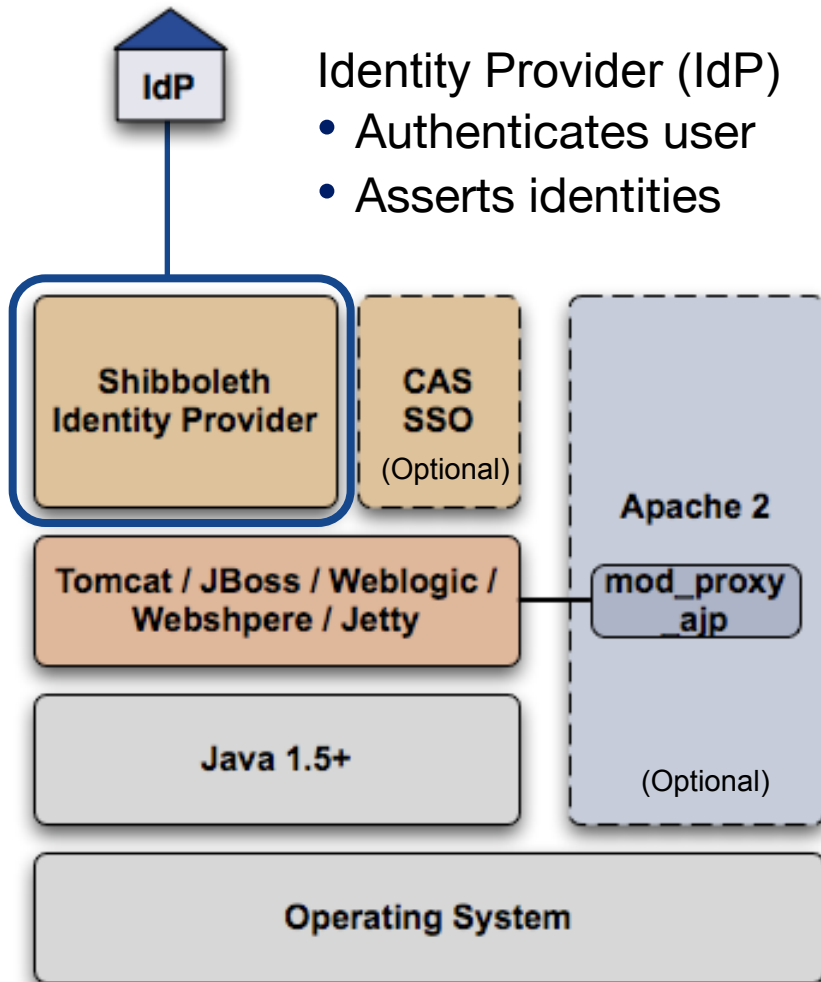
Shibboleth

- Open Source Software
 - Developed under Apache 2 license
- Supports various protocols
SWITCHaaai mainly uses SAML 2
 - SAML 2 has become the standard in the academic world
- Shibboleth Consortium:
Internet2 (US), JISC (UK) and SWITCH (CH)
 - SWITCH funds and develops components of Shibboleth



<http://www.shibboleth.net>

The Shibboleth Components



From the federation's early roots...

e-Academia / AAI Concept



Vision of e-Academia

"We want a virtual community across our institutions in which all persons associated with the Swiss Higher Education System are able to gain access to its electronic resources, independent of the accrediting organization and independent of the place where they happen to be working."

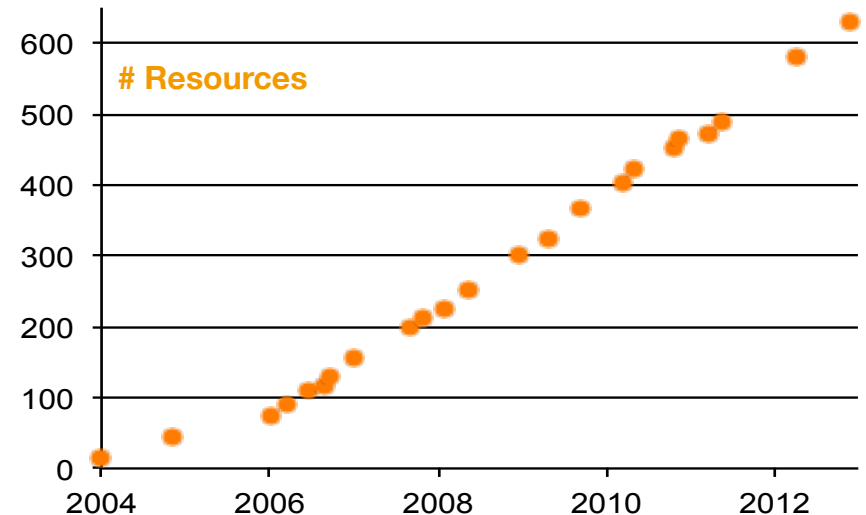
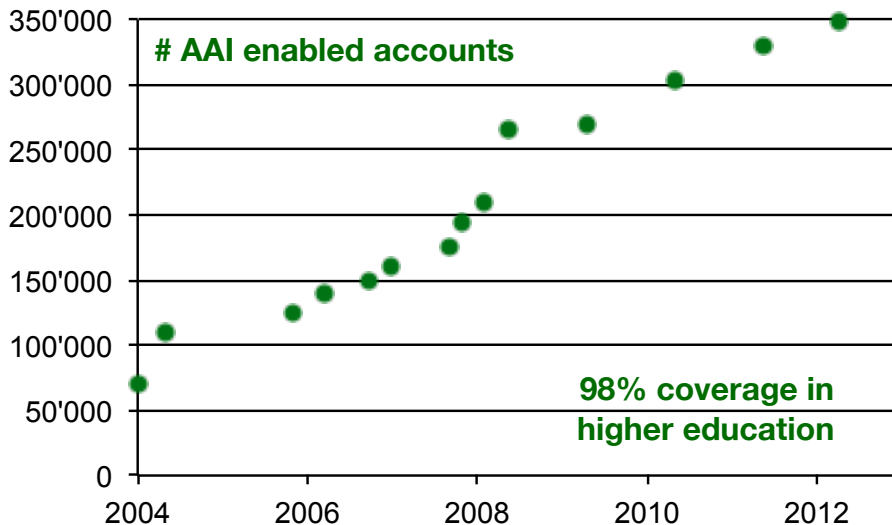
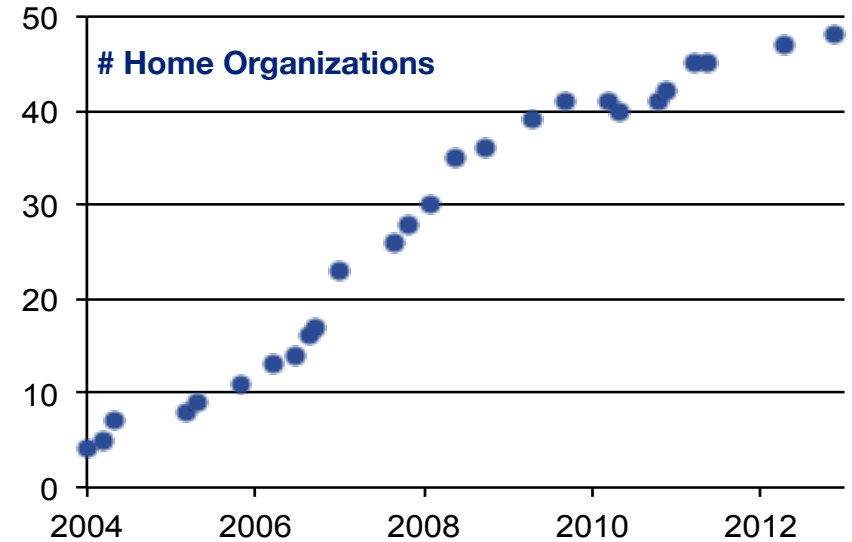
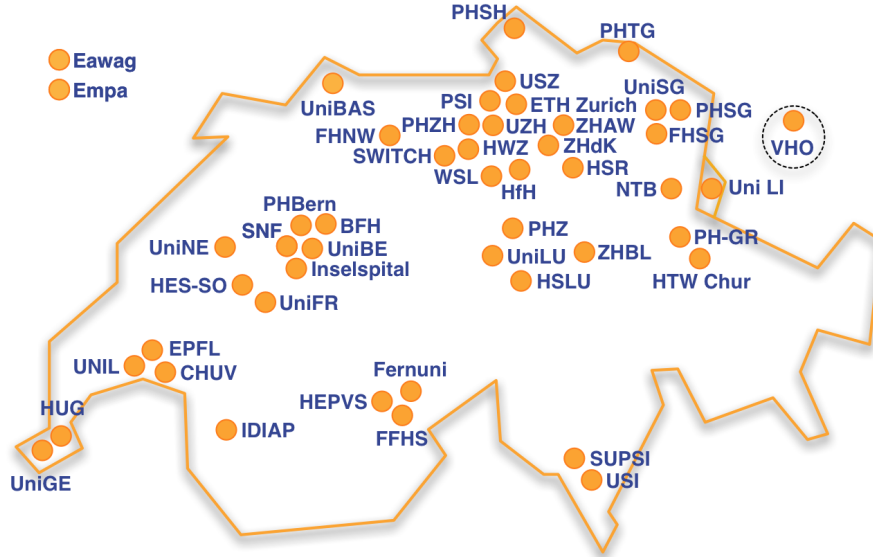
AAI as the foundation of e-Academia

"... let's develop e-Academia, let us build the foundations in the form of a uniform authentication and authorization infrastructure (AAI) for the higher education system in Switzerland..."

Roadmap



... to the current SWITCHaai federation in 2013



Content

- Introduction to SWITCHaai
- Components
 - **Resource Registry**
 - Ensuring compliance
 - Attribute Aggregation
- Interfederation

How to scale the management of the federation?

- The problem:
 - How to manage the SAML configurations for 600+ entities?
 - Almost 50 institutions with their IdPs
 - 600+ Service Providers
- Use federated management
 - SWITCH developed a «Resource Registry» web application
- Signing of SAML Metadata on a dedicated host
Trust root is always off-line, stored in a safe
- SWITCH provides deployment guides for quick set-up

The Resource Registry (1/3)

- Contains the necessary information about SP's and IdP's in the federation.
- Consists of a small database and a (shibbolized) web application on top.
- The responsibility for correctness is delegated to the admins.
- Addition of resources requires authoritative approval by authorized local admins.

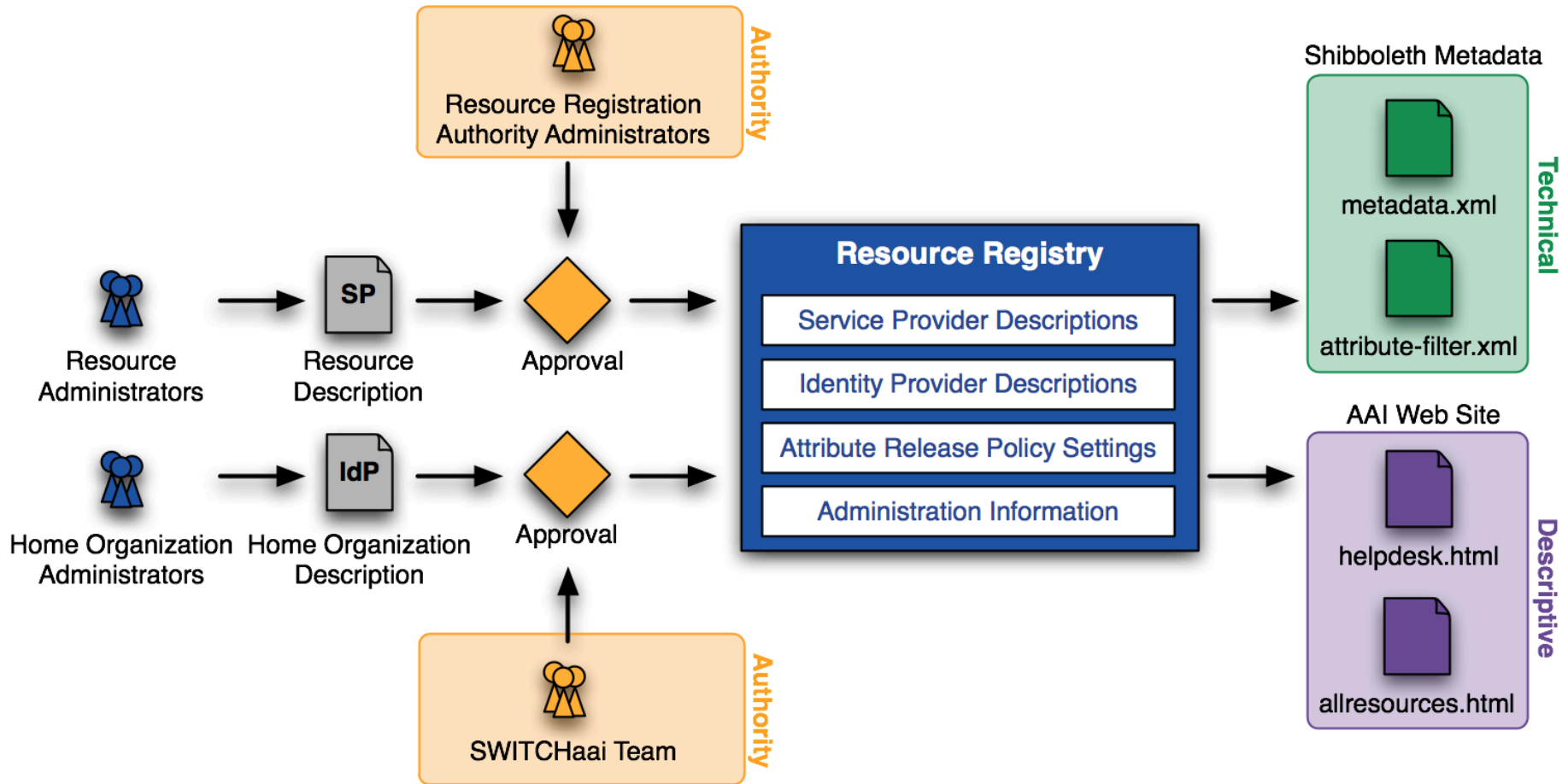
<http://switch.ch/aai/resourceregistry>

The Resource Registry (2/3)

- It can generate SAML metadata, and it can provide tailored attribute-filter templates for each IdP
- IdPs and SPs regularly retrieve the latest metadata, check the signature and activate it.
- New feature for IdP's: it includes basic monitoring which periodically initiates a login request and checks if the Identity Provider's login page is available

<http://switch.ch/aai/resourceregistry>

The Resource Registry (3/3)



<http://switch.ch/aai/resourceregistry>

Content

- Introduction to SWITCHaai
- Components
 - Resource Registry
 - **Ensuring compliance**
 - Attribute Aggregation
- Interfederation

Trusting “them”...

1. Make sure “they” are the ones they claim to be: → certificates, signed metadata
2. Make sure “they” behave correctly:
→ contracts and compliance agreements

Compliance agreements

1. Description of ideal world (BCP's)
2. Verification criteria have to be measurable (→ Score)
3. B has to be verified (Maturity Scans)
4. Trust (A trusts B)

BCP's: an extract

4.5.2. Network Security

Firewall



R-111

Protect the SP with a firewall or a packet filter.

S-112

Ensure that the HTTPS port (usually 443) and HTTP (usually 80) are the only ports accessible from the external network.

HTTPS

S-113

Redirect HTTP to HTTPS.

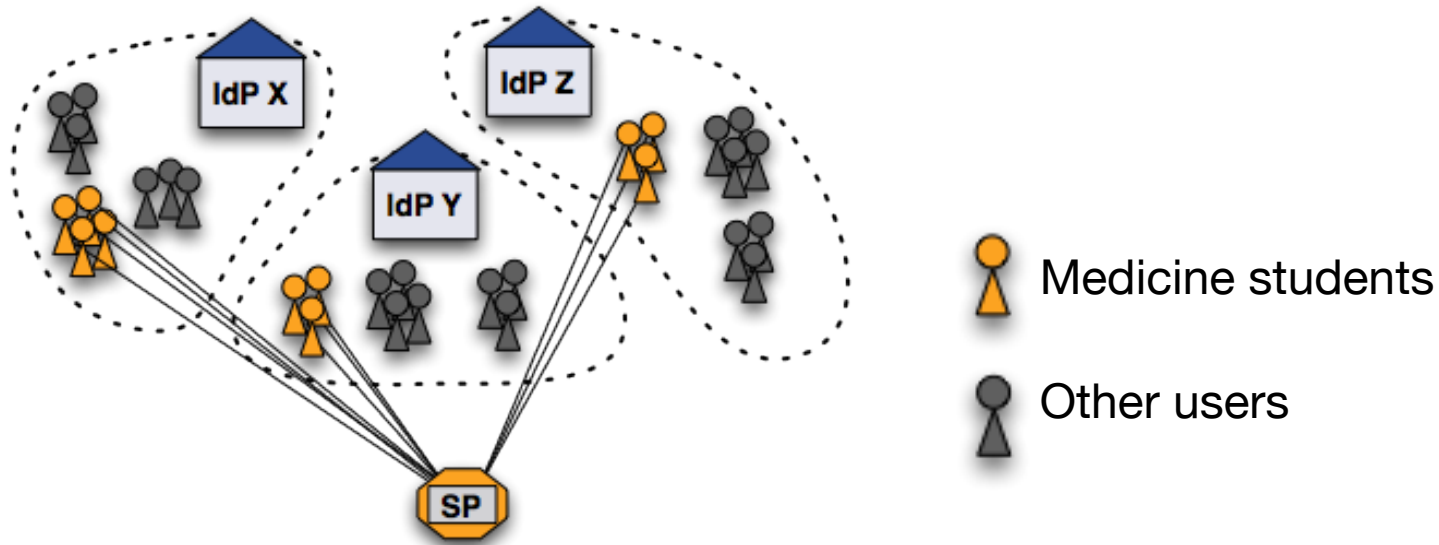
S-114

Use an extended validation (EV) certificate from a browser trusted CA.

Content

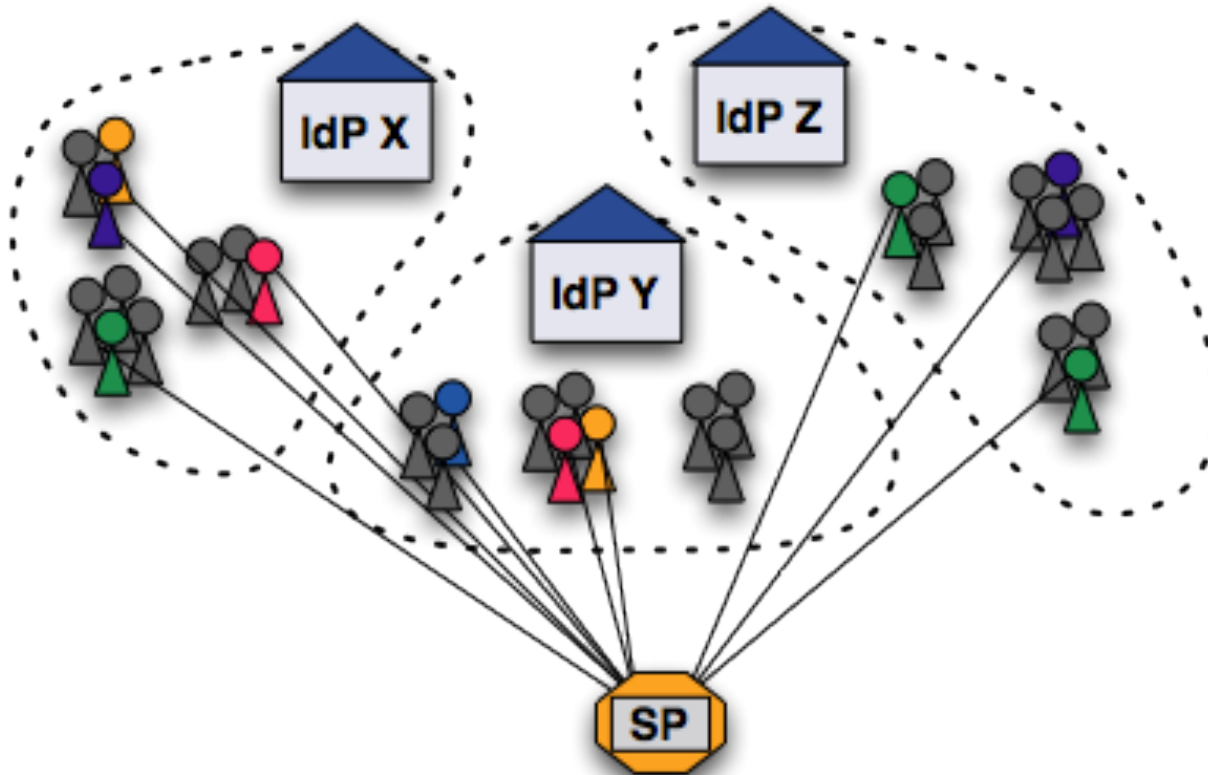
- Introduction to SWITCHaai
- Components
 - Resource Registry
 - Ensuring compliance
 - **Attribute Aggregation**
- Interfederation

Scenario Where Authorization Is Easy

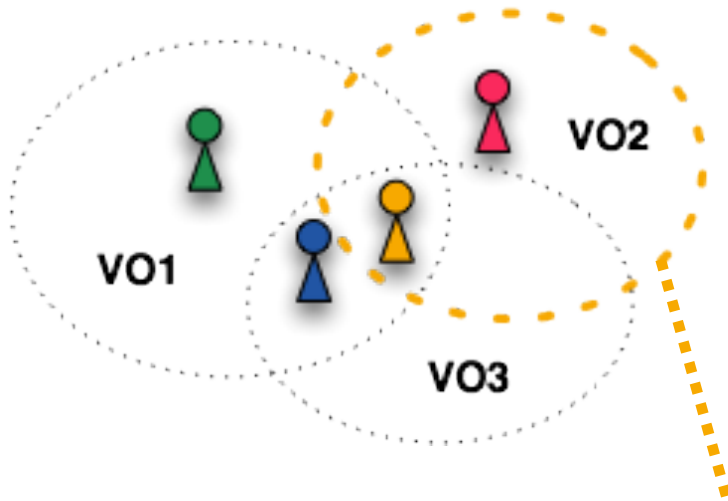


```
AuthType Shibboleth
ShibRequireSession On
ShibRequireAll
require homeOrg idpX.ch idpY.ch idpZ.ch
require affiliation student
require studyBranch medicine
```

More Common Authorization Scenario







Approach for Authorization in VOs



```
AuthType Shibboleth
ShibRequireSession On
require isMemberOf VO2
```

VO Attribute:

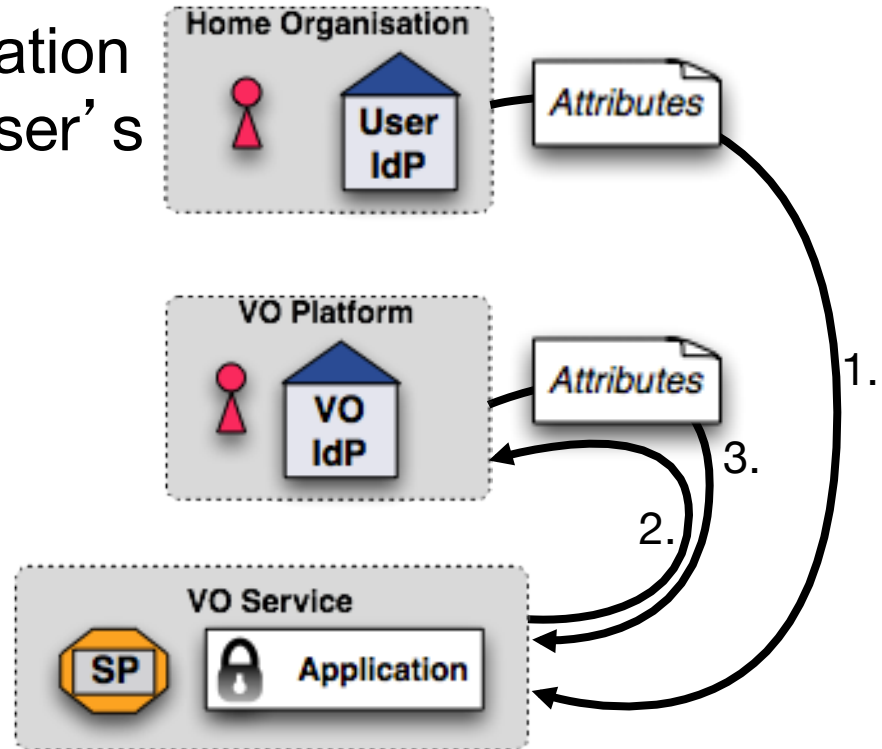
-  isMemberOf=VO1
-  isMemberOf=VO1;VO2;VO3
-  isMemberOf=VO2
-  isMemberOf=VO1;VO3

How the Attribute Aggregation works

- VO Service Provider aggregates attributes from:

1. User's Home Organisation
Attributes are set by user's Home Organisation

2. VO Platform(s)
Attributes are set by VO administrator



➡ SP receives aggregated set of attributes

VO Summary

- Membership for a VO is expressed by an attribute
- VO attributes are aggregated from VO Platform(s)
- Access control using VO Attributes very easy with Shib
- VO Attributes are managed on VO Platform
- **This mechanism is *not restricted* to VO Attributes, but can be used for *any* attributes.**

SWITCHaai Summary

- SWITCHaai is the federated identity management system of the higher education sector of Switzerland
- It is based on Shibboleth
- It covers over 98 % of all academic users and comprises now 600+ resources
- It took 10 years to build

Interfederation



SWITCH

Serving Swiss Universities

andres.aeschlimann@switch.ch



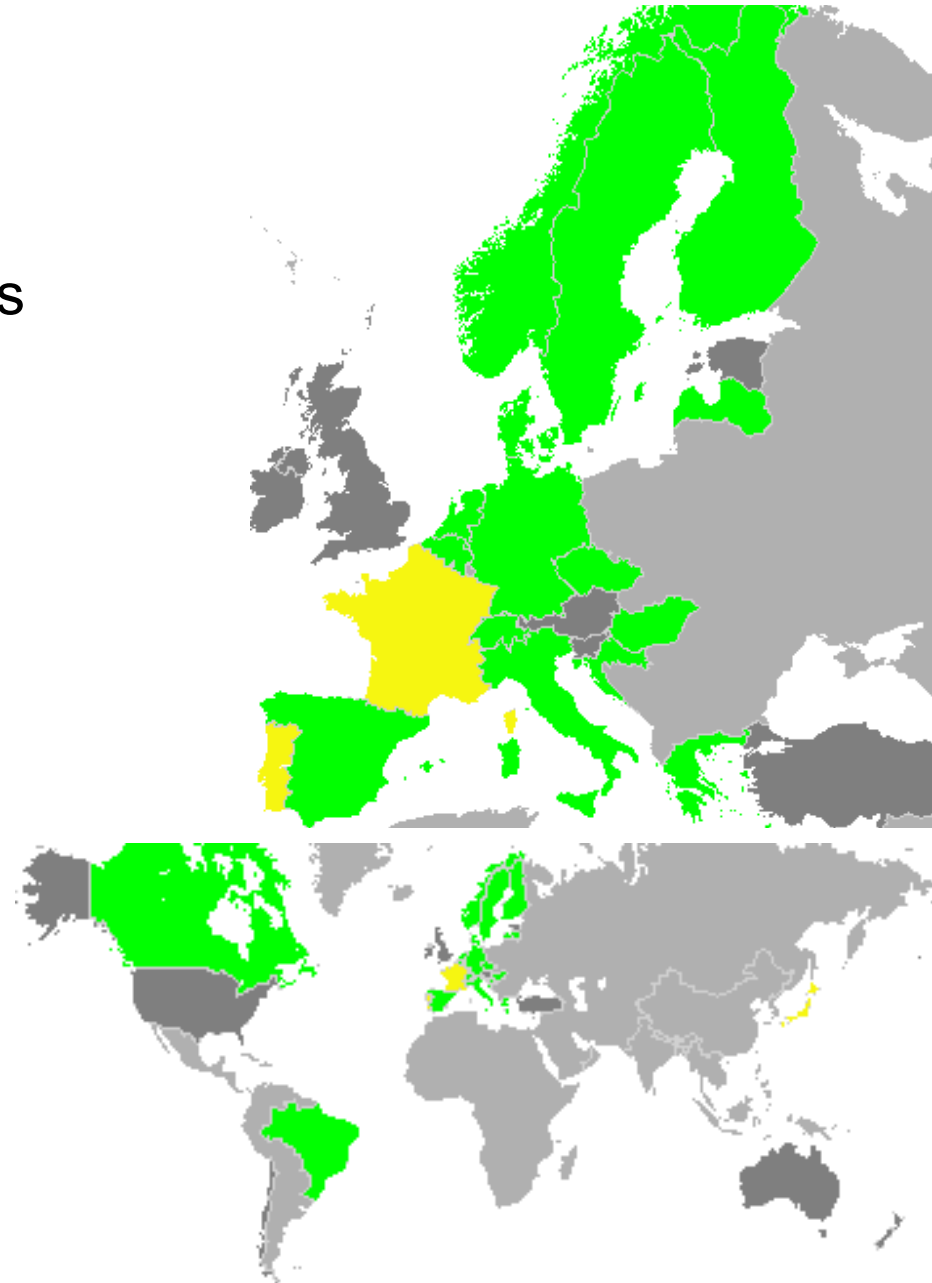
11.3.2013

Content

- Overview and Use Cases
- Metadata
- Discovery Service(s)
- Legal aspects

Interfederation

- Users to get access to services from other federations
- eduGAIN is the GÉANT interfederation service
- SWITCHaai Participants will have to opt-in
 - Deployment guides are available
 - IdPs will need to decide upon what data to provide to SPs in other federations



Some example use cases

SWITCHaai SP offered to international community:

1. DOIT
2. Forge

Usable by SWITCHaai users with Interfederation:

3. REDI
4. TERENA services
5. Foodle



Lernen

Wissensangebot zur
Dermatologie

Üben

Fallbasierte Übungen
und Prüfungsfragen

Testen

Spielerisches Lernen



Repetieren

Podcasts und
Bildgalerie

Extras

Vorlesungs-
unterlagen, etc.

[Dermatology Online with Interactive Technology](#) >
 [Lernen](#) >
 [Hauterkrankungen](#) >
 [1 Entzündliche Dermatosen](#) >
 [1.1 Allergische und nicht allergische Intoleranzreaktionen](#) >
 [1.1.1 Urtikaria](#)

Schwierigkeitsgrad Fortgeschrittene

1.1.1 Urtikaria 2DTEG

Review:

B. Ballmer, Zürich

Überblick

- [Synonyme](#)
- [Definition](#)
- [Ätiologie & Pathogenese](#)
- [Symptome](#)
- [Klassifikation](#)
- [Labor](#)
- [Diagnose](#)
- [Differentialdiagnose](#)
- [Therapie](#)

Synonyme Nesselfieber, (Brennessel = lat. Urtica dioica).

Definition Durch flüchtige, juckende Quaddeln (Urticae) gekennzeichnetes Exanthem.

Personal notes

Klinische Bilder



SWITCH Forge

SWITCH

[Overview](#) | [Activity](#) | [Roadmap](#) | [Issues](#) | [New issue](#) | [News](#) | [Wiki](#) | [Files](#) | [Repository](#) | [Settings](#)[My account](#) | [Mite](#) | [Logout](#)[↑ www.switch.ch](#)[Home](#) » [AAI](#) » [SWITCHwayf](#)

Search:

» SWITCHwayf

Overview

[+ New subproject](#)

The SWITCH WAYF is a PHP implementation of the Shibboleth WAYF and SAML Discovery Service protocol.

Public Subversion Access

```
svn co https://subversion.switch.ch
```

- Homepage:
<http://www.switch.ch/aai/support/tools/>

Issue tracking

- Bug: 1 open / 22
- Change: 0 open / 1
- Feature: 6 open / 23
- Support: 0 open / 1
- Question: 0 open / 1

[View all issues](#)

Members

Manager: Daniel Lutz, Lukas Hämmerle, Thomas Lenggenhager
Developer: Daniel Lutz, Lukas Hämmerle, Thomas Lenggenhager
Reporter: Daniel Lutz, Lukas Hämmerle, Olivier Salaün, Peter Schober, Simona Venuti, Stefano Gargiulo, Takeshi NISHIMURA, Thomas Lenggenhager, Tom Scavo

Latest news

Version 1.17.1 released
Version 1.17.1 of the SWITCHwayf is a bug fix release
Added by Lukas Hämmerle 9 months ago

Version 1.17 released

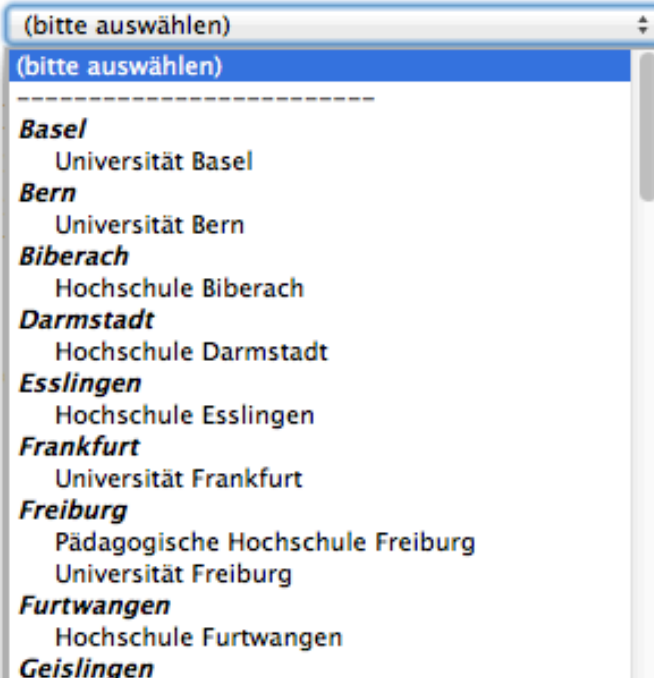
- Homepage
- Aktuell
- Datenbanken
- Zugang/Passwort
- Kontakt
- Login

Status: kein Zugriff

Um auf die ReDI-Datenbanken zugreifen zu können, müssen Sie sich einloggen! Sie sehen das gesamte ReDI-Angebot.

Login: Einrichtungsauswahl

Bitte wählen Sie die Einrichtung aus, der Sie angehören. Wenn Ihre Einrichtung nicht zur Auswahl angeboten wird, können Sie sich nicht mit Benutzerkennung und Passwort in ReDI einloggen:



The screenshot shows a web form for logging into ReDI. At the top, there is a dropdown menu with the placeholder text "(bitte auswählen)". Below the dropdown, a list of institutions is displayed, each preceded by a bold header for the institution name. The institutions listed are:

- Basel**: Universität Basel
- Bern**: Universität Bern
- Biberach**: Hochschule Biberach
- Darmstadt**: Hochschule Darmstadt
- Esslingen**: Hochschule Esslingen
- Frankfurt**: Universität Frankfurt
- Freiburg**: Pädagogische Hochschule Freiburg, Universität Freiburg
- Furtwangen**: Hochschule Furtwangen
- Geislingen**

To the right of the dropdown menu, there is a yellow button with a right-pointing arrow.

mit Benutzerkennung und Passwort nur eigenen Identity Provider (Login-Server) an oder in Kürze betreiben werden. Wenn Ihre Einrichtung nicht zur Auswahl angeboten wird, können Sie sich nicht mit Benutzerkennung und Passwort einloggen. Bitte erkundigen Sie sich, wie Sie ReDI von ausserhalb des

<http://www.redi-bw.de>

TERENA Services

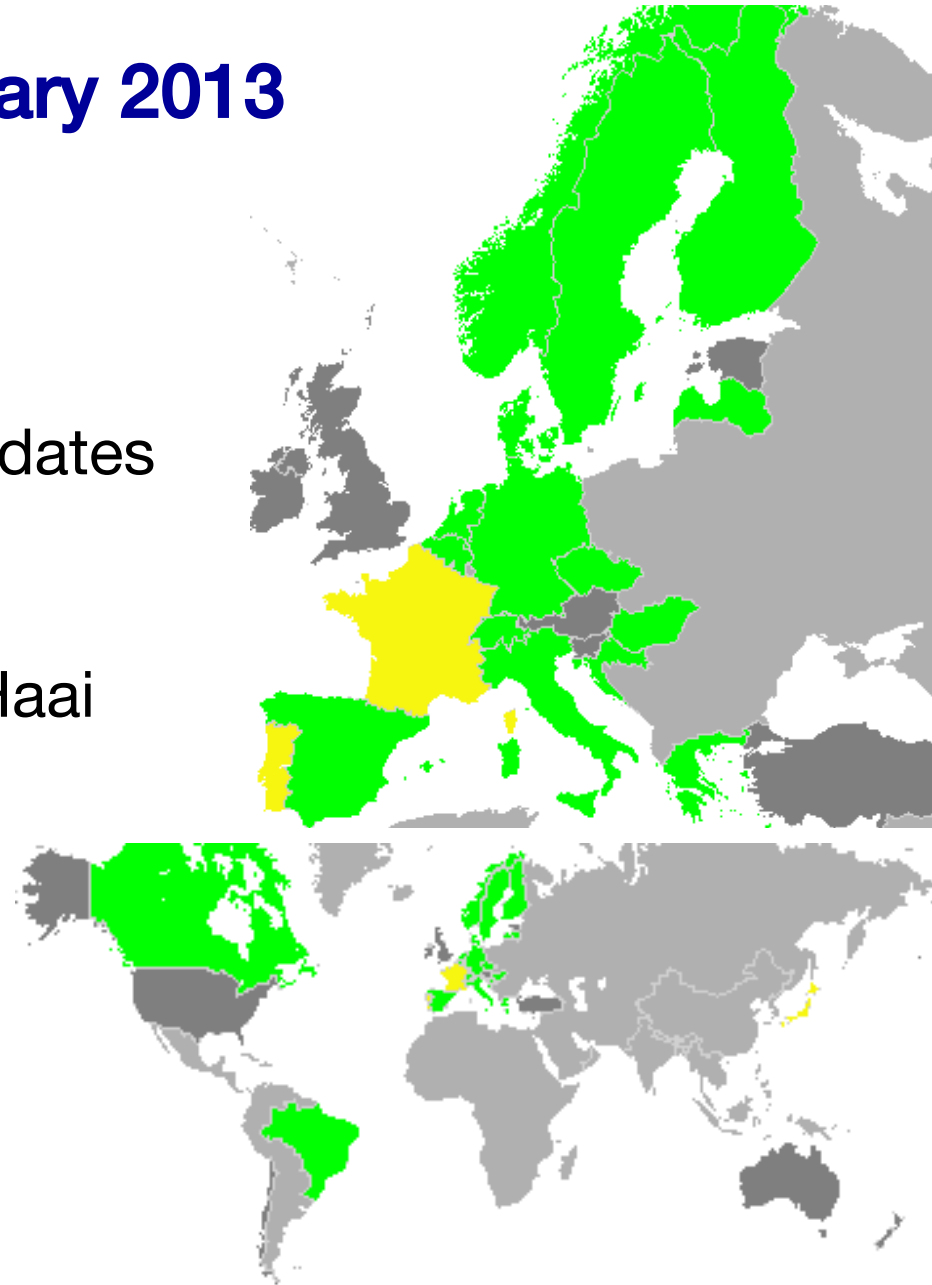
- TERENA = Trans-European Research and Education Networking Association
- SWITCH is member of TERENA
- International collaboration activities and meetings
- Example Services:
 - Federation Wiki: <https://refeds.terena.org>
 - Conference Registration: <http://tnc2013.terena.org>

Foodle

- Federated Doodle
- Offers many more features
- Service usable via eduGAIN
 - Could be used by your users
- Developed by UNINETT from Norway
- Link: <http://foodl.org>

The numbers for February 2013

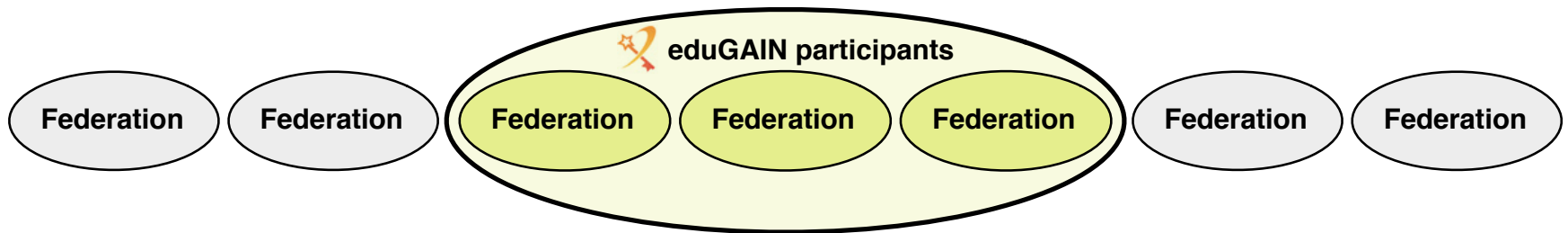
- 17 Federations
 - 3 more joining, 10 candidates
- 84 IdPs, 1 from SWITCHaai
- 38 SPs, 4 from SWITCHaai



<http://www.edugain.org>

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

Width and Depth in Numbers



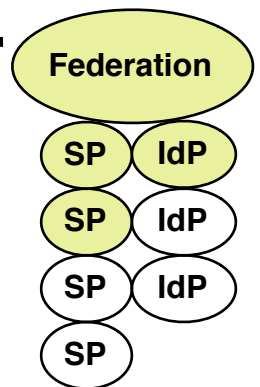
- **65% of European national federations are eduGAIN participants**

Or 51% of total 33 national federations worldwide

Source: REFEDs Wiki, <https://refeds.terena.org/index.php/Federations>

- **About 5% entities are in eduGAIN so far**

- out of 2'290 SPs and IdPs operated by eduGAIN participants



- Not every SP and IdP has good reasons to interfederate!

Content

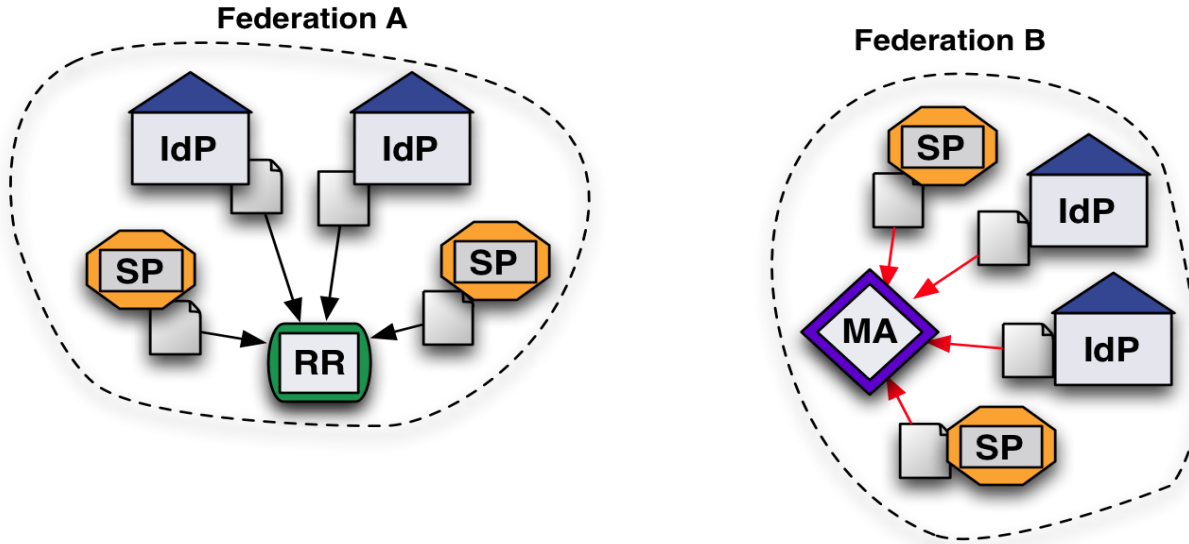
- Overview and Use Cases
- **Metadata**
- Discovery Service(s)
- Legal aspects

Metadata handling in a single federation

The federation metadata contains all the entities

- 1) The entities register with the federation and provide the metadata
- 2) The federation operator signs and publishes the metadata file
- 3) The entities regularly fetch the metadata file and consume it

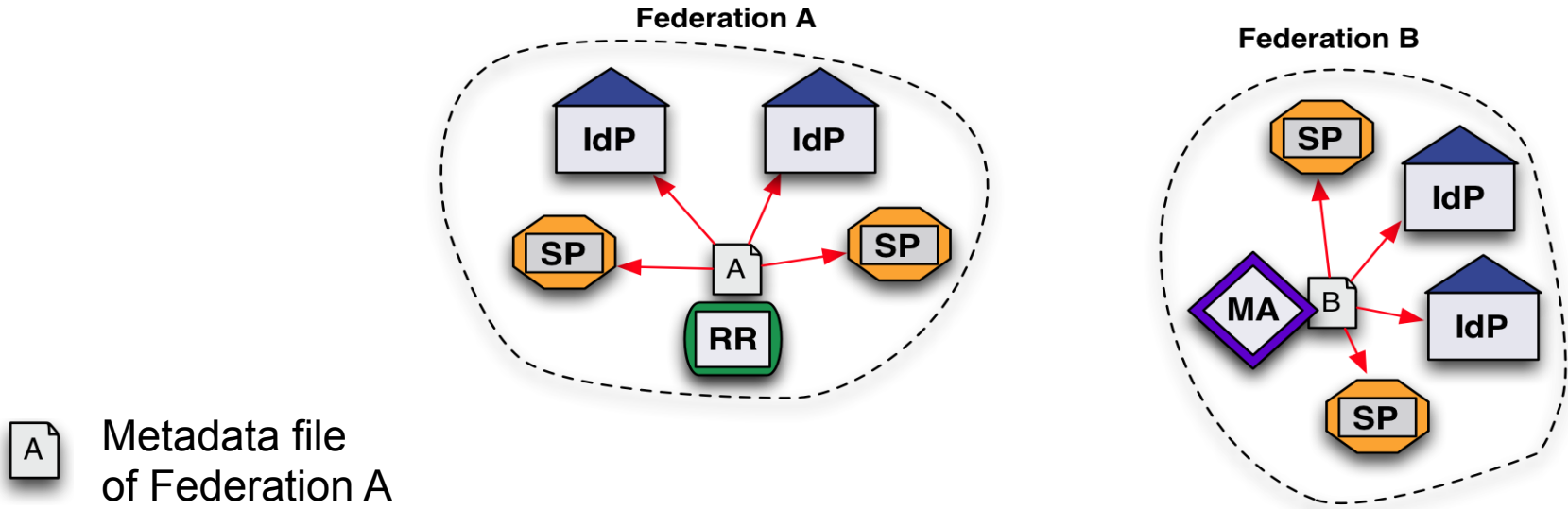
Collect Metadata from Entities



- Federation collects metadata from the entities e.g. with
 - a Resource Registry
 - a Metadata Aggregator that pulls its metadata

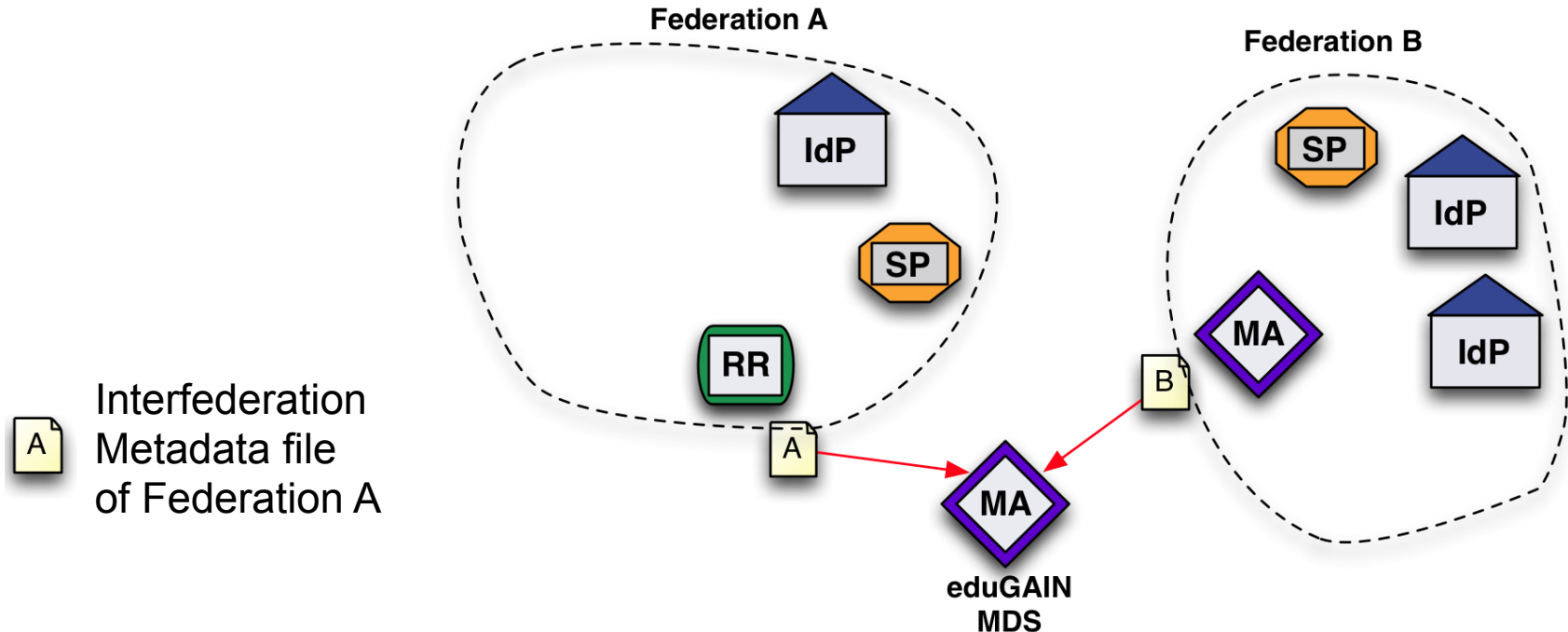


Publish Federation Metadata



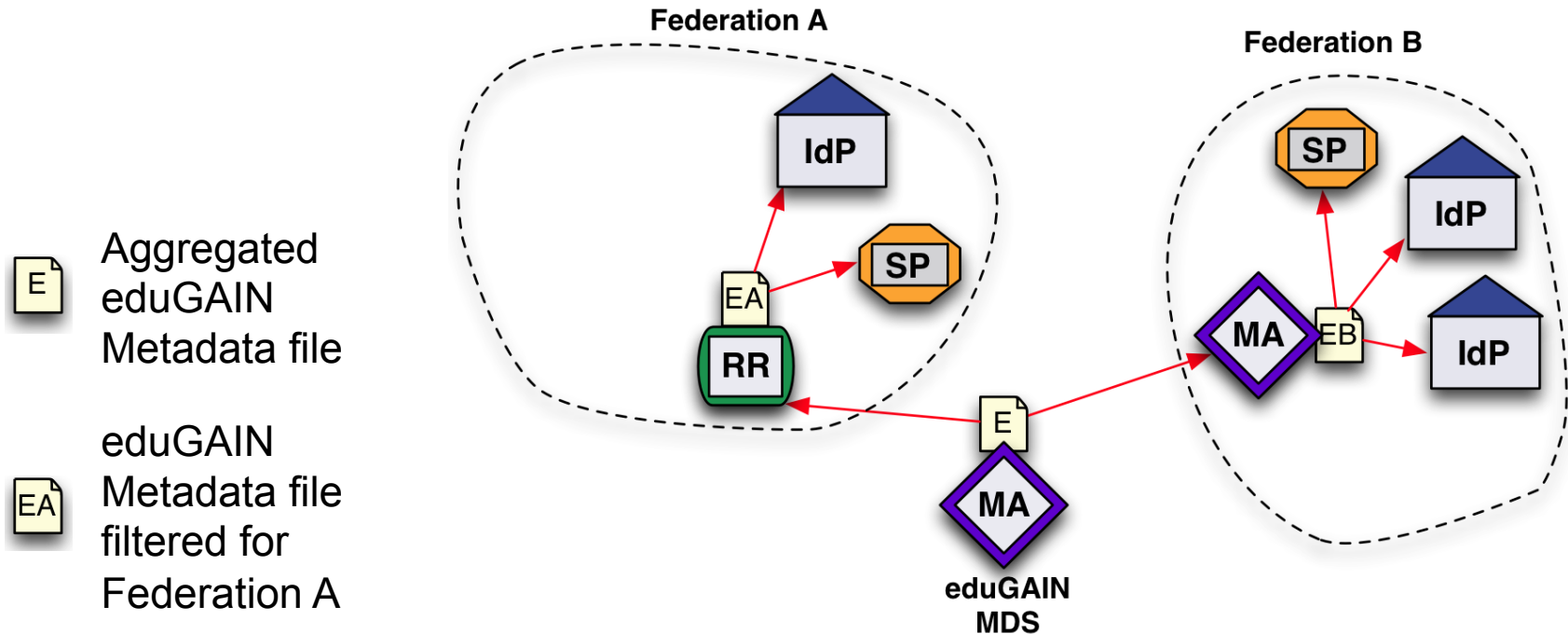
- Each Federation publishes its metadata file
- Entities fetch it from their Federation

Publish Metadata for Interfederation



- Each Federation publishes a Metadata file with the entities that want to interfederate.
- The eduGAIN Metadata Data Service fetches them

Consume and Republish Interfederation Metadata



- eduGAIN MDS aggregates all metadata and republishes it
- Federations fetch it and filter-out their own entities
- Entities consume the filtered eduGAIN metadata file in addition to the one from the federation

Content

- Overview and Use Cases
- Metadata
- **Discovery Service(s)**
- Legal aspects

Discovery Service: Ways of doing it

- SWITCH Embedded WAYF



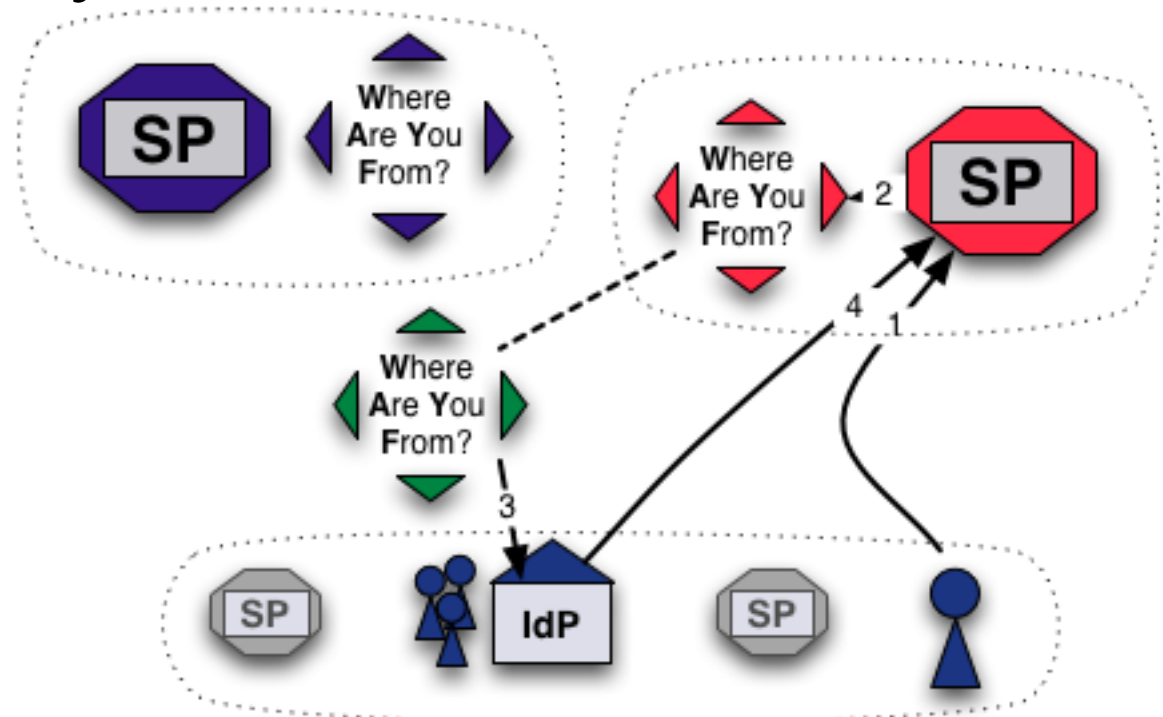
- Shibboleth Embedded Discovery Service



- Discojuice

Embedded WAYF

- Embed WAYF on Web Application
- customize look and feel
- still transparently use central WAYF



Information and Configuration

More information about the embedded WAYF:



<http://www.switch.ch/aai/support/serviceproviders/sp-embedded-wayf.html>

Generate the embedded WAYF code for your SP:



https://rr.aai.switch.ch/gen_embedding_code.php

Embedded Discovery Service

- Uses the Discovery Feed provided by the SP
- Embed the DS directly into the service
- Search-as-you-type or select from list
- JS, CSS and HTML only
- developed and maintained by the Shibboleth team
- download from

 <http://shibboleth.net/downloads/embedded-discovery-service/latest/>

- Documentation can be found at:

 <https://wiki.shibboleth.net/confluence/display/EDS10/Embedded+Discovery+Service>

Embedded Discovery Service

AAI Attribute Viewer



The AAI Attribute Viewer displays all attributes that are available about an AAI user. All user information is stored 10 days in a log file before it is automatically deleted.

Please select your Home Organization and log in to see the [AAI attributes](#) that are available for you.

Use a suggested selection:



VHO - Virtual Home
Organization



WSL - Swiss Federal
Institute for...









SWITCH

Or enter your organization's name

Continue

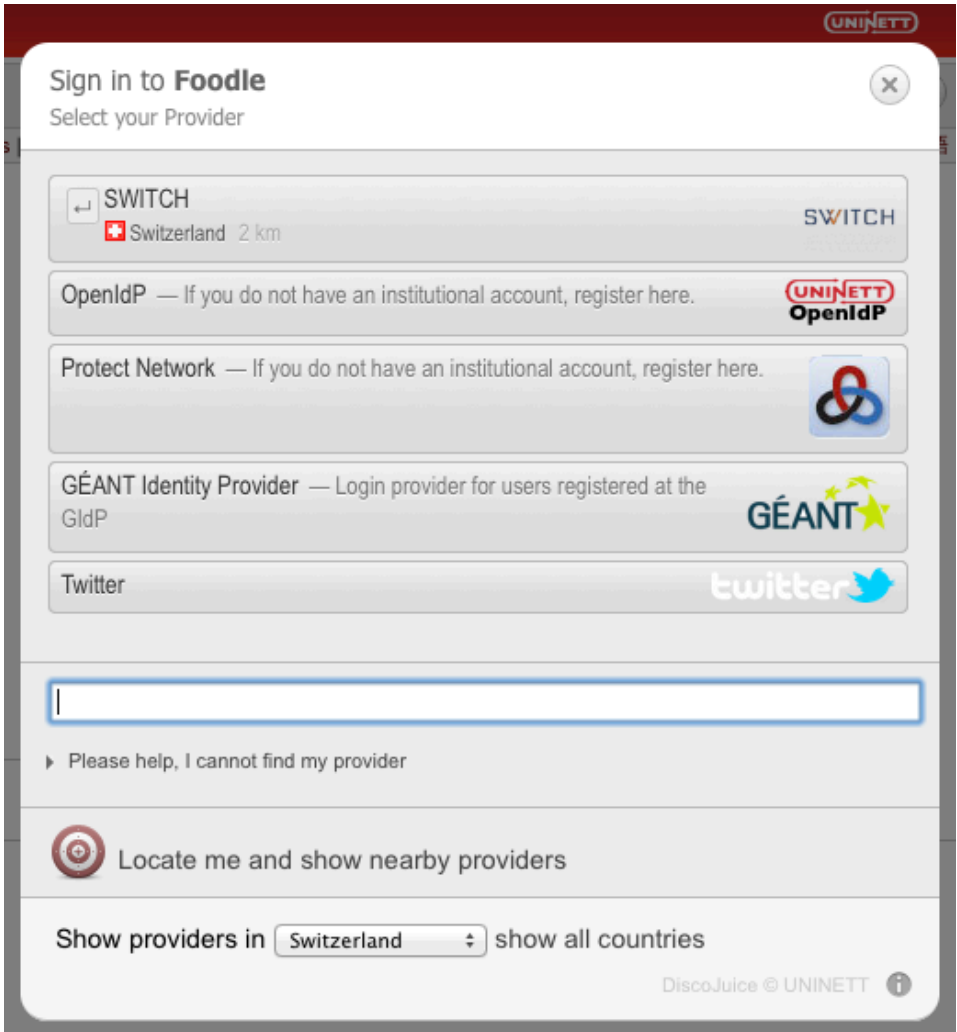
[Help](#)

-  FHNW - University of Applied Sciences Northwestern Switz
-  HES-SO : University of Applied Sciences Western Switzerl
-  HSR - Hochschule für Technik Rapperswil
-  PHZ - University of Teacher Education Central Switzerlan
-  SNSF - Swiss National Science Foundation
-  SUPSI - University of Applied Sciences Southern Switzerl
-  SWITCH
-  VHO - Virtual Home Organization
-  WSL - Swiss Federal Institute for Forest, Snow and Lands


Disco Juice


- Very comprehensive Discovery Service
- Well suited for services with users from many IdPs
- Search-as-you-type only
- Uses Geo IP and metric to guess user's IdP
- Based on PHP and JS


 <http://discojuice.org/>





Sign in to **Foodle**
Select your Provider

 **SWITCH**
Switzerland 2 km


OpenIdP — If you do not have an institutional account, register here. 

Protect Network — If you do not have an institutional account, register here. 

GÉANT Identity Provider — Login provider for users registered at the GIdP 

Twitter 

► Please help, I cannot find my provider

 Locate me and show nearby providers

Show providers in Switzerland show all countries

DiscoJuice © UNINETT

Foodle frontpage

[English](#) | [Bokmål](#) | [Nynorsk](#) | [Dansk](#) | [Svenska](#) | [Suomeksi](#) | [Nederl](#)

Welcome to Foodle

Foodle is a service for simple surveys or polls and for scheduling meetings.

You are currently not logged in.

[Create a new Foodle](#)

Statistics

Foodle had 89 responses last 7 days.

More information

- The Foodle Software
- Foodle Privacy Policy
- Feide RnD blog

Sign in to Foodle

Select your Provider

**SWITCH**

Switzerland 12 km

SWITCH

OpenIdP — If you do not have an institutional account, register here.



Protect Network — If you do not have an institutional account, register here.



GÉANT Identity Provider — Login provider for users registered at the GIdP



Twitter



► Please help, I cannot find my provider



Locate me and show nearby providers

Show providers in Switzerland [show all countries](#)

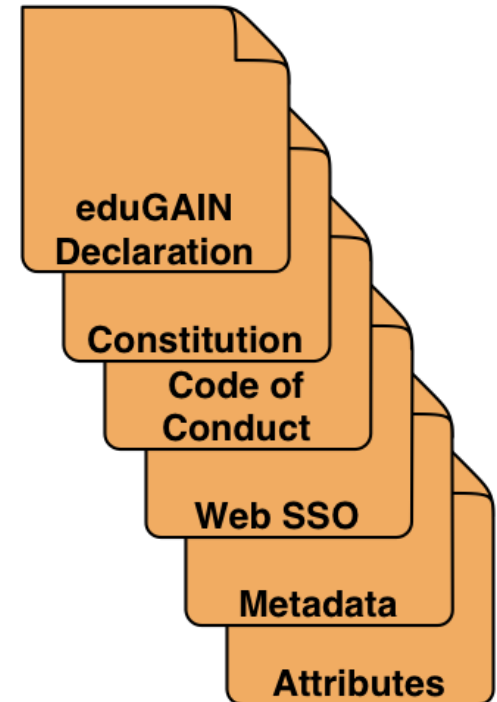
DiscoJuice © UNINETT

Content

- Overview and Use Cases
- Metadata
- Discovery Service(s)
- **Legal aspects**

The Rules for eduGAIN

- The set of documents gets soon a minor revision
 - eduGAIN Declaration
 - *SWITCH signed it in 2011*
 - eduGAIN Constitution
 - eduGAIN Metadata Profile
 - eduGAIN Attribute Profile
 - A small set of standard attributes
 - eduGAIN SAML 2.0 WebSSO Profile
 - GÉANT Data Protection Code of Conduct



<http://www.geant.net/service/edugain/resources>

SWITCHaai

SWITCH

[About AAI](#) | [FAQ](#) | [Help](#) | [Privacy](#)

You are about to access the service:
'Neptun Store' of [ETHZ - ETH Zürich](#).

Description as provided by this service:
Bestellungen von Neptun Produkten

Requested Data

Surname	Aeschlimann
Given name	Andres
Affiliation	member staff
E-mail	andres.aeschlimann@switch.ch
Unique ID	225503@switch.ch
Home organization	switch.ch

The data above is requested to access the service. Do you accept that this data about you is sent to the service whenever you access it?

Reject

Accept

The Steps Required to Interfederate

- 1) SWITCHaai Participant need to sign an “interfederation access declaration”.
- 2) SWITCH then sets the 'flag' in the Resource Registry for them.
- 3) Then IdP and SP admins 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	<input checked="" type="checkbox"/> Enable interfederation for this Home Organisation <small>Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources.</small>

<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>

Summary Interfederation/edugain

- Use Cases are growing
- Metadata can be handled
- Discovery Service(s) to choose from
- Legal aspects

That's it.

Thank you



SWITCH

Serving Swiss Universities

andres.aeschlimann@switch.ch



11.3.2013