

Interfederation

Introduction, update & current status



SWITCH

Thomas Lenggenhager
thomas.lenggenhager@switch.ch

Berne, 13 August 2014

Agenda

- Why Interfederation?
- Status
- Scalable Attribute Release
- GÉANT Data Protection Code of Conduct & Privacy Policy
- Entity Category Attributes
- How to Interfederate in SWITCHaai?
- Tools to explore Interfederated Entities

Why Interfederation?

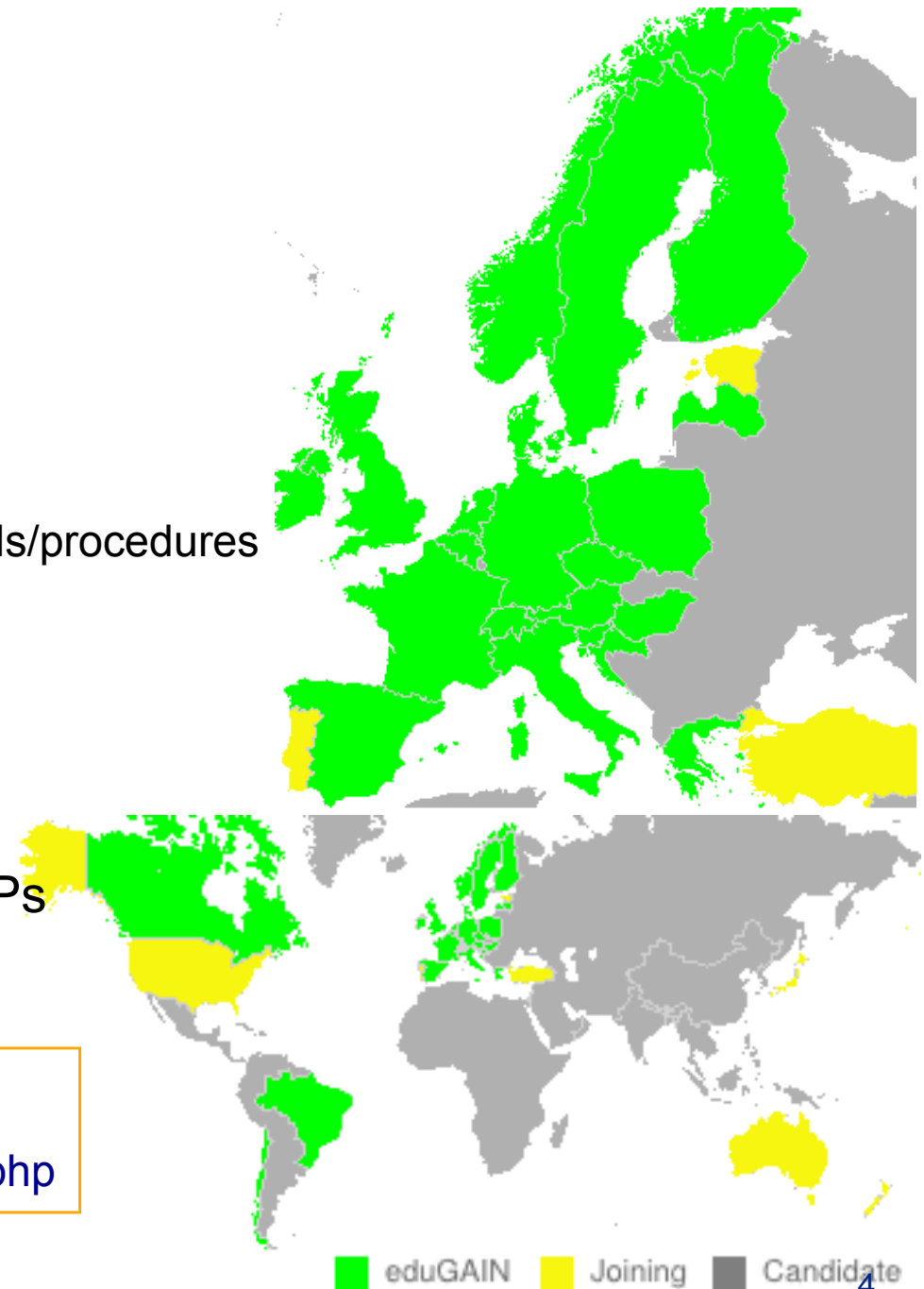
- Federations are mostly of national scope
 - Services may need to register in many federations to serve all their users. That's time consuming and becomes a huge overhead. e.g. EBSCO Publishing is registered in 21 federations!
 - Research projects are mostly multi-national
 - **Interconnecting national federations → Interfederation**
- Register the IdP or SP in only one federation and enable it for interfederation
- Enable the IdP for interfederation
 - Its users will be able access services from other federations
 - Enable the SP for interfederation
 - The service can serve users from other federations

eduGAIN Status

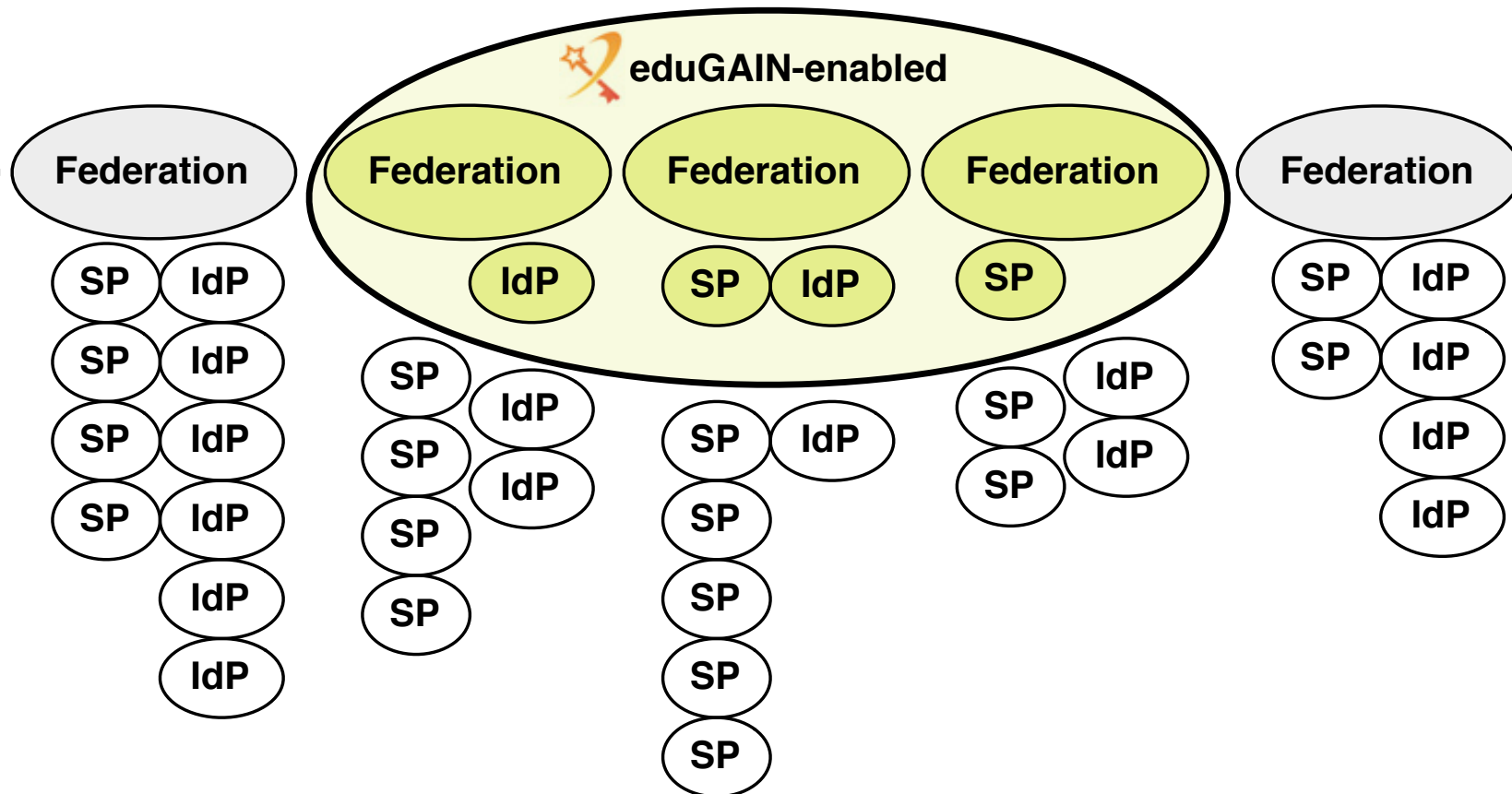
- eduGAIN is the GÉANT Interfederation Service
- eduGAIN design principles
 - Low barrier to entry
 - No mandate to change local standards/procedures
 - Minimal central infrastructure
- Status July 2014
 - Total: 513 IdPs, 138 SPs
 - From SWITCHaai: 12 IdPs, 8 SPs

<http://www.edugain.org>

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

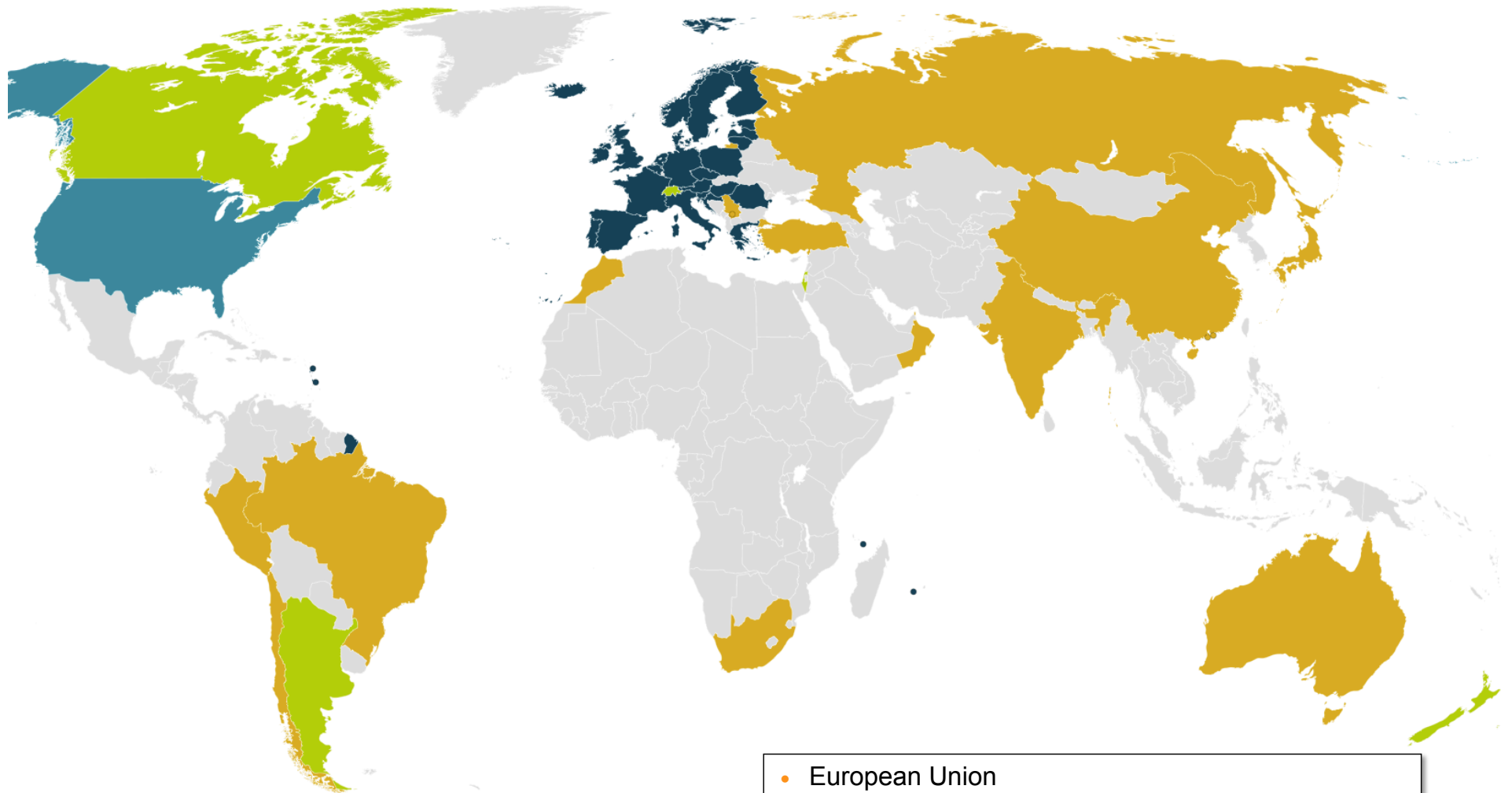


eduGAIN Adoption Width vs. Depth



- Good federation adoption (Width)
- Entity Adoptions (Depth) is growing (110% increase in 2013, 129% for SPs)
- Not every SP and IdP has requirements to interfederate

Federations & GÉANT Data protection Code of Conduct



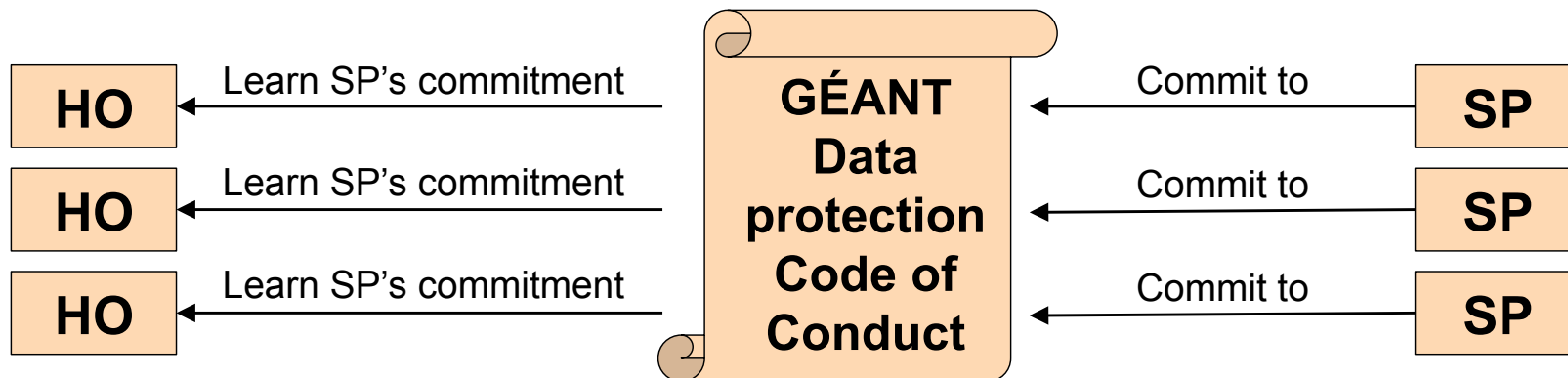
- 25 EEA Data Protection
- 5 EEA Compatible DP
- 1 Safe Harbor (USA)
- 13 Federations outside GÉANT CoCo (4 in or joining)

- European Union
- European Economic Area
- countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC
 - e.g. Switzerland
 - e.g. the US safe harbour

GÉANT Code of Conduct – Data Protection within eduGAIN

Increase the trust in Service Providers (SPs)

- The method is based on the EU Data Protection directives
- The SP has to provide a Privacy Policy (in English, according to the guideline)
- That will encourage the Home Organisation IdP to release attributes
→ attribute release will scale



Code of Conduct Toolkit

- **Data Protection Code of Conduct for SPs in EU/EEA**
- Entity category attribute definition for the Code of Conduct
- SAML2 profile for the Data Protection Code of Conduct

Data Protection Code of Conduct (DP CoCo)

Normative documents

- **Data Protection Code of Conduct for SPs in EU/EEA**
- Entity category attribute definition for the DP CoCo
- SAML2 profile for the DP CoCo

<http://www.geant.net/uri/dataprotection-code-of-conduct/v1/>

Non-normative, informational documents

- Introduction
- Introduction to the DP directive
- Risk management
- **Privacy policy guidelines**
- What attributes can an SP request
- Good practice for Home Organisations
- Federation operator guidelines
- Handling non-compliance
- IdP GUI guidelines

https://refeds.terena.org/index.php/Data_protection_coc

Data Protection Code of Conduct Cookbook

https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook

Entity Category Attributes

- A means to express 'conformance' to a definition in SAML, in a machine readable way
 - An Entity Category requires a proper definition and a process
 - According to the process, the Federation Operator includes the 'SAML-snippet' into the entity description in metadata
- Motivation to introduce Entity Categories for interfederation?
 - Better scalable attribute release for interfederation due to (hopefully) wide deployment of these definitions
- The first two internationally accepted entity category definitions
 - GÉANT Data Protection Code of Conduct (CoCo)
<http://www.geant.net/uri/dataprotection-code-of-conduct/v1/>
 - REFEDS Research & Scholarship
<https://refeds.org/category/research-and-scholarship/>

A CoCo Entity Attribute Example

```
<EntityDescriptor entityID="https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth">
  <Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://rr.aai.switch.ch/"
      registrationInstant="2014-08-06T14:17:48Z">
      <mdrpi:RegistrationPolicy xml:lang="en">
        https://www.switch.ch/aai/federation/switchaai/
        metadata-registration-practice-statement-20110711.txt
      </mdrpi:RegistrationPolicy>
    </mdrpi:RegistrationInfo>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        Name="http://macedir.org/entity-category"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>
          http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

REFEDS Research & Scholarship (R&S) (1)

- Suitable for
 - *"Service Providers that support research and scholarship interaction, collaboration or management as an essential component"*
 - *"The service enhances the research and scholarship activities of some subset of the registrar's user community"*
- However
 - ***"Not to be used for licensed content such as e-journals"***
- R&S Category Attributes Bundles
 - **personal identifiers:** email address, person name, eduPersonPrincipalName
 - **pseudonymous identifier:** eduPersonTargetedID
 - **affiliation:** eduPersonScopedAffiliation
- Minimal Subset of the R&S Attribute Bundle
 - eduPersonPrincipalName
 - mail
 - displayName OR (givenName AND sn)

mostly less than what
is in a mail-footer
but enough for
most R&S services

REFEDS Research & Scholarship (R&S) (2)

- How will it work?
 - SP administrator applies for inclusion into this category
 - Federation operator (e.g. SWITCH, DFN, RENATER, GARR) checks application, approves it and adds snippet to metadata
 - SP requests a subset of R&S Category Attributes
 - IdP knows from metadata that SP is in the R&S Category
 - IdP that supports R&S Category is ready to release attributes
 - User consents the release
- An SP that is in the R&S Entity Category should increase confidence of IdP administrators
 - more likely to receive more attributes than without

<https://refeds.org/category/research-and-scholarship/>

The Steps to Interfederate in SWITCHaai

- 1) Once per SWITCHaai Participant from the SWITCH Community a signature is required (see next slide)
- 2) SWITCH will set the 'flag' in the Resource Registry
- 3) Now, SP and IdP administrators can opt-in for interfederation;
 - they first adapt their SP and IdP configurations according to the [Enabling Interfederation Support](#) guides
 - the IdP administrator installs and configures uApprove to enable user consent
 - Finally the administrator can click the checkbox in the Resource Registry!

Interfederation	
Interfederation	<input checked="" type="checkbox"/> Enable interfederation for this resource Activate this checkbox if the resource shall be accessed by users from non-SWITCHaai organizations.

Interfederation	
Interfederation	<input checked="" type="checkbox"/> Enable interfederation for this Home Organisation Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources.

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

SWITCHaai Interfederation Access Declaration

Signing the Interfederation Access Declaration asserts:

- 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 deploys a user consent module (uApprove)
- 4) the SPs will adhere to the "Data Protection Code of Conduct" (CoCo) and implement a privacy policy along the CoCo-criterias

<https://www.switch.ch/aai/interfederation>
https://wiki.edugain.org/How_to_write_the_privacy_policy

Tools to explore interfederated entities

- Is a university IdP or an SP already interfederated?
 - go to: <http://www.edugain.org/technical/status.php>
 - pick the country where the entity might be registered
 - under 'Metadata URL' click on 'validate this metadata set', then on 'show entities list'
- or try the **Is Federated Checker** (beta)
 - go to: <https://wiki.edugain.org/isFederatedCheck/>
 - provide email addresses or domain names
- Which interfederated SPs are committed to the GEANT Data Protection Code of Conduct (CoCo)?
 - go to: <http://monitor.edugain.org/coco>
- **Federation Service Catalog** (proof of concept, best effort)
 - go to: <http://www.terena.org/~schofield/servicecatalogue/>
- Upcoming **REFEDS Metadata Explorer Tool** (MET) (beta)
 - go to: <http://met.refeds.org/met/>

How to bake CoCo and R&S

GÉANT Code of Conduct (CoCo) and R&S for SP and IdP



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 13. August 2014

Recipe Book



Table of Contents

1. CoCo for Home Organisations/IdP **CoCo/IDP**
2. CoCo for Resources/SP **CoCo/SP**
3. R&S for Home Organisations/IdP **R&S/IdP**
4. R&S for Resources/SP **R&S/SP**

More detailed Recipe on:

https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook

<https://refeds.org/category/research-and-scholarship/>

Main Ingredients for CoCo Recipes

- **1 unit of will power:**
To deal with „boring“ but important data protection issues
- **15 minutes of precious Time:**
To read and understand the Code of Conduct:
<http://www.geant.net/uri/dataprotection-code-of-conduct/v1>
Don't worry, it's only 4 pages (103 lines) long
- **A few minutes more**
To implement the necessary steps (time depends on SP/
IdP and already available ingredients)

CoCo for Home Organisations/IdP

- Full CoCo Recipe for Identity Providers:
https://wiki.edugain.org/Recipe_for_a_Home_Organisation
 - Not all of the 5 steps apply for SWITCHaai organisations
- Additional Ingredient for this Recipe: uApprove
 - Attribute Release Consent module
<https://www.switch.ch/aai/support/tools/uApprove.html>
 - uApprove plugin is strongly recommended to deploy for Home Organisations that enabled Interfederation-support.
 - Can be disabled when users access Swiss Resources

Attribute Consent with uApprove

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.

Data Requested by Service	
Display Name	Lukas Haemmerle
E-mail	lukas.haemmerle@switch.ch
Preferred Language	en

[Data privacy information of service.](#)

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?

Adapt Attribute Release Policies

- Identity Providers that want to support the CoCo, „only“ need to adapt Attribute Release Policies (e.g. attribute-filter.xml)
- For SWITCHaai Identity Providers using Shibboleth, this can be conveniently done via the Resource Registry
 - Shibboleth IdPs by default are configured to download attribute-filter.xml file from Resource Registry.
 - For ADFS-based Identity Providers this is not possible

CoCo Default Settings

- For SWITCHaai Home Organisations the default setting is to release required attributes to services that committed to the CoCo
 - EU data protection laws are adequate to Swiss laws
 - uApprove asks user for consent before data is released to non-SWITCHaai services
 - Use the CoCo within Switzerland only is also possible but should generally not be necessary
- Home Organisations will be able to change their settings (opt-out) in section „7. Attribute Release Settings“

2. Entity Category Policies

Entity Category Policies apply whenever a Resource claims to meet the category's requirements. The claim is part of the Service Provider's metadata. Entity Category Policies have higher priority than the default release policies for individual attributes. However, they have lower priority than the Resource Specific Attribute Release Policy rules.

Together with a user attribute release consent module (i.e. [uApprove](#)), attribute release based on the entity categories below should provide enough confidence from a data protection point of view to release the requested attributes also to Interfederation-enabled resources abroad.

available end of August 2014

GÉANT Data Protection Code of Conduct (CoCo)

Resources in the [GÉANT Data Protection Code of Conduct \(CoCo\)](#) entity category declare to respect the CoCo's behavioral rules and that they are located in either EU/EEA or a country with adequate data protection (e.g. Switzerland).

The CoCo was created by [GÉANT](#), the international research infrastructure project that also created and operates [eduGAIN](#) and [eduroam](#). SWITCH contributes to GÉANT.

Release required attributes (default)

Provided a Resource is in the GÉANT Data Protection Code of Conduct entity category and attribute release for this entity category is enabled, an attribute is only released if its release scope is neither **nobody** nor **my organisation's resources**. Is the attribute release for this entity category disabled, only the default and specific release rules apply.

REFEDS Research & Scholarship (R&S)

Resources in the [REFEDS Research & Scholarship \(R&S\)](#) category "enhance the research and scholarship activities" and are of benefit to R&S user communities.

[REFEDS](#) specified this entity category. It is the interest group of research and education identity federations world-wide. SWITCH contributes to REFEDS.

Release minimal set of R&S attributes (default)

The minimal R&S attribute set includes the attributes:

- **Principal name**
- **E-mail**
- Name (**Given name** and **surname** or alternatively **Display name**)

The complete set with all R&S attributes additionally includes:

- **Targeted ID/Persistent ID**
- **Scoped Affiliation**

Is the attribute release for this entity category disabled, only the default and specific release rules apply.

Default settings for Home Organisations. Will be available in RR end August 2014.

CoCo for Resources/SP

- Full Coco Recipe for Service Providers:
https://wiki.edugain.org/Recipe_for_a_Service_Provider
– No extra work needed for steps 2, 4 and 5 for SWITCHaai Resources
- **Quick Start**
To (technically) commit to CoCo:
 1. Create/extend Privacy Statement web page
 2. Add URL to privacy statement web page in Resource Registry
 3. Enable CoCo support in Resource Registry

1. Create Privacy Statement

- Template available on:
https://refeds.terena.org/index.php/Privacy_policy_guidelines_for_Service_Providers
Format of the template is not strict but a recommendation
- Important is a reference to the CoCo, e.g.:
„Personal data will be protected according to the Code of Conduct for Service Providers, a common standard for the research and higher education sector to protect the user's privacy.“
The link must point to:
<http://www.geant.net/uri/dataprotection-code-of-conduct/v1>

Example Privacy Policy for AAI Interfederation Attribute Test.

Interfederation Attribute Test Privacy Statement

Name of the service	Interfederation Attribute Test
Description of the service	Allows to check if an organisation/Identity Provider releases the attributes recommended by eduGAIN .
Data controller and a contact person	SWITCH , the Swiss education & research network.
Jurisdiction	CH Switzerland Zurich.
Personal data processed	<p>1. For all users</p> <ul style="list-style-type: none"> • IP address • Referrer address (the web page a user is coming from) <p>2. Only for authenticated users The following attributes are only processed/displayed if they are released by the organisation of the user that is accessing the Interfederation Attribute Test</p> <ul style="list-style-type: none"> • E-mail • Home organization • Home organization type • Affiliation • Targeted ID/Persistent ID • Principal name • Scoped affiliation • Display Name • Common Name • SCHAC Home Organisation • SCHAC Home Organisation Type <p>All of the above attributes are declared as required to check if they really are released by an organisations.</p>
Purpose of the processing of personal data	The IP and referrer addresses of all web page visitors are stored in the web server log file for debugging purposes. For authenticated users, the Interfederation Service may receive all personal data mentioned-above. This personal data is only used to check if a Home Organisation is able to release all the attributes that the eduGAIN attribute profile recommends to support.
Third parties to whom personal data is disclosed	No data will be released to third parties. Personal data is only shown to the user himself. Data might also be used by SWITCH staff members for debugging purposes.
How to access, rectify and delete the personal data	Contact via aai@switch.ch . To rectify the data released by an organisation about you, contact that Home Organisation's IT helpdesk.
Data retention	Personal data, IP address and referrer are only stored in log files created by the web server and the SAML software. Log files are kept only for 30 days and are deleted automatically after this time.
Data Protection Code of Conduct	Personal data will be protected according to the Code of Conduct for Service Providers , a common standard for the research and higher education sector to protect the user's privacy.

Created with standard CoCo template.

2. Add Privacy URL


- Go to Resource Registry, <https://rr.aai.switch.ch>
- Click on „Edit Resource Description“ of Resource
- Add Privacy URL in section „2. Descriptive Information“


English Resource Information	
Name	<input type="text" value="AAI Viewer Interfederation Test"/> <p>Display name to show for this Resource. Ideally no longer than 33 characters. May be displayed to the user during login.</p>
Description	<input type="text" value="This service is used to test the interfederation readiness of SWITCHaai Identity Providers."/> <p>In the description you should briefly describe the purpose of this Resource. For example "The purpose of this service is to ...". Ideally no longer than 100 characters. May be displayed to the user during login.</p>
Information URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/"/> <p>URL to a web page that provides more comprehensive description than the one above. In order to request to be included in the REFEDS Research & Scholarship (R&S) entity category, provide a URL to a general information page about this service. This information page must be in English. After providing the URL, enable the R&S support in section '7. Intended Audience'.</p>
Privacy URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/privacy-statement.html"/> <p>URL to a web page contains a privacy statement that describes how identity information will be used and managed. This URL must be publicly accessible. In order to commit to the GÉANT Data Protection Code of Conduct (CoCo), provide a URL to a privacy statement page that contains a link to http://www.geant.net/uri/dataprotection-code-of-conduct/v1. The privacy statement must be in English and ideally follows this privacy policy template. After providing a privacy statement URL, enable the CoCo support in section '7. Intended Audience'.</p>
Keywords	<input type="text"/> <p>Space-separated keywords (locations, tags, categories, labels) related to this Resource. Multiple connected words can be separated by the + character. The keywords are primarily used to search for this entity.</p>

3. Commit to CoCo

- Go to section „Intended Audience and Interfederation“
 - Check „Commit to GÉANT Data Protection Code of Conduct (CoCo)“

GÉANT Data Protection Code of Conduct (CoCo)

Commit to the [GÉANT Data Protection Code of Conduct \(CoCo\)](#) 

The [GÉANT Data Protection Code of Conduct](#)  (CoCo) contains a set of data privacy rules that the operator of a service can commit to. The effect is that Identity Providers from abroad are more likely to release user attributes to this service because the commitment to the CoCo enhances the trust that users data is processed with care. Supporting the GÉANT Data Protection Code of Conduct should not be a problem for most Swiss services because the rules mentioned in the CoCo are also covered in the Swiss data privacy law.

SWITCH recommends to commit to the GÉANT Data Protection Code of Conduct for Interfederation services.

 All requirements to support the GÉANT Data Protection Code of Conduct would be met.

available end of August 2014

– Warning is shown if any CoCo requirements are not met

- Finally, submit Resource Description for approval

R&S for Home Organisations/IdP

- Similar to CoCo: Attribute release
- For SWITCHaai Home Organisations the default setting is to release the minimal set of R&S attribute to services in the Research & Scholarship entity category
 - Services enhance research and scholarship
 - uApprove asks user for consent before data is released to non-SWITCHaai services
 - Use of R&S within Switzerland only is also possible but should generally not be necessary
- Home Organisations will be able to change their settings in section „7. Attribute Release Settings“

2. Entity Category Policies

Entity Category Policies apply whenever a Resource claims to meet the category's requirements. The claim is part of the Service Provider's metadata. Entity Category Policies have higher priority than the default release policies for individual attributes. However, they have lower priority than the Resource Specific Attribute Release Policy rules.

Together with a user attribute release consent module (i.e. [uApprove](#)), attribute release based on the entity categories below should provide enough confidence from a data protection point of view to release the requested attributes also to Interfederation-enabled resources abroad.

GÉANT Data Protection Code of Conduct (CoCo)

Resources in the [GÉANT Data Protection Code of Conduct \(CoCo\)](#) entity category declare to respect the CoCo's behavioral rules and that they are located in either EU/EEA or a country with adequate data protection (e.g. Switzerland).

The CoCo was created by [GÉANT](#), the international research infrastructure project that also created and operates [eduGAIN](#) and [eduroam](#). SWITCH contributes to GÉANT.

Release required attributes (default)

Provided a Resource is in the GÉANT Data Protection Code of Conduct entity category and attribute release for this entity category is enabled, an attribute is only released if its release scope is neither **nobody** nor **my organisation's resources**. Is the attribute release for this entity category disabled, only the default and specific release rules apply.

available end of August 2014

REFEDS Research & Scholarship (R&S)

Resources in the [REFEDS Research & Scholarship \(R&S\)](#) category "enhance the research and scholarship activities" and are of benefit to R&S user communities.

[REFEDS](#) specified this entity category. It is the interest group of research and education identity federations world-wide. SWITCH contributes to REFEDS.

Release minimal set of R&S attributes (default)

The minimal R&S attribute set includes the attributes:

- **Principal name**
- **E-mail**
- **Name (Given name and surname or alternatively Display name)**

The complete set with all R&S attributes additionally includes:

- **Targeted ID/Persistent ID**
- **Scoped Affiliation**

Is the attribute release for this entity category disabled, only the default and specific release rules apply.

Default settings for Home Organisations. Will be available in RR end August 2014.

R&S for Resources/SP

- Full R&S specification:
<https://refeds.org/category/research-and-scholarship/>
- **Quick Start**
To (technically) commit to CoCo.
In Resource Registry:
 1. Add InformationURL in section "2. Descriptive Information"
 2. Ensure only R&S attributes are requested
 3. Request inclusion in R&S Entity Category in section "7. Intended Audience and Interfederation"

1. Add Information URL

- Go to Resource Registry, <https://rr.aai.switch.ch>
- Click on „Edit Resource Description“ of Resource
- Add Information URL in section „2. Descriptive Information“

English Resource Information	
Name	<input type="text" value="AAI Viewer Interfederation Test"/> Display name to show for this Resource. Ideally no longer than 33 characters. May be displayed to the user during login.
Description	<input type="text" value="This service is used to test the interfederation readiness of SWITCHaai Identity Providers."/> In the description you should briefly describe the purpose of this Resource. For example "The purpose of this service is to ...". Ideally no longer than 100 characters. May be displayed to the user during login.
Information URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/"/> URL to a web page that provides more comprehensive description than the one above. In order to request to be included in the REFEDS Research & Scholarship (R&S) entity category , provide a URL to a general information page about this service. This information page must be in English. After providing the URL, enable the R&S support in section '7. Intended Audience'.
Privacy URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/privacy-statement.html"/> URL to a web page contains a privacy statement that describes how identity information will be used and managed. This URL must be publicly accessible. In order to commit to the GÉANT Data Protection Code of Conduct (CoCo) , provide a URL to a privacy statement page that contains a link to http://www.geant.net/uri/dataprotection-code-of-conduct/v1 . The privacy statement must be in English and ideally follows this privacy policy template . After providing a privacy statement URL, enable the CoCo support in section '7. Intended Audience'.
Keywords	<input type="text"/> Space-separated keywords (locations, tags, categories, labels) related to this Resource. Multiple connected words can be separated by the + character. The keywords are primarily used to search for this entity.

2. Limit Attribute to R&S Set

- In section "6. Requested Attributes" select one of the R&S attribute sets to mark the attributes in that set
- Then request from the marked attributes those as required that are needed by the service

Common Attribute Sets

Select in the list an attribute set to mark frequently requested sets of attributes.

SWITCHaai Attributes

Non-identifiable SWITCHaai Core attributes

SWITCHaai Core attributes

All SWITCHaai attributes

eduGAIN attributes recommended to implement for Identity Provider

Non-identifiable recommended attributes

All recommended attributes

REFEDS Research & Scholarship Attributes

Minimal R&S attributes

All R&S attributes

Request Subset of R&S Attributes

SWITCHaai Core Attributes			
SWITCHaai Core attributes must be available for all users. Therefore, a Home Organisation must be able to release these attributes. However, the Home Organisation's attribute release policy controls whether or not an attribute is released to a Resource.			
Attribute	Coverage	Necessity	Declare why the resource needs it
Affiliation eduPersonAffiliation		Required	<input type="text"/>
E-mail email		Required	<input type="text"/>
Given name givenName		-	<input type="text"/>
Home organization swissEduPersonHomeOrganization		-	<input type="text"/>
Home organization type swissEduPersonHomeOrganizationType		-	<input type="text"/>
Surname surname		-	<input type="text"/>
Targeted ID/Persistent ID eduPersonTargetedID		Required	<input type="text"/>
Unique ID swissEduPersonUniqueID		-	<input type="text"/>

3. Apply for R&S Entity Category

- Go to section „Intended Audience and Interfederation“
 - Check „Apply for to the REFEDS Research & Scholarship (R&S)“

REFEDS Research & Scholarship (R&S)

Apply for to the [REFEDS Research & Scholarship \(R&S\)](#)

The [REFEDS R&S \(R&S\)](#) entity category is applicable to resources that "support research and scholarship interaction, collaboration or management as an essential component". If the requirements to be in this service category are met Identity Providers from other higher education and research insitutions abroad are more likely to release user attributes to this service.

SWITCH recommends in particular to Interfederation-enabled services to apply for the R&S category.

 **Requirements to support the REFEDS Research & Scholarship Entity Category are likely to be met.**

available end of August 2014

– Warning is shown if any R&S requirements are not met

- Finally, submit Resource Description for approval. SWITCH then will check and approve the application.

Baking can be fun 😊



Resource Registry Updates

A look through the keyhole at upcoming changes



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 13. August 2014

Disclaimer

- Following Updates in Resource Registry will become active only end of August
- Implementation still subject to changes
- Feedback on Resource Registry in general is welcome

Upcoming Changes in Resource Registry

- In Resource Administration:
 - Section "6. Requested Attributes"
 - Section "7. Intended Audience and Interfederation"
- In Home Organisation Administration:
 - Section "7. Attribute Release Settings"
- And some smaller changes not worth mentioning



Requested Attributes I

Requested Attributes

Specify on this page the user attributes which are **required** or **desired** by the resource. A Resource receives at maximum those attributes that it requests. It is, however, not guaranteed that a Resource always receives all attributes it requests because not all attributes are implemented by all organisations and sometimes organisations decide not to release certain attributes about their users.

General Recommendations

A Resource MUST request only the attributes that are adequate, relevant and not excessive to the Resource. One of the key principles of the data protection law is: **Request as few attributes as necessary!** Consequently, only declare attributes as required if they are essential for the operation of the resource. Declare attributes as desired if they are "nice-to-have".

- [Show recommendations for Resources accessed primarily by SWITCHaai users](#)
- [Show recommendations for interfederation Resources als accessed by non-SWITCHaai users](#)


Common Attribute Sets

Select in the list an attribute set to mark frequently requested sets of attributes.

SWITCHaai Attributes
Non-identifiable SWITCHaai Core attributes
SWITCHaai Core attributes
All SWITCHaai attributes

eduGAIN attributes recommended to implement for Identity Provider
Non-identifiable recommended attributes
All recommended attributes

REFEDS Research & Scholarship Attributes
Minimal R&S attributes
All R&S attributes

 Remove all attributes

Recommendations for SWITCHaai / Interfederation use-cases

Assistant to mark attributes of popular attribute sets

Requested Attributes II

New categorization of attributes:
SWITCHaai Core, Standardized,
Other, Local/Bilateral

Marked attribute. In this
case non-identifying
SWITCHaai core attributes

Attributes

Select for each attribute whether it is **required** or **desired** by the Resource. Also describe in the text field (in english) why and for what reason an attribute is required or desired. This helps Home Organization administrators managing their attribute release policies.

SWITCHaai Core Attributes			
SWITCHaai Core attributes must be available for all users. Therefore, a Home Organisation must be able to release these attributes. However, the Home Organisation's attribute release policy controls whether or not an attribute is released to a Resource.			
Attribute	Coverage	Necessity	Declare why the resource needs it
Affiliation eduPersonAffiliation		Required	To test whether this attribute is available
E-mail email		Required	
Given name givenName		-	
Home organization swissEduPersonHomeOrganization		Required	
Home organization type swissEduPersonHomeOrganizationType		Required	
Surname surname		-	
Targeted ID/Persistent ID eduPersonTargetedID		Required	To test whether this attribute is available
Unique ID swissEduPersonUniqueID		-	

How many organisations can
release the attribute

Intended Audience and Interfederation

GÉANT Data Protection Code of Conduct (CoCo)

Commit to the [GÉANT Data Protection Code of Conduct \(CoCo\)](#)

The [GÉANT Data Protection Code of Conduct \(CoCo\)](#) contains a set of data privacy rules that the operator of a service can commit to. The effect is that Identity Providers from abroad are more likely to release user attributes to this service because the commitment to the CoCo enhances the trust that users data is processed with care. Supporting the GÉANT Data Protection Code of Conduct should not be a problem for most Swiss services because the rules mentioned in the CoCo are also covered in the Swiss data privacy law.

SWITCH recommends to commit to the GÉANT Data Protection Code of Conduct for Interfederation services.

⚠ Currently, you cannot commit to the GÉANT Data Protection Code of Conduct because the following requirement is not met: No English privacy URL provided! In order to be compliant with the GÉANT Data Protection Code of Conduct, a URL to an English privacy policy page must be provided for this Resource. Please [add a Privacy Statement URL](#) that meets the requirements and then return to this page to enable the CoCo.

REFEDS Research & Scholarship (R&S)

Apply for to the [REFEDS Research & Scholarship \(R&S\)](#)

The [REFEDS R&S \(R&S\)](#) entity category is applicable to resources that "support research and scholarship interaction, collaboration or management as an essential component". Candidates for the Research and Scholarship (R&S) Category are Resources that support research and scholarship interaction, collaboration or management as their primary activity. This excludes services for access to licensed content such as e-journals. If a Resource is in the R&S entity category, Identity Providers from higher education and research insitutions abroad are more likely to release user attributes to it.

SWITCH recommends in particular to Interfederation-enabled services to apply for the R&S category.

⚠ Currently, you cannot apply for the REFEDS R&S category because the following requirement is not met: The service must have an information URL to get in the R&S category. Please [set an Information URL](#) for this resource and then return to this page.

Support for entity categories

Interactive warning messages if entity category requirements are not met

Attribute Release I

Entity Categories policies influence IdP attribute release:

1. Default Policies

General release rules for individual attributes, depending on whether they are required or desired.

2. Entity Category Policies

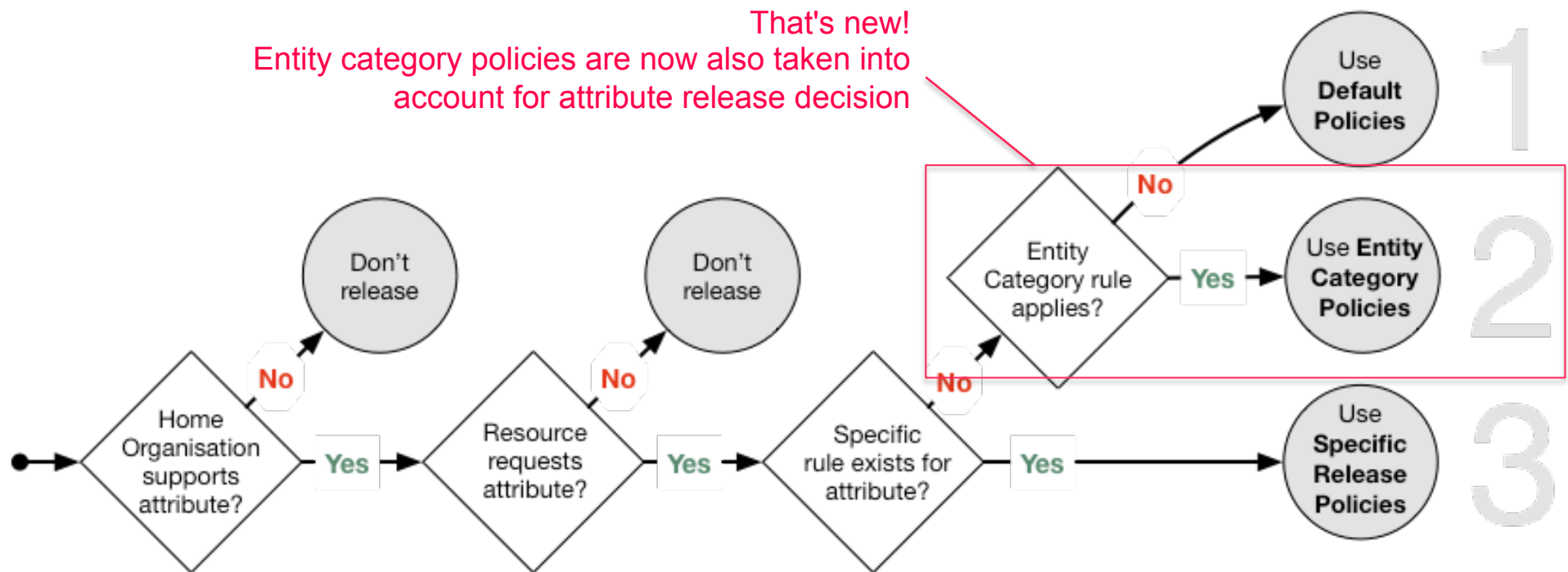
Release rules that apply if Resources belong to a certain entity

3. Resource Specific Policies

Release rules for specific Resources to create rules that always have precedence

Attribute Release II

Decision tree of new attribute release



Attribute Release III

New policy section for entity category-based attribute release

2. Entity Category Policies

Entity Category Policies apply whenever a Resource claims to meet the category's requirements. The claim is part of the Service Provider's metadata. Entity Category Policies have higher priority than the default release policies for individual attributes. However, they have lower priority than the Resource Specific Attribute Release Policy rules.

Together with a user attribute release consent module (i.e. [uApprove](#)), attribute release based on the entity categories below should provide enough confidence from a data protection point of view to release the requested attributes also to Interfederation-enabled resources abroad.

GÉANT Data Protection Code of Conduct (CoCo)

Resources in the [GÉANT Data Protection Code of Conduct \(CoCo\)](#) entity category declare to respect the CoCo's behavioral rules and that they are located in either EU/EEA or a country with adequate data protection (e.g. Switzerland).

The CoCo was created by [GÉANT](#), the international research infrastructure project that also created and operates [eduGAIN](#) and [eduroam](#). SWITCH contributes to GÉANT.

Release required attributes (default)

-

Release required attributes (default)

Release all required and desired attributes

an attribute is only released if its release scope is neither **nobody** nor **my organisation's resources**. Is the attribute release for this entity category disabled, only the default and specific release rules apply.

REFEDS Research & Scholarship (R&S)

Resources in the [REFEDS Research & Scholarship \(R&S\)](#) category "enhance the research and scholarship activities" and are of benefit to R&S user communities.

[REFEDS](#) specified this entity category. It is the interest group of research and education identity federations world-wide. SWITCH contributes to REFEDS.

Release minimal set of R&S attributes (default)

The minimal R&S attribute set includes the attributes:

- **Principal name**
- **E-mail**
- **Name (Given name and surname or alternatively Display name)**

The complete set with all R&S attributes additionally includes:

- **Targeted ID/Persistent ID**
- **Scoped Affiliation**

Is the attribute release for this entity category disabled, only the default and specific release rules apply.

RRA Administrator Duties

SWITCH

AAI Team
aai@switch.ch

Bern, 13.08.2014

Why is it important

- Responsibility of an SP lies with the organization
- Check for correctness and compliance
- Service Description:
https://www.switch.ch/aai/docs/SWITCHaai_Service_Description.pdf
- Resource Registry Guide:
<https://www.switch.ch/aai/docs/AAI-RR-Guide.pdf>

What to check

- Is the person allowed to operate an SP in the name of your organization?
- Is the contact information (administrative, support, technical) correct and up-to-date?
- Are the attribute requirements adequate w.r.t. the resource description?
- Do the service locations point to a host operated by your institution?
- Does the persons that registered the resource possess the private key of any self-signed certificate?

Account Checking on a SP

Based on SAML AttributeQuery

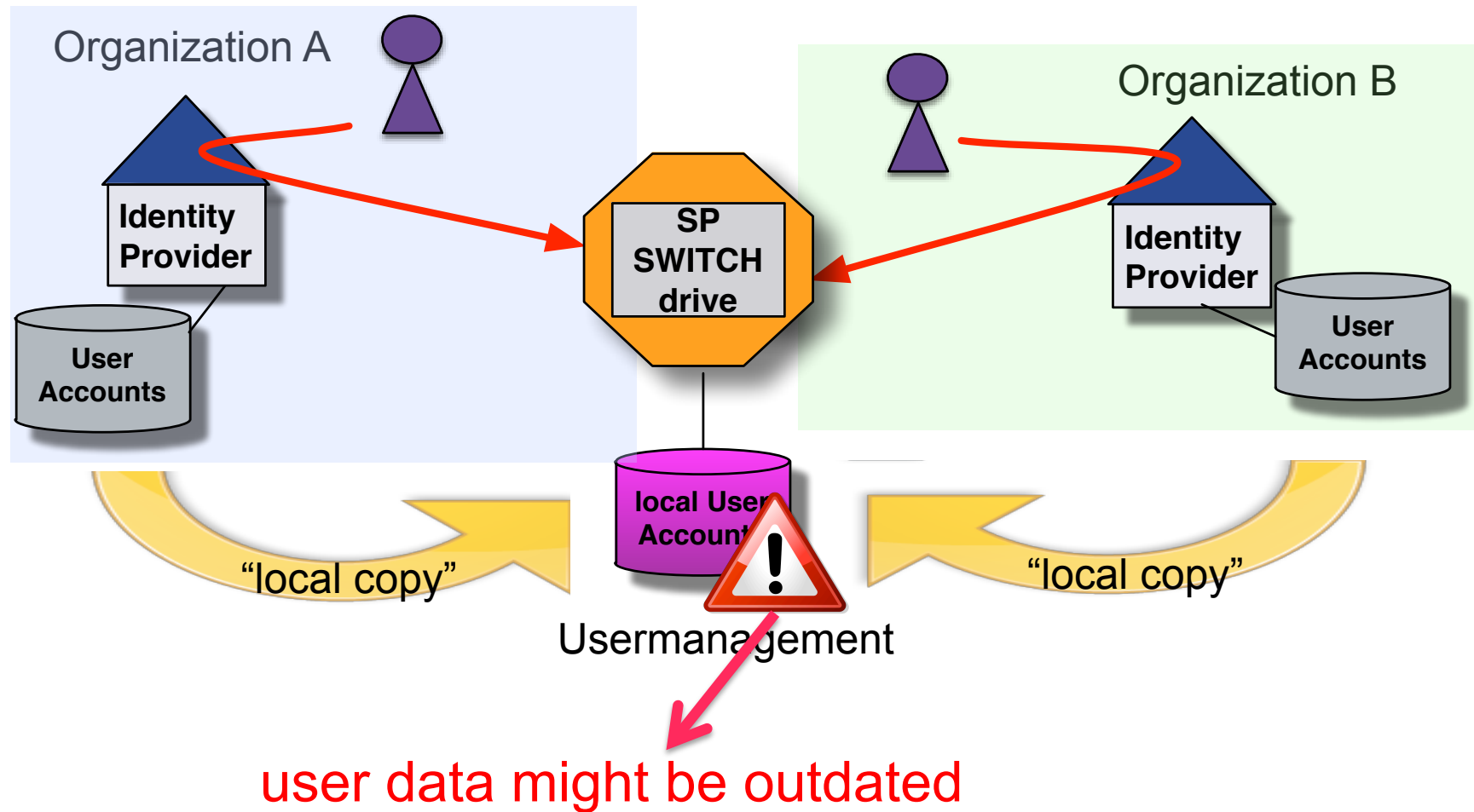


SWITCH

SWITCHaai Team
aai@switch.ch

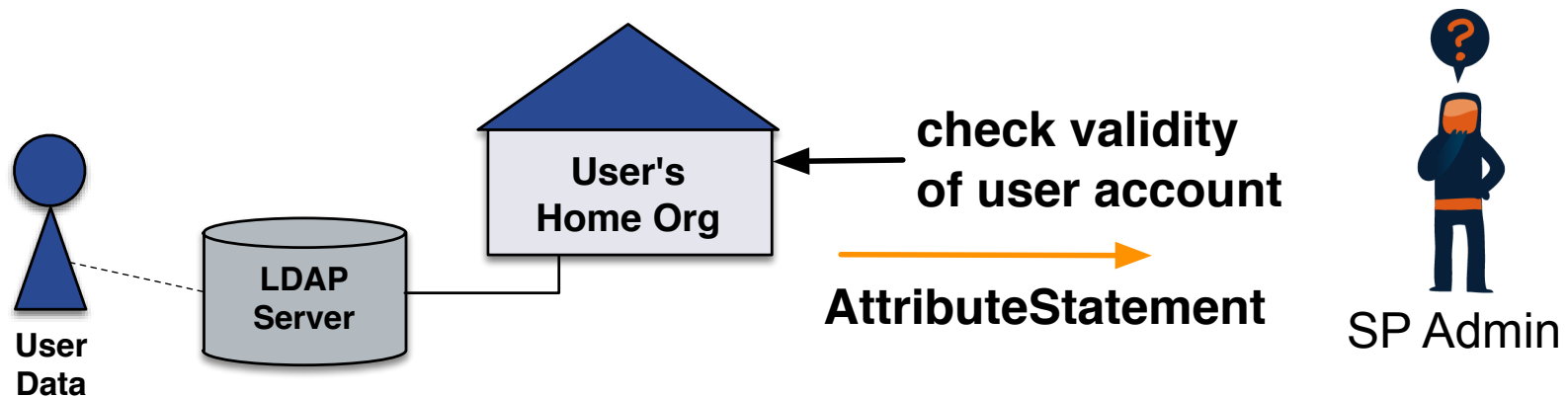
Berne, 13 August 2014

Why do account checking?



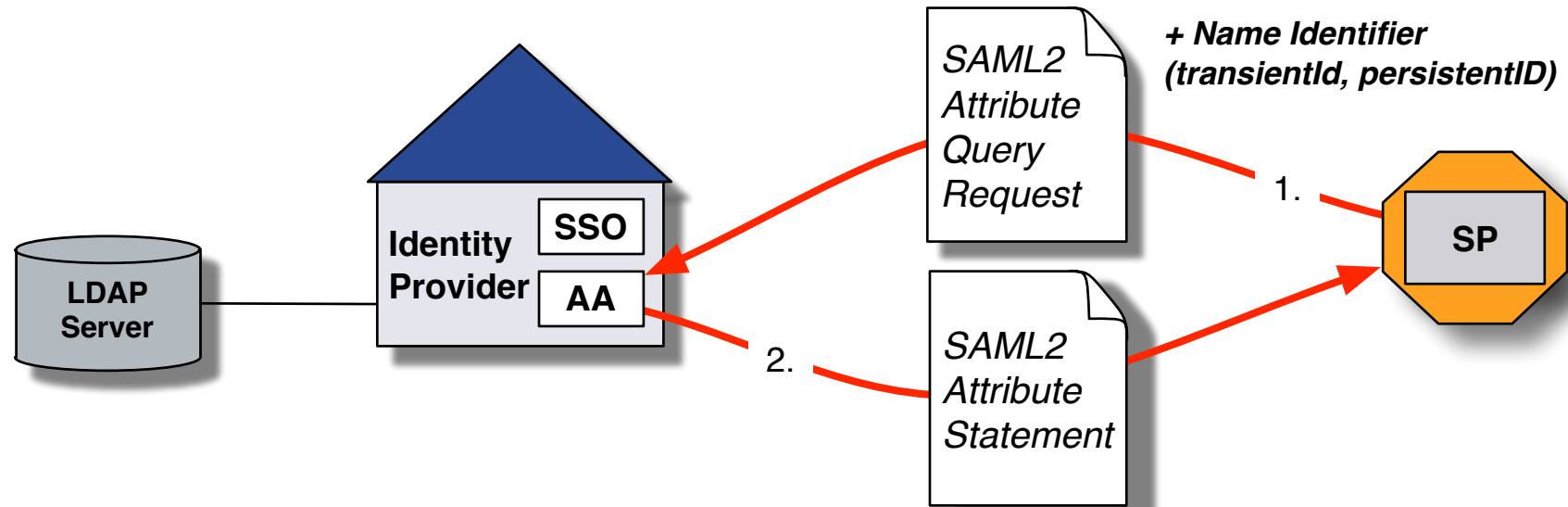
Idea

Validity of user account



- The SP sends an AttributeQuery to the IdP
- The SP receives an AttributeStatement from the IdP
- Process the result and do the “housekeeping” in your application

SAML Attribute Query



- Service Provider (SP) directly queries Attribute Authority (AA) of Identity Provider for user attributes using a NameID
- Usually transient or persistent NameID is used
- Shibboleth SP/IdP supports Attribute Queries

- All SWITCHaai IdPs support stored persistentIDs (persistentID stored in database that maps to the localID)

Persistent ID and Attribute Queries

Serialized Example of a persistentID:

<https://aai-login.tw.switch.ch/idp/shibboleth!>
<https://testsp.tw.switch.ch/shibboleth!>
<jrdV9rog57INTKp9EB1vmyRfmgc=>

localEntity	peerEntity	principalName	localId	persistentId	peerProvidedId	creationDate	deactivationDate
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-viewer.switch.ch/shibboleth	student1	2490257@example.org	dfF12dKdk1ymiJrn34NaLsM8bw=	NULL	2013-07-23 15:13:22	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-demo.switch.ch/shibboleth	student2	8548997@example.org	ANS7jbdGduIMWCevMqHyKgaQqs4=	NULL	2013-07-23 15:52:45	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-viewer.switch.ch/shibboleth	student2	8548997@example.org	01L0D0/Ji5GfMQxEeHq6NZ6Mqx8=	NULL	2013-07-23 16:00:46	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://rr.aai.switch.ch/shibboleth	student1	2490257@example.org	Jy1jI/XxpTK34NeM5VXFQ4U/Uw=	NULL	2013-08-05 09:28:19	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-demo.switch.ch/shibboleth	student1	2490257@example.org	SzPThGVlohQaXZerDcC2+FPw8AU=	NULL	2013-09-18 12:55:01	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://testsp.tw.switch.ch/shibboleth	student1	2490257@example.org	hJM3b+/aqWYv1Tuj+IQylylqj2A=	NULL	2013-09-19 16:10:35	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-viewer.switch.ch/shibboleth	staff3	7622788@example.org	3oiPFq38oIyS4+h7J/VRwwAZTGI=	NULL	2014-01-06 11:24:36	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://aai-demo.switch.ch/shibboleth	staff3	7622788@example.org	2m2ipfQvPCLfReyyL+bR3h9v3gU=	NULL	2014-01-06 11:25:01	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://testsp.tw.switch.ch/shibboleth	student2	8548997@example.org	jrdV9rog57INTKp9EB1vmyRfmgc=	NULL	2014-01-30 08:50:28	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://testsp.tw.switch.ch/shibboleth	staff3	7622788@example.org	YVIAKbj81gi5E+EF+f2rUS+2FGk=	NULL	2014-01-30 09:08:30	NULL
https://aai-login.tw.switch.ch/idp/shibboleth	https://attribute-viewer.aai.switch.ch/shibboleth	student1	2490257@example.org	bbVdShG0bKqP0NJHYT6eSYwtNIA=	NULL	2014-06-13 16:32:34	NULL

11 rows in set (0.00 sec)

- Opaque
- Targeted: Same user has different persistentIDs for different services
- Once SP has user's persistentID, attributes can be queried at any time (without users involvement)

Requirements

- Shibboleth SP \geq 2.5.0
- SP must use persistentID
- Requires attribute query extension by Japanese Federation GakuNin
 - requests the AttributeStatement based on user's identifier to an IdP and outputs the resulting attribute in JSON format.
 - Provides a handler to make fast Attribute Queries via web
 - Extension will be integrated on SP in the near future



Attribute Query with extension

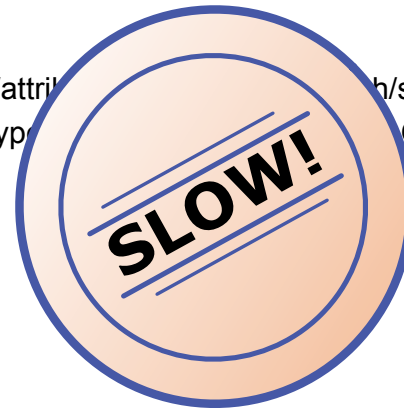
- `curl -k 'https://localhost/Shibboleth.sso/AttributeQuery?entityID=https://aai-logon.switch.ch/idp/shibboleth&nameId=NRDnNTHBcKe4fwB7AG9p/psQG1o='`
- Result: JSON Object:

```
{
  "displayName" : "Thomas Weller",
  "postalAddress" : "SWITCH$Werdstrasse 2$CH-8004 Zürich",
  "telephoneNumber" : "+41 44 268 1550",
  "isMemberOf" : "abc; x123, b312",
  "mail" : "thomas.weller@switch.ch",
  "persistent-id" : "https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shibboleth!P2HjBH.....",
  "schacHomeOrganizationType" : "urn:schac:homeOrganizationType:ch:others;urn:schac:homeOrganizationType:int:nren",
  "gender" : "1",
  "dateOfBirth" : "....",
  "cn" : "Thomas Weller",
  "homeOrganizationType" : "others",
  "uniqueID" : "74....@switch.ch",
  "homeOrganization" : "switch.ch",
  "schacHomeOrganization" : "switch.ch",
  "preferredLanguage" : "en",
  "givenName" : "Thomas",
  "surname" : "Weller",
  "scoped-affiliation" : "staff@switch.ch;member@switch.ch",
  "principalName" : "74.....@switch.ch",
  "affiliation" : "member;staff",
  "uid" : "weller"
}
```

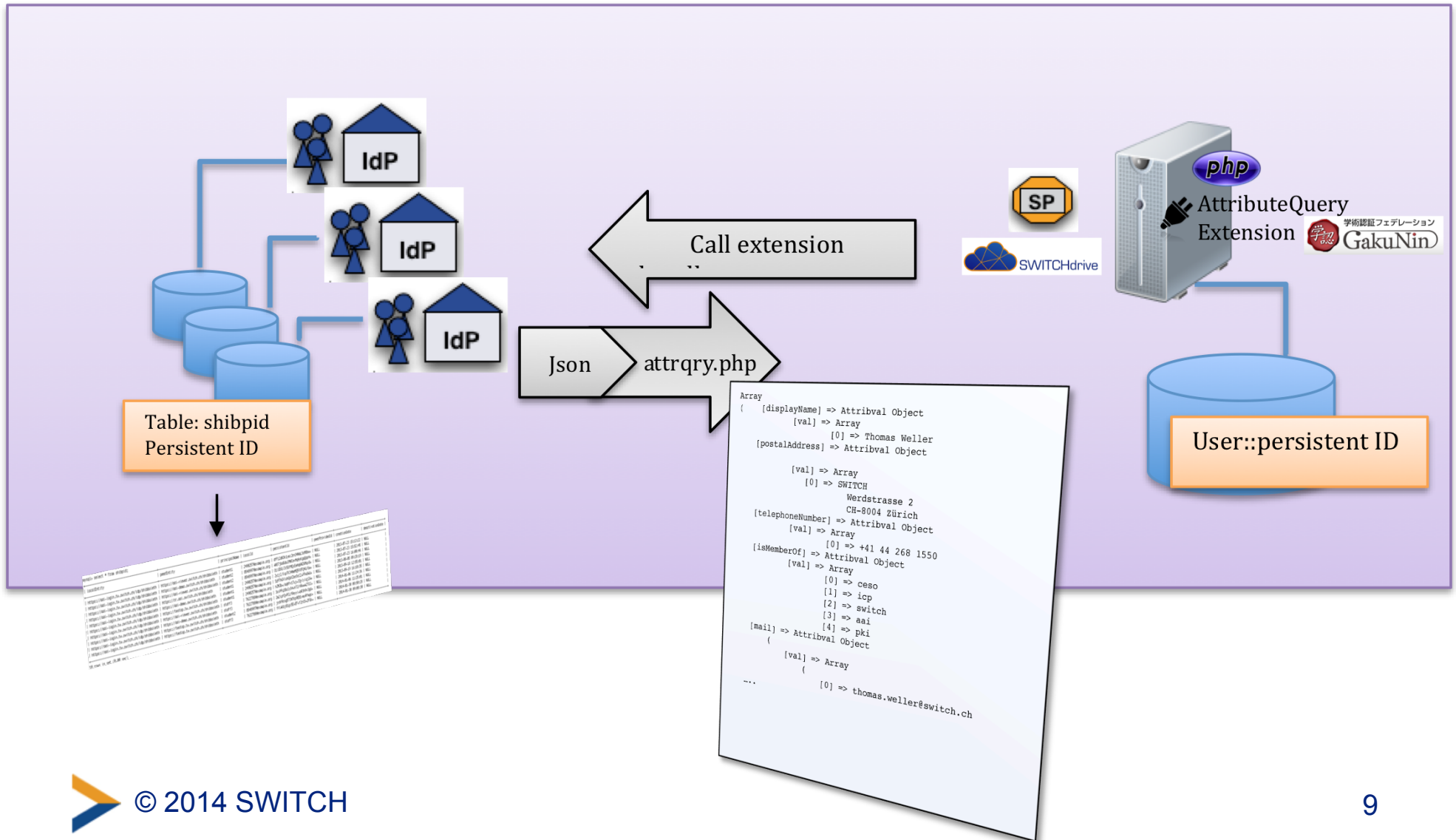
Attribute Query with resolvertest

- `./resolvertest -n PDg6jPP2HjBHuOFD4RFzb+2x+IM= -i https://aai-logon.switch.ch/idp/shibboleth -saml2 -f urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`

displayName: Thomas Weller
postalAddress: SWITCH\$Werdstrasse 2\$CH-8004 Zürich
telephoneNumber: +41 44 268 1550
isMemberOf: abc; x123, b312
mail: thomas.weller@switch.ch
persistent-id: https://aai-logon.switch.ch/idp/shibboleth!https://attribu...h/shibboleth!PDg6jPP.....
schacHomeOrganizationType: urn:schac:homeOrganizationType... OrganizationType:int:nren
gender: 1
dateOfBirth:.....
cn: Thomas Weller
homeOrganizationType: others
uniqueID: 74....@switch.ch
homeOrganization: switch.ch
schacHomeOrganization: switch.ch
preferredLanguage: en
givenName: Thomas
surname: Weller
scoped-affiliation: staff@switch.ch; member@switch.ch



Implementation Idea for SWITCHdrive



Known issues

- wrong or persistentID does not exist
- User on LDAP does not or no longer exist
 - ⇒ return of defined staticAttributes or / and Default values (IdP attribute-resolver) e.g.:
- uApprove: attribute consent set to “not released”
 - ⇒ Attribute query plugin delivers always attributes
- User is not deleted in LDAP and has no login
 - ⇒ Attribute query plugin delivers the attributes

- SP is responsible for ensuring that the IdP is not overloaded

Deployment and effort required

- Sources Attribute Query handler:
 - <https://wiki.shibboleth.net/confluence/display/SHIB2/Contributions#Contributions-ServiceProviderExtensions>
- Installation and first tests
 - ~ 1/2 - 1 day

If you are interested to deploy, get in contact with SWITCHaai: aai@switch.ch

Additional links

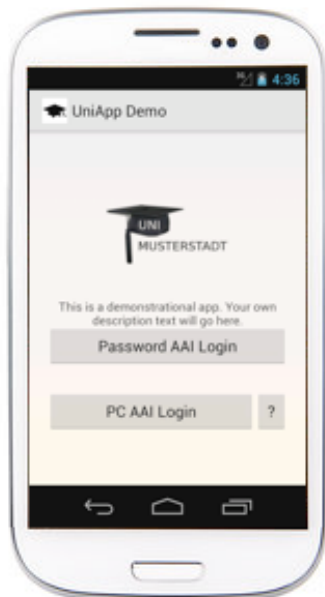
- AAI for mobile apps
 - <https://www.switch.ch/aai/support/tools/aai-for-apps.html>
- Documentation resolver test
 - [https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPresolver test](https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPresolver+test)

Comments and summary

- AttributeQuery: approach to keep user accounts “clean”
- SP Admin: “Which approach for the solution?”
 - ResolverTest vs. attribute query handler (< 20 queries and synchronization \geq 6 months)
 - costs and benefits should be balanced:
 - How many users
 - frequency of “synchronization”
 - further processing of return values

AAI for Mobile Apps

How mobile Apps can use SAML Authentication and Attributes



SWITCH

Serving Swiss Universities

Lukas Hämmerle

lukas.haemmerle@switch.ch

Berne, 13. August 2014

Introduction



App by University of St. Gallen

- Universities offer apps, e.g. for e-learning and campus info
- Apps need authentication
- Apps usually are non-browser applications
- Authentication and Authorisation Infrastructure (AAI) based on SAML2 are difficult to use for non-browser applications

Prerequisites for a Solution

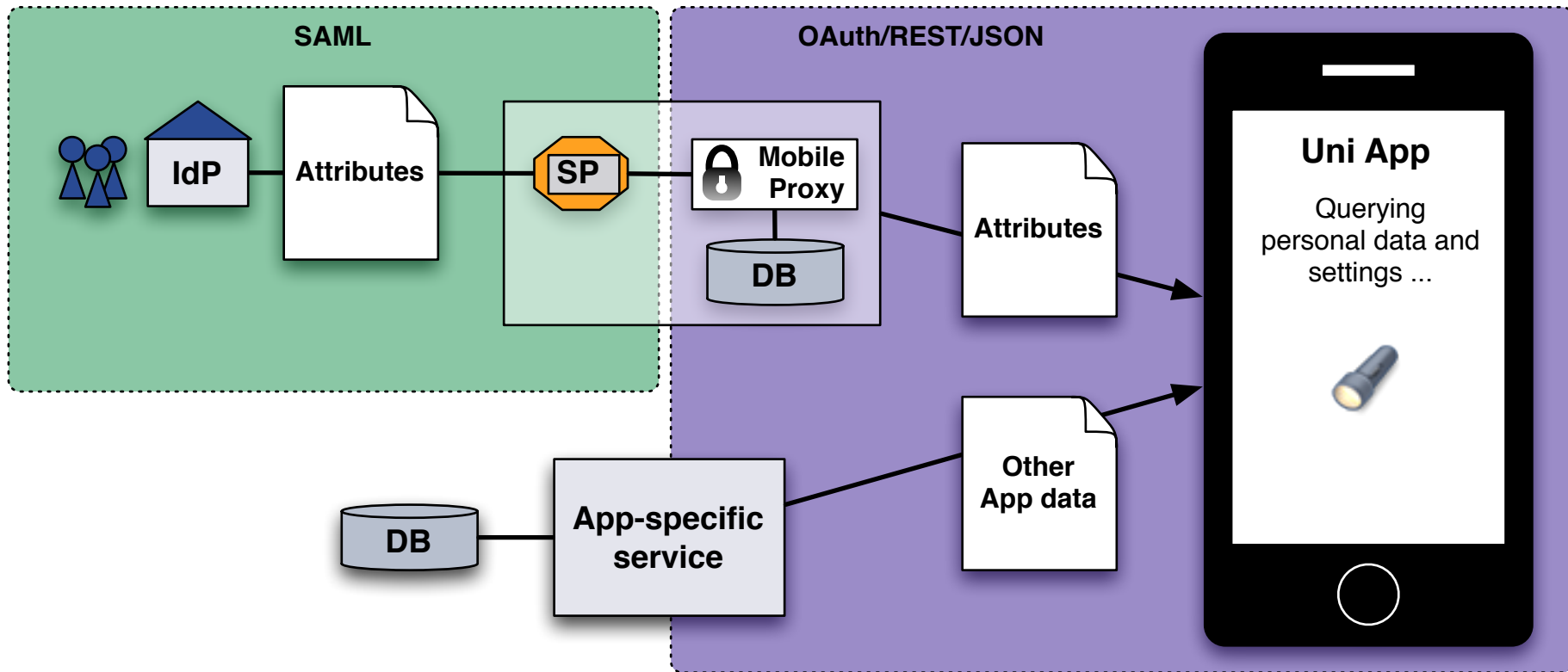
- App users from **many AAI organisations**
 - Excludes authentication with LDAP or HTTP Basic Auth
- **No changes/updates/plugins** for Identity Provider needed
 - Excludes SAML Enhanced Client and Proxy (ECP) profile

Solution wanted that works today in AAI!

App Requirements

- App should **not “emulate” a web-browser** for authentication
 - Excludes already known approaches
- App should **not save user’s university password**
 - Would cause problems (app data stolen by other app, commercial company offering app, password change)
- App should **not ask user to authenticate too often**
 - Apps should be easy to use and behave like other apps
- App should **always get up-to-date user attributes** on start
 - Excludes approaches based on caching user attributes

Solution



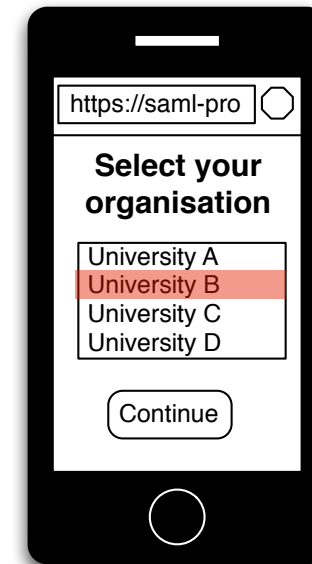
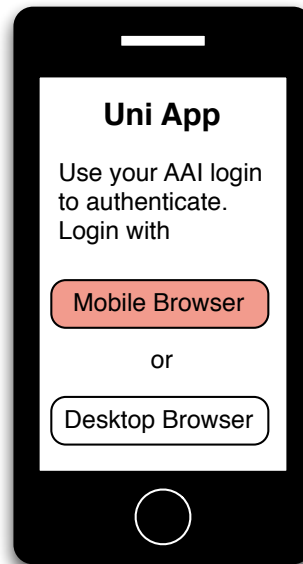
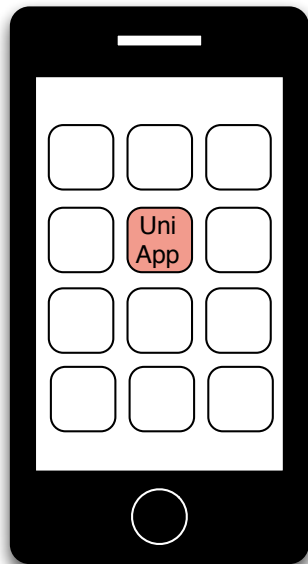
- A **(Mobile) Proxy** translates authentication/attribute information from SAML2 to OAuth/REST/JSON
- Mobile Proxy includes an OAuth2 Server that grants access tokens, which are mapped to a SAML2 persistent ID

Concept of Mobile Proxy

- 1 User authenticates once at Mobile proxy via web browser
- 2 Mobile Proxy gets persistent ID of user
- 3 Proxy stores persistent ID and binds it to an OAuth2 access token, which is stored in the App
- 4 App queries Mobile proxy for AAI attributes with token
- 5 Mobile Proxy uses persistentId to query user's AAI attributes via a SAML Attribute Query

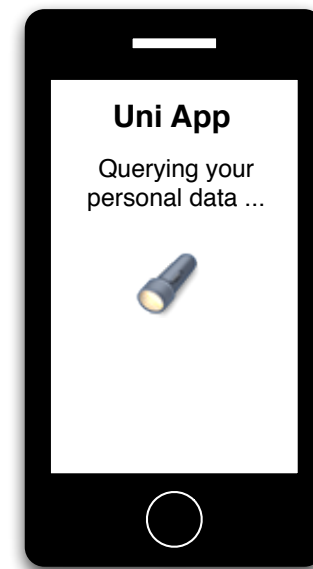
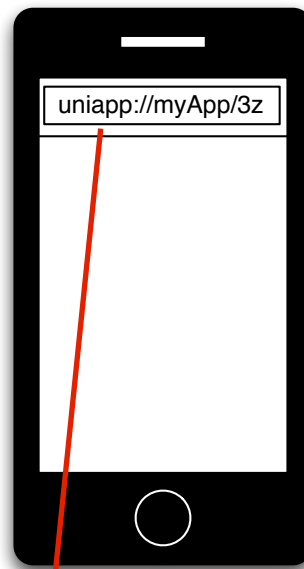
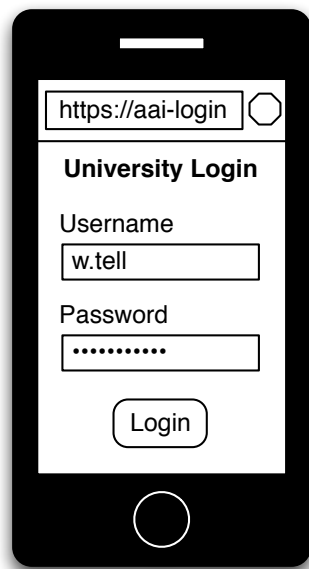
User's Perspective: First App Start

- User starts app for the first time
- App asks user to authenticate with AAI on device or desktop PC
- Mobile browser opens and user selects his organisation



User's Perspective: First App Start Continued

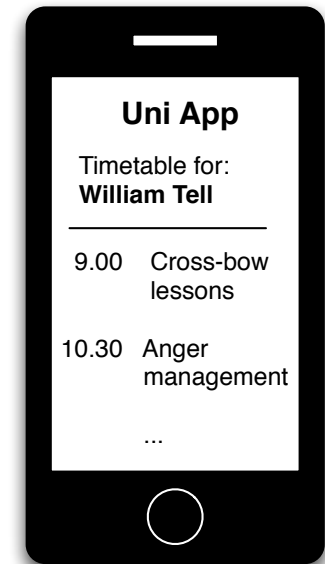
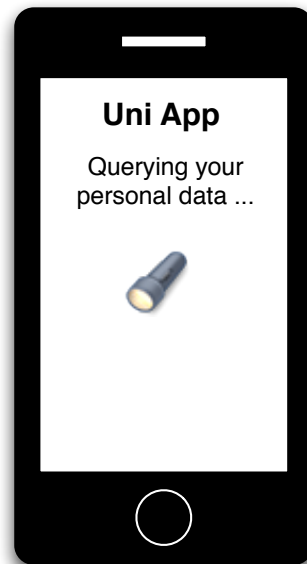
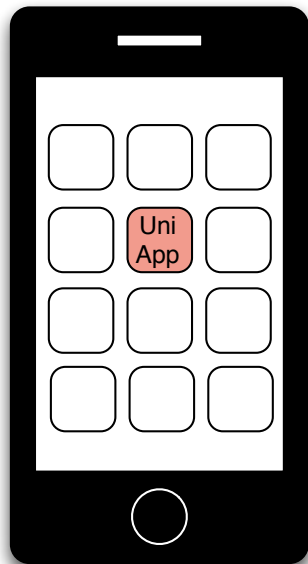
- Authentication with AAI at home organisation in web browser
- Mobile Proxy SP gets user's attributes including persistentId and issues OAuth token
- Uni App uses token to get user attributes from Mobile Proxy



Link with custom URL scheme is opened automatically
E.g. `uniapp://{App-Identifier}/{40-Byte-Access Token}`

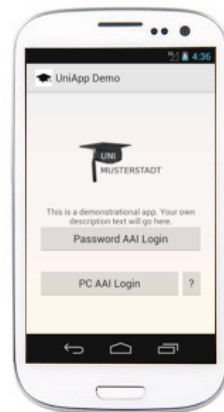
User's Perspective: Further App Starts

- User starts app
- App fetches user attributes with OAuth access token from proxy
- App gets other app-specific data with access token



Demo of Sample Uni App

- A quick demo is available on the AAI for Apps web page:
<https://www.switch.ch/aai/support/tools/aai-for-apps.html>



- Two options for initial AAI login:
 - Browser on mobile device
 - Browser on another computer (requires typing or scanning QR code)

Mobile Browser vs Desktop Browser

To get persistent ID, User must login with a web browser at least once with AAI. But with which browser?

- **In-App browser:**

- In app browser might not have access to browser saved passwords user has to type in again username password at IdP

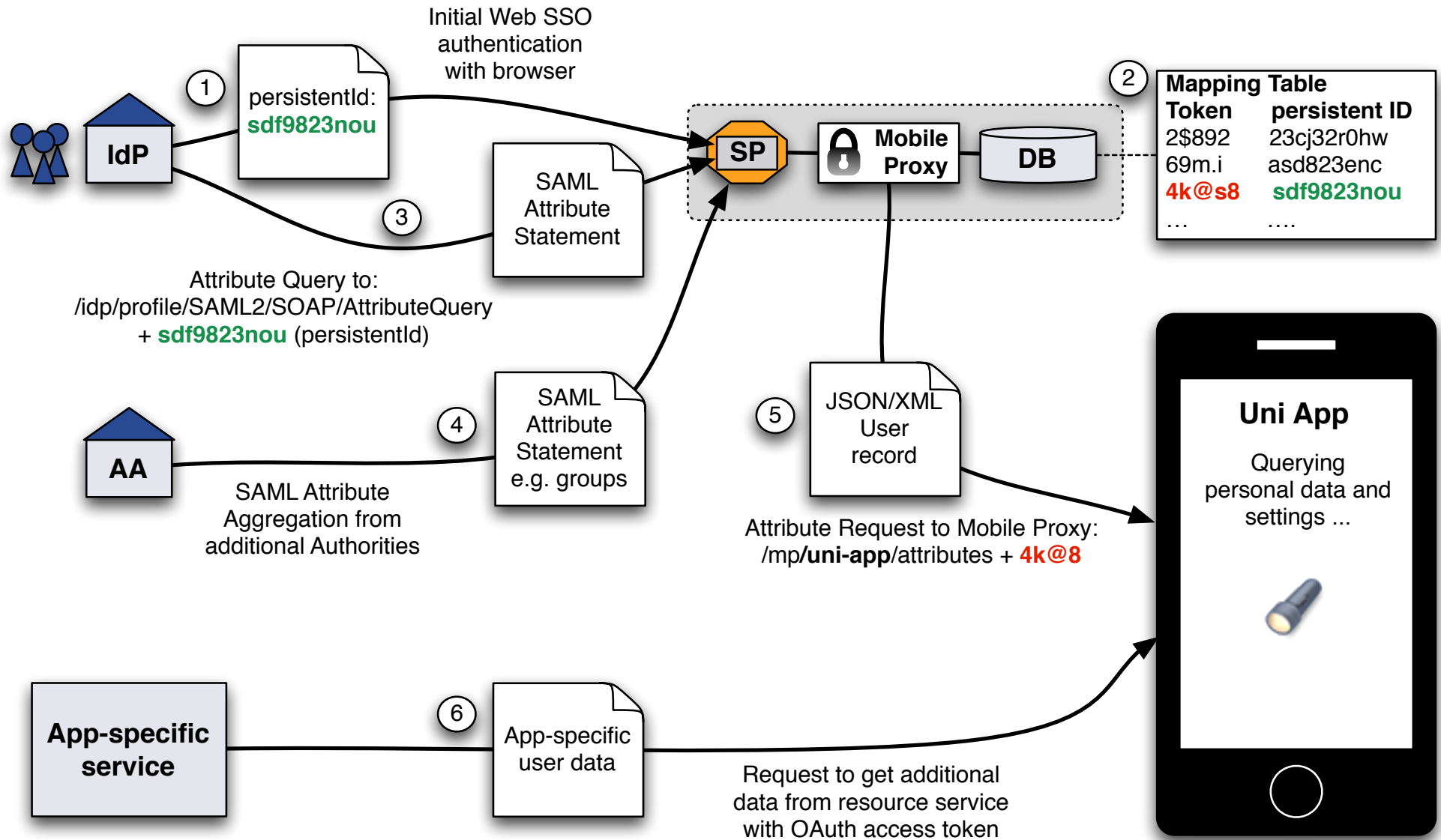
- **Browser on mobile device:**

- Benefit from SSO session that user might have already
- Default browser on device is used

- **Browser on Desktop:**

- Most flexible browser that might support authentication methods other than username/password. E.g. X.509
- Requires user to type URL/token or scan a QR code

Data Flow



App Logout / Access Token Revocation

How about revocation of OAuth access token?

For example in case the device is sold or lost.

- OAuth Access token is used to:
 - Authenticate with Mobile Proxy
 - Retrieve up-to-date AAI attributes from Mobile Proxy
 - Retrieve arbitrary protected resources from third party resource server
- Token can be revoked by:
 - Expiration because validity is configurable
 - User within App by clicking on “Logout”
 - User via administration interface with web browser

Logout/Token Revocation via Web Interface

Mobile Proxy Device Administration

↑ About Mobile Proxy

Mobile Proxy Device Administration

On this page all your Devices registered with University Apps are listed. You can revoke any of them by clicking the *revoke* Link beneath.

App Name	Device	Requested	Expires	Revoke
UniApp Demo	Galaxy S3	29.04.13 11:11:19	08.08.13 11:11:19	Revoke
UniApp Demo	Android Emulator	29.04.13 11:19:13	08.08.13 11:19:13	Revoke

Multiple devices for same user and same app

Authenticated user

Advantages of this Approach

- App never gets user's AAI credentials
 - Any type of authentication can be used
- Can be deployed immediately without changes to federation
 - Requires that IdPs support persistentId (with storedId) and attribute queries. This is the case for all SWITCHaai IdPs.
 - Approach also works when SP aggregates attributes from additional attribute authorities (Virtual Organization/Group attribute providers)
- One instance of Mobile Proxy can serve multiple apps
 - Apps can have different attribute requirements
 - Individual <EntityDescriptors> for each app possible

Availability and Future Plans

- Software available as Open Source software (BSD license)
 - **Sample Uni App**: Java, Android App ready for customization
 - **Mobile Proxy**: PHP, Includes OAuth server and simple web interface
 - **Resource Server**: PHP, Returns back a default time table
- Developed as Prototype. No production quality yet.
- More information and link to SVN repository:
<http://swit.ch/aai-for-apps>
- SWITCH is considering to turn Mobile Proxy into a service if community is interested and contacts us!

Shibboleth Identity Provider 3.0

Recent developments and current status



SWITCH

SWITCHaai Team

aai@switch.ch

IdP v3 Development Timeline

- work on design document begun in 2011
- development with new team members intensified in 2013
- version 3.0.0-alpha1 released on 26 June 2014
- version 3.0.0-alpha2 released on 29 July 2014
- release currently scheduled for Q3 2014 (“betas in the late summer time frame”) ... may further shift, though

IdP v3 Main Goals

- “to create a more modular platform that makes customizing profile flows and many other behaviors simpler with less code”
- “remove most/all SAML dependencies from the core of the platform”

<https://wiki.shibboleth.net/confluence/display/DEV/IdP3Details>

IdP v3 What's New

- will include features which were only available as separate extensions for the IdP v2:
 - user consent for attribute release (uApprove) *
 - support for SAML ECP (“Enhanced Client or Proxy”) profile without the need for container-based authentication
 - X.509 certificate based authentication *
- more flexible configuration
 - native Spring XML configuration
 - Velocity templates which support on-the-fly modification of UI pages (in contrast to JSP pages, which require a container restart)
- support for stateless clustering
 - uses client-side (cookie) session storage by default

* not yet implemented in the alpha versions released so far

IdP v3 Requirements

- Java 7 or later
 - incompatibilities with the JavaScript engine in Java 8 (“Nashorn”), which is used for script-based attribute definitions (for Java versions up to 7, the “Rhino” engine is used)
- servlet container with Servlet API 3.0 support, such as
 - Tomcat 7 or later
 - Jetty 8 or later

Note: the IdP v3 will *not run* with Java or servlet container versions older than those listed above.

IdP v3 Backward Compatibility

- v3 feature set is a superset of v2
- keeping existing configuration files from v2 is partly supported:
 - `relying-party.xml` (deprecated, migration to new configuration syntax is recommended, in particular for using new/advanced features)
 - `attribute-resolver.xml` (some parts deprecated: `<PrincipalConnector>` elements and NameID encoders)
 - `attribute-filter.xml` (with the exception of four `AttributeIssuer` rules)
- authentication component fundamentally redesigned
 - based on Spring Web Flows (SWF), configuration completely new
 - login handlers for IdP v2 need to be adapted/rewritten

Current status and outlook

- initial alpha release tests at SWITCH in July/August
 - OpenJDK 7, Tomcat 7, Apache httpd 2.2 + mod_proxy_ajp
 - some hiccups with alpha1 (mostly addressed in alpha2)
 - basic features (SAML 2 Web Browser SSO, LDAP backend for authentication and attribute resolution, SQL backend for persistent ID) is working fine
 - user consent and X.509 authentication not yet implemented
- more testers from the community welcome
 - see <https://wiki.shibboleth.net/confluence/display/IDP30/Home>
 - documentation is relatively sparse, for the time being (familiarity with IdP v2 configuration required)
- SWITCH will overhaul its deployment and upgrade guides for IdP v3

Discovery Service Options

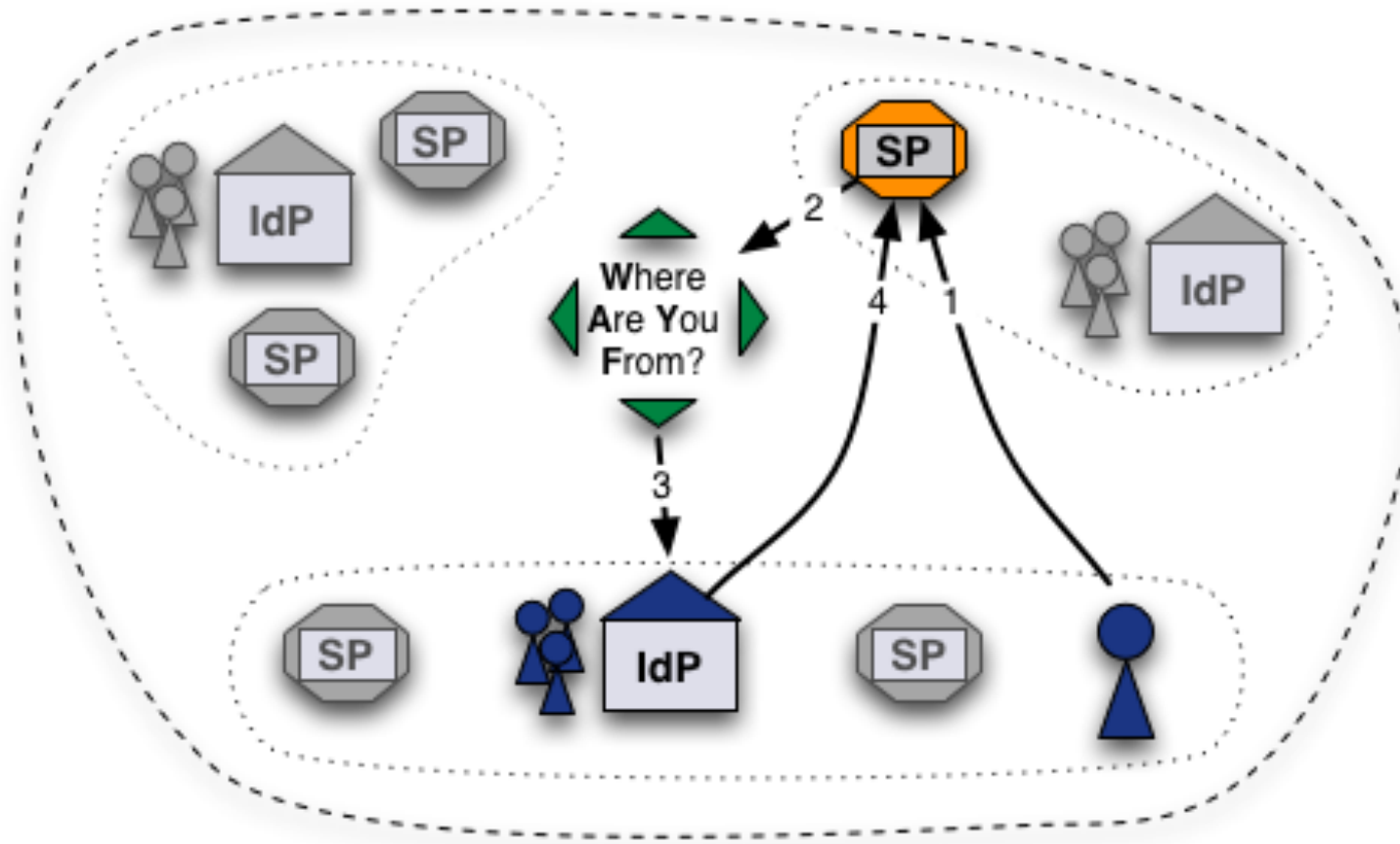


SWITCH

SWITCHaai Team
aai@switch.ch

No Central WAYF for Interfederation

- The classic way: One WAYF per Federation



WAYF achieves high availability through redundancy and IP Anycast.

Alternatives to Central WAYF

- Direct Login URLs
- SWITCH Embedded WAYF
- Shibboleth Embedded Discovery Service



Solution 1: Direct Login URLs

- A separate login link for a specific IdP
- 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 Munich University of Technology](#)

[Login via Eindhoven University of Technology](#)

Composing Login URLs

Service Provider Login Link Composer

This web page lets one compose login links for a Shibboleth-protected resource. The link will redirect users directly to a specific Home Organization for authentication. This way users will skip the WAYF/Discovery Service.

Example link: [Login via SWITCH \(SWITCHaai\)](#)

However, in case your resource has users from more than a hand full of different organizations, it is recommended to use a WAYF/Discovery Service or the [embedded WAYF](#).

Required information

Service Provider Session Initiator Handler URL

Session Initiator /Login /DS

Since Shibboleth 2.5 the default Session Initiator is **/Login**, for older version you might have to use the **/DS** Session Initiator.

Enter the hostname of your SWITCHaai or AAI Test service and select one of the matching entries from the auto-completion feature.

Examples for valid Service Provider Session Initiator handler URLs are

https://myhost.uni.ch/Shibboleth.sso/Login or
https://otherhost.uni.ch/Shibboleth.sso/DS.

Service Provider Target URL

Specify here the URL of the web page that the user shall be redirected after authentication. This is usually a Shibboleth protected page. If you don't have such a page yet, use

https://your.host.ch/Shibboleth.sso/Session provided you are using a Service Provider 2.x. This page then will display all available attributes and other session information.

Identity Provider entityID

Universität Bern (SWITCHaai)

<https://aai-idp.unibe.ch/Idp/shibboleth>

Universität Bern - Test-Homeorg (AAI Test)

<https://aai-testidp.unibe.ch/Idp/shibboleth>

Examples for valid entityIDs

with IdP 2.3 or newer)

provider-initiated URLs work

in some cases but are generally not

recommended to use.



<https://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html>



Solution 2: Embedded WAYF

ILIAS
Universität Bern


OLAT login


Please select your university.

You will be redirected for authentication.

SWITCH

Login




Login with: 


Select the organisation you are affiliated with. ...

Remember selection for this web browser session.

Wählen Sie bitte oben Ihre Organisation aus und klicken Sie auf "Anmelden". Falls dies nicht funktioniert, verwenden Sie bitte [diesen alternativen Zugang](#).

Bei Fragen dazu wenden Sie sich bitte an die [ILIAS Administration](#).


UNIL | Université de Lausanne

Login with: 




SWITCH

Remember selection for this web browser session.














Embedded WAYF

Enter the name of the organisation you are affiliated with...





Last used

-  University of Basel
-  EPFL - EPF Lausanne
-  SWITCH



Universities

-  EPFL - EPF Lausanne
-  ETHZ - ETH Zurich
-  Università della Svizzera Italiana
-  University of Basel
-  University of Bern
-  University of Fribourg
-  University of Geneva
-  University of Lausanne
-  University of Liechtenstein
-  University of Lucerne
-  University of Neuchâtel
-  University of St. Gallen
-  University of Zurich

University Hospitals



-  CHUV - University Hospital Lausanne
-  HUG - Univ. Hospitals of Geneva
-  Inselspital - University Hospital Bern
-  University Hospital Zurich

From other federations


-  Dalarna University
-  Esslingen University of Applied Sciences

Zu

Universities

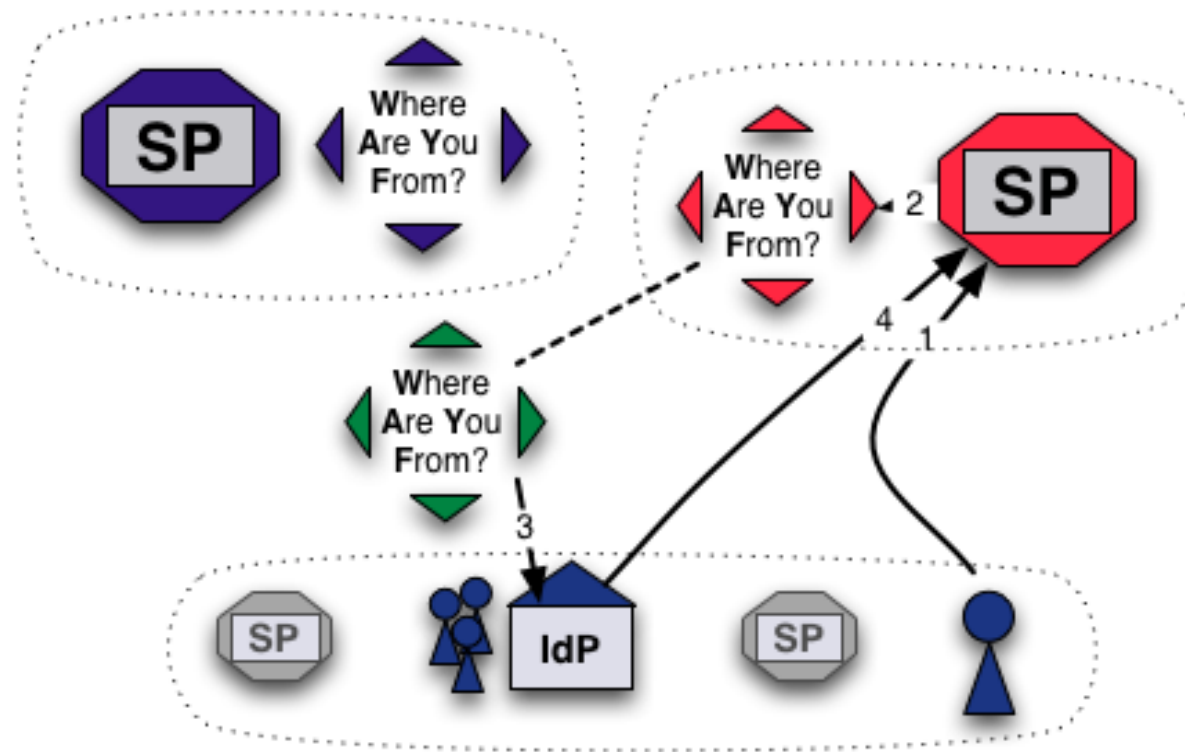
-  ETHZ - ETH Zurich
-  University of Zurich

University Hospitals

-  University Hospital Zurich

Embedded WAYF

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



Information and Configuration

More information about the Embedded WAYF:



<https://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

Configuration Example of Embedded WAYF

```
// Example of how to add Identity Provider from other federations
var wayf_additional_idps = [
    {name:"Esslingen University of Applied Sciences",
      entityID:"https://idp.hs-esslingen.de/idp/shibboleth",
      logoURL:"https://www2.hs-esslingen.de/favicon.ico"
    },
    {name:"Dalarna University",
      entityID:"https://login.du.se/idp/shibboleth",
      logoURL:"https://login.du.se/duse-logo-16x16.png"
    }
];
```

Configuration (2)

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 to use local metadata of SP

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



JSON result of an example discovery feed:
<https://sp.example.org/Shibboleth.sso/DiscoFeed>

```
[
{ "entityID": "https://shibboleth-idp.uni-goettingen.de/uni/shibboleth",
  "DisplayNames": [
    { "value": "Georg-August Universität Göttingen", "lang": "de" },
    { "value": "Georg-August University Göttingen", "lang": "en" }
  ]
},
{ "entityID": "https://login.ntua.gr/idp/shibboleth",
  "DisplayNames": [
    { "value": "National Technical University of Athens", "lang": "en" },
    { "value": "Εθνικό Μετσόβιο Πολυτεχνείο", "lang": "el" }
  ]
},

```

Configuration (3)

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 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, default:false]

var wayf_use_disco_feed = true;
```

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://shibboleth.fhwn.ac.at/idp/shibboleth</Include>
```

```
    <Include>https://idp.it.su.se/idp/shibboleth</Include>
```

```
    <Include>https://tumidp.lrz.de/idp/shibboleth</Include>
```

```
  </MetadataFilter>
```

```
</MetadataProvider>
```

Solution 3: Embedded Discovery Service

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

 <https://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

SWITCH

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

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 (<2.4)	✓	(✓)	
Categories supported	(✓)	✓	
Uses cached recent IdP selection across different services		✓	

When to use what ?

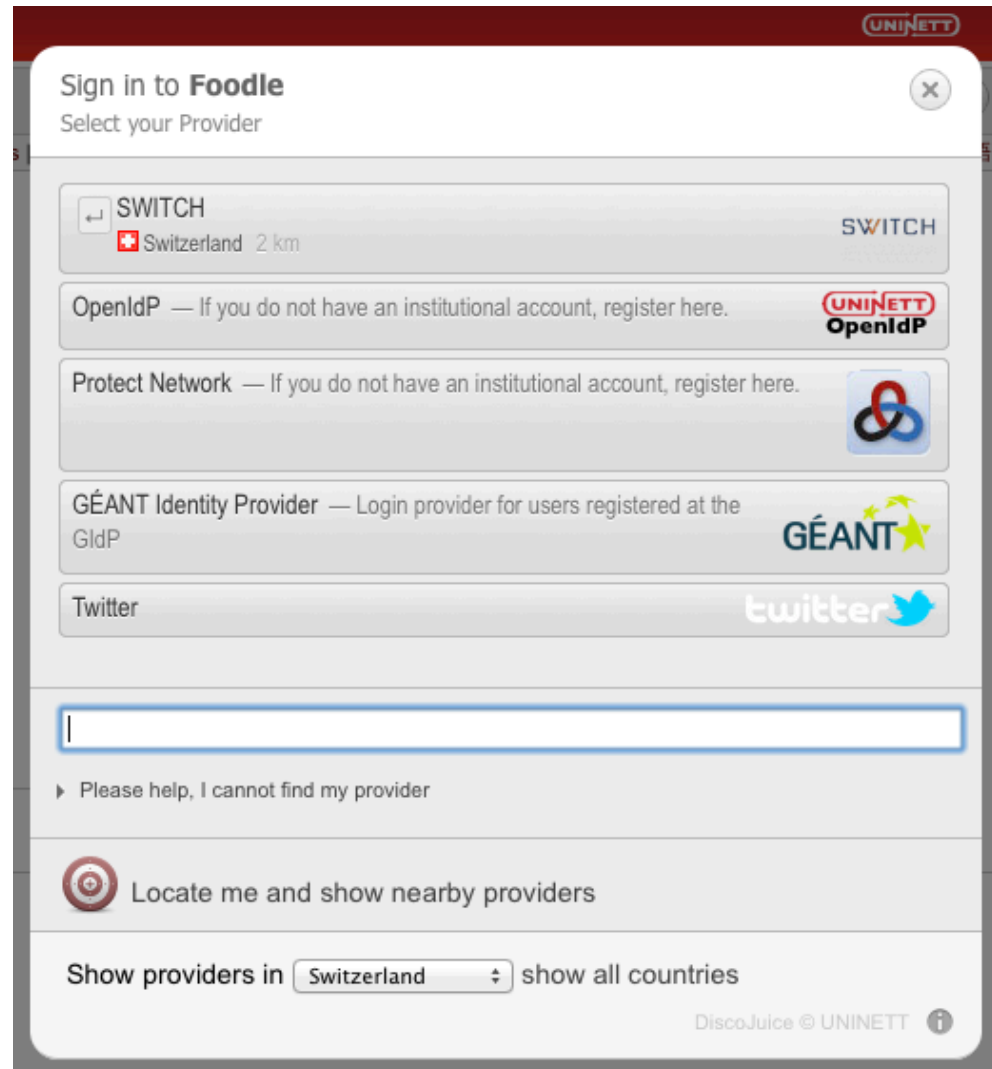
Numbers of IdPs	Login Link(s)	Embedded WAYF SWITCH	EDS  Shibboleth.
1 - 5	✓	✓	✓
1 - 500		✓	✓

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/>



Embedded WAYF: The new features

How to spice up the Home Organisation discovery



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 13. August 2014

Features Overview

- Improved Drop-Down List
- Most Used/Favourite Identity Providers
- Last Used Identity Providers
- Force remember-for-session
- Text customizations
- CSS customization

Embedded WAYF Overview

- WAYF/Discovery Service that shows organisation drop-down list on any web page
- Allows customizing appearance and behaviour of drop-down list
 - Show only certain Identity Providers
 - Change size, color, etc.
- Copy & Paste some HTML code to integrate in web page
<https://wayf.switch.ch/SWITCHaai/WAYF/embedded-wayf.js/snippet.html>
- More information on <http://swit.ch/embedded-wayf>
- Some examples...

```

1 <!-- EMBEDDED-WAYF-START -->
2 <script type="text/javascript"><!--
3 // To use this JavaScript, please access:-
4 // https://wayf.switch.ch/SWITCHaai/WAYF/embedded-wayf.js/snippet.html-
5 // and copy/paste the resulting HTML snippet to an unprotected web page that -
6 // you want the embedded WAYF to be displayed-
7 -
8 -
9 //////////////////////////////////////////////////////////////////// ESSENTIAL SETTINGS ////////////////////////////////////////////////////////////////////
10 -
11 // URL of the WAYF to use-
12 // Examples: "https://wayf.example.org/SWITCHwayf/WAYF"-
13 // [Mandatory]-
14 var wayf_URL = "https://wayf.switch.ch/SWITCHaai/WAYF";-
15 -
16 // EntityID of the Service Provider that protects this Resource-
17 // Value will be overwritten automatically if the page where the Embedded WAYF-
18 // is displayed is called with a GET argument 'entityID' as automatically set by Shibboleth-
19 // Examples: "https://econf.switch.ch/shibboleth", "https://dokeos.unige.ch/shibboleth"-
20 // [Mandatory]-
21 var wayf_sp_entityID = "https://my-app.switch.ch/shibboleth";-
22 -
23 // Shibboleth Service Provider handler URL-
24 // Examples: "https://point.switch.ch/Shibboleth.sso", "https://rr.aai.switch.ch/aai/test/Shibboleth.sso"-
25 // [Mandatory, if wayf_use_discovery_service = false]-
26 var wayf_sp_handlerURL = "https://my-app.switch.ch/Shibboleth.sso";-
27 -
28 // URL on this resource that the user should be returned to after authentication-
29 // Examples: "https://econf.switch.ch/aai/home", "https://olat.uzh.ch/my/courses"-
30 // [Mandatory]-
31 var wayf_return_url = "https://my-app.switch.ch/aai/index.php?page=show_welcome";-
32 -
33 -
34 //////////////////////////////////////////////////////////////////// RECOMMENDED SETTINGS ////////////////////////////////////////////////////////////////////
35 -
36 // Width of the embedded WAYF in pixels or "auto"-
37 // This is the width of the content only (without padding and border). -
38 // Add 2 x (10px + 1px) = 22px for padding and border to get the actual -
39 // width of everything that is drawn.-
40 // [Optional, default: "auto"]-
41 // var wayf_width = 250;-
42 -
43 // Height of the embedded WAYF in pixels or "auto"-
44 // This is the height of the content only (without padding and border). -
45 // Add 2 x (10px + 1px) = 22px for padding and border to get the actual -
46 // height of everything that is drawn.-
47 // [Optional, default: "auto"]-
48 // Example for fixed size: -
49 // var wayf_height = 150;-
50 -
51 // Whether to show the checkbox to remember settings for this session-
52 // [Optional, default: true]-
53 //var wayf_show_remember_checkbox = true;-
54 -
55 // Hide the Logo-
56 // If true, no logo is shown-
57 // [Optional, default: false]-
58 // var wayf_hide_logo = false;-
59 -

```

4 essential settings

Many optional settings:
- Recommended
- Advanced

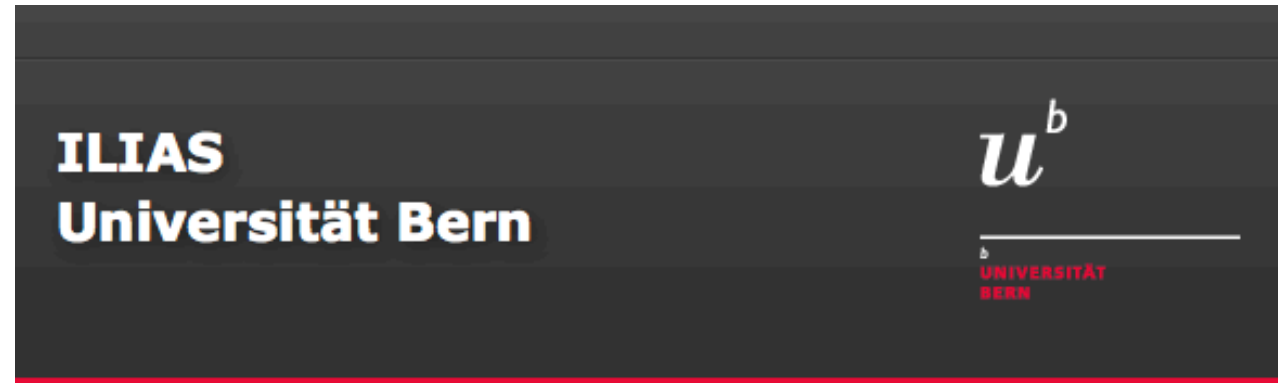
Cyberlearn HES-SO: cyberlearn.hes-so.ch

In portrait format, without using the improved drop-down list






The screenshot displays the website's header with the logo 'CYBERLEARN' and navigation links for 'Blog', 'Team', 'Contact', and 'Langue'. A user status indicator shows 'Non connecté. (Connexion)'. A 'CONNEXION AAI' modal is open, featuring a 'Login with:' section with an 'AAI' icon and a dropdown menu currently set to 'SWITCH'. Below this is a checkbox for 'Remember selection for this web browser session.' and a 'Login' button. A red line points from the text above to the dropdown menu. To the left, a 'NAVIGATION' sidebar lists 'Accueil', 'Blogs du site', and 'Cours'. The main content area is titled 'Moodle HES-SO' and includes a sub-header 'Besoin d'un conseil? Un problème technique?' followed by two photos of staff members, Bernard and Luca, at their desks. Below the photos, text states: 'Au helpdesk de Cyberlearn, Bernard et Luca répondent volontiers à toutes vos questions.' and provides the contact information 'cyberlearn@hes-so.ch - 027/606.90.17'. The footer identifies the team as 'L'équipe Cyberlearn'.

ILIAS Uni Bern: ilias.unibe.ch



In landscape format, using the improved drop-down list

Login with:

 SWITCH  AAI 

Remember selection for this web browser session.

Wählen Sie bitte oben Ihre Organisation aus und klicken Sie auf "Anmelden". Falls dies nicht funktioniert, verwenden Sie bitte [diesen alternativen Zugang](#).

Bei Fragen dazu wenden Sie sich bitte an die [ILIAS Administration](#).

ADAM Unibas: adam.unibas.ch

UNIVERSITÄT BASEL

ADAM
ADVANCED DISTRIBUTION & MORE

Herzlich Willkommen auf ADAM

ADAM ist eine webbasierte Applikation für den Austausch von Dateien. Hilfe finden Sie [hier](#).
Die Neuerungen von ADAM ab dem Herbstsemester 2014 finden Sie [hier](#).

Login via AAI

Login für alle schweizerischen Universitäten und Fachhochschulen sowie allen an SWITCH AAI angeschlossenen Organisationen .

SWITCH
aai

Login with:
Enter the name of the organisation you are affiliated with...

Remember selection for this web browser session.

Login

With some custom styling, integrated in container box

OLAT: www.olat.uzh.ch

Please select your language English [Help ?](#)

OLAT - Online Learning And Training

OLAT login

Please select your university.

You will be redirected for authentication.

SWITCH

[Guest access](#)

Alternative login possibilities

- Don't you belong to one of the universities mentioned above? [Next](#)

Yes, even that is the Embedded WAYF but with many customizations

Improved Drop Down List

- Activate by setting:

```
var wayf_use_improved_drop_down_list = true;
```

- Available since February 2014
- Has to be enabled manually for now
 - Requires reloading of additional JavaScript incl. JQuery
 - Goal was go gain experience
- Adds same features to the Embedded WAYF that have been available on the central WAYF (wayf.switch.ch)

AAI Attribute Viewer

SWITCH

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.

Name, domain, location can be entered to search organisation.

Login with: > AAI

> SWITCH

Enter the name of the organisation you are affiliated with...

Last used

- > SWITCH
- CERN
- VHO - Virtual Home Organization

Universities

- EPFL EPFL - EPF Lausanne
- ETHZ - ETH Zurich
- USI - Universita della Svizzera Italiana
- University of Basel
- University of Bern
- University of Fribourg
- University of Geneva
- UNIL - University of Lausanne
- University of Liechtenstein
- University of Lucerne
- University of Neuchâtel
- University of St. Gallen
- UZH - University of Zurich

Universities of Applied Sciences

- BFH - Bern University of Applied Sciences

Logos are dynamically loaded and displayed if available

Most Used/Favourite Identity Providers

- Activate by setting:

```
var wayf_most_used_idps = new Array(  
    "https://aai-logon.unibas.ch/idp/shibboleth",  
    "https://aai.unil.ch/idp/shibboleth"  
);
```

- If set, shows organisations at top of the drop-down list
- Identity Provider's entityIDs has to be configured manually

Last Used Identity Providers

- Activated by default (set to 3). To deactivate:

```
var wayf_num_last_used_idps = 0;
```

- Shows last used organisations at top of the drop-down list
- Information read from web browser cookie

Most/Last Used Identity Providers

Login with: > AAI

> SWITCH

Enter the name of the organisation you are affiliated with...

Last used

- > SWITCH
- CERN
- > VHO - Virtual Home Organization

Most frequently used organisations

- ☼ University of Basel
- UNIL University of Lausanne

Universities

- EPFL EPFL - EPF Lausanne
- ETHZ ETHZ - ETH Zurich
- USI Università della Svizzera Italiana
- ☼ University of Basel
- u^b University of Bern

Set by SP
Administrator

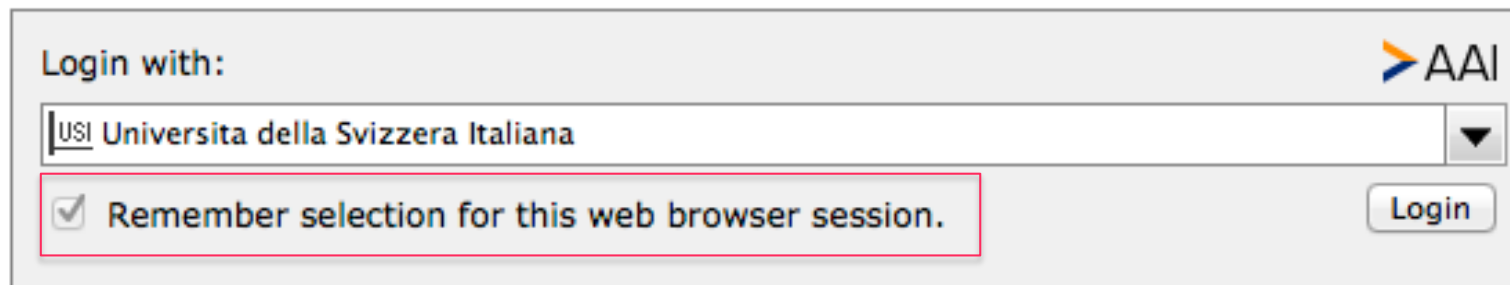
Only shown
if at least one
organisation
has been
used previously

Force Remember Session

- Activate setting:

```
var wayf_force_remember_for_session = true;
```

- Forces automatic login if other service is using the Embedded WAYF/ Central WAYF by SWITCH
- Useful if user is sent to additional AAI services after first login
- Valid only for current web browser session, is reset after browser restart




The screenshot shows a login interface. At the top left, it says "Login with:". To the right is the AAI logo. Below this is a dropdown menu showing "USI Università della Svizzera Italiana". A red box highlights a checkbox labeled "Remember selection for this web browser session." which is checked. To the right of the checkbox is a "Login" button.

Text Customization

- All text strings can be customized:


```
var wayf_overwrite_checkbox_label_text =  
    'Save setting for today';  
var wayf_overwrite_submit_button_text = 'Go';  
var wayf_overwrite_intro_text =  
    'Select your Home Organisation to log in';  
var wayf_overwrite_most_used_idps_text =  
    'Most popular';  
var wayf_overwrite_last_used_idps_text =  
    'Previously used';  
var wayf_overwrite_from_other_federations_text =  
    'Other organisations';
```

Customized Text:

Select your Home Organisation to log in 

▼




Save setting for today

Select your Home Organisation to log in 



▼

Enter the name of the organisation you are affiliated with...

Previously used

-  SWITCH
-  CERN
-  VHO - Virtual Home Organization

Most popular

-  University of Basel
-  University of Lausanne

Universities

CSS Customizations

If the basic appearance configuration options are not sufficient:

#wayf_div	Container for complete Embedded WAYF
#wayf_logo_div	Container for logo
#wayf_logo	Image for logo
#wayf_intro_div	Container of drop-down list intro label
#wayf_intro_label	Label of intro text
#IdPList	The form element
#user_idp	Select element for drop-down list
#wayf_remember_checkbox_div	Container of checkbox and its label
#wayf_remember_checkbox	Checkbox to remember selection
#wayf_remember_checkbox_label	Text of checkbox
#wayf_submit_button	Submit button

Summary

- Embedded WAYF integrates user-friendly and customizable Home Organisation selection into any web page
- Can also be used as standard Shibboleth Discovery Service. In shibboleth2.xml configuration use for example:

```
<SSO discoveryProtocol="SAMLDS"  
      discoveryURL="https://www.example.ch/ew.html">  
  SAML2  
</SSO>
```

Page ew.html must contain Embedded WAYF.

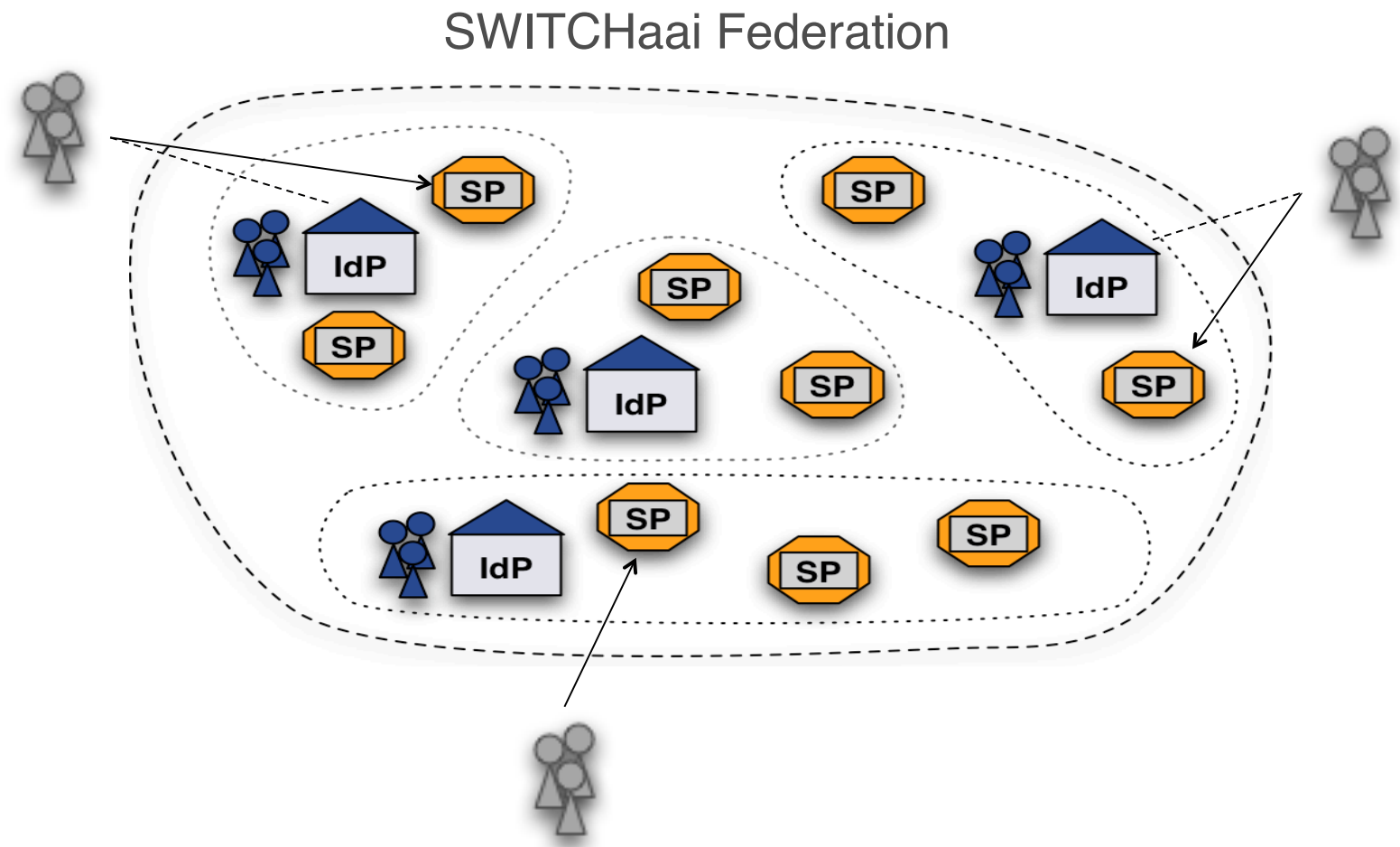
Virtual Home Organization & Guest Login



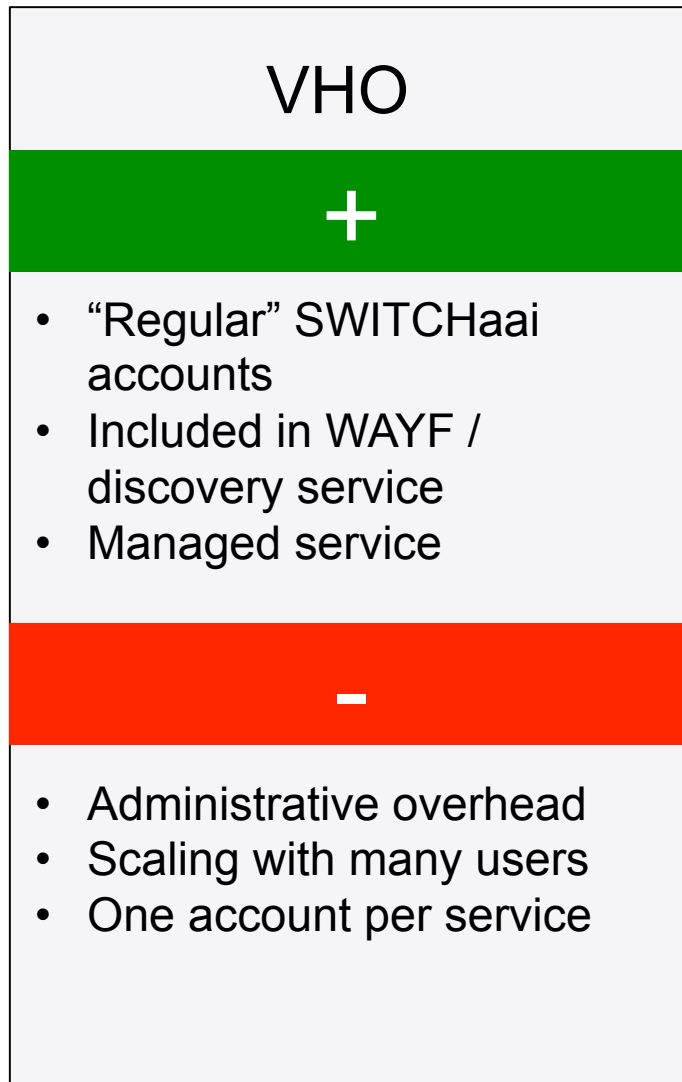
SWITCH

SWITCHaai Team
aai@switch.ch

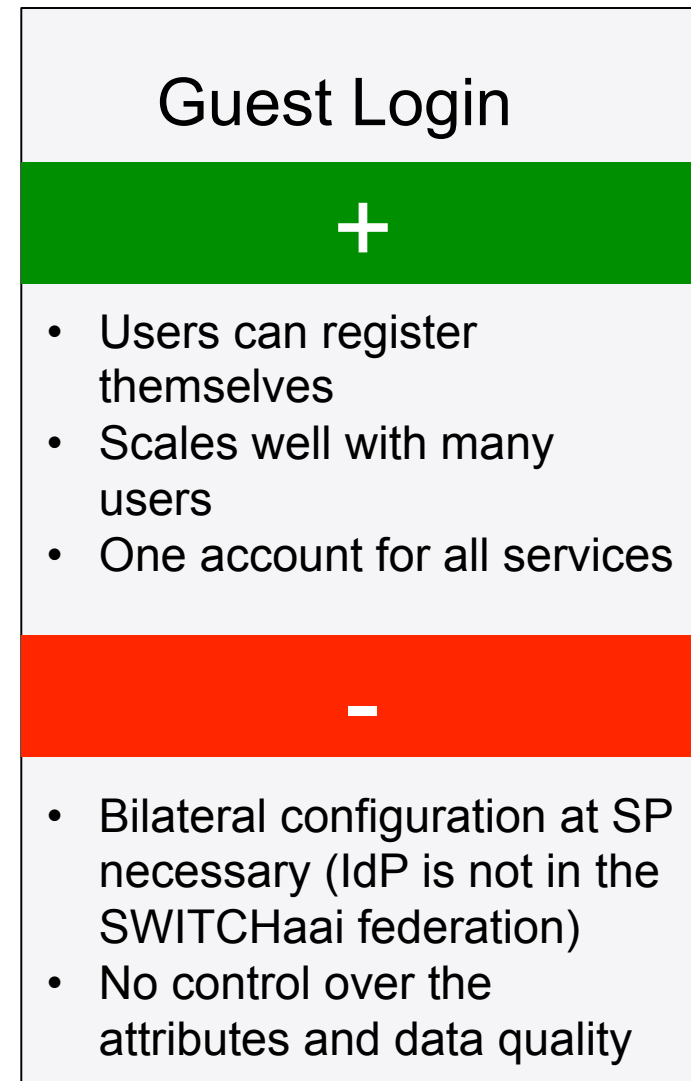
Motivation – loose relationships



Possible solutions



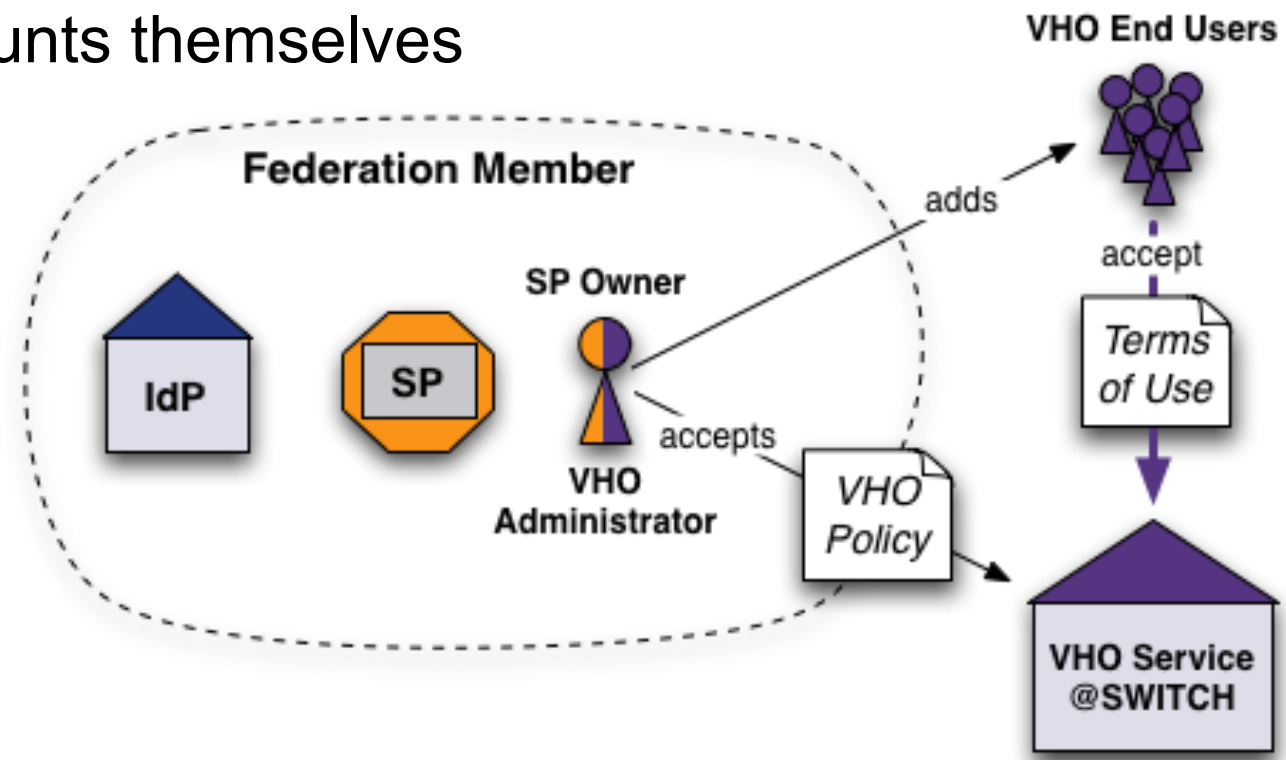
<https://www.switch.ch/aai/vho>



<https://www.switch.ch/aai/support/serviceproviders/guest-login.html>

SWITCH VHO Service

- Targeted end user groups
 - Attendees of a further education or other training
 - Collaboration projects from private companies or foreign universities, which are not in the SWITCHHaai federation
- Groups are created by SWITCH
- Resource owners can manage end user accounts themselves



VHOtools - Key functionalities

- Administrator services
 - Manage one or more groups, which can be structured hierarchically
 - Define description for each group (support contact, mail templates)
 - Create new user accounts with some AAI attributes (E-Mail, entitlement, ...)
 - Modify, delete and expire user accounts (incl. password resets)
 - Import and export of user lists
 - View group statistics
 - Account expiration reminder
- End user services
 - Login
 - User self-service password changes
 - Support information

Screenshots VHO tool (1)

demogroupa : 81 active - 18 expired - 0 deleted users

Choose action: **Set expiration date = now**
 Choose expiration date
 Update field
 Delete
 Purge
 Download HTML

Search: Search
 (use * or % for wildcard search. Search is performed on username, first and last name, id and custom fields)









































long Inactive orphans

3 4 5 6 ... 9 10 Next »

search users

sort by any attribute

shortcuts to: edit, expire, delete & password reset

	Expiration date	Last modification date	Last login date	Actions
<input type="checkbox"/>	dga-user01	09.11.2007	31.07.2012	   
<input type="checkbox"/>	dga-user02	09.11.2007	26.06.2012	   
<input type="checkbox"/>	dga-user03	03.07.2011	13.08.2012	   
<input checked="" type="checkbox"/>	dga-user04	01.05.2013	25.06.2012	   
<input type="checkbox"/>	dga-user05	11.05.2014	12.05.2012	   
<input type="checkbox"/>	dga-user06	05.06.2014	07.08.2012	   
<input type="checkbox"/>	dga-user07	30.08.2012	10.08.2012	   
<input type="checkbox"/>	dga-user08	09.08.2014	08.06.2012	   
<input type="checkbox"/>	dga-user09	05.2012	07.07.2012	   
<input type="checkbox"/>	dga-user10	1.10.2014	29.06.2012	   

predefined actions

user's state indicator

Choose action:

Page: << Previous 1 2 3 4 5 6 ... 9 10 Next >>

View: short medium long Inactive orphans

Legend: active expired deleted

paged users list & custom views

dates: creation, last modification, last login, expiration & custom info

Screenshots VHO tool (2)

Create or modify user accounts using web forms...

demogroupa : Edit user

Fields marked with an asterisk (*) are mandatory.

Username dga-user06
uniqueID d642431@test.vho-switchchai.ch

Last name * Walker
First name * William
E-mail * William.Walker@dga.edu.us
Entitlement * http://example.edu.org/dga

Business phone number +1 4444 333 22 06
e.g. +41 44 268 15 05

Business postal address Golden Lane 6
6000 San Francisco

Preferred Language en

Description

Affiliation affiliate
Home organization vho-switchchai.ch
Home organization type vho

Expiration date or enter date 05.06.2014
*The date format is dd.mm.YYYY
After the expiration date is reached the user won't be able to login with his VHO account*

Custom field 1
*This is a field for your own purpose, i.e.: project, training or applicant name
It will never be released to any resource*

Custom field 2
*Another field for your own purpose
It will never be released to any resource*

demogroupa : View active user

Expire Delete Reset password Edit

Username: dga-user06
uniqueID: d642431@test.vho-switchchai.ch

Last name: Walker
First name: William
E-mail: William.Walker@dga.edu.us
Entitlement: http://example.edu.org/dga

Business phone number: +1 4444 333 22 06
Business postal address: Golden Lane 6
6000 San Francisco


Preferred Language: en
Affiliation: affiliate
Home organization: test.vho-switchchai.ch
Home organization type: vho

Expiration date: 05.06.2014 14:03:11
Creation date: 09.11.2007 15:48:35
Last modification date: 09.11.2007 15:48:35
Last login date: 07.08.2012 14:03:11

Cancel Save

Screenshots Guest Login

Registration



[Login](#) | [About](#) | [Help](#) | [Terms of Use](#)

1 Account Creation 2 Email Confirmation 3 Account Activation

Please complete the following form to create a new Guest Login account.


Authentication Data	
Email (login name)	<input type="text"/>
Password	<input type="password"/>
Re-type Password	<input type="password"/>

Required Data	
First Name	<input type="text"/>
Last Name	<input type="text"/>
How much is: 22 + 12 + 4	<input type="text"/>

Optional Data	
Business Address	<input type="text"/>
Business Phone	<input type="text"/>
Home Address	<input type="text"/>
Home Phone	<input type="text"/>
Mobile Phone	<input type="text"/>
Preferred Language	<input type="text" value="English"/>

I fully understand and accept the [Terms of Use](#) for creating and using a Guest Login account.

Registration




[Login](#) | [About](#) | [Help](#) | [Terms of Use](#)

1 Account Creation 2 Email Confirmation 3 Account Activation

✓ Congratulations, your account was successfully registered. Before your account can be activated, the email address you provided has to be verified. Therefore, an email has been sent to thomas.baerecke@switch.ch. Please follow the instructions in the email in order to confirm your email address.

Due to SPAM filters it may take a few minutes until you receive the email. The email address must be verified within 5 days. Otherwise, the account will be discarded.

Registration



[Login](#) | [About](#) | [Help](#) | [Terms of Use](#)

1 Account Creation 2 Email Confirmation 3 Account Activation

✓ Your email address thomas.baerecke@switch.ch was successfully verified and your Guest Login account is now active. You should soon receive a confirmation email with further details.

When asked to authenticate at the login page of the Guest Login, use as login name your email address you provided during account creation and the password.

Groups Inside FHNW:

Why it's not just another AAI SP

Michael Hausherr, Business Applications FHNW



Agenda

- Introduction (Groups) Inside FHNW
- Issue 1: authentication for different user groups
- Issue 2: simple creation of collaboration space
- Issue 3: End-user choice of Identity Provider
- Findings
- Questions?

Inside FHNW

Vision and high level goals

Vision (Zielsystem)

«Inside FHNW unterstützt die Hochschulen und das Zusammenwirken von Mensch und Campusgrenzen sinnvoll erscheinen. Effizienz, Effektivität und gemeinsamen Zeitgemässe Forderungen sind ein fortwährendes Anliegen der FHNW-Angehörigen der FHNW. Das Fortanfordert die Organisationkultur, die Partizipation, den Wissenstransfer sowie den Austausch untereinander als auch mit der wissenschaftlichen Gemeinschaft – national und international – und schafft dadurch Raum für Kreativität.»

Übergeordnete Zielsetzung

- Hohe Unterstützung der FHNW-Angehörigen
- Nachhaltige Wissenssicherung
- Förderung der hochschulübergreifenden Zusammenarbeit

«Inside FHNW» is **THE** central entry point to **ALL** relevant information, tools and applications that are **integrated** into the FHNW system landscape.

Guiding principles (1/2)

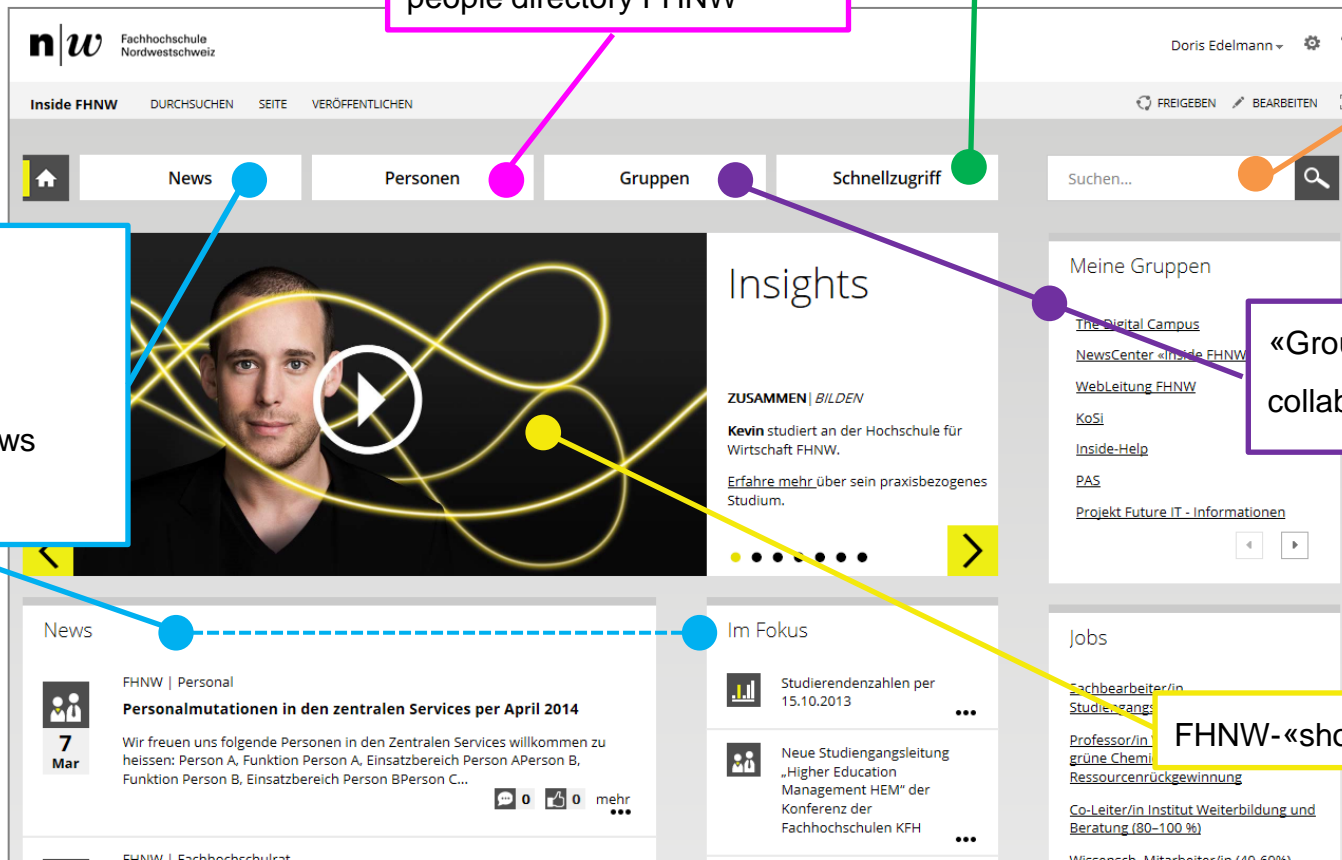
At the center are the members of FHNW (staff and students) with their individual needs



Guiding principles (2/2)



Key features (stage 1)



Optimized access to existing tools and platforms

people directory FHNW

search across all Inside content

Transparent news center
personalized news on start page

«Groups Inside FHNW» collaboration platform

FHNW-«showcase»

Groups Inside FHNW: core functionality

Document collaboration



Collectively work on documents and store them in a central location.

Create collaboration space



All FHNW members, no administrator needed

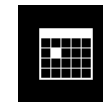


Task list



Plan, assign and supervise tasks.

Group calendar



Perfect overview of all common dates.

Discussion forum



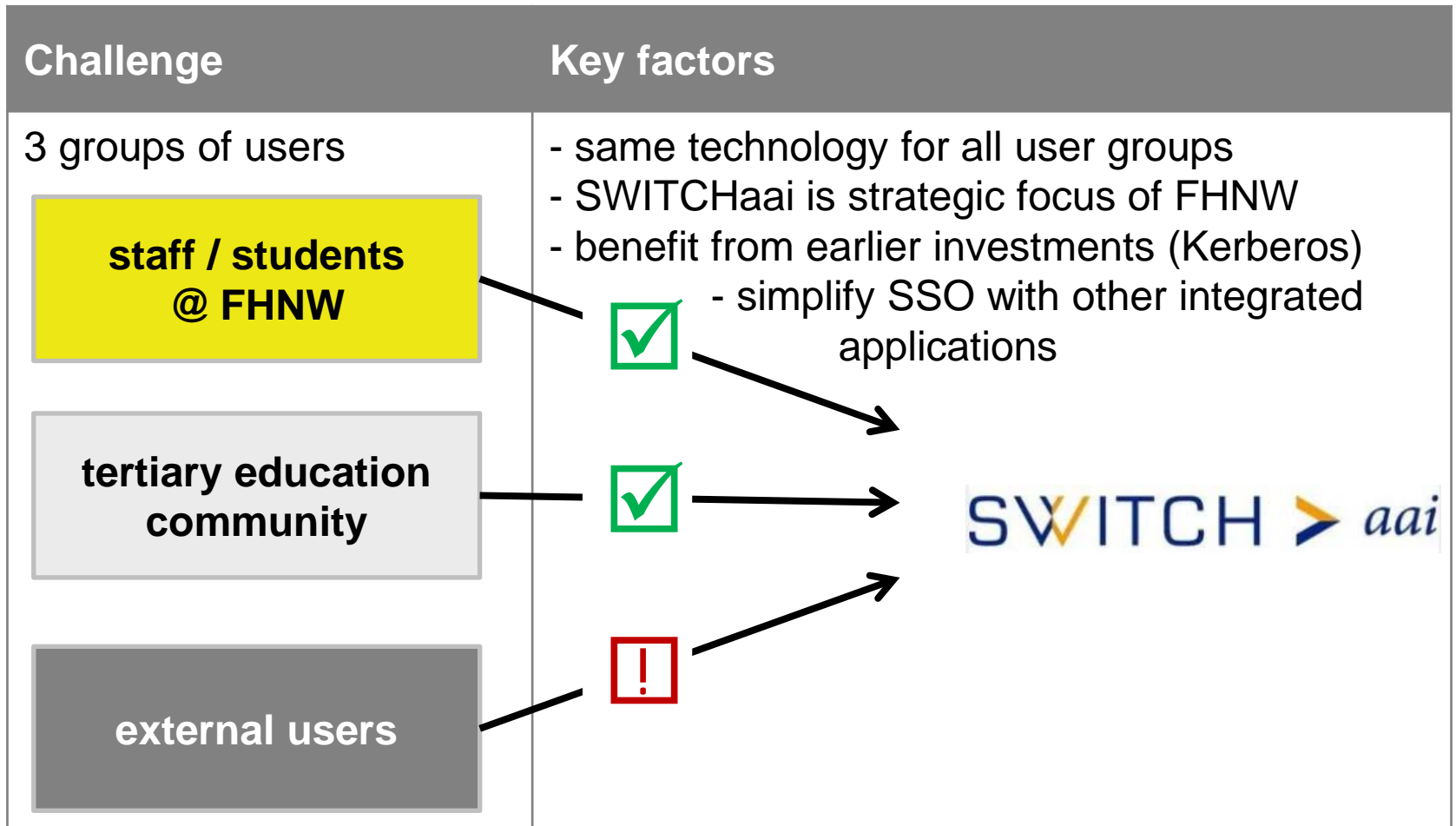
Efficient group communication.

Collaboration spaces: as diverse as the groups

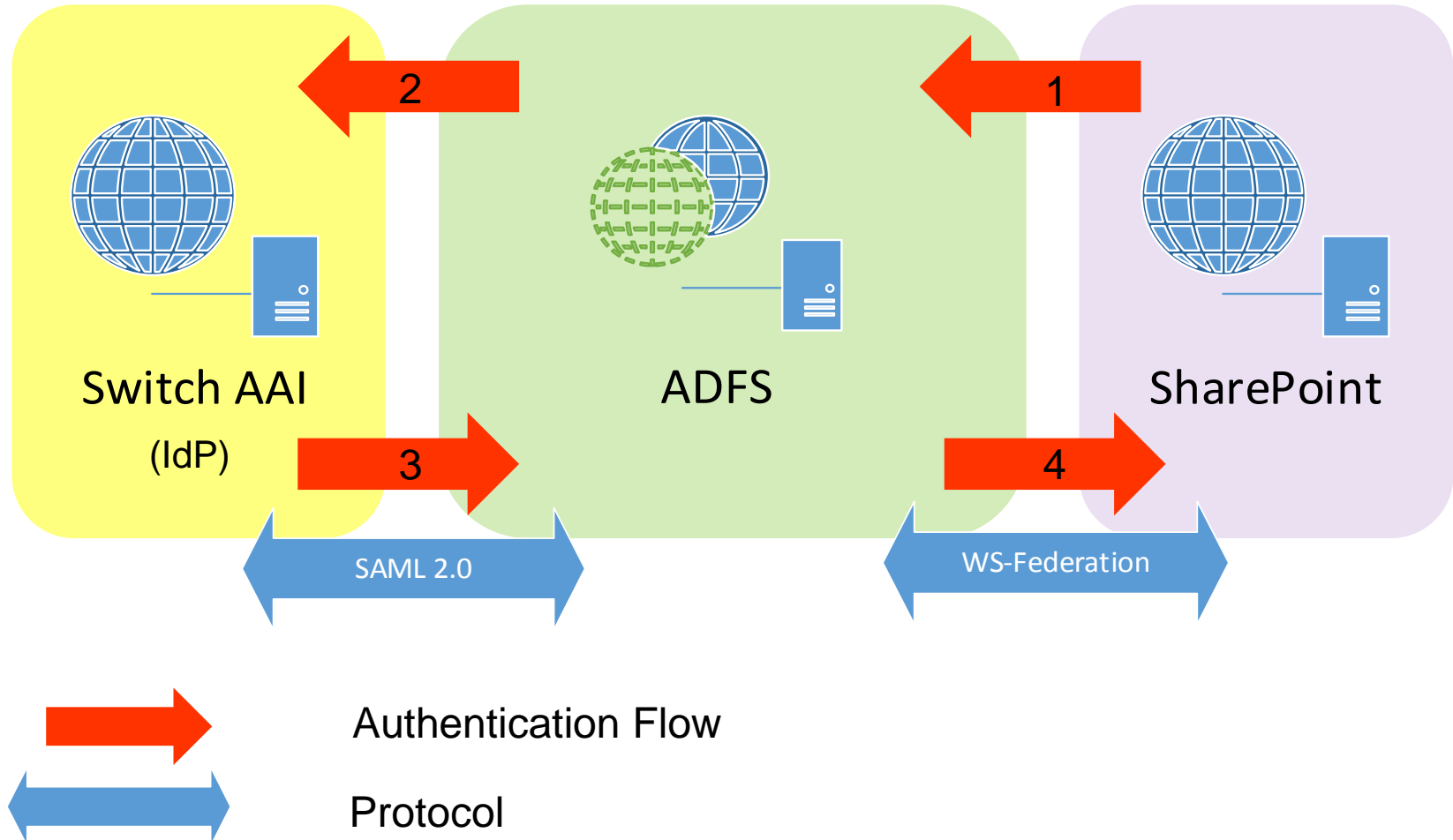
Users should not be overwhelmed by the full SharePoint functionality in a newly created collaboration space, so three templates for different use cases have been created:

		Types of collaboration spaces		
		File share	theme group	project group
Core features	calendar	X	X	X
	document library	X	X	X
	discussion forum		X	X
	task list		X	X
	Image gallery	extendable according to needs	extendable according to needs	X
	contact list			X
	link list			X
Additional functionality				extendable according to needs

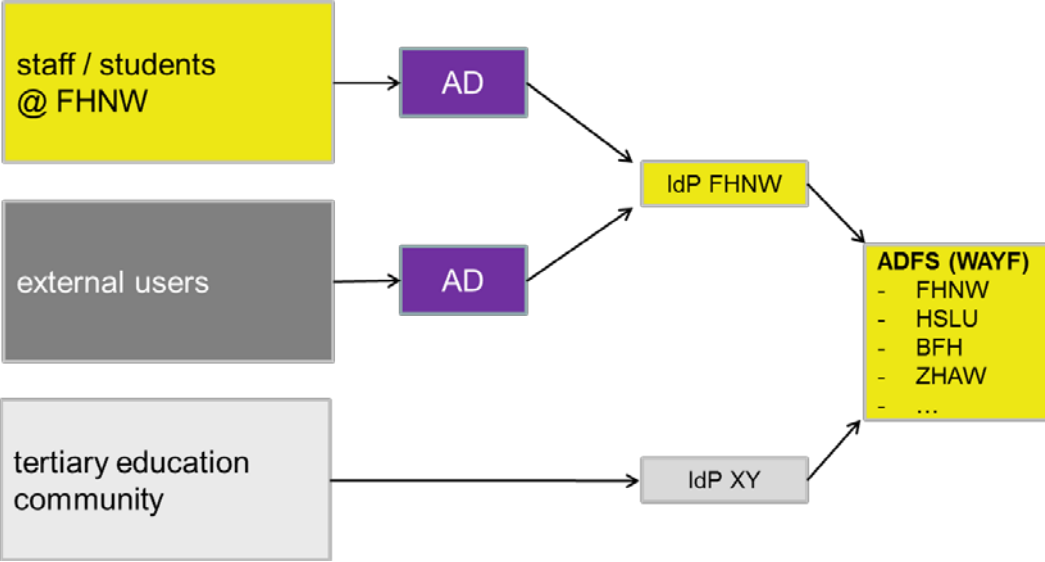
Issue 1: authentication for different user groups



Using ADFS as the gateway between AAI and SharePoint



Issue 2: simple creation of collaboration space

Requirements	Architecture
<ul style="list-style-type: none"> - possible for every staff member or student - without administrator intervention - integrated invitation of external users 	<p>Additional directory (AD) for external users</p>  <pre> graph LR S[staff / students @ FHNW] --> AD1[AD] E[external users] --> AD2[AD] T[tertiary education community] --> IdP_XY[IdP XY] AD1 --> IdP_FHNW[IdP FHNW] AD2 --> IdP_FHNW IdP_FHNW --> ADFS[ADFS WAYF] IdP_XY --> ADFS ADFS --- L["- FHNW
- HSLU
- BFH
- ZHAW
- ..."] </pre> <p>VHO not suitable for this case, because comprehensive integration is not possible</p>

Implementation

Neuen User-Account erstellen ✕


Erstellen Sie einen neuen User. Das Passwort wird dem User per E-Mail zugestellt.

Vorname*

Nachname*

E-Mail*

Meldung von Webseite ✕



Der User wurde erfolgreich angelegt. Der Username ist michael.test.hausherr@guest.fhnw.ch

Gruppen - Neues Element

Vielen Dank, dass Sie "Groups *inside* FHNW" verwenden.

- Bitte füllen Sie das Formular vollständig aus; Felder mit einem Stern (*) sind Pflichtfelder
- Für externe Gruppen-Mitglieder muss zuerst ein FHNW-User-Account eröffnet werden. Sie können dies direkt in diesem Formular über die Schaltfläche "Neuen User-Account eröffnen" erledigen. Selbstverständlich können Sie später weitere Mitglieder in Ihren Gruppenraum einladen.
- Schliessen Sie Ihre Gruppenraum-Bestellung mit "Speichern" ab

Ihr Gruppenraum wird Ihnen in wenigen Minuten zur Verfügung stehen. Sie erhalten eine E-Mail mit allen wichtigen Informationen.

Gruppenname *

Beschreibung

Geben Sie eine kurze Beschreibung zum Gruppenraum an

Ablaufdatum *

Bitte definieren Sie bis wann der Raum genutzt wird. Nach Ablauf dieses Datums erhalten Sie die Möglichkeit, die Laufzeit des Gruppenraums zu verlängern oder ihn zur Archivierung freizugeben.

Ansprechperson *

Neuen User-Account erstellen
Diese Person ist die primäre Kontaktperson und trägt die organisatorische Verantwortung für den Gruppenraum

Administratoren *

Neuen User-Account erstellen
Diese Personen haben Vollzugriff auf den Gruppenraum und sind erste Kontaktstelle bei Supportfragen der übrigen Gruppenmitgliedern.

Mitwirkende

Neuen User-Account erstellen
Diese Personen dürfen alle Inhalte des Gruppenraumes lesen sowie neue Inhalte hinzufügen und bestehende Inhalte bearbeiten

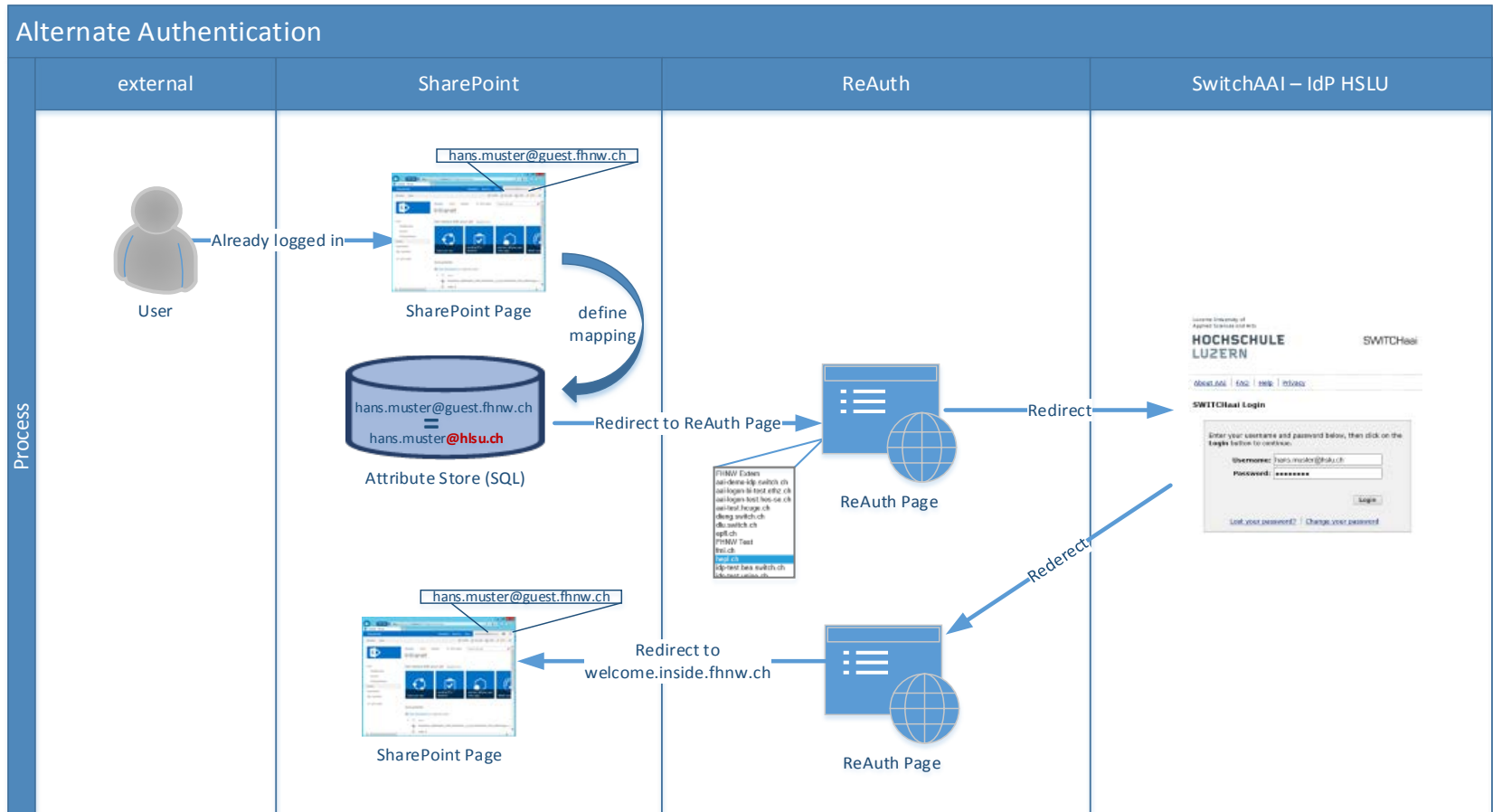
AAI user categories at FHNW

- «member» group
 - affiliation: staff, member (max.musterdozent@fhnw.ch)
 - affiliation: student, member (max.musterstudent@student.fhnw.ch)
- «affiliate» group
 - affiliation: affiliate (max.musterpartner@guest.fhnw.ch)

Issue 3: End-user choice of Identity Provider

Requirements	Architecture
<ul style="list-style-type: none">- external users should be able to use an AAI-enabled account of their choice to access a collaboration space- extendable to include further login scenarios (i.e. Google) at a later stage	<ul style="list-style-type: none">- SharePoint does not need to know about how the user was authenticated- ADFS server provides possibility to link different login credentials to the same SharePoint user- Self-service app allows user to switch login method (IdP) and re-authenticate himself <p>See also the slides of the 'AAI and ADFS with SharePoint' workshop https://www.switch.ch/aai/events/adfs-sharepoint-2013/</p>

Choosing an alternate authentication provider



Findings

- external user integration key success factor for collaboration platform (a few hundred accounts in six months)
- Shibboleth interoperability is good
 - ADFS (V2.1 in production, V3 in testing)
 - SAP Enterprise Portal (NW7.4 in production, NW7.3 used before)
- added complexity (architecture, operation, troubleshooting)
- important to spread awareness that AAI User is not always a student or staff member
- from an AAI point of view more and more Services will be «hidden» behind a portal SP or protocol gateway SP (i.e. ADFS) rather than have their own SP
- some issues with non-browser access (i.e. MS Office applications) left

Questions?



Contact

Michael Hausherr

Business Applications

Team leader ERP & Collaboration group

+41 56 202 71 56

michael.hausherr@fhnw.ch

Authorizing Access to SPs



SWITCH

SWITCHaai Team
aai@switch.ch

Berne, 13 August 2014

Require valid-user

"Considered harmful!"

Don't accept just any valid user

- The single access rule *Require valid-user* is usually not well-suited. This would allow any AAI user to access your resource, including guest users and VHO users. In most cases, that's not what you want to allow.
- You should require specific attribute values, e.g. specific affiliations like *staff/student/faculty*. (Guest and VHO users just have affiliation *affiliate*).
- You should take care while designing access control rules.

Content Protection and Session Initiation

- Before access control can occur, a Shibboleth session must be initiated on the SP.
 - Session initiation and content protection go hand in hand.
 - Session initiation is done by the Shibboleth SP software.
- Requiring a session means the user has to authenticate.
- Only authenticated users can access protected content.
- AAI attributes are available only if a valid session has been initiated.

Where to Require a Shibboleth Session

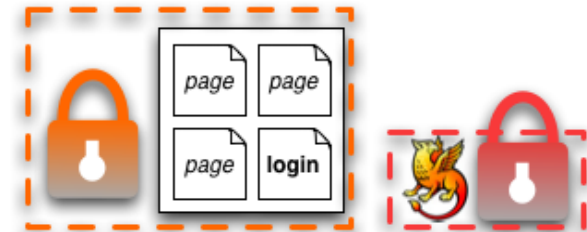
- **Whole application with "required" Shibboleth session**

- Easiest way to protect a set of documents
- No other authentication methods possible like this
- Problems with lost HTTP POST requests



- **Whole application with "lazy" Shibboleth session**

- Also allows for other authentication methods
- Authorization can only be done in application



- **Only page that sets up application session**

- Well-suited for dual login
- Application can control session time-out
- Generally the best solution



Options for Access Control

3 ways to protect an application with access rules:

- **Apache Access Rules (Apache only)**
 - Static configuration
(Changes require restart of Apache)
 - Directory configuration (.htaccess) file
(Restricted to existing directories in the filesystem)
- **Shibboleth XML Access Control (Apache, IIS, others)**
 - Configuration in shibboleth2.xml (or via .htaccess)
- **Application Access Control (Apache, IIS, others)**
 - Access control done by application itself based on attribute values

Options for Access Control: Overview

	1.a apache2.conf <VirtualHost>	1.b .htaccess	2. XML AccessControl *	3. Application Access Control
⊕	<ul style="list-style-type: none"> Easy to configure Can also protect locations or virtual files URL Regex 	<ul style="list-style-type: none"> Dynamic Easy to configure 	<ul style="list-style-type: none"> Platform independent Powerful boolean rules URL Regex Dynamic 	<ul style="list-style-type: none"> Very flexible and powerful with arbitrarily complex rules URL Regex Support
⊖	<ul style="list-style-type: none"> <i>Only works for Apache</i> Not dynamic Very limited rules 	<ul style="list-style-type: none"> <i>Only works for Apache</i> Only usable with "real" files and directories 	<ul style="list-style-type: none"> XML editing Configuration error can prevent SP from restarting 	<ul style="list-style-type: none"> You have to implement it yourself You have to maintain it yourself

* Configured in RequestMap or referenced by an .htaccess file

Apache Access Rules

Example:

```
# Force user to authenticate on protected-directory
<Location /protected-directory>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession true
  Require shib-attr homeOrganizationType university uas
</Location>
```

- Enforces Shibboleth session for all resources at the path `/protected-directory`
- User must be member of a university or a university of applied sciences (*university uas*).

Notes for Apache 2.2

- The option *ShibCompatWith24 On* is recommended in case Apache 2.2 is used (to simplify a later migration).
- This option is provided by the Shibboleth SP Apache module. It adds support for extended "Require" rules that the Shibboleth SP supports in Apache 2.4.

*In case you already use Apache 2.4, you need to remove the option *ShibCompatWith24 On*.*

Apache: Static vs. Directory Configuration

- **Static configuration:**

- Access rules are configured in main configuration.
(e.g. `/etc/apache/sites-available/www.example.org`)
- Changes require restart of Apache.
- Applicable to "real" files and directories as well as to virtual files and locations

```
# Force user to authenticate on protected-directory
<Location /protected-directory>
    AuthType shibboleth
    ShibCompatWith24 On
    ShibRequestSetting requireSession true
    Require shib-attr homeOrganizationType university uas
</Location>
```

Apache: Static vs. Directory Configuration

- **Directory configuration:**

- Access rules are configured in `.htaccess` files in the (filesystem) directories that need to be protected.
(e.g. `/var/www/protected-directory/.htaccess`)
- Changes take effect immediately.
- Not applicable to virtual files and locations

Example:

```
/var/www/protected-directory/.htaccess:
```

```
# Force user to authenticate
AuthType shibboleth
ShibCompatWith24 On
ShibRequestSetting requireSession true
Require shib-attr homeOrganizationType university uas
```

Shibboleth XML Access Control

- Access rules are directly embedded in shibboleth2.xml file or included from external file.
- The Shibboleth SP dynamically loads access rules. Changes take effect immediately.
- If using Apache, XML access rules defined in an external file might be included in an .htaccess file.
(Not discussed here; refer to the comprehensive documentation on our SWITCHaai website.)

Shibboleth XML Access Control: shibboleth2.xml

Proper place of XML access rules in shibboleth2.xml:

```
<SPConfig ...>
  [...]
  <RequestMapper type="Native">
    <RequestMap applicationId="default">
      <Host name="www.example.com">
        [...]
      </Host>
      [...]
    </RequestMap>
  </RequestMapper>

  <ApplicationDefaults ...>
    [...]
  </ApplicationDefaults>
  [...]
</SPConfig>
```

Shibboleth XML Access Control: Example

```
...  
<Host name="www.example.org">  
  <Path name="protected-directory" authType="shibboleth" requireSession="true">  
    <AccessControl>  
      <AND>  
        <Rule require="affiliation">student</Rule>  
        <OR>  
          <Rule require="homeOrganization">ethz.ch</Rule>  
          <Rule require="homeOrganization">uzh.ch</Rule>  
        </OR>  
        <NOT>  
          <!-- assert that VHO users are never allowed -->  
          <Rule require="homeOrganization">vho-switchaai.ch</Rule>  
        </NOT>  
      </AND>  
    </AccessControl>  
    <Path name="unprotected" authType="shibboleth" requireSession="false" />  
  </Path>  
</Host>  
...
```

Shibboleth XML Access Control: Example

Meaning:

- Affiliation MUST be "student"
- Home Organization MUST be either "ethz.ch" or "uzh.ch"
- Home Organization MUST NOT be "vho-switchaai.ch"
(Although this last rule is always fulfilled because of the previous rules, this requirement is explicitly expressed, using a NOT operator.)

Shibboleth XML Access Control: Apache

- Using Apache, to support XML Access Rules embedded in shibboleth2.xml, you still need something similar to the following configuration (else, the rules won't take effect).

```
# Activate Shibboleth but don't enforce a session
<Location />
  AuthType shibboleth
  Require shibboleth
</Location>
```

Application Access Control

- Application can access and use Shibboleth attributes by reading them from the web server environment.
- The Shibboleth SP exports the attributes to a set of environment variables (Apache) or HTTP request headers (IIS)
- Attributes then can be used for access control.
- The names of the attributes may differ between various application containers (e.g. prefixed with "AJP_" if using Apache and Tomcat).

Application Access Control

- See the appropriate pages on the SWITCHaai website and on the Shibboleth Wiki for details:

<https://www.switch.ch/aai/support/serviceproviders/sp-access-rules.html>

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeAccess>

- Many applications, such as e-learning systems, have built-in support for Shibboleth (e.g. Moodle, Ilias). They don't need manual modifications.

Application Access Control: Example

PHP:

```
$affiliations = preg_split("/\s*;\s*/",  
    $_SERVER['affiliation']);  
  
if (in_array("staff", $affiliations)) {  
    grantAccess();  
}
```

(Affiliation: "staff;member")

Pitfalls

- If you have run your Shibboleth SP for a long time, you may still use deprecated configuration directives. You may want to update them to simplify a later migration.

Example:

Old: `ShibRequireSession On`

New: `ShibRequestSetting requireSession true`

Consult the Shibboleth Wiki for details about configuration changes and to find deprecated directives:

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig>

Pitfalls

- If you use Apache together with XML access rules, and if you have configured multiple hostnames in your virtual hosts in Apache, make sure that the option *UseCanonicalName* is set to *On* in Apache. Else, the XML access rules might be bypassed.

Further Information

- You can find detailed information about access control for SWITCHaai, including a lot of examples, on the following web page:
 - Shibboleth Service Provider Access Control
<https://www.switch.ch/aai/support/serviceproviders/sp-access-rules.html>
- Comprehensive information and examples:
Shibboleth Service Provider Training March 2014, "Hands-On":
 - <https://www.switch.ch/aai/support/presentations/sp-training-2014/>
Shibboleth SP Training Hands-On, slides 75 to 104

Further Information

- General documentation from the Shibboleth Project:
 - Apache Configuration:
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig>
 - Apache .htaccess:
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPhtaccess>
 - XML-based mechanism:
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPXMLAccessControl>

Apache 2.4 vs. 2.2



SWITCH

SWITCHaai Team
aai@switch.ch

Berne, 13 August 2014

Changes and new features in Apache 2.4

- Apache 2.4 introduces harmonization of authentication and authorization mechanisms.
- `Require` directives now allow to specify the order of authorization rules.
 - Multiple authorization methods are called in the same order in which the `Require` directives appear in the configuration.
- New authorization container directives:
 - `<RequireAll>`, `<RequireAny>`, `<RequireNone>`
 - This enables you to specify complex authorization rules, similar to the Shibboleth XML access rules.
 - Default for `Require` directives corresponds to `<RequireAny>`, if no container is explicitly used.

Changes and new features in Apache 2.4

- Host and IP based authorization is now handled by `Require` directives.
 - `Order`, `Allow`, `Deny`, `Satisfy` are deprecated, but still supported.

Changes in Shibboleth SP affecting Apache

- For Apache 2.4 and SP 2.5.2 or later, the syntax of the Apache configuration statements regarding access control and Shibboleth has slightly changed.
- The Shibboleth SP module introduces new and updated statements that reflect the changes in Apache 2.4.

Changes in Shibboleth SP affecting Apache

- Use new syntax of Shibboleth directives even in Apache 2.2:

- Requires that directive `ShibCompatWith24 On` is used

- Old syntax:

```
Require homeOrganizationType university uas
```

- New syntax:

```
ShibCompatWith24 On  
Require shib-attr homeOrganizationType university uas
```


Changes in Shibboleth SP affecting Apache

- Enforce that ALL `Require` directives must be satisfied (default is that ANY `Require` statement must be satisfied):

– Apache 2.2:

```
ShibRequireAll On  
Require ...  
Require ...
```

– Apache 2.4:

```
<RequireALL>  
    Require ...  
    Require ...  
</RequireALL>
```

Pitfalls

- `<RequireAll>` and `<RequireAny>` can't be used at all in Apache 2.2 (only in Apache 2.4)
 - Directive `ShibCompatWith24 On` doesn't help.
- Before doing an upgrade from 2.2 to 2.4, you should update your Apache configuration accordingly to avoid deprecated directives.
 - Else, the migration might fail.

Further Information

- SWITCHaai Website
 - Shibboleth Service Provider Access Control
 - Considers the differences between Apache 2.2 and 2.4*
 - <https://www.switch.ch/aai/support/serviceproviders/sp-access-rules.html>
- Shibboleth Wiki
 - Apache Configuration
 - Considers the differences between Apache 2.2 and 2.4*
 - <https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig>
- Apache Project
 - General instructions to upgrade to 2.4 from 2.2
 - <http://httpd.apache.org/docs/2.4/upgrading.html>
 - Authentication and Authorization, section "Beyond just authorization"
 - <http://httpd.apache.org/docs/2.4/howto/auth.html>

SWITCHaai usage statistics

Some numbers and graphs

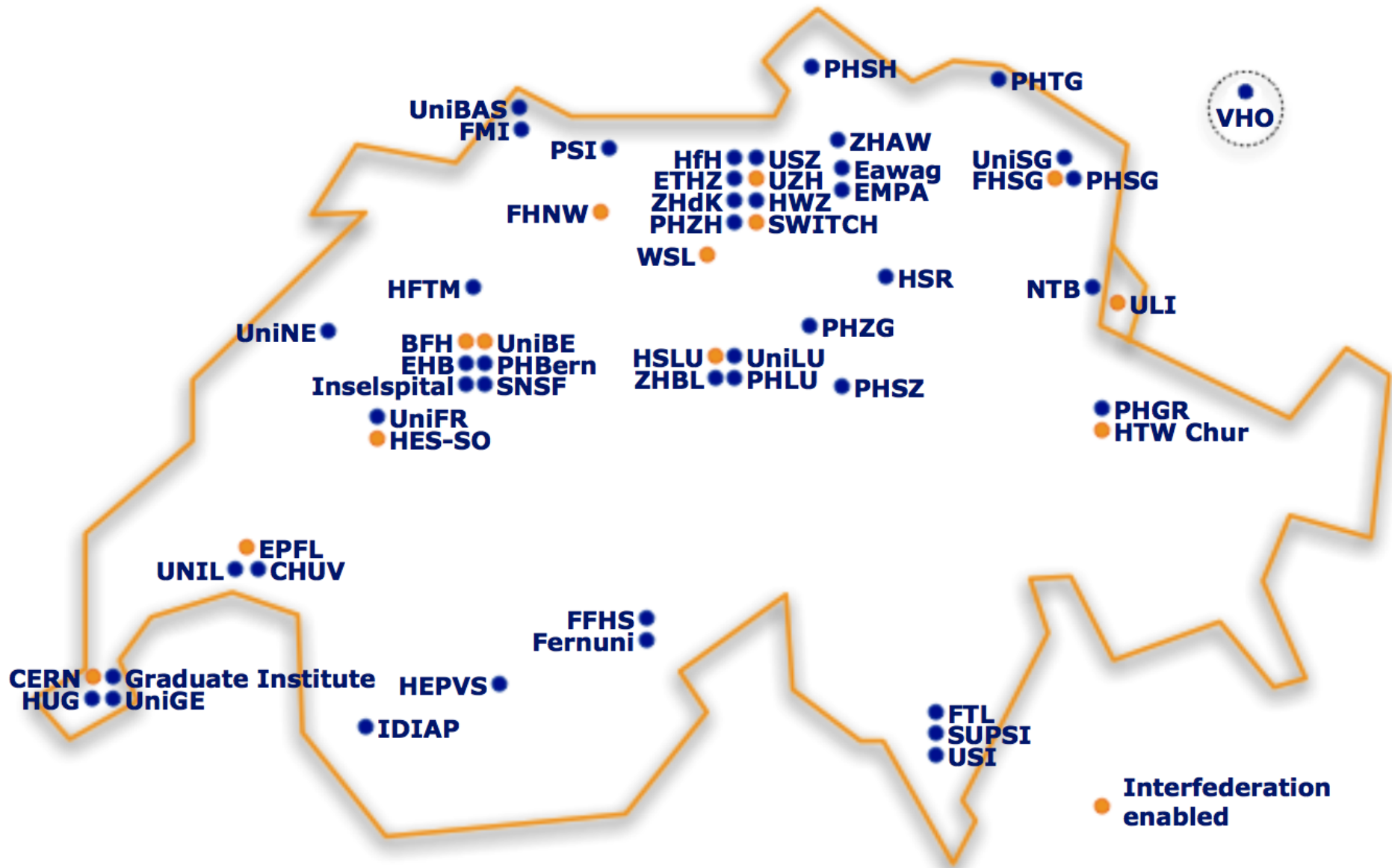


SWITCH

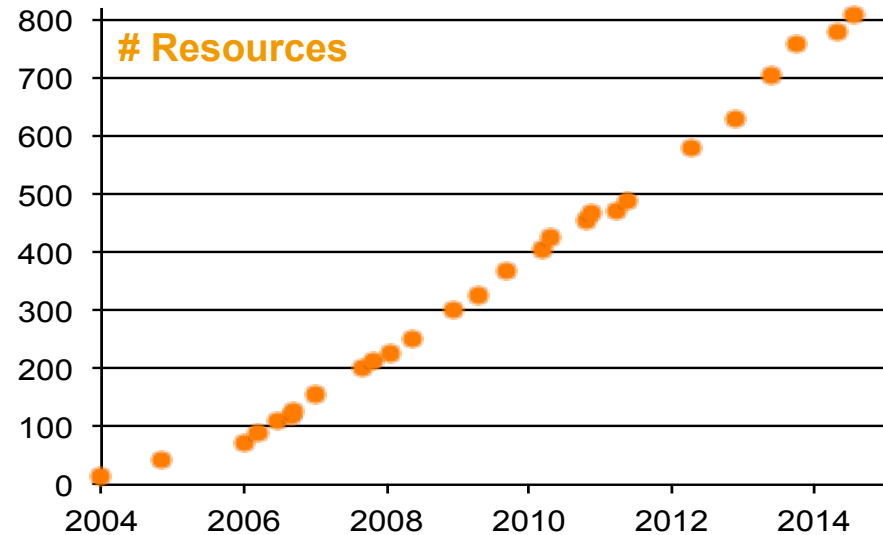
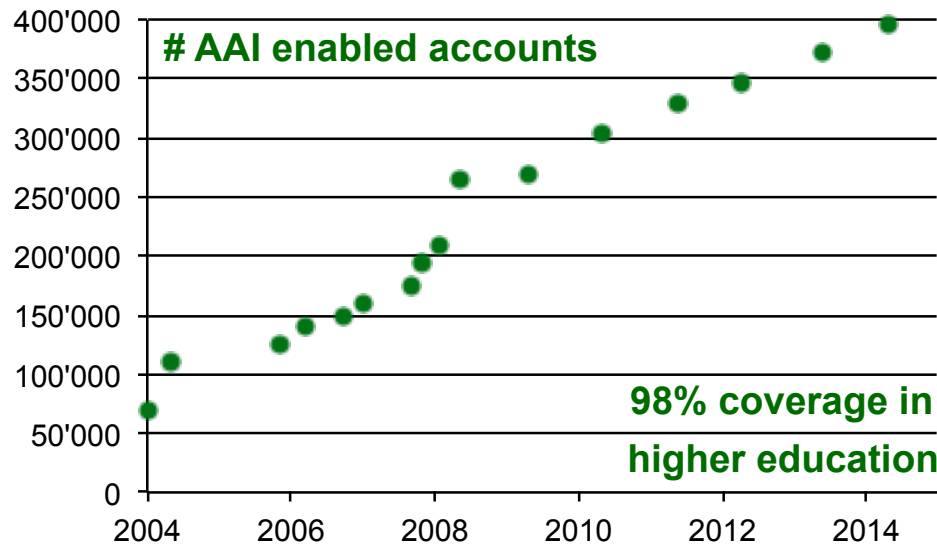
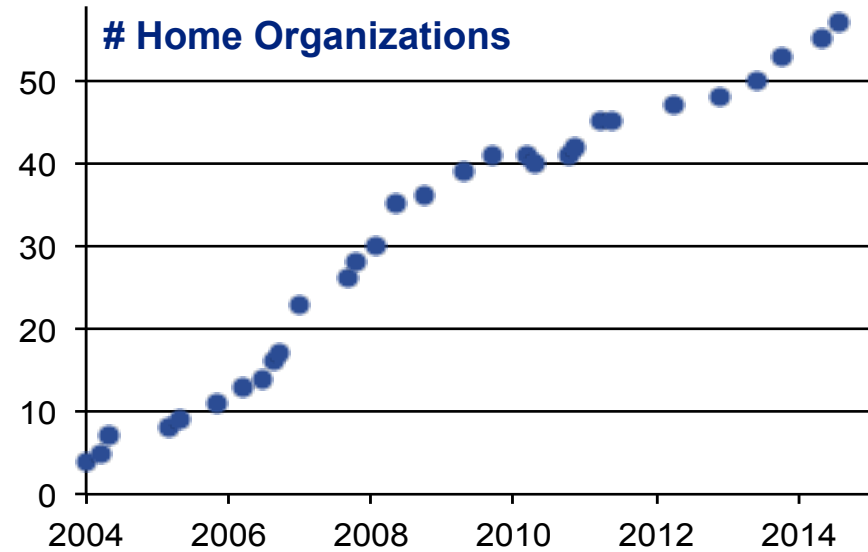
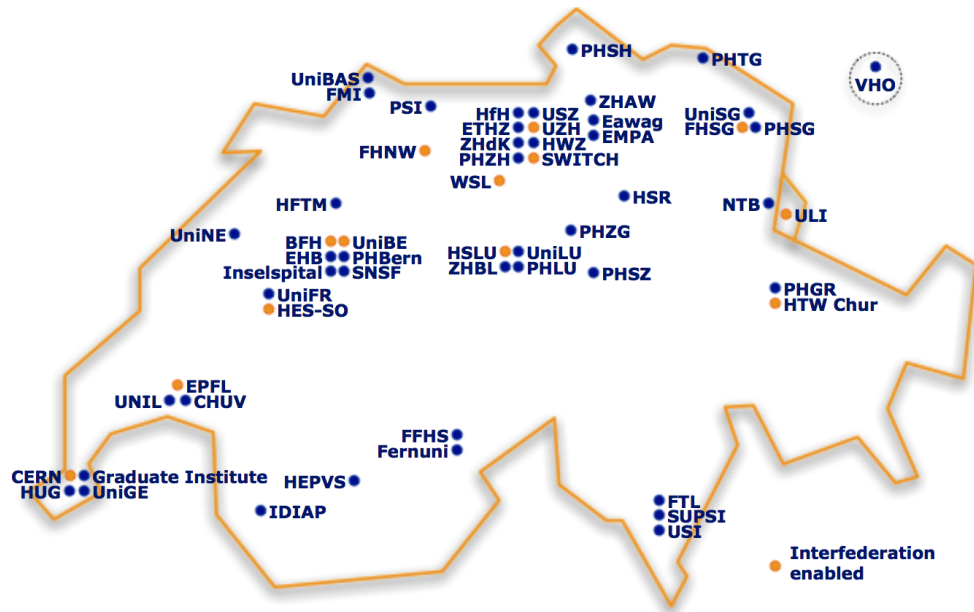
SWITCHaai Team
aai@switch.ch

Berne, 13 August 2014

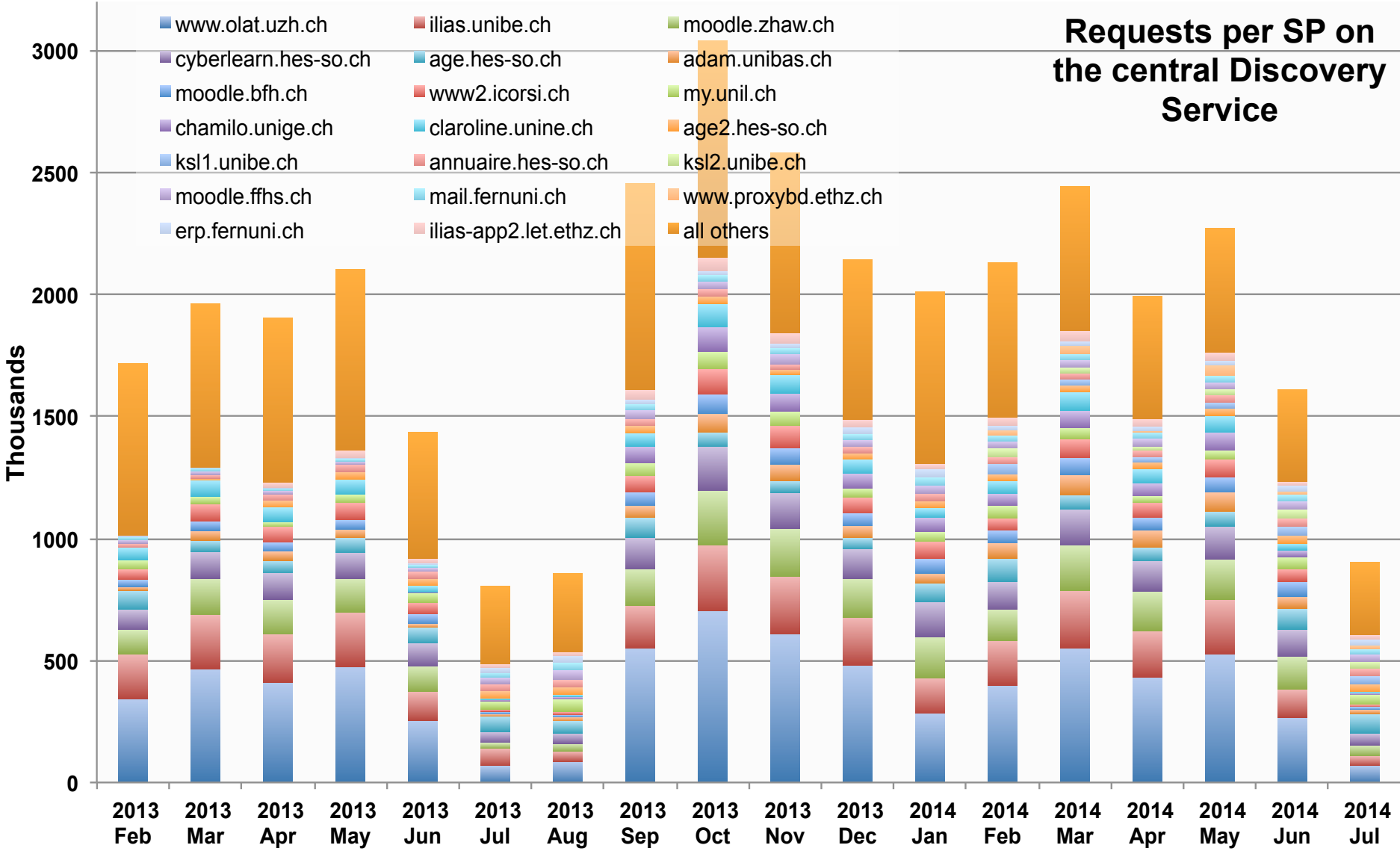
SWITCHhai Federation Summer 2014



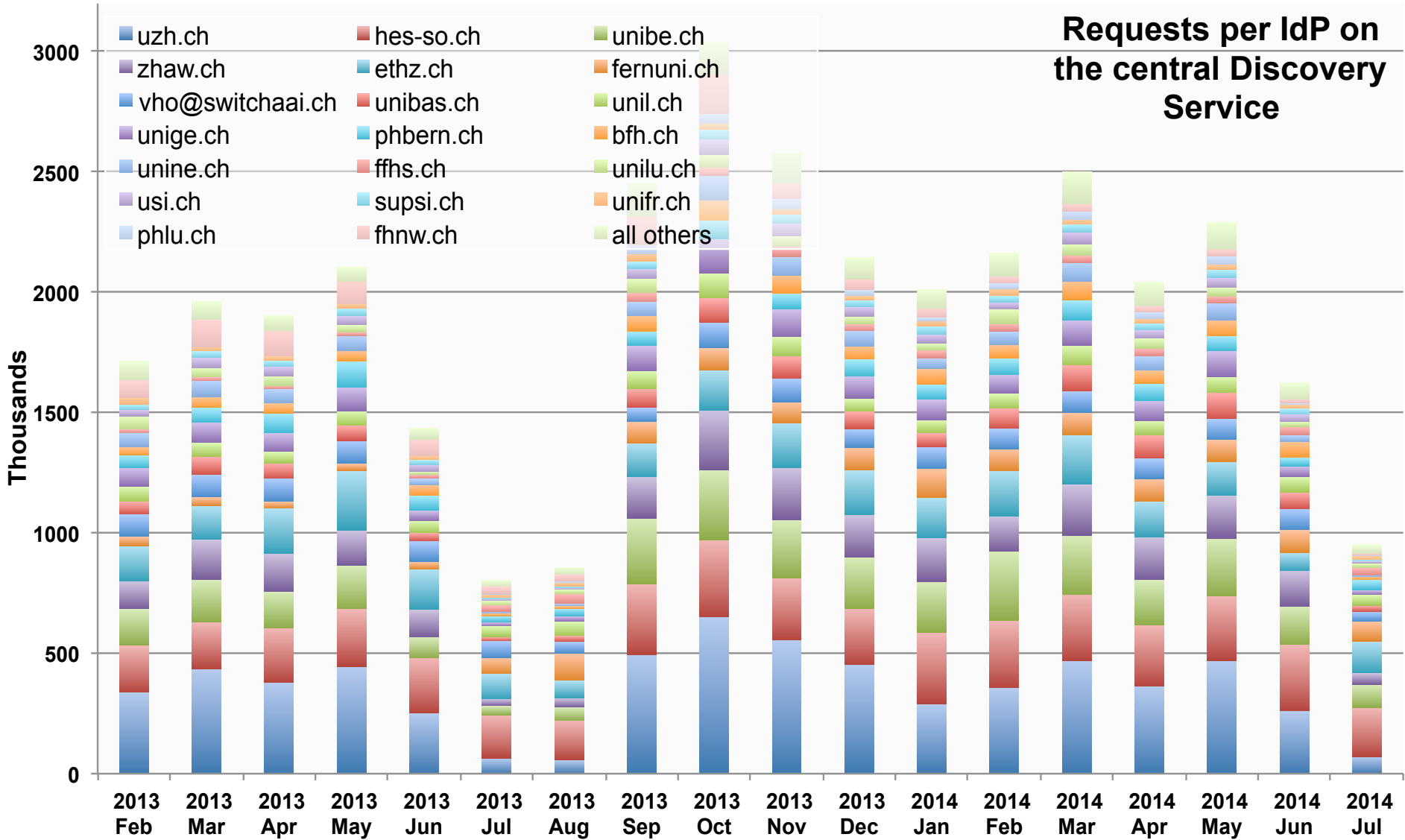
SWITCHaai Federation Summer 2014



AAI User Authentication Requests Feb 13 – Jul 14



AAI User Authentication Requests Feb 13 – Jul 14



Discovery type on Central Discovery Service

