Interfederation Crash Course

SWITCHaai Team
aai@switch.ch

Bern, 1. March 2013

Overview

- Interfederation - Getting ready to cross borders
- eduGAIN
  - What's eduGAIN?
  - Example Show Cases - DOIT, REDI, TNC, Foodle
- *Coffee Break*
- How to Deploy Interfederation?
  - The Administrative Task – SWITCHaai Interfederation Access Declaration
  - The Technical Tasks
    - Attribute Support & Consent
    - Configuring the IdP for interfederation use
    - Configuring the SP for interfederation use
    - Discovery Service Options for SP Administrators
    - Service Provider "Code of Conduct"
  - What else? - How to proceed when you want to interfederate a service

Interfederation

Getting ready to cross borders

SWITCH

Daniel Lutz
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

Internationalization

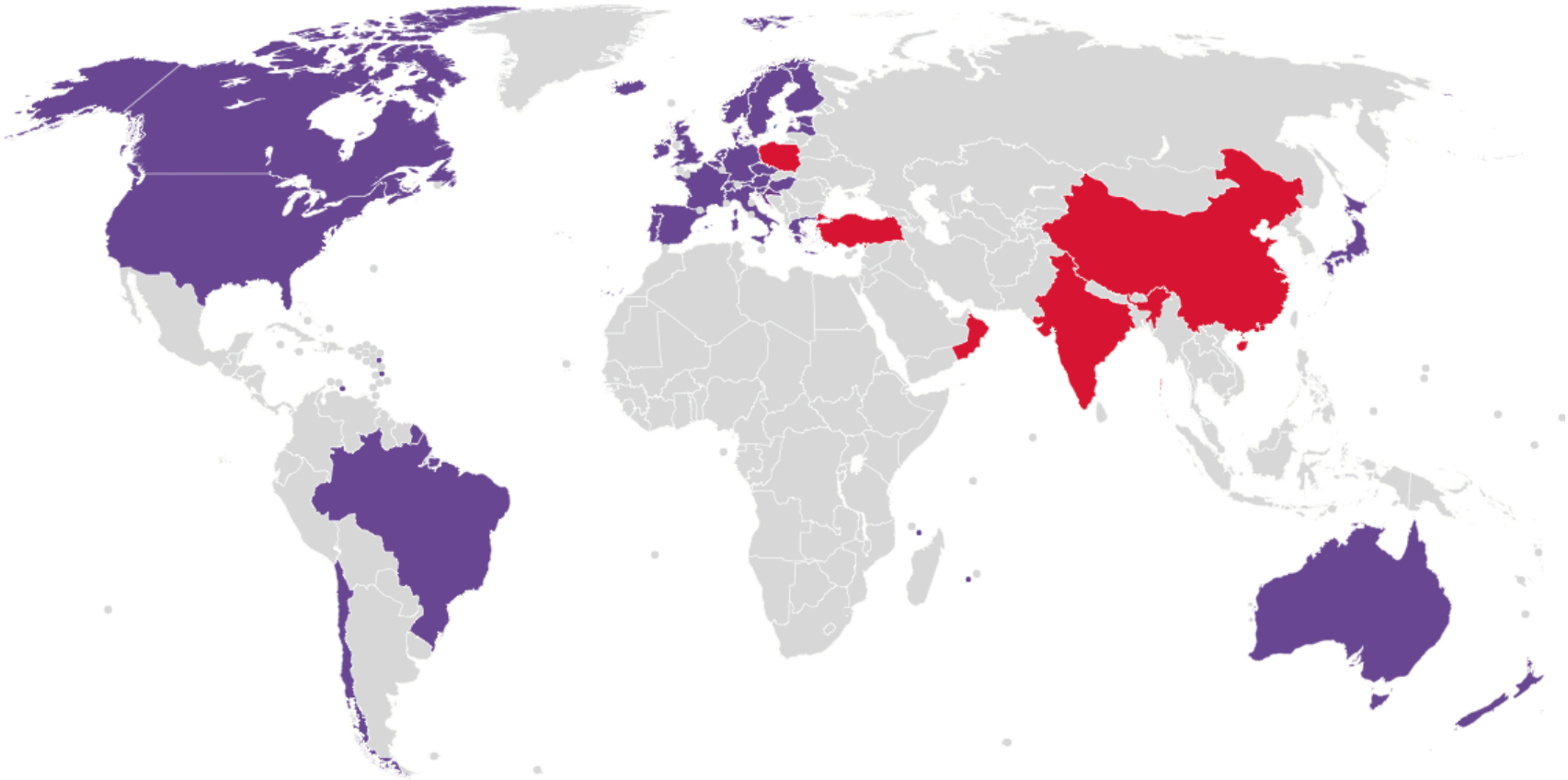
Many established **national** Identity Federations

- but research projects are **international**
- but content publishers' customers are **international**
- but audience of research wikis and blogs is **international**

Interconnecting national federations → Interfederation

- Interfederation service facilitates international research collaboration
- Content publishers can offer their services without concluding contracts with each single federation

Identity Federations of the World



REFEDS

In production In pilot (Last update: January 2013)

Getting ready for the future

- Today
  - SWITCHaai is mostly bound to CH/LI borders
    - Exception
      - International Federation Partners (mostly content publishers)
      - Foreign users in the Virtual Home Organization (VHO)
        (usually already have an account in their local federation)
  - Many national AAI's in place

- With interfederation we are able to cross the borders
  - Swiss users are able to access opted-in foreign SPs
  - Foreign users are able to access opted-in Swiss SPs
  - Single Sign-On across federations

- eduGAIN from GÉANT3 is the first interfederation service SWITCHaai co-operates with
  - Others might follow

http://edugain.org

What's different with interfederation?

- No longer a single legal or policy framework
  - Each federation has its own
  - eduGAIN has one as well [1]
- No single 'interfederation helpdesk' in case of problems
  - Debugging involves probably more parties
  - Involved parties will generally know less about each other
- Different sets of attributes used internationally
  - e.g. no studyLevel or studyBranch attributes

[1] http://www.geant.net/service/edugain/resources

eduGAIN

An Interfederation Service of GÉANT

SWITCH

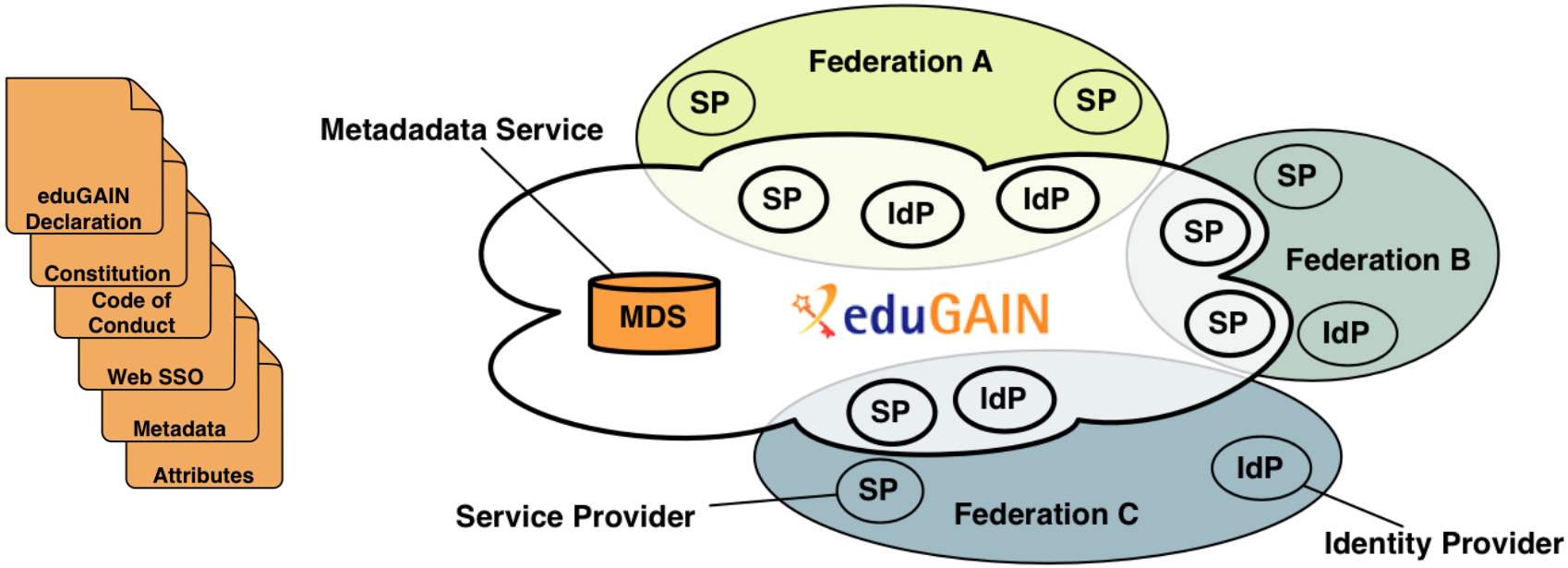
Thomas Lenggenhager
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

Overview

- Interfederation with eduGAIN
  - The Structure, the Numbers, the Scope
  - How it works
  - The Rules
  - Showcases

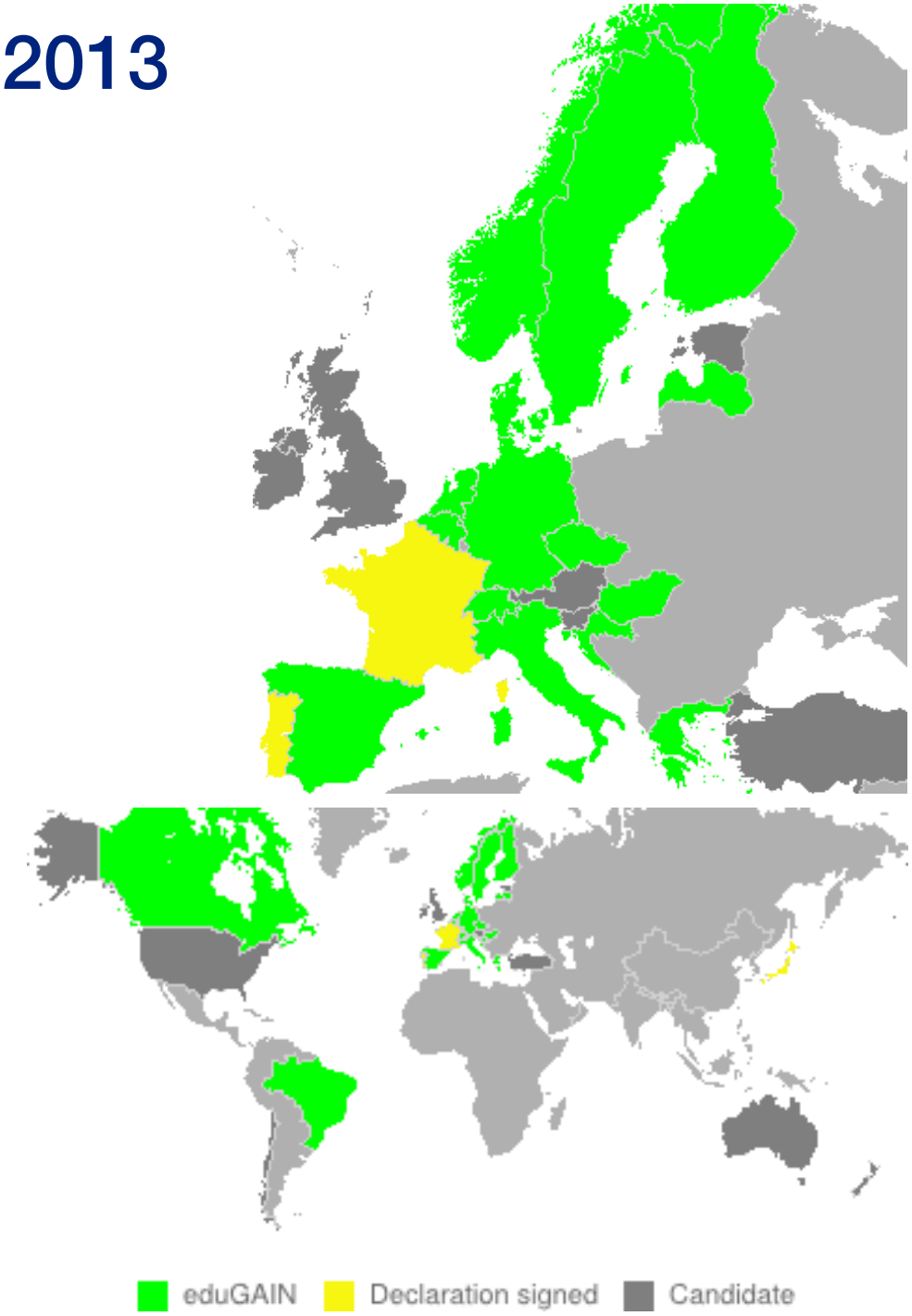
The Structure



- eduGAIN provides policy framework and standards to build trust
- SPs and IdPs of participating federations should opt-in for eduGAIN
- MDS fetches, aggregates and republishes metadata

The numbers February 2013

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

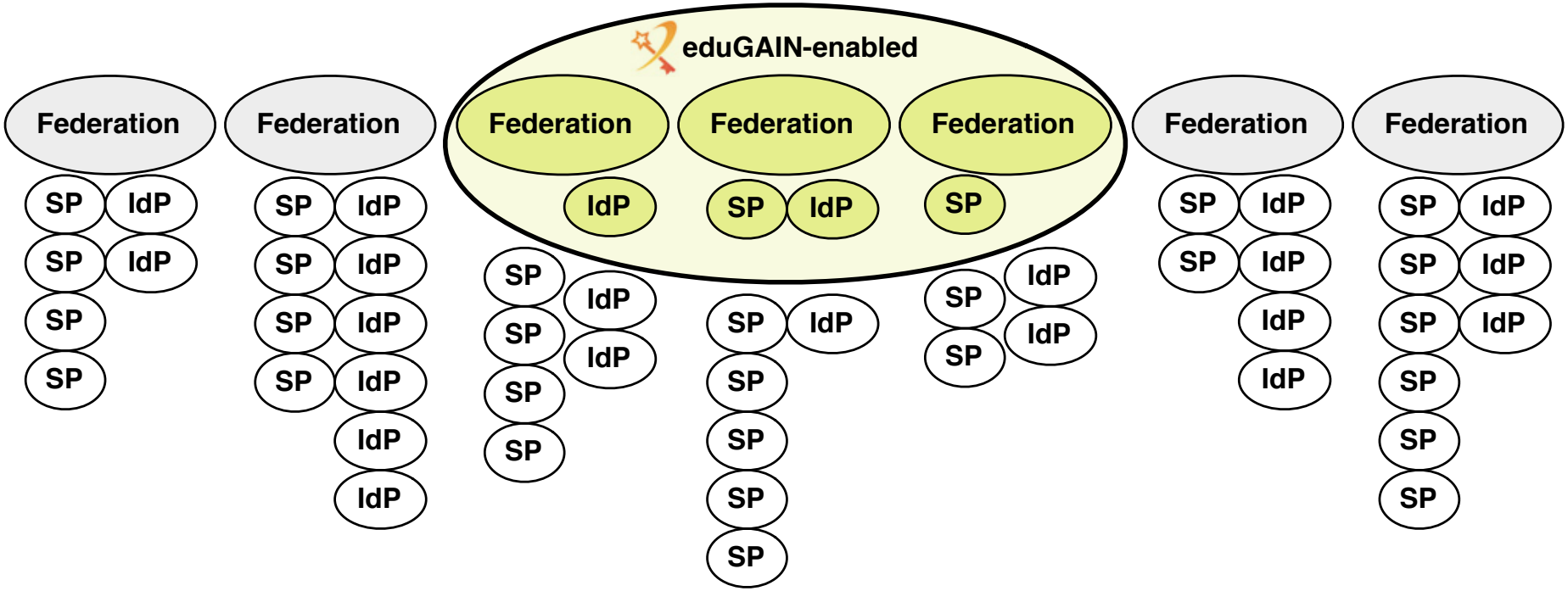


http://www.edugain.org

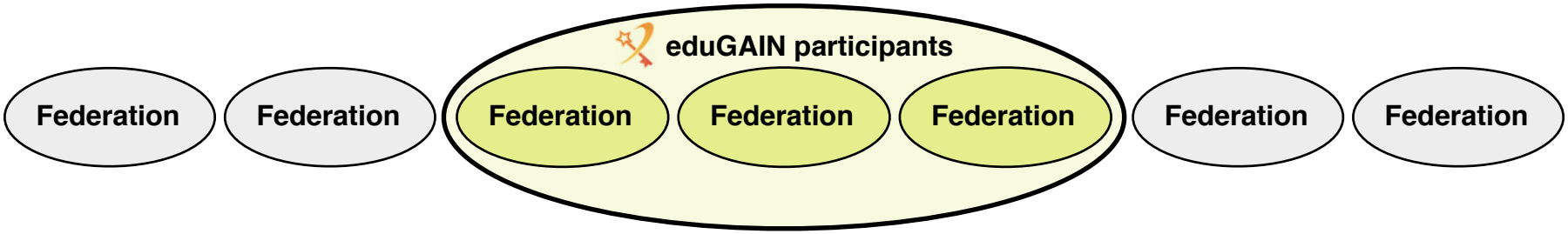
http://www.edugain.org/technical/status.php

Adoption Width vs. Depth

- Good federation adoption (Width)
- Entity Adoptions (Depth) has yet to grow

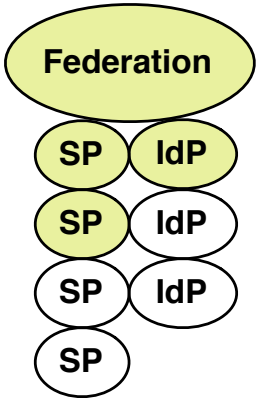


Width and Depth in Numbers



- **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

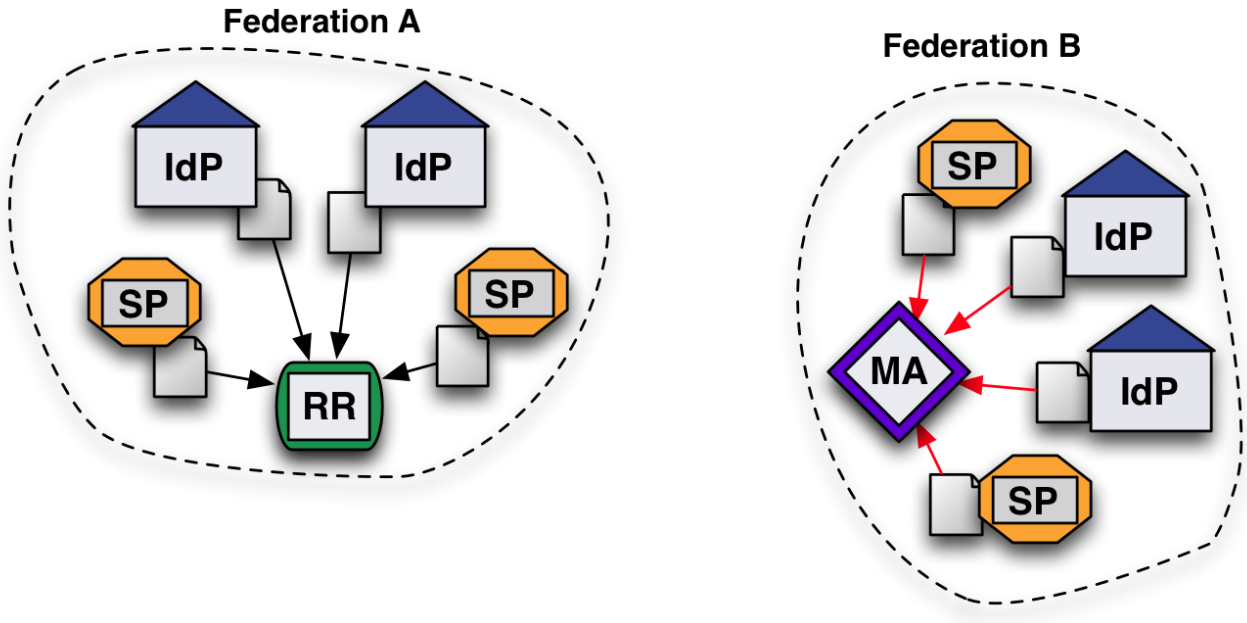


- Not every SP and IdP has good reasons to interfederate!

How it works

- The situation with 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 publishes the metadata file
    3) The entities regularly fetch the metadata file and consume it

Collect Metadata from Entities

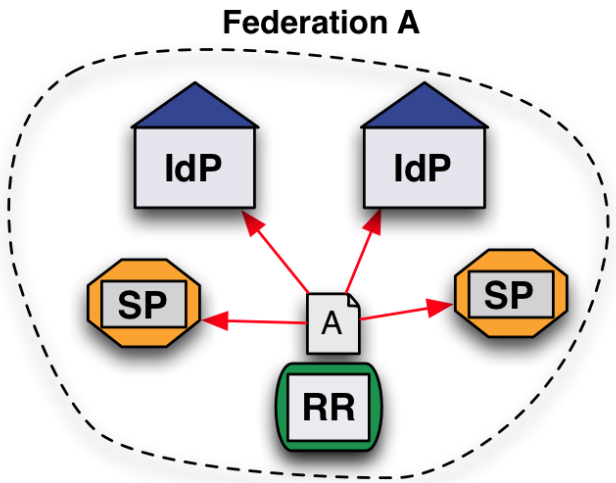


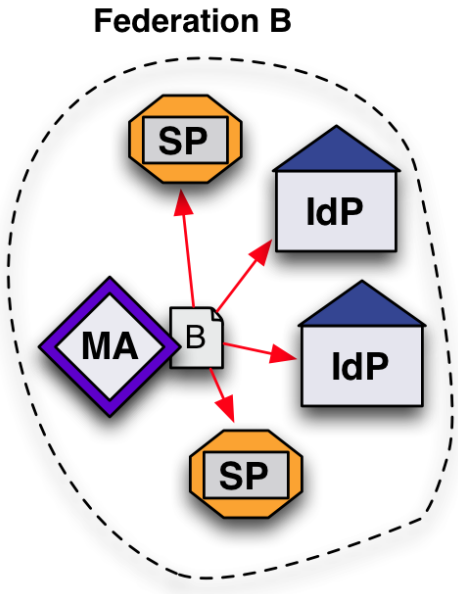
- Federation collects metadata from the entities e.g. with
  - a Resource Registry 

  - a Metadata Aggregator that pulls its metadata 

Publish Federation Metadata

Metadata file
of Federation A



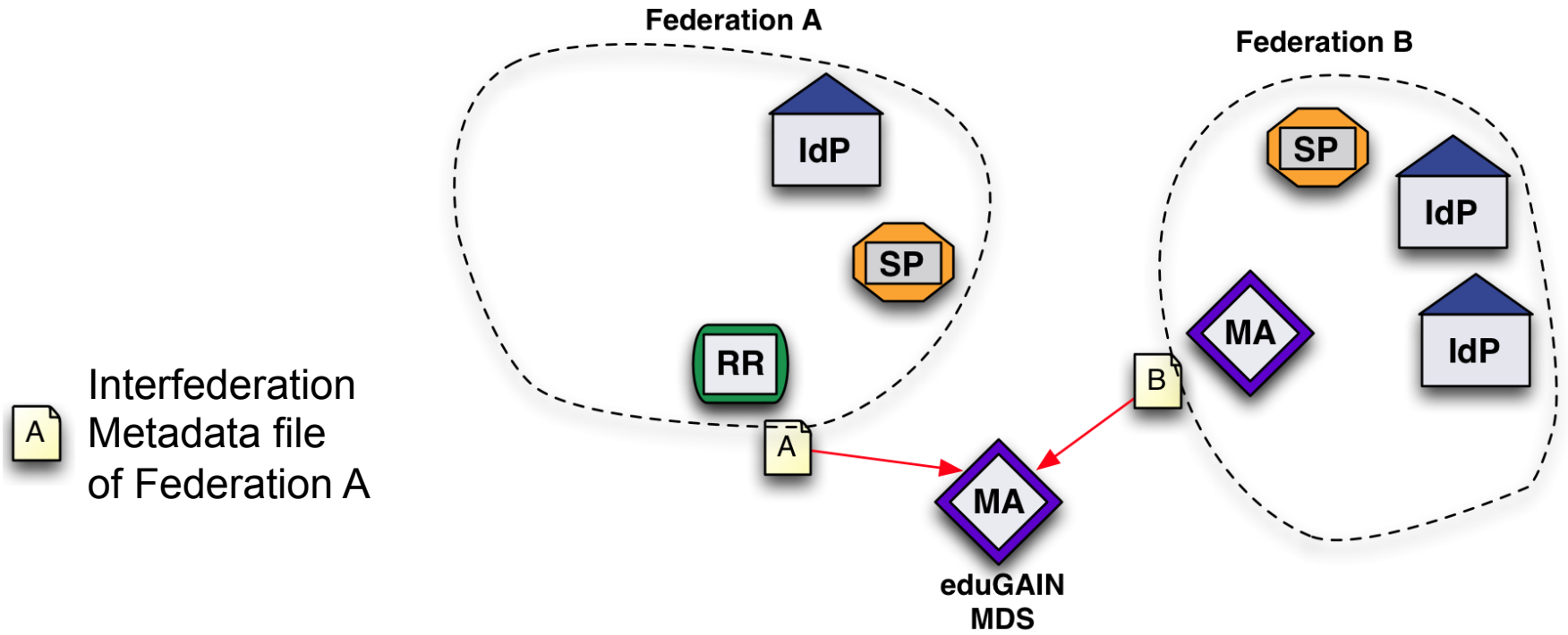


- Each Federation publishes its metadata file
- Entities fetch it from their Federation

How it works (2)

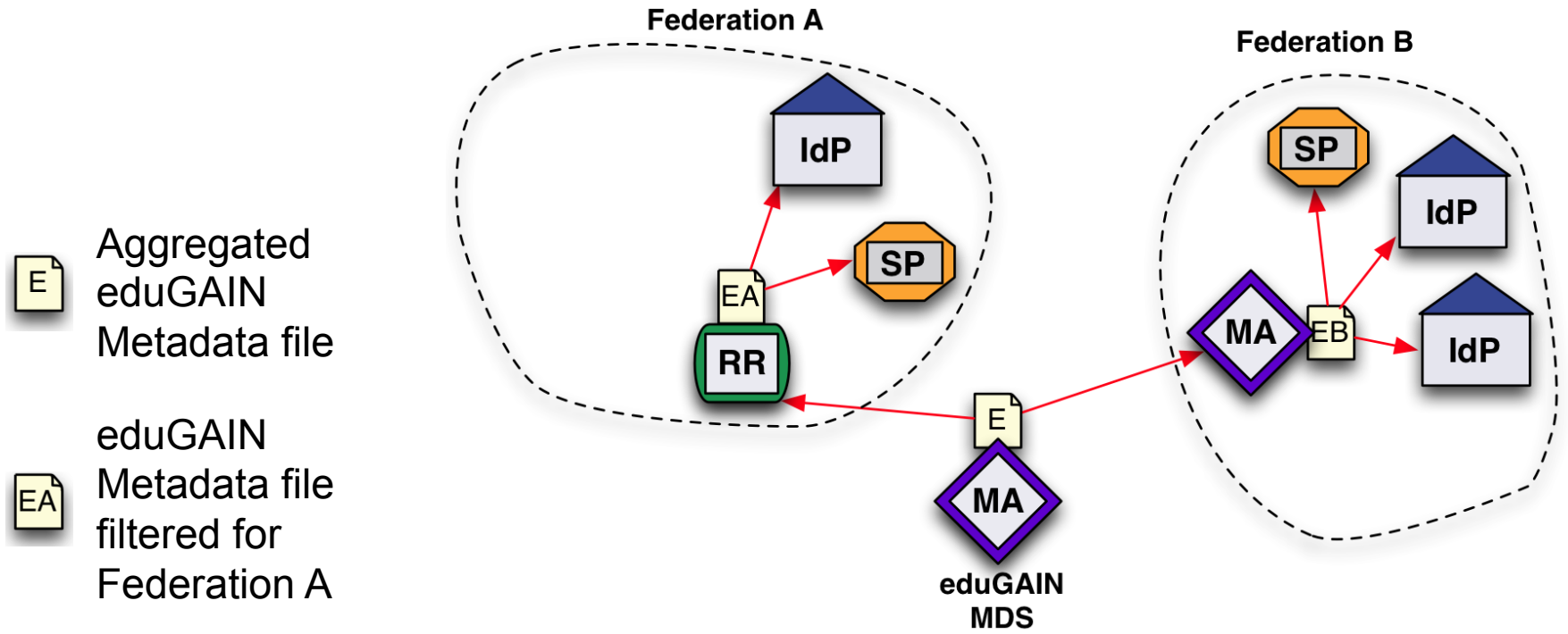
- How to get hold of entities from all the other federations?
  1) Each Federation publishes an additional metadata file with the entities participating in interfederation
  2) eduGAIN Metadata Service MDS checks and aggregates these files and publishes an aggregated eduGAIN metadata file
  3) Each Federation fetches the aggregated file, filters out the own entities and publishes it for the local entities that participate in interfederation.

Publish Metadata for Interfederation



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

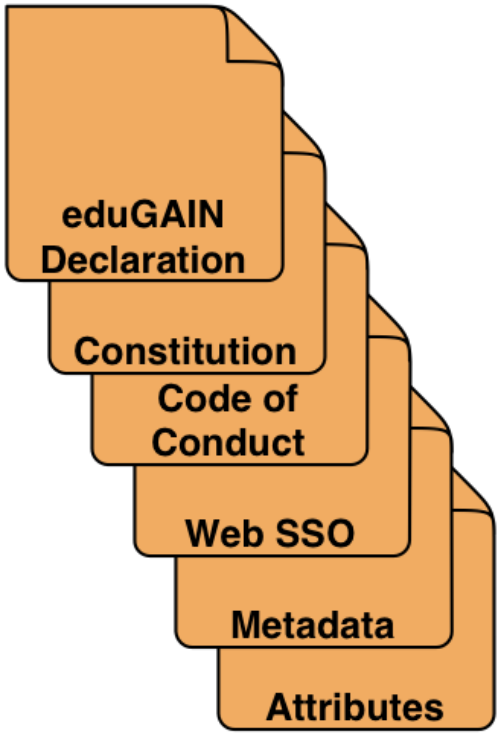
Consume and Republish Interfederation Metadata



- 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

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

Example Show Cases

DOIT, Forge, REDI, Terena Services, Foodle

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 1. March 2013

Overview

SWITCHaai SP offered to international community:

1. DOIT
2. Forge

Usable by SWITCHaai users with Interfederation:

3. REDI
4. TERENA services
5. Foodle

1. SWITCH Forge

- Service operated by SWITCH
- Redmine project management platform: issue tracker, wiki, calendar, news, version control integration, road map, etc.
- > 60 public/private SWITCH projects
- Accessible via SWITCHaai/eduGAIN
- Link: https://forge.switch.ch

SWITCH Forge Use Case

- Bug reporting and contributions for open source projects
- Users from all around the world
- Authenticated users:
  - can be assigned higher privileges
  - are notified when issues are updated
  - can work in non-public projects
- Useful for Open Source projects

Home | My page | Projects | Administration | Help | All Services by SWITCH | Logged in as haemmer

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.c
```

- 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

2. DOIT - Dermatology Online

- E-Learning material to teach dermatologists around the world
- Initiated by University of Zurich
- Accessible via SWITCHaai/eduGAIN
- Interested partner universities in 40 countries
- Link: http://doit.swisdom.org

DOIT Use Case

- To learn dermatology DOIT hosts many pictures showing horrible skin diseases
- Therefore, only dermatology students should get access
- Manual registration and validation by DOIT administrators is time consuming
- Validation not necessary with AAI/ Interfederation

DOIT Dermatology Online with Interactive Technology | European Dermatology Forum | Editiermodus | Willkommen Lukas Hämmerle | Logout | German

Founding Editor: Günter Burg,M.D., Zürich

E-Mail | Kontaktinformationen | Drucken | Suchen...

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

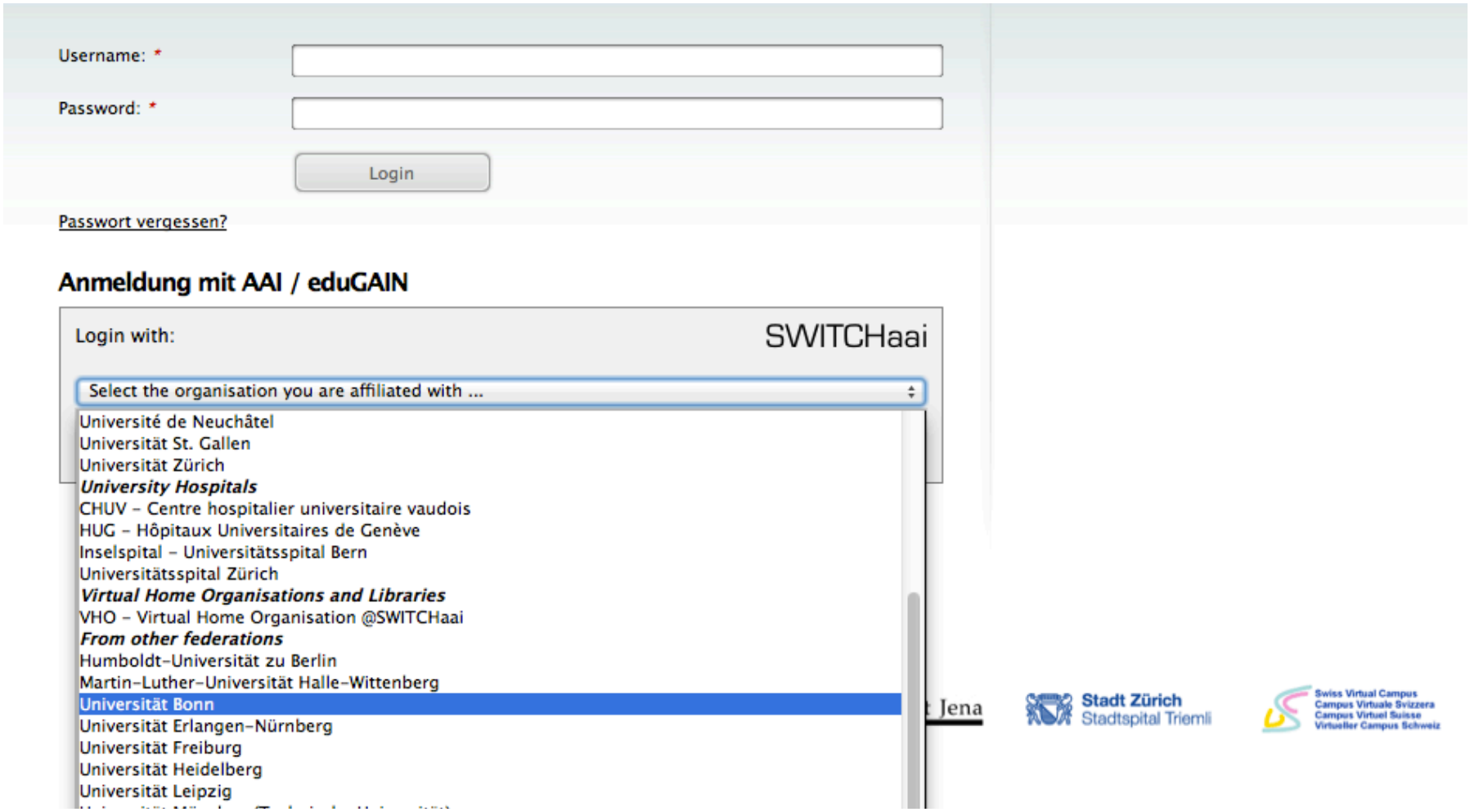
- Synonyme
- Definition
- Aetiologie & Pathogenese
- Symptome
- Klassifikation
- Labor
- Diagnose
- Differentialdiagnose
- Therapie

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

Definition Durch flüchtige, juckende Quaddeln (Urticae) gekennzeichnetes Exanthem

Personal notes

Klinische Bilder


Username: *
Password: *
Login
Passwort vergessen?
Anmeldung mit AAI / eduGAIN
Login with:
SWITCHaai
Select the organisation you are affiliated with ...
Université de Neuchâtel
Universität St. Gallen
Universität Zürich
University Hospitals
CHUV – Centre hospitalier universitaire vaudois
HUG – Hôpitaux Universitaires de Genève
Inselspital – Universitätsspital Bern
Universitätsspital Zürich
Virtual Home Organisations and Libraries
VHO – Virtual Home Organisation @SWITCHaai
From other federations
Humboldt-Universität zu Berlin
Martin-Luther-Universität Halle-Wittenberg
Universität Bonn
Universität Erlangen-Nürnberg
Universität Freiburg
Universität Heidelberg
Universität Leipzig
Jena
Stadt Zürich
Stadtspital Triemli
Swiss Virtual Campus
Campus Virtuale Svizzera
Campus Virtuel Suisse
Virtueller Campus Schweiz

3. REDI

- ReDI - Regionale Datenbank-Information
- Access > 950 science databases
- Currently a SWITCHaai federation partner
  - REDI needed to sign Federation Partner agreement and bilaterally configure foreign IdPs
- Link: http://www.redi-bw.de

REDI Use Case

- Used by Swiss and German universities and libraries
- With Interfederation, no need for REDI to sign another federation agreement if other universites should be granted access (e.g. from Austria)

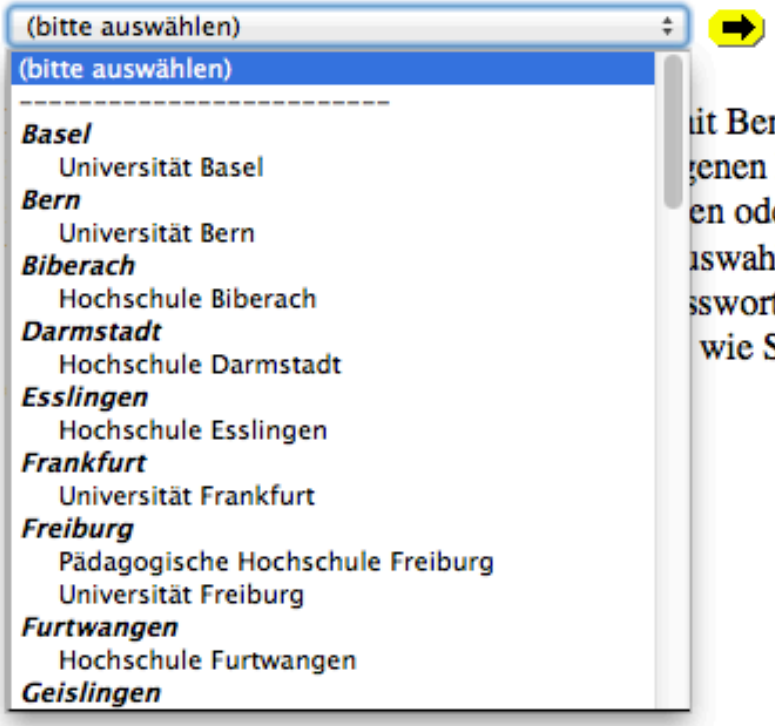
- Homepage
- Aktuell
- Datenbanken
- Zugang/Passwort
- Kontakt
- Login

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:



it Benutzerkennung und Passwort nur
genen Identity Provider (Login-Server)
en oder in Kürze betreiben werden.
uswahl angeboten wird, können Sie
sswort einloggen. Bitte erkundigen Sie
wie Sie ReDI von ausserhalb des

4. TERENA Services

- TERENA = Trans-European Research and Education Networking Association
- SWITCH is member of TERENA
- International colloboration activities and meetings

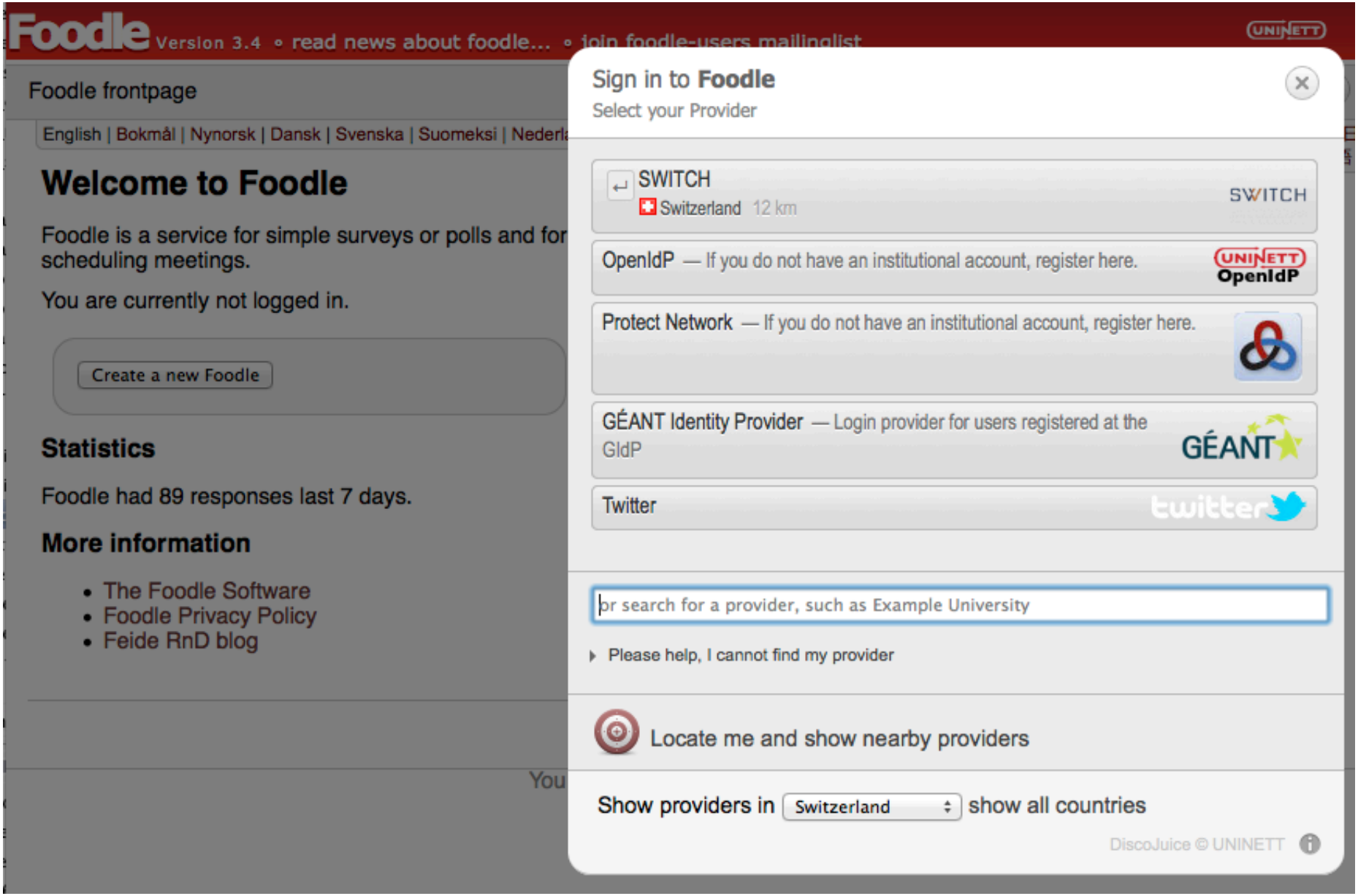
- Example Services:
  - Federation Wiki: https://refeds.terena.org
  - Conference Registration: http://tnc2013.terena.org

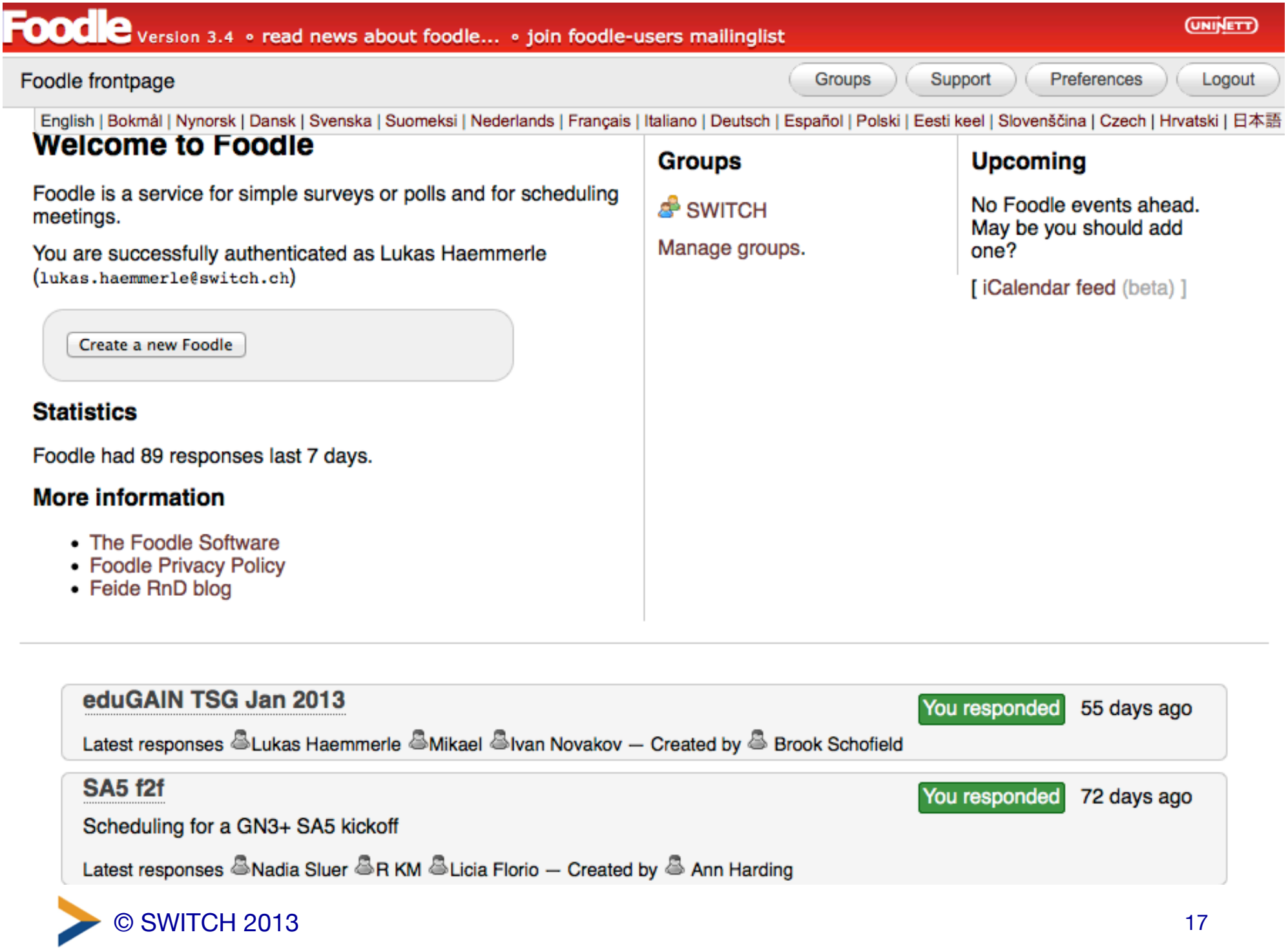
5. Foodle

- 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

Foodle Use Case

- Used by users all around the world
- Authentication allows additional features like:
  - History of answered surveys
  - Email address is known from participants
  - Calendar integragion via feed


Foodle
Version 3.4
read news about foodle...
join foodle-users mailinglist
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
You
Sign in to Foodle
Select your Provider
SWITCH
Switzerland 12 km
SWITCH
OpenIdP — If you do not have an institutional account, register here.
UNINETT OpenIdP
Protect Network — If you do not have an institutional account, register here.
GÉANT Identity Provider — Login provider for users registered at the GIdP
GÉANT
Twitter
twitter
or search for a provider, such as Example University
Please help, I cannot find my provider
Locate me and show nearby providers
Show providers in Switzerland show all countries
DiscoJuice © UNINETT


Foodle Version 3.4 • read news about foodle... • join foodle-users mailinglist
UNINETT
Foodle frontpage
Groups
Support
Preferences
Logout
English | Bokmål | Nynorsk | Dansk | Svenska | Suomeksi | Nederlands | Français | Italiano | Deutsch | Español | Polski | Eesti keel | Slovenščina | Czech | Hrvatski | 日本語
Welcome to Foodle
Foodle is a service for simple surveys or polls and for scheduling meetings.
You are successfully authenticated as Lukas Haemmerle (lukas.haemmerle@switch.ch)
Create a new Foodle
Statistics
Foodle had 89 responses last 7 days.
More information
The Foodle Software
Foodle Privacy Policy
Feide RnD blog
Groups
SWITCH
Manage groups.
Upcoming
No Foodle events ahead. May be you should add one?
[iCalendar feed (beta)]
eduGAIN TSG Jan 2013
You responded
55 days ago
Latest responses Lukas Haemmerle Mikael Ivan Novakov — Created by Brook Schofield
SA5 f2f
You responded
72 days ago
Scheduling for a GN3+ SA5 kickoff
Latest responses Nadia Sluer R KM Licia Florio — Created by Ann Harding

Summary

Interfederation/eduGAIN helps:

- Home Organisations to:
  - Allow students/researchers access more AAI services in other countries

- Service operators to:
  - Allow users from other countries to authenticate with their own AAI account
  - Get rid/minimize account management

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!

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"

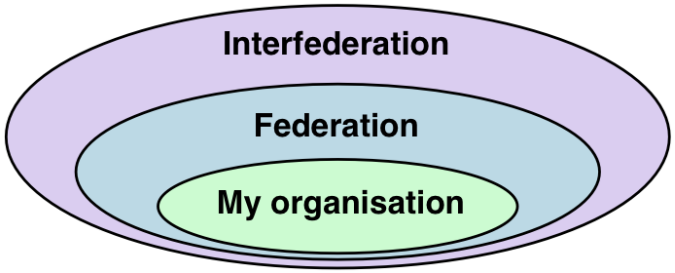
3) that the IdP supports user consent (uApprove module)

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

Attribute Availability & Release

Support of international attributes and uApprove

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 1. March 2013

Overview

1. Supporting International Attributes
2. Data Protection and uApprove
3. Recommendations

1. Supporting International Attributes

- SWITCHaai was the first production federation in Europe
- Attributes used in SWITCHaai are sometimes specific for Switzerland due to swissEduPerson schema
- Internationally it is recommended to support alternative/other attributes than the swissEduPerson attributes

Recommended International Attributes

Attributes that should be additionally be supported:

- Scoped Affiliation ("staff@unibe.ch")
- Display Name ("Pierre Müller")
- Common Name ("Pierre Müller")
- SCHAC Home Organization ("unibe.ch")
- SCHAC Home Organization Type ("urn:schac:homeOrganizationType:ch:university")
- eduPersonPrincipalName ("sdc8932rhc@unibe.ch")

How to Support Int. Attributes

- User data is already available:
  - No modifications in user directory needed
  - Just the format and the name has to be configured
  - All values can be dynamically added by IdP

- Only a matter of IdP configuration
  - Attribute resolver configuration
  - Link: https://www.switch.ch/aai/docs/interfederation/international-attributes.html

Additional Benefits/Needs

- International Attributes are not only needed for Interfederation!
- Potential SWITCHaai Federation Partners require them too (e.g. scoped affiliation)
- Supporting International Attributes is important for future interoperability

SCHAC Attributes

- SCHAC = **SCH**ema for **AC**ademia
- Defines 21 Attributes for LDAP
- Some attributes similar to swissEduPersonSchema

- Link: http://www.terena.org/activities/tf-emc2/schac.html

SCHAC Example Definition

5.2.1 schacHomeOrganization

Name	**schacHomeOrganization**
Description	Specifies a person´s home organization using the domain name of the organization
Format	Domain name according to RFC 1035
# of values	Single
References	• **RFC 1035** – Domain names – implementation and specification
RFC 4517 definition	(schacAttributeType:9 NAME 'schacHomeOrganization' DESC 'Domain name of the home organization' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SINGLE-VALUE SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)
Examples	• schacHomeOrganization = tut.fi

Data Protection and Privacy

Do you know of any data protection problems/law suits in your organisation regarding the release of user information?

Why Care About Data Protection?

- Most users don't care, so why should we?

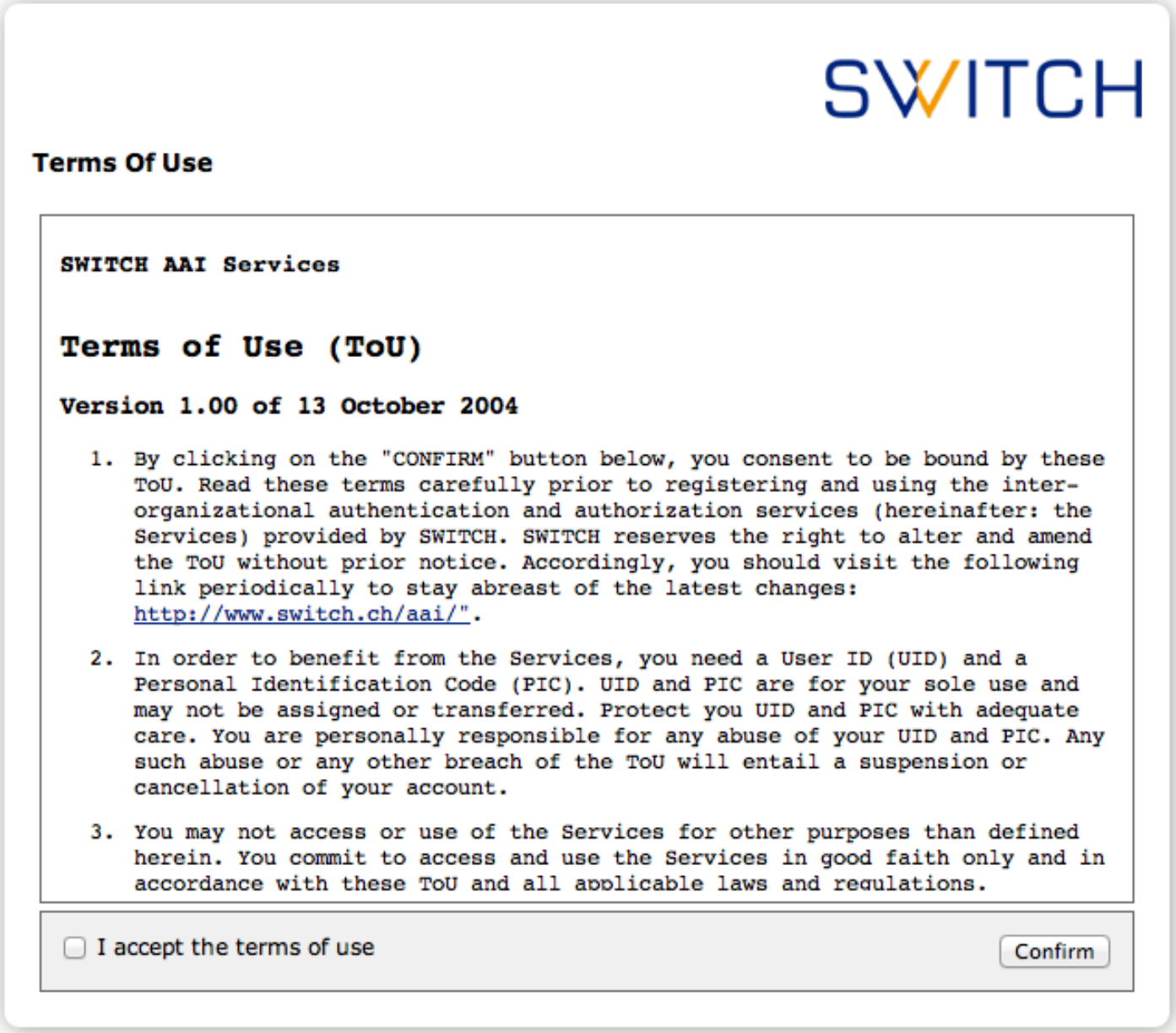
- **Why to care:**
  - With interfederation students and staff members access services operated in other jurisdictions
  - Organisation could be held liable
  - Reason why Facebook's reputation suffered

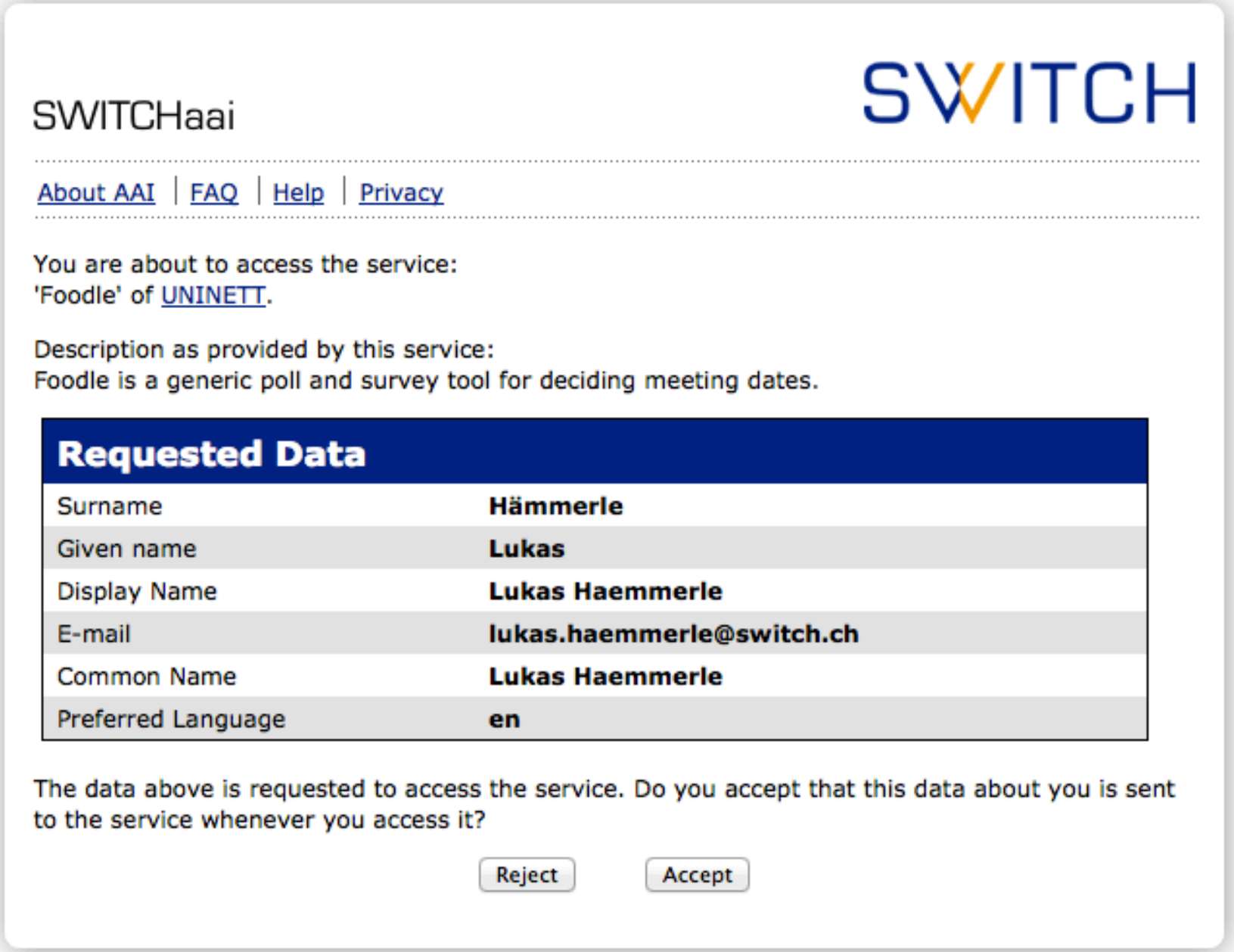
2. Data Protection and uApprove

- Attributes are personal data of enduser
- Home Organisation is responsible and liable for personal data/attributes
  - Release may infringe users privacy when he accesses services outside organisation
- User should agree/consent to attribute release
  - Formally with Terms of Use and/or technically
- Discussions with Swiss Data Protection Officer:
  -> User Consent is strongly recommended

Getting User's Consent with uApprove

- uApprove = Plug-In for the Shibboleth IdP
- Asks user to:
  - accept IdP terms of use once (optional)
  - allow attribute release on first access of service or if attributes changed
- Developed by SWITCH as Open Source
- Used internationally
- Link: http://www.switch.ch/aai/uapprove


SWITCH
Terms Of Use
SWITCH AAI Services
Terms of Use (ToU)
Version 1.00 of 13 October 2004
1. By clicking on the "CONFIRM" button below, you consent to be bound by these ToU. Read these terms carefully prior to registering and using the inter-organizational authentication and authorization services (hereinafter: the Services) provided by SWITCH. SWITCH reserves the right to alter and amend the ToU without prior notice. Accordingly, you should visit the following link periodically to stay abreast of the latest changes: http://www.switch.ch/aai/".
2. In order to benefit from the Services, you need a User ID (UID) and a Personal Identification Code (PIC). UID and PIC are for your sole use and may not be assigned or transferred. Protect you UID and PIC with adequate care. You are personally responsible for any abuse of your UID and PIC. Any such abuse or any other breach of the ToU will entail a suspension or cancellation of your account.
3. You may not access or use of the Services for other purposes than defined herein. You commit to access and use the Services in good faith only and in accordance with these ToU and all applicable laws and regulations.
I accept the terms of use
Confirm


SWITCHaai
SWITCH
About AAI | FAQ | Help | Privacy
You are about to access the service:
'Foodle' of UNINETT.
Description as provided by this service:
Foodle is a generic poll and survey tool for deciding meeting dates.
Requested Data
Surname Hämmerle
Given name Lukas
Display Name Lukas Haemmerle
E-mail lukas.haemmerle@switch.ch
Common Name Lukas Haemmerle
Preferred Language en
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

uApprove Deployment

- Requires a MySQL database
  - Already deployed by all SWITCHaai IdPs
- Easy to deploy
- Templates can and should be adapted

- Example terms and configurations: http://www.switch.ch/aai/legaltemplates (SWITCH legal approved)

Recommendations

- Support International Attributes even without interfederation participation
  - It's easy to support them
  - Publishers may require some of them in the future

- SWITCH strongly recommends deploying uApprove for interfederation support
  - Transparent for users regarding data release
  - Organisation should be on the safe side
  - Not very invasive if blacklisting is used

Configuring the IdP for interfederation use

A short How-to

Daniel Lutz
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

High-level overview of the procedure (1)

Assumptions:

- Your IdP is running the currently supported release of the Shibboleth Identity Provider (as of February 2013, this is version 2.3.8)
- Your IdP is already registered in the SWITCHaai federation and is properly working for SWITCHaai users
- The SWITCHaai Interfederation Access Declaration has been signed by the organization

High-level overview of the procedure (2)

Required steps:

1. Enable user consent (module uApprove) on the Identity Provider
2. Adapt Identity Provider configuration
   - Load the interfederation metadata
   - Release all the attributes recommended for interfederation support
3. Adapt entry in Resource Registry
   - Enable Interfederation for the Home Organization
   - Enable the additional attributes
4. Pass Interfederation Test

Enable user consent: Install uApprove (1)

- Install uApprove following the installation instructions: http://www.switch.ch/aai/downloads/uApprove-manual/

- In case you haven't yet used uApprove:
  Optionally disable uApprove for some SWITCHaai Service Providers in the file `uApprove.properties` (e.g. Service Providers of your own organization)

Enable user consent: Install uApprove (2)

Disabling uApprove for some Service Providers by blacklisting them in the uApprove configuration (`uApprove.properties`):

- Disabling uApprove for your own organization's services only:

```
services = ^https://[^/]+\.example\.org/.*$ \
           ^https://[^/]+\.example\.edu/.*$
[...]
services.blacklist = true
```

- Disabling uApprove for all services in ".ch" domain:
  (Warning: might also match non-Swiss Service Providers that use a ".ch" domain)

```
services = ^https://[^/]+\.ch/.*$
[...]
services.blacklist = true
```

Add additional Attribute Definitions

- 6 additional attributes required for interfederation
- Values of these attributes are based on already existing information; no changes in user directory required
- Additional attributes:
  - Display Name
  - Common Name
  - Principal Name
  - SCHAC Home Organisation
  - SCHAC Home Organisation Type
  - Scoped Affiliation
- Add these attributes to `attribute-resolver.xml`
- Furthermore, you should make sure that the attribute "Affiliation" contains the value "member" for the affiliations "student", "staff" and "faculty".

Attributes: Example Values

Display Name: Peter Jones

Common Name: Peter Jones

Principal Name: 256973496@example.org

SCHAC Home Organisation: example.org

SCHAC Home Organisation Type:
urn:schac:homeOrganizationType:int:university
urn:schac:homeOrganizationType:ch:university

Scoped Affiliation:
student@example.org
member@example.org

Attributes: Example Configuration: Display Name

Case 1: Attribute is available in your LDAP directory
Use the value from the LDAP directory

```
<!-- Display Name (displayName) -->
<!-- Attribute displayName is contained in your LDAP directory:
     use the value from the LDAP directory-->
<resolver:AttributeDefinition id="displayName" xsi:type="ad:Simple"
    sourceAttributeID="displayName">

    <resolver:Dependency ref="myLDAP" />

    <resolver:DisplayName xml:lang="en">Display Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
          The name that should appear in white-pages-like applications for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:displayName" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.16.840.1.113730.3.1.241" friendlyName="displayName" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Display Name

Case 2: Attribute is not available in your LDAP directory
Compose the value with JavaScript

```
<!-- Attribute displayName is not contained in your LDAP directory:
     compose the value with JavaScript -->
<resolver:AttributeDefinition id="displayName" xsi:type="ad:Script">
    <resolver:Dependency ref="givenName" />
    <resolver:Dependency ref="surname" />

    <resolver:DisplayName xml:lang="en">Display Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        The name that should appear in white-pages-like applications for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:displayName" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.16.840.1.113730.3.1.241" friendlyName="displayName" />
```

(continued on next page)

Attributes: Example Configuration: Display Name

(continued from previous page)

```
    <ad:Script>
      <![CDATA[

         importPackage(Packages.edu.internet2.middleware.shibboleth.common
                .attribute.provider);

        // Initialize displayName
        displayName = new BasicAttribute("displayName");

        // compose value from givenName and surname
        displayName.getValues().add( givenName.getValues().get(0) + " " +
                surname.getValues().get(0) );
      ]]>
    </ad:Script>
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Common Name

Case 1: Attribute is available in your LDAP directory
Use the value from the LDAP directory

```
<!-- Common Name (commonName) -->
<!-- Attribute commonName is contained in your LDAP directory:
     use the value from the LDAP directory -->
<resolver:AttributeDefinition id="commonName" xsi:type="ad:Simple" sourceAttributeID="cn">
    <resolver:Dependency ref="myLDAP" />

    <resolver:DisplayName xml:lang="en">Common Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        One or more names that should appear in white-pages-like applications
        for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:cn" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.5.4.3" friendlyName="cn" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Common Name

Case 2: Attribute is not available in your LDAP directory
Use the same value as of displayName

```
<!-- Common Name (commonName) -->
<!-- Attribute commonName is not contained in your LDAP directory:
     Use the value of the attribute displayName -->
<resolver:AttributeDefinition id="commonName" xsi:type="ad:Simple"
     sourceAttributeID="displayName">

    <resolver:Dependency ref="displayName" />

    <resolver:DisplayName xml:lang="en">Common Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        One or more names that should appear in white-pages-like applications
        for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:cn" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.5.4.3" friendlyName="cn" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Principal name

Use the same value as of swissEduPersonUniqueID

```
<!-- Principal name (eduPersonPrincipalName) -->
<!-- Use the same value as the attribute swissEduPersonUniqueID -->
<resolver:AttributeDefinition id="eduPersonPrincipalName" xsi:type="ad:Simple"
    sourceAttributeID="swissEduPersonUniqueID">

    <resolver:Dependency ref="swissEduPersonUniqueID" />

    <resolver:DisplayName xml:lang="en">Principal Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        A unique identifier for a person, mainly for inter-institutional
        user identification.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:eduPersonPrincipalName" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        friendlyName="eduPersonPrincipalName" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: SCHAC Home Organisation

Use static attributes

```
<!-- SCHAC Home Organisation (schacHomeOrganization) -->
<resolver:AttributeDefinition id="schacHomeOrganization" xsi:type="ad:Simple"
    sourceAttributeID="schacHomeOrganization">

    <resolver:Dependency ref="staticAttributes" />

    <resolver:DisplayName xml:lang="en">Home organization</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        Home Organization: Domain name of a Home Organization
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:terena.org:schac:schacHomeOrganization" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.25178.1.2.9"
        friendlyName="schacHomeOrganization" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: SCHAC Home Organisation Type

Use static attributes

```
<!-- SCHAC Home Organisation Type (schacHomeOrganizationType) -->
<resolver:AttributeDefinition id="schacHomeOrganizationType" xsi:type="ad:Simple"
    sourceAttributeID="schacHomeOrganizationType">

    <resolver:Dependency ref="staticAttributes" />

    <resolver:DisplayName xml:lang="en">Home organization type</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        Home Organization Type: Type of a Home Organization
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:terena.org:schac:schacHomeOrganizationType" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.25178.1.2.10"
        friendlyName="schacHomeOrganizationType" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Static Attributes

Static attributes

```
<!-- Static Connector -->
<resolver:DataConnector id="staticAttributes" xsi:type="dc:Static">
    <dc:Attribute id="swissEduPersonHomeOrganization">
        <dc:Value>example.org</dc:Value>
    </dc:Attribute>
    <dc:Attribute id="schacHomeOrganization">
        <dc:Value>example.org</dc:Value>
    </dc:Attribute>
    <dc:Attribute id="swissEduPersonHomeOrganizationType">
        <dc:Value>university</dc:Value>
    </dc:Attribute>
    <dc:Attribute id="schacHomeOrganizationType">
        <dc:Value>urn:schac:homeOrganizationType:int:university</dc:Value>
        <dc:Value>urn:schac:homeOrganizationType:ch:university</dc:Value>
    </dc:Attribute>
</resolver:DataConnector>
```

Attributes: Example Configuration: Scoped affiliation

Use value of eduPersonAffiliation with scope

```
<!-- Scoped affiliation (eduPersonScopedAffiliation) -->
<resolver:AttributeDefinition id="eduPersonScopedAffiliation" xsi:type="ad:Scoped"
    scope="example.org" sourceAttributeID="eduPersonAffiliation">

    <resolver:Dependency ref="eduPersonAffiliation" />

    <resolver:DisplayName xml:lang="en">Affiliation</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        Affiliation: Type of affiliation with Home Organization
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1ScopedString"
        name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
        friendlyName="eduPersonScopedAffiliation" />
</resolver:AttributeDefinition>
```

Load the interfederation metadata (1)

- Change the metadata configuration in the file `relying-party.xml`:
  - Look for the existing **`MetadataProvider`** element which loads the SWITCHaai metadata and insert **just after** it the following snippet:

```
<metadata:MetadataProvider id="InterfederationURLMD"
    xsi:type="metadata:FileBackedHTTPMetadataProvider"
    metadataURL="http://metadata.aai.switch.ch/entities/interfederation+sp"
    backingFile="/opt/shibboleth-idp/metadata/metadata.interfederation-sps.xml"
    requireValidMetadata="true" maxRefreshDelay="PT1H">
    <metadata:MetadataFilter xsi:type="metadata:ChainingFilter">
        <metadata:MetadataFilter xsi:type="metadata:RequiredValidUntil"
            maxValidityInterval="P7D"/>
        <metadata:MetadataFilter xsi:type="metadata:SignatureValidation"
            trustEngineRef="shibboleth.InterfederationMetadataTrustEngine"
            requireSignedMetadata="true"/>
    </metadata:MetadataFilter>
</metadata:MetadataProvider>
```

Load the interfederation metadata (2)

- Make sure that the added `MetadataProvider` element inserted above is added within a **`MetadataProvider`** element of type="ChainingMetadataProvider". Otherwise the Identity Provider won't be able to start.
- Look for the **`TrustEngine`** element with **id="shibboleth.MetadataTrustEngine"**, which defines the metadata signature validation. Insert just after another trust engine with in form of the following configuration snippet:

```
<security:TrustEngine id="shibboleth.InterfederationMetadataTrustEngine"
    xsi:type="security:StaticPKIXSignature">
    <security:TrustedName>
        SWITCHaai Interfederation Metadata Signer
    </security:TrustedName>
    <security:ValidationInfo id="SWITCHaaiFederationCredentials"
        xsi:type="security:PKIXFilesystem" verifyDepth="2">
        <security:Certificate>
            /opt/shibboleth-idp/credentials/SWITCHaaiRootCA.crt.pem
        </security:Certificate>
    </security:ValidationInfo>
    <security:ValidationOptions xsi:type="security:CertPathValidationOptionsType"
        forceRevocationEnabled="true"/>
</security:TrustEngine>
```

Restart the Identity Provider

- Check that XML files are still well-formed:

```
# xmlwf attribute-resolver.xml
# xmlwf relying-party.xml
```

- Restart Identity Provider (e. g. Tomcat Java Container)

```
# /etc/init.d/tomcat6 restart
```

- Check for errors:

```
# tail -f /opt/shibboleth-idp/logs/idp-process.log
```

Test the configuration

You may want to test whether all still works by accessing the AAI Viewer:

https://av.aai.switch.ch/aai

Note: You can't yet see the newly configured attributes because they are not yet released.

Changes in Resource Registry

Changes to do:

1. Activate interfederation support for this Identity Provider (i.e. Home Organization)
2. Add the attributes configured above as supported attributes
3. Adapt the default attribute release policy for interfederation

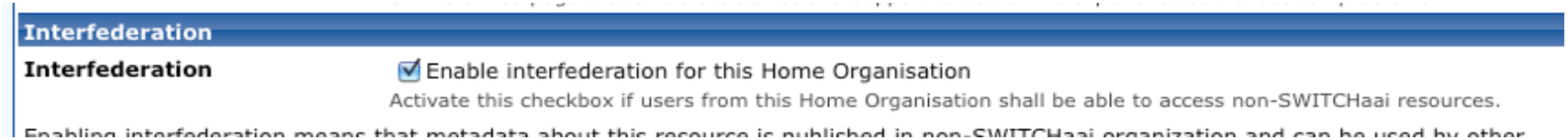
Access to Resource Registry: https://rr.aai.switch.ch

1. Click on the tab "Home Organizations"
2. Click on the link "Edit Home Organization Description" of your Home Organization

Activate Interfederation

- Click on "1. General Information"

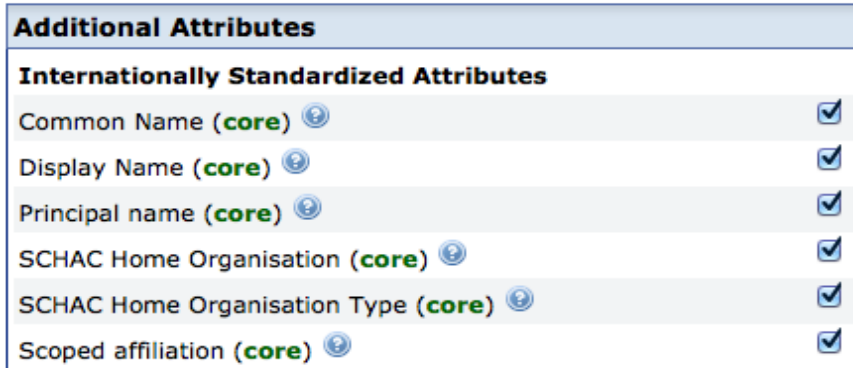
- Enable interfederation for this Home Organisation



Add additional supported attributes

- Click on "6. Supported Attributes"

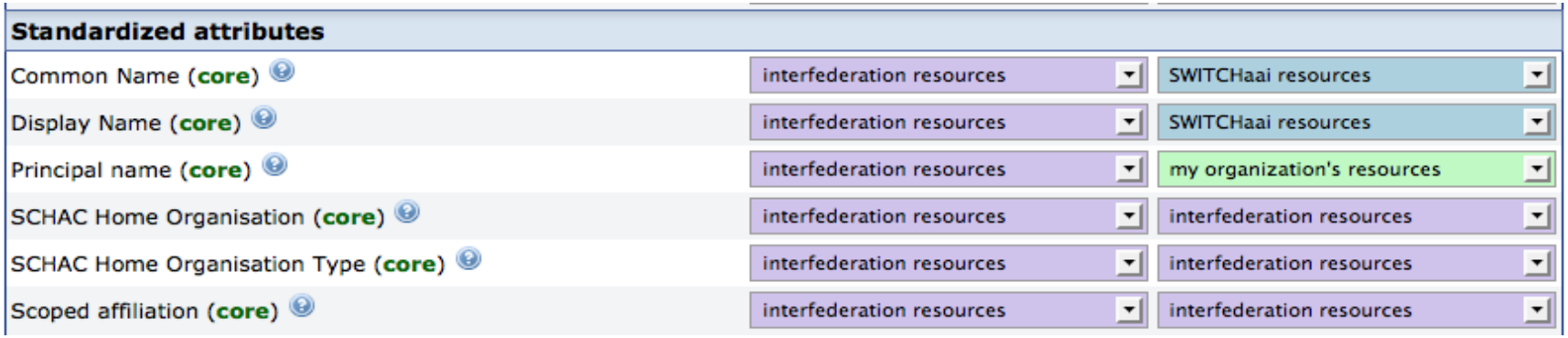
- Enable the new attributes previously added to the IdP's Attribute Resolver configuration



Adapt Attribute Release Policy (1)

- Click on "7. Default Attribute Policy Rules"

- Release the new attributes as required

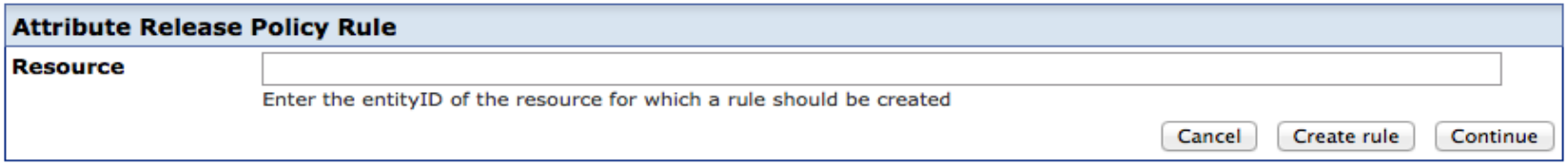


Note: All changes applied to the default Attribute Release Policy only will become active when the Identity Provider downloads the attribute-filter.xml the next time from the Resource Registry.

Adapt Attribute Release Policy (2)

- Set specific attribute release policy
  (allows to override the default attribute policy in order to release fewer or more attributes to very specific resources)

  Click on "8. Specific Attribute Policy Rules"



Note: All changes applied to the specific Attribute Release Policy only will become active when the Identity Provider downloads the attribute-filter.xml the next time from the Resource Registry.

Pass Interfederation Test

- Perform the Interfederation Attribute Test

  https://av.aai.switch.ch/interfederation-test/

- You should see all attributes required for interfederation:

Attributes	Values
principalName	532669@switch.ch
mail	daniel.lutz@switch.ch
cn	Daniel Lutz
displayName	Daniel Lutz
affiliation	member staff
scoped-affiliation	staff@switch.ch member@switch.ch
schacHomeOrganization	switch.ch
schacHomeOrganizationType	urn:schac:homeOrganizationType:ch:others urn:schac:homeOrganizationType:int:nren
persistent-id	https://aai-logon.switch.ch/idp/shibboleth! https://aai-viewer.switch.ch/interfederation-test/shibboleth! ghcXgnR3DLw+tYai5pGyaApMsV8=

Success: 

Failure: 

Links

- Further reading
  - Step-by-step guide to enable interfederation support for a Shibboleth Identity Provider in SWITCHaai:

    https://www.switch.ch/aai/docs/interfederation/idp-deployment.html

  - Add the remaining six international attributes:

    https://aai-viewer.switch.ch/aai/redirect-to-attribute-guide.php

Configuring the SP for interfederation use

A short How-to

SWITCH

Kaspar Brand
aai@switch.ch

Interfederation Crash Course
Berne, 1 March 2013

High-level overview of the procedure

- Assumptions
  - your AAI-enabled resource is running the currently supported release of the Shibboleth Service Provider (as of 2013, this is version 2.5.x)
  - your resource is already registered in the SWITCHaai federation and is properly working for users of that federation
- Required steps
  1. Making the SP aware of additional attributes:
     `attribute-map.xml`
  2. Enabling the retrieval of interfederation metadata:
     `shibboleth2.xml`
  3. Adapting access control rules:
     `httpd.conf`, **`.htaccess`**, **`<RequestMap>/<Host>`** et al.
  4. Adapting the IdP discovery process: → next presentation
  5. Reconfiguring the description in the AAI Resource Registry

Making the SP aware of additional attributes

Either download the current recommended **`attribute-map.xml`** from the SP configuration guide and store it in the configuration directory:
https://www.switch.ch/aai/docs/shibboleth/SWITCH/latest/sp/deployment/download/attribute-map.xml

or manually add the following attributes to the **`attribute-map.xml`** file in the configuration directory, if not yet present:

```
<!-- Display Name -->
<Attribute name="urn:mace:dir:attribute-def:displayName" id="displayName"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.241" id="displayName"/>

<!-- Common Name -->
<Attribute name="urn:mace:dir:attribute-def:cn" id="cn"/>
<Attribute name="urn:oid:2.5.4.3" id="cn"/>

<!-- SCHAC Home Organisation -->
<Attribute name="urn:mace:terena.org:schac:homeOrganization” id="schacHomeOrganization"/>
<Attribute name="urn:oid:1.3.6.1.4.1.25178.1.2.9” id="schacHomeOrganization"/>

<!-- SCHAC Home Organisation Type -->
<Attribute name="urn:mace:terena.org:schac:homeOrganizationType” id="schacHomeOrganizationType"/>
<Attribute name="urn:oid:1.3.6.1.4.1.25178.1.2.10” id="schacHomeOrganizationType"/>
```

Enabling the retrieval of interfederation metadata

Either download a customized shibboleth2.xml file from the SP configuration guide (with the “Configure Service Provider for Interfederation” checkbox ticked):
https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.5/sp/deployment/configuration.html

or manually add the following MetadataProvider element to the shibboleth2.xml file in the configuration directory:

```
<!-- Interfederation Metadata -->
<MetadataProvider type="XML" validate="true"
                  uri="http://metadata.aai.switch.ch/entities/interfederation+idp"
                  backingFilePath="metadata.interfederation-idps.xml"
                  reloadInterval="3600">
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="604800"/>
  <MetadataFilter type="Signature">
    <TrustEngine type="StaticPKIX"
                 certificate="SWITCHaaiRootCA.crt.pem" verifyDepth="2"
                 checkRevocation="fullChain"
                 policyMappingInhibit="true" anyPolicyInhibit="true">
      <TrustedName>SWITCHaai Interfederation Metadata Signer</TrustedName>
      <PolicyOID>2.16.756.1.2.6.8</PolicyOID>
    </TrustEngine>
  </MetadataFilter>
</MetadataProvider>
```

Adapting access control rules

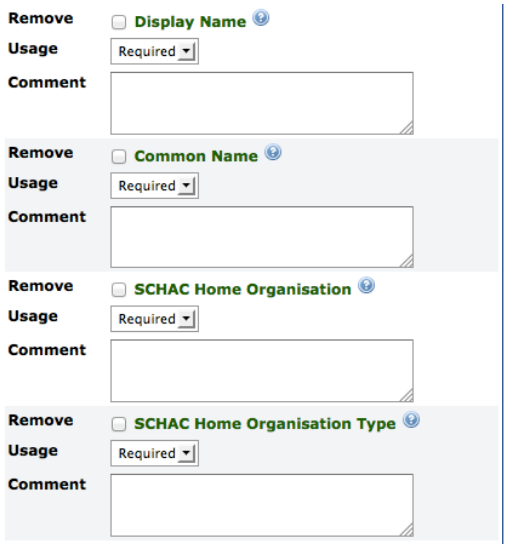
- Access control (authorization) can be configured in multiple ways:
  - for Apache httpd only: either in the global or a **`VirtualHost`** specific configuration file, or in per-directory **`.htaccess`** or XML access rule files
  - in the **`shibboleth2.xml`** file
  - in a separate XML file referenced by **`shibboleth2.xml`**
- If you are interfederation-enabling your SP, verify that you're not inadvertently opening up access to an audience larger than the intended one, i.e.
  - configure attribute requirements for *affiliation* or *homeOrganizationType* etc. accordingly
  - make sure that your existing rules are still specific enough, e.g. when using regular expressions for attribute values

Adapting the IdP discovery process

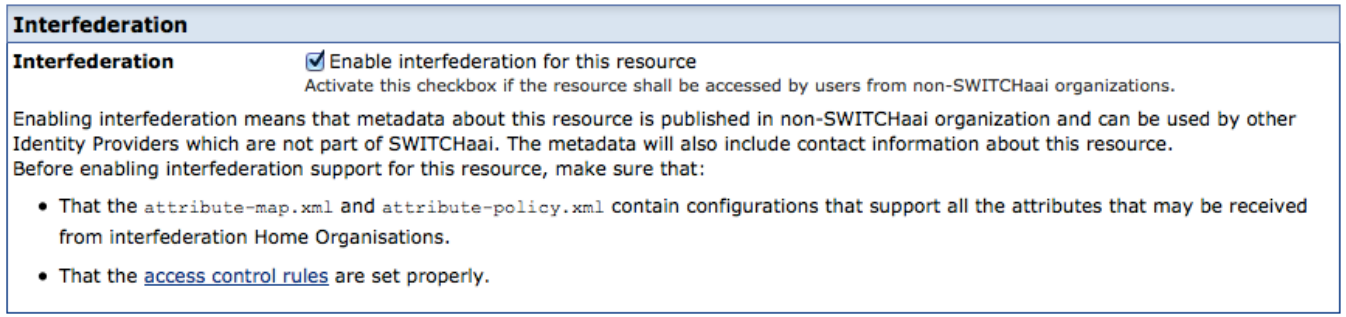
→ next presentation “Discovery Service Options”

Reconfiguring the SP description in the Resource Registry

- under “Required Attributes”, mark the relevant attributes as “Required”:



- under “Intended Audience”, enable the publication of the resource description in interfederation metadata:



Summary

- Required steps
  - making the SP aware of additional attributes
  - enabling the retrieval of interfederation metadata
  - adapting access control rules
  - adapting the IdP discovery process: → next presentation
  - reconfiguring the description in the AAI Resource Registry

- Further reading: step-by-step guide at https://www.switch.ch/aai/docs/interfederation/sp-deployment.html

Discovery Service Options

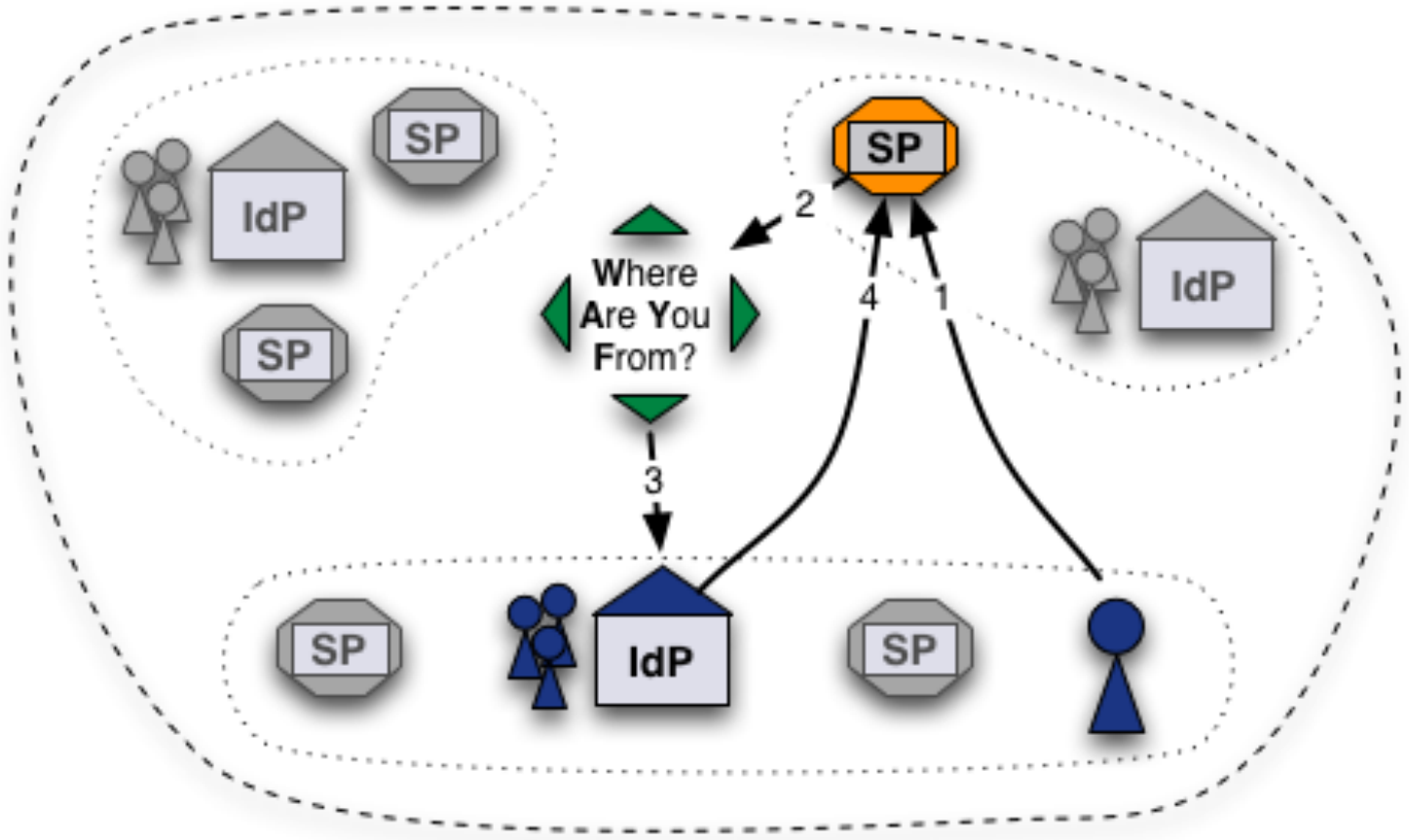
SWITCH

Bea Huber
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

No Central WAYF for Interfederation

- The classic way: One WAYF per Federation



Alternatives

- Direct Login URLs
- SWITCH Embedded WAYF

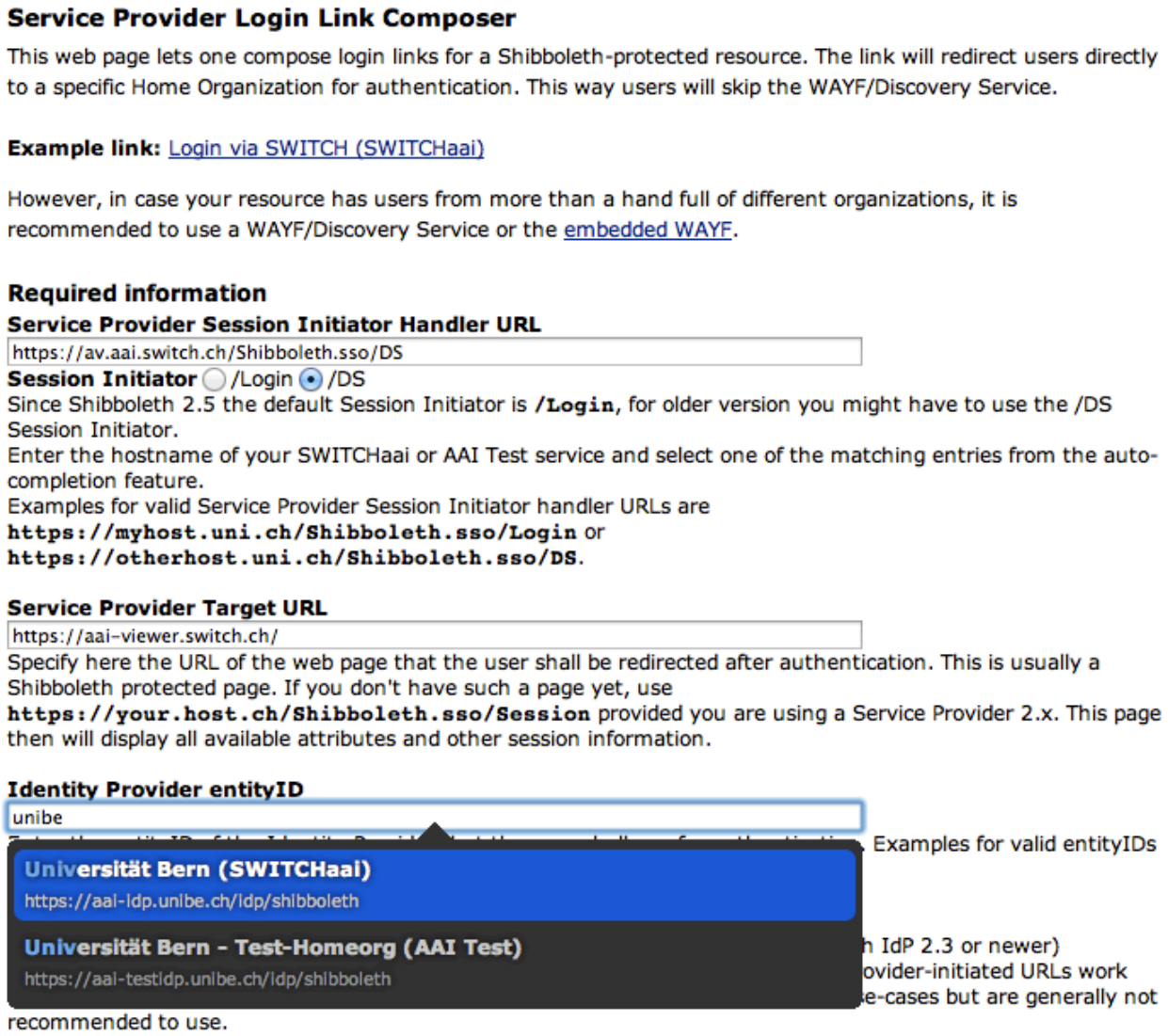
- Shibboleth Embedded Discovery Service

Solution 1: Direct Login URLs

- A separate login link for specific IdPs
- 1 click direct redirect to IdP without going via WAYF
- Useful when only users of few IdPs use resource

Login links:
Login via SWITCH (SWITCHaai)
Login via Stockholm University (Interfederation)
Login via University of Gothenburg (Interfederation)

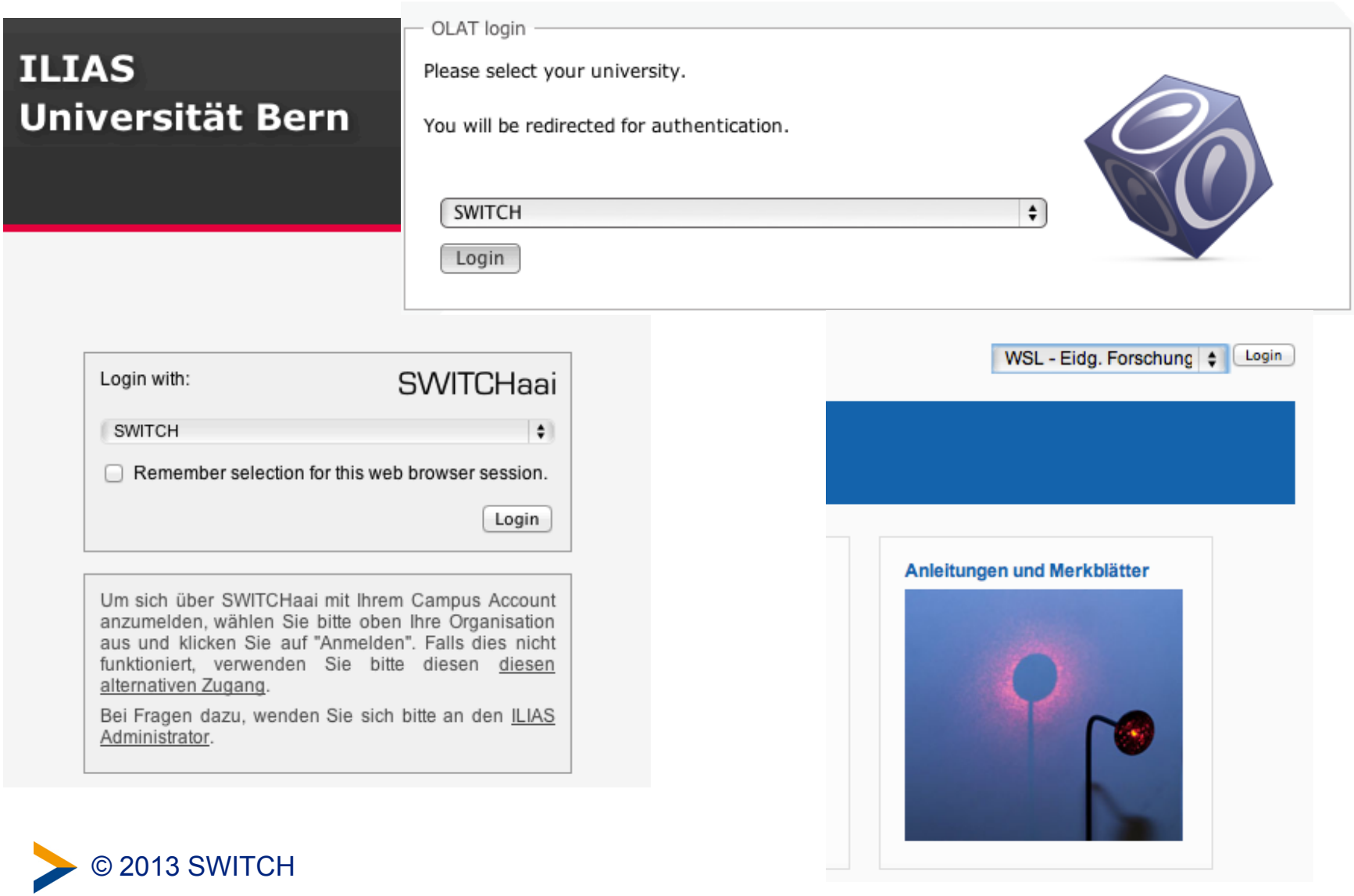
Composing Login URLs



http://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html

Solution 2: Embedded WAYF

SWITCH WAYF



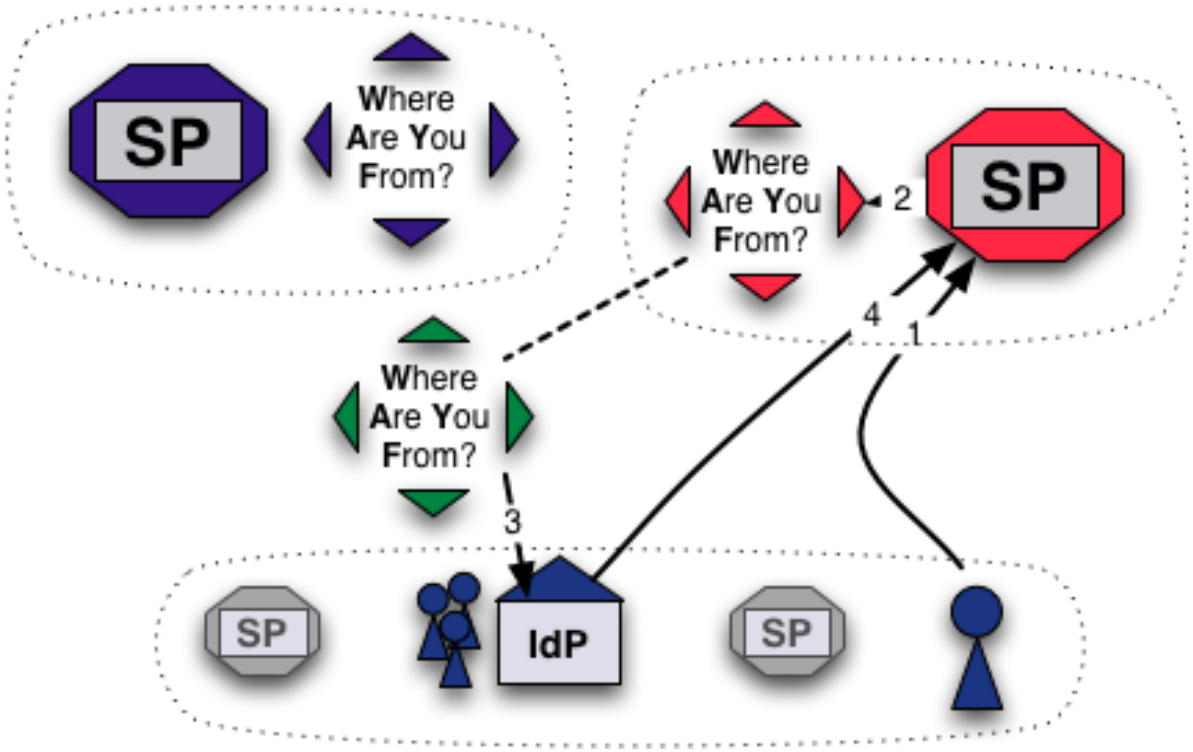
Embedded WAYF

SWITCH
WAYF

Embedded WAYF

SWITCH WAYF

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



Information and Configuration

SWITCH WAYF

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

Configuration

SWITCH WAYF

Configuration Example of embedded wayf

```
// Example of how to add Identity Provider from other federations

var wayf_additional_idps = [

        {name:"University of Trieste IdP",
        entityID:"https://idemfero.units.it/idp/shibboleth"},

        {name:"Stockholm University",
        entityID:"https://idp.it.su.se/idp/shibboleth"}
 ];
```

Configuration

SWITCH WAYF

Configuration Example of embedded wayf

```
// EntityIDs of Identity Provider that should not be shown at all
// [Optional, commented out by default]

var wayf_hide_idps = new Array ("https://idemfero.units.it/idp/shibboleth",
"https://idp.it.su.se/idp/shibboleth");


// Categories of Identity Provider that should not be shown
// Possible values
  are:"university","uas","hospital","library","vho","others","all"

var wayf_hide_categories =  new Array("library","vho","others","hospital");
```

Enable JSON Discovery feed

In shibboleth2.xml:

```
  <Sessions lifetime="28800"
                  timeout="3600"
                  relayState="ss:mem"
                  checkAddress="false"
                  consistentAddress="true"
                  handlerSSL="true"
                  cookieProps="https">
...
 <!-- JSON feed of discovery information. -->
      <Handler type="DiscoveryFeed” Location="/DiscoFeed"/>
  </Sessions>
```

JSON Discovery feed example


```
[ { "entityID": "https://idp.ids-mannheim.de/idp/shibboleth",
 "DisplayNames": [
 { "value": "Institut für Deutsche Sprache (IDS)”, "lang": "de” },
  { "value": "Institut für Deutsche Sprache (IDS)”, "lang": "en” }
 ]
},
{ "entityID": "https://idp.it.gu.se/idp/shibboleth",
"DisplayNames": [
 { "value": ”Göteborgs universitet", "lang": "sv" },
 { "value": "University of Gothenburg", "lang": "en" }
 ],
"Logos": [
{ "value": "https://www.gu.se/digitalAssets/1374/1374690_lo_gu_left.png", "height": "50", "width": "344",
"lang": "sv" },
{ "value": "https://www.gu.se/digitalAssets/1374/1374690_lo_gu_left.png", "height": "50", "width": "376",
"lang": "en" }
 ] }
]
```

Configuration

SWITCH WAYF

Configuration Example of embedded wayf

```
// Whether to load Identity Providers from the Discovery Feed provided by
// the Service Provider.
// IdPs that are not listed in the Discovery Feed and that the SP therefore is
// not  are able to accept assertions from, are hidden by the Embedded WAYF
// IdPs that are in the Discovery Feed but are unknown to the SWITCHwayf
// are added to the wayf_additional_idps.
// The list wayf_additional_idps will be sorted alphabetically
// The SP must have configured the discovery feed handler that generates a
// JSON object. Otherwise it won't generate the JSON data containing the IdPs.
// [Optional, commented out by default]

var wayf_use_disco_feed = true;
```

Solution 3:
Embedded Discovery Service

Shibboleth
EDS

- Also 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

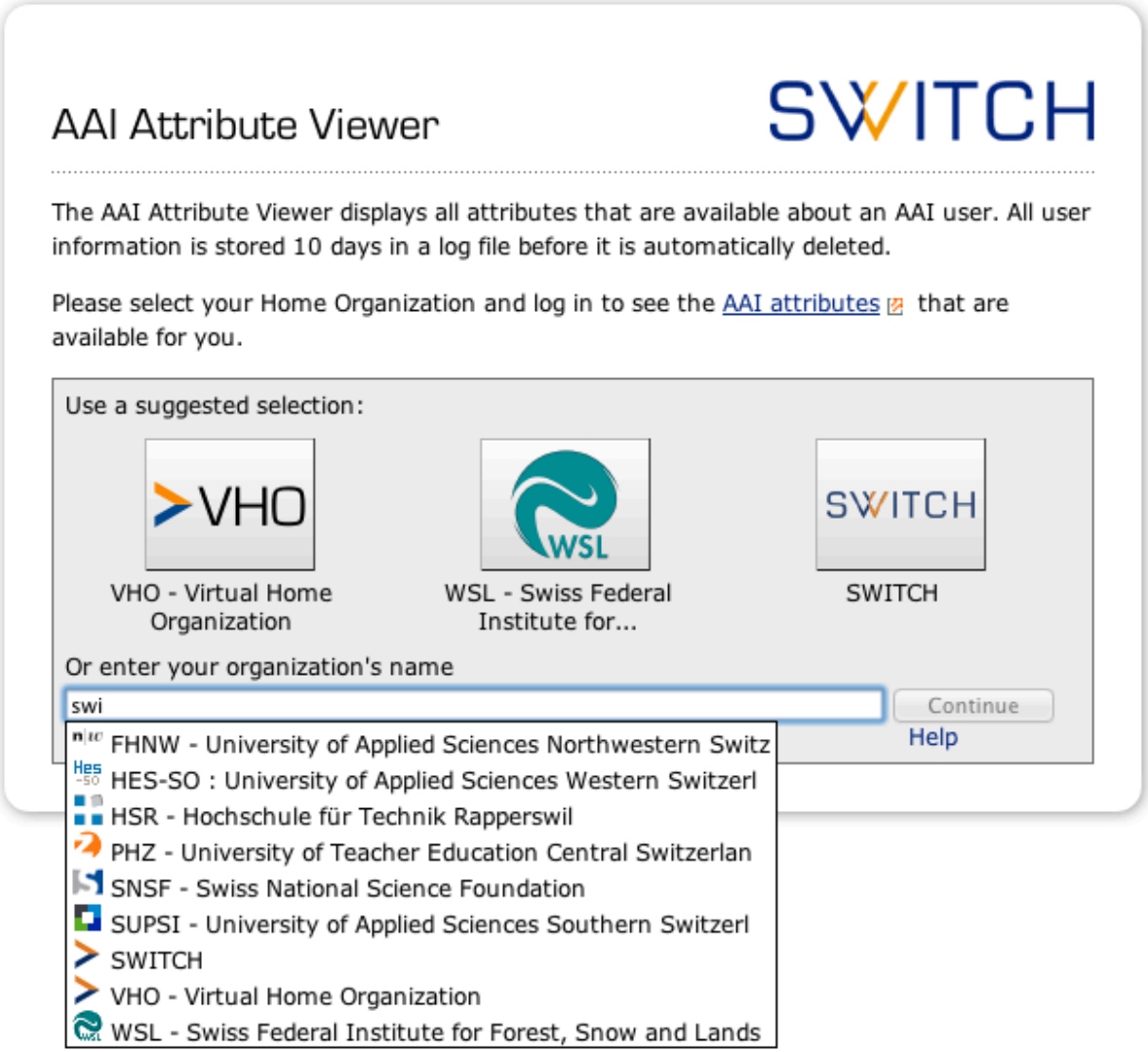

http://shibboleth.net/downloads/embedded-discovery-service/latest/

- Documentation can be found at:


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

Embedded Discovery Service

Shibboleth EDS



MetadataFilter Example

In shibboleth2.xml:

```
<MetadataProvider type="XML" .....>

    <MetadataFilter type="Whitelist">
        <Include>https://idp.nordu.net/idp/shibboleth</Include>
        <Include>https://idp.ids-mannheim.de/idp/shibboleth</Include>
        <Include>https://idp.it.su.se/idp/shibboleth</Include>
    </MetadataFilter>

</MetadataProvider>
```

Embedded WAYF vs Embedded DS

Properties	Login Link	Embedded WAYF SWITCH	EDS Shibboleth
Independent from central server	✓		✓
Display only “valid” IdPs for SP		(✓)	✓
Search as you type feature			✓
Show Home Org Logo	(✓)		✓
Very easy deployment	✓	✓	✓
Can be used with old SPs	✓	(✓)	
Categories supported	(✓)	✓	
Caches last IdP selection across different services		✓	

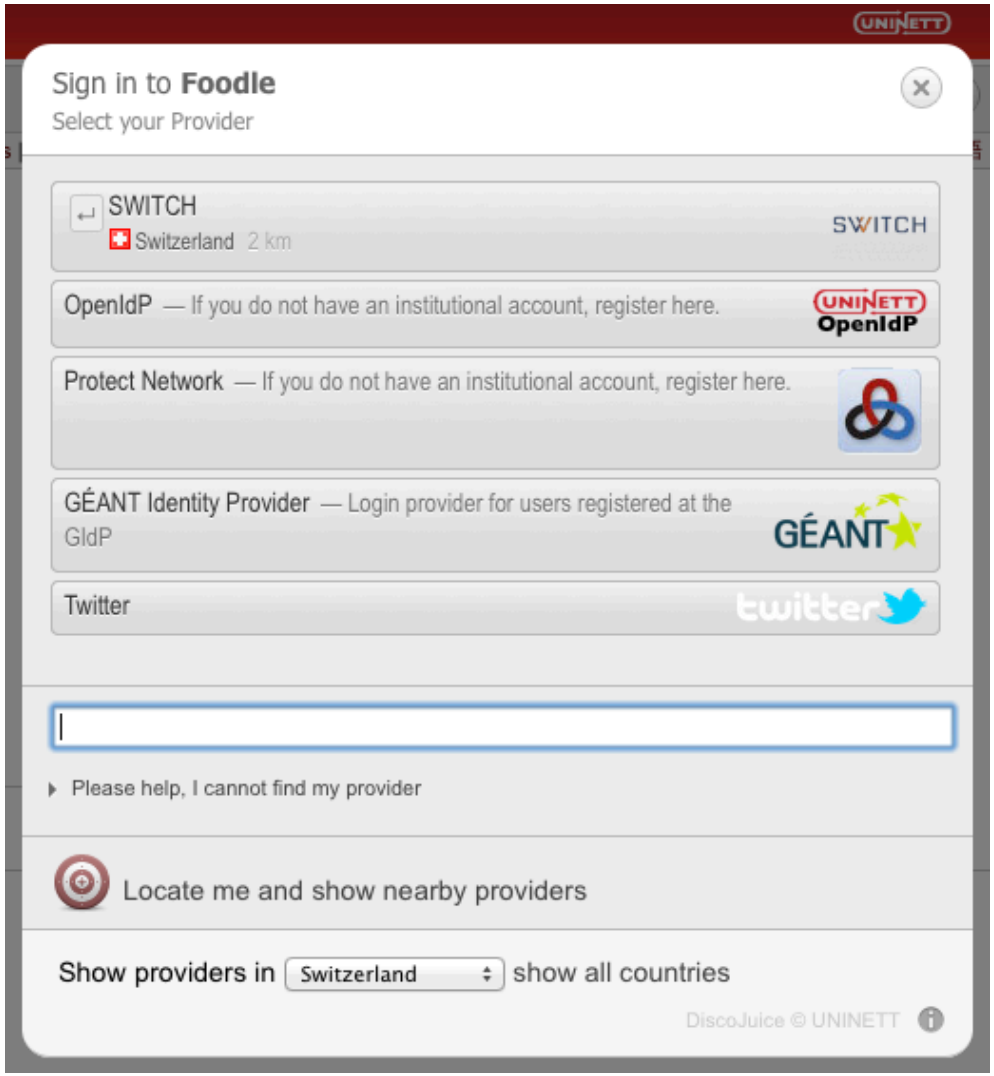
When to use what ?

Numbers of IdPs	Login Link(s)	Embedded WAYF SWITCH	EDS Shibboleth
1 - 5	✓	✓	✓
1 - 50		✓	✓
1 - 500			✓

To mention: 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/



GÉANT Code of Conduct

To address data protection issues in Europe

SWITCH

Thomas Lenggenhager
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

GÉANT Data Protection Code of Conduct

- Full title of the GÉANT CoC:
  - GÉANT Data Protection Code of Conduct for Service Providers in EU/EEA
  - It is still in draft status
    - https://refeds.terena.org/index.php/Code_of_Conduct_for_Service_Providers

- The GÉANT CoC is expected to satisfy the data protection issues for parties within:
  - European Union
  - European Economic Area
  - countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC
    - e.g. Switzerland

- During GN3+, the concept of CoC should get enhanced to also cover SPs in any other countries

GÉANT Data Protection Code of Conduct (2)

- With the CoC, SPs confirm that they adhere to the rules listed in it
  - It is mostly what is anyhow required by national law or best practices, just explicitly listed in a single document
  - Specific requirement to provide a link to the SP's **Privacy Policy** that includes:
    a) the name, address and jurisdiction of the Service Provider;
    b) the purpose or purposes of the processing of the Attributes;
    c) a description of the Attributes being processed;
    d) the third party recipients or categories of third party recipient to whom the Attributes might be disclosed, and proposed transfers of Attributes to countries outside of the European Economic Area;
    e) the existence of the rights to access, rectify and delete the Attributes held about the End User;
    f) the retention period of the Attributes;
    g) a reference to the GÉANT Code of Conduct;

→The Resource Registry already allows you to add a Privacy Policy URL for an SP

GÉANT Data Protection Code of Conduct (3)

- SP's confirmation to be included in the SP's metadata as an Entity Category attribute, e.g.:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://service.example.com/entity">
  <Extensions>
    <EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category">
        <AttributeValue>
          http://www.edugain.org/dataprotection/coc-eu-01-draft
        </AttributeValue>
      </Attribute>
    </EntityAttributes>
  </Extensions>
   ...
</EntityDescriptor>
```

GÉANT Data Protection Code of Conduct (4)

- It is expected that
  - the CoC makes IdPs more comfortable to decide to release attributes to SPs from other federations
  - IdPs will choose to release certain attributes only to SPs that have a CoC Entity Category attribute in metadata

- The CoC is one of the means for federations without a scalable attribute release to support scaling for interfederation
  - SWITCHaai supports default attribute release policy and tailored `attribute-filter.xml` files.

- SWITCH will keep you up-to-date about developments in the area of CoC.

What else?

How to proceed when you want to interfederate a service

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 1. March 2013

What can you do next?

Starting Points

- Basic Interfederation Information: http://www.switch.ch/aai/interfederation

- SP and IdP Guides
  - https://www.switch.ch/aai/docs/interfederation/idp-deployment.html
  - https://www.switch.ch/aai/docs/interfederation/sp-deployment.html

Interfederatin Assistance

- Interfederation is no rocket science.
  - It's just AAI extended across national borders
  - Data privacy has to be taken care of properly

- SWITCHaai team assists you to enable your service or your Identity Provider for interfederation

Recommendations

- For interfederation to be widely useable, it is important to reach a critical mass
  - Overcome the chicken and egg problem
  - This may take a few years, like for SWITCHaai

- Home Organisations could help by enabling Interfederation already now before own use cases emerge