

SWITCHhai Status Update

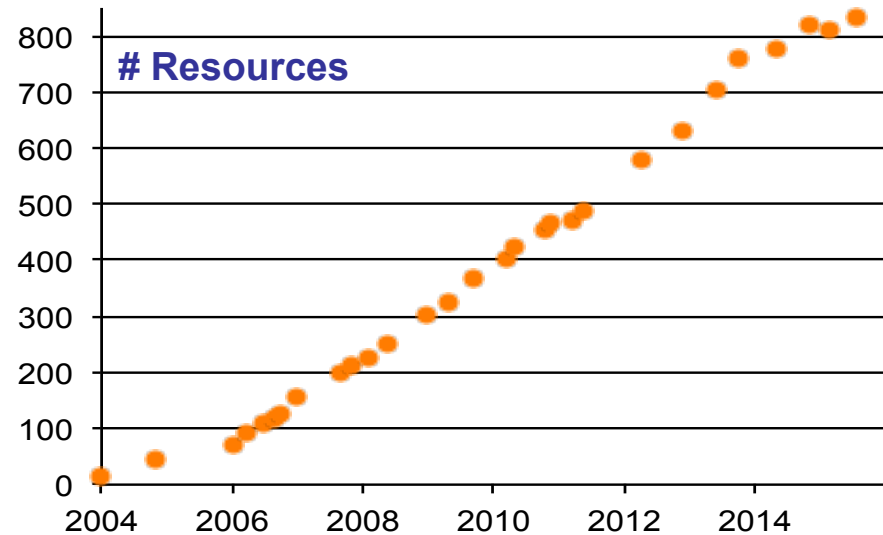
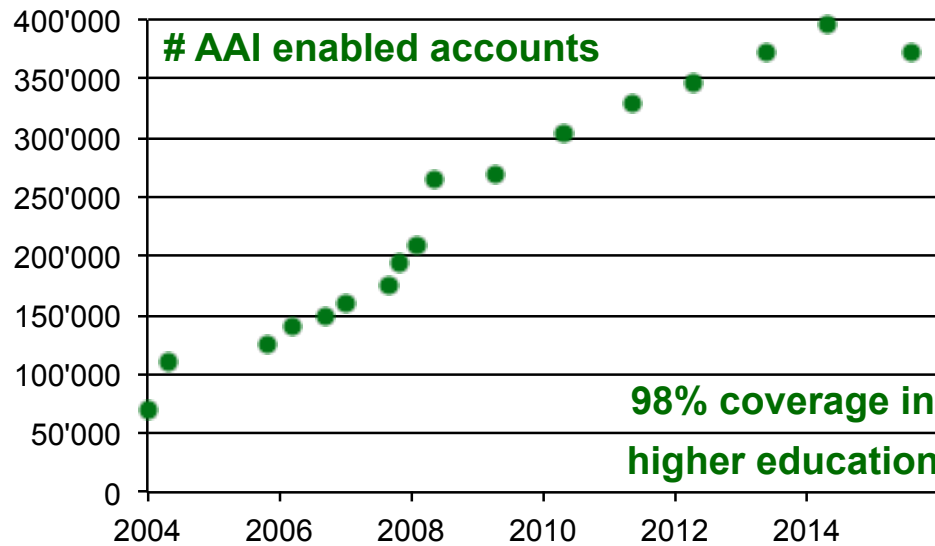
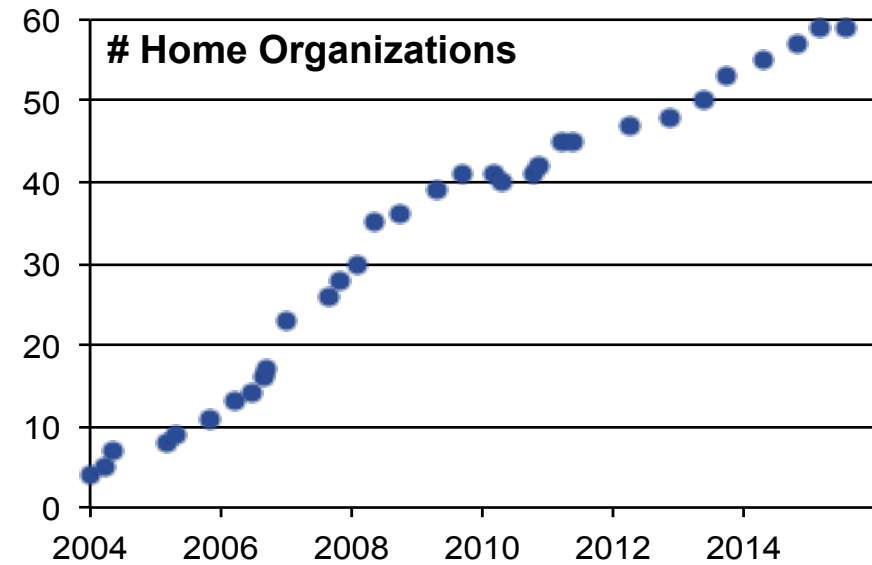
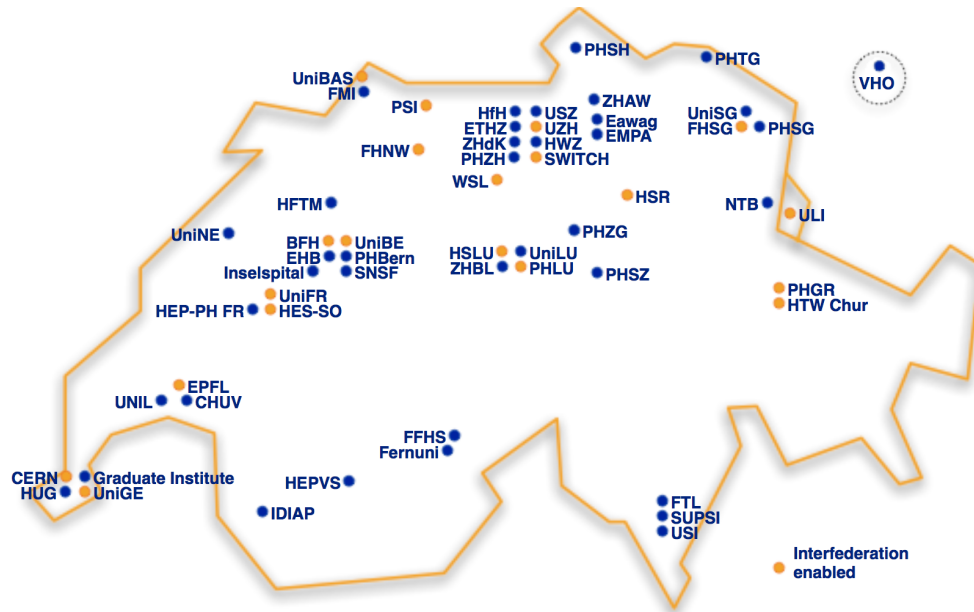


SWITCH

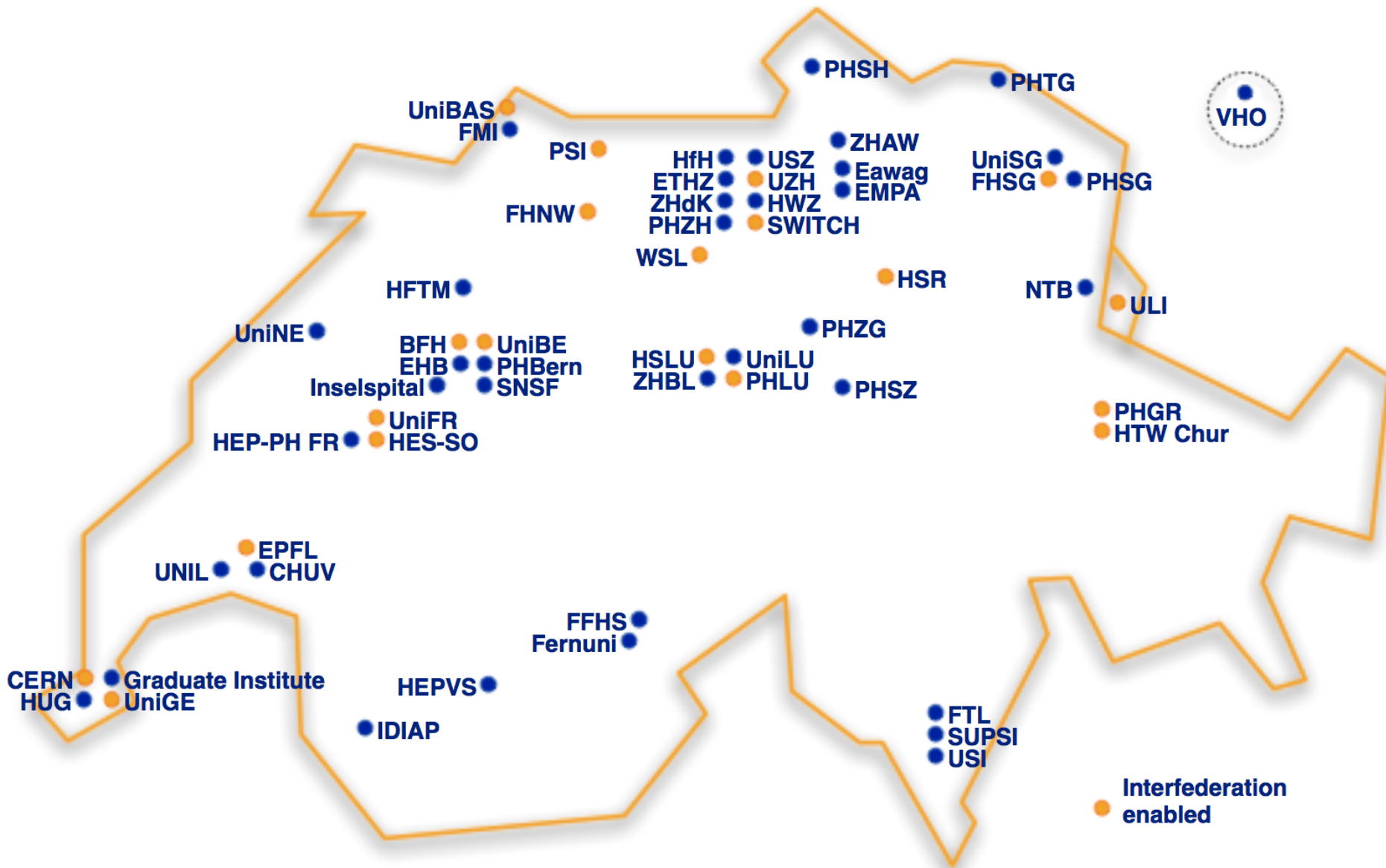
Thomas Lenggenhager
thomas.lenggenhager@switch.ch

Berne, 13 August 2015

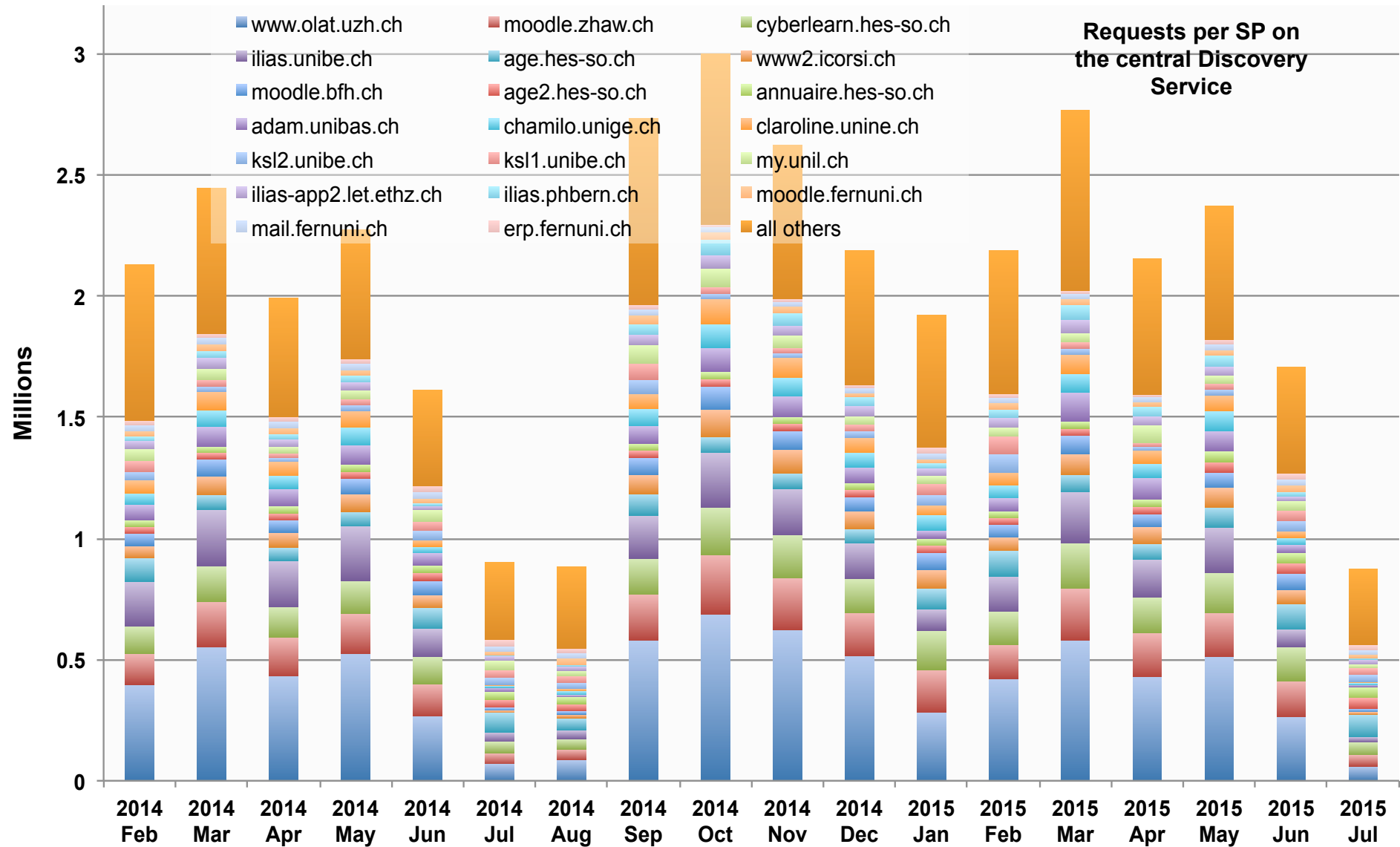
SWITCHaai Federation Summer 2015



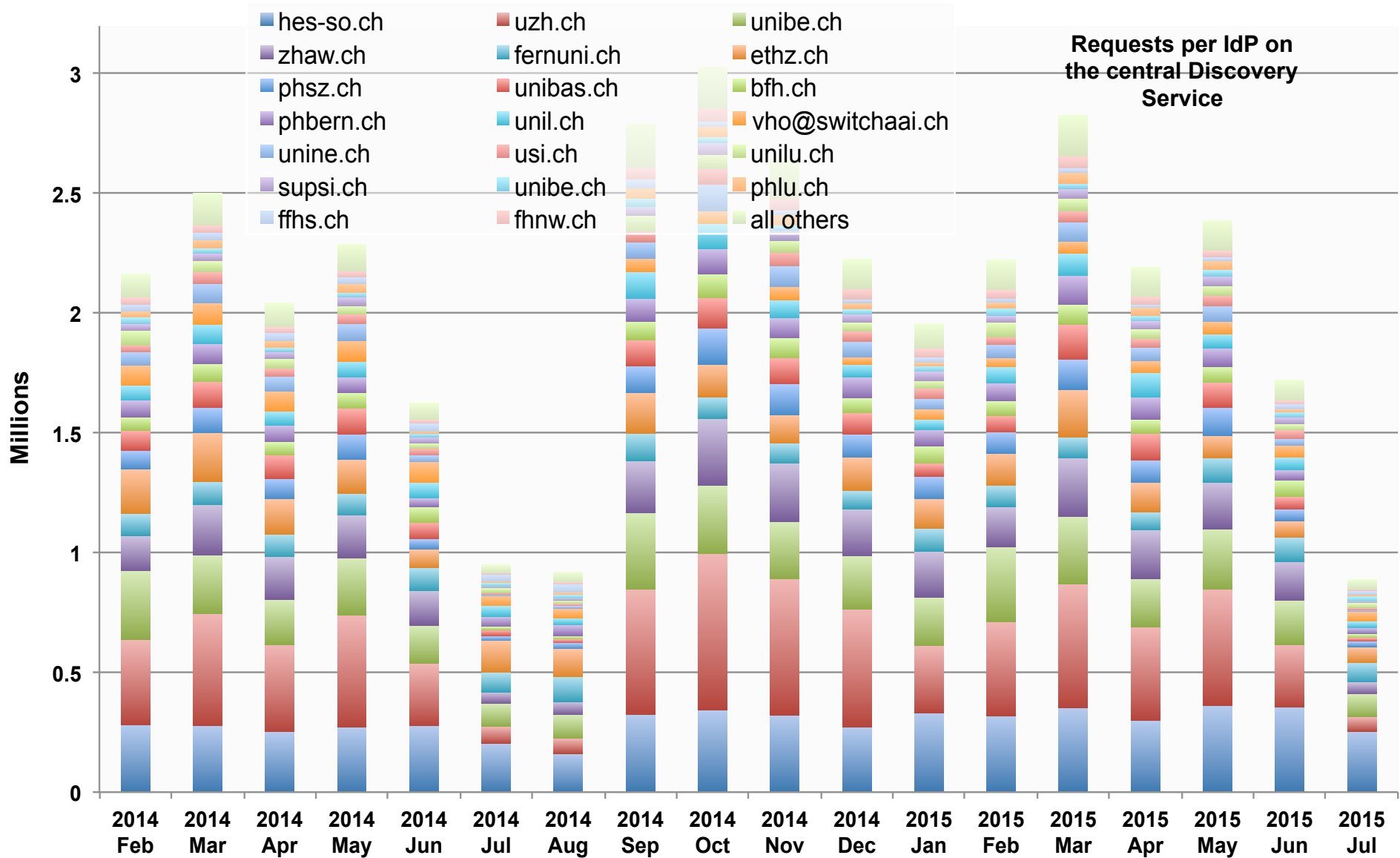
SWITCHhai Federation Summer 2015



AAI User Authentication Requests Feb 14 – Jul 15



AAI User Authentication Requests Feb 14 – Jul 15



SWITCHaai – What's new?

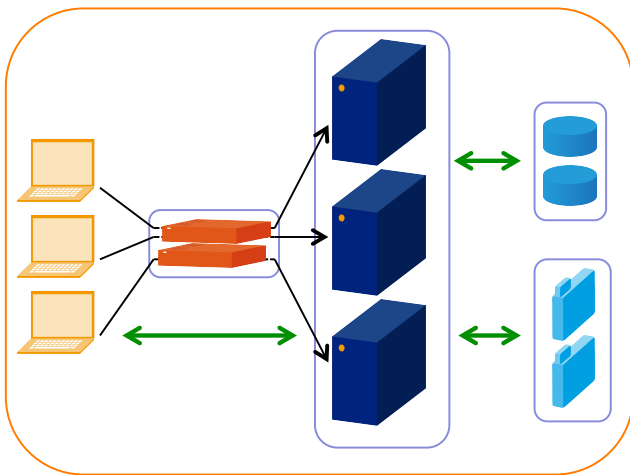
- SAML2 is now 10 years old!
 - SAML1 only SPs should disappear!
 - Some publishers are the most difficult ones
- Swiss edu-ID IdP version 1.0 in SWITCHaai
- Shibboleth IdPv3
 - Completely new configuration guide
<https://www.switch.ch/aai/guides/idp/>
 - IdPv3.2 (ca. Sept 2015)
main new feature expected: Single Logout Support
- SWITCH continues to support the Shibboleth Consortium as Principal Member
<http://shibboleth.net/consortium/>

Shibboleth IdP & SP Training

- A few seats left for the Shibboleth IdP & SP Training in Zurich
 - Tue 1 Sept SWITCHaai Introduction (only afternoon)
 - Wed 2 Sept Shibboleth SP Training
 - Thu 3 Sept Shibboleth IdP Training
- Details & Registration
<https://www.switch.ch/aai/events/>

IdP Clustering

High Availability and Load Balancing



SWITCH

SWITCHaai Team
aai@switch.ch

You want to prevent

- HW failures
 - Server component failure
 - Power failure
 - Network failure
- Service overload
- Downtimes due to maintenance (major upgrades)
- ...

What you usually do

- Take one box
 - Harden it through redundant components (power, network, disk, memory, CPU's, backplane (?))
- Or take another box
 - Organize failover (cold standby)
- Or take a couple of boxes
 - Organize load balancing
- Or take a VM from a “HA environment”

An academic question: Stateful or not?

- The IdP is stateful, simply because it maintains a “conversational state” with each of the clients.
- This conversational state is implemented in software other than the IdP, namely in Spring Web Flow, typically using a session ID.
- However, at present, there is no solution provided to replicate the per-request conversational state.
- So, this is a hard problem, and we have no solution out of the box. What can we do?

Storage Recommendations

Storage Entity	Recommended Storage	Scope
Persistent ID	<i>Common Database</i>	Cluster
User consent	<i>Common Database</i>	Cluster
IdP User Session	Client	Per Client
Transient ID (Backchannel)	<i>Common Database</i>	Cluster
SAML artifact	<i>Common Database</i>	Cluster
Conversation Session	Memory	Per Node
Message replay cache	Memory	Per Node

Remarks:

- <https://wiki.shibboleth.net/confluence/display/IDP30/Clustering>
- "Common Database" means some central/clustered database or a database replicated between nodes.
- SAML artifact:
Irrelevant if SAML 2.0 artifacts not used/required at all
- Alternatives for Message replay cache:
Common Database or memcached (depending on security requirements)

From the IdPv3 business case

- “The choice of **Terracotta** as a primary clustering solution for high availability has not worked out particularly well for the project and we have been evaluating possible directions and design implications from the early planning stages. While the original intent was to move toward a technology called **Infinispan** as a replacement, recent experience from the community has not been positive (feedback for which we are tremendously appreciative).”
- + “Much design attention has been given to ensuring support will be possible for other popular solutions such as **databases** and **memcached**.”

<https://shibboleth.net/documents/business-case.pdf>

Do it yourself

Then you need to think about

- Network
- Processing (CPU, memory)
- Persistent storage (Disks and DBs)

Tools

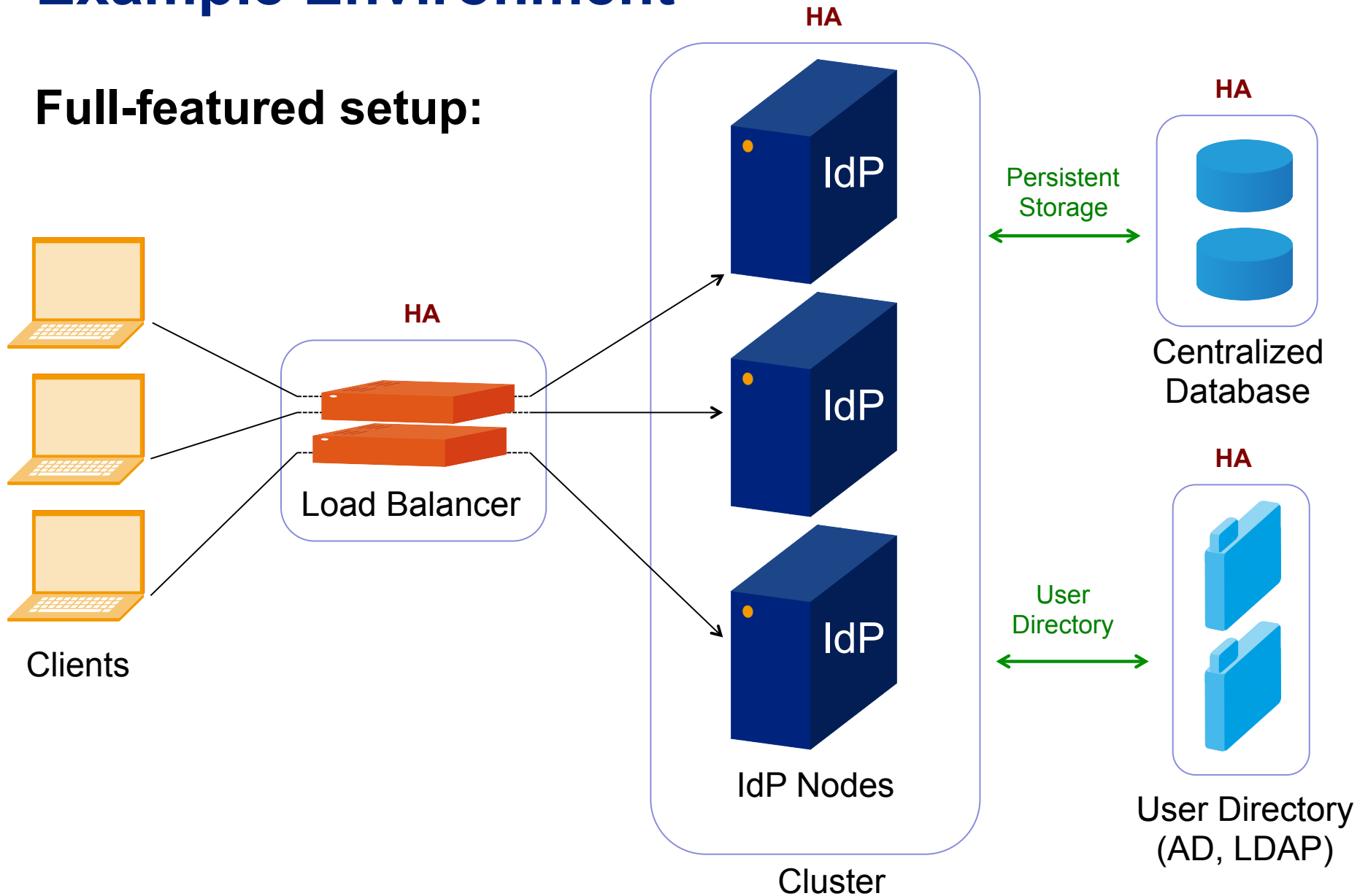
- NGINX: popular HTTP load balancer, but additional features may cost
- PostgresDB: recommended DB by Shibboleth
- Memcached: Cache or even alternative to DBs, in-memory, key-value data store.
- DRDB: a “network based raid-1 block devices to put a filesystem on”

Examples

Who	Network	Processing	Persistent storage
Uni Bern (IdPv3)	NGINX (active-active) HTTP Loadbalancer	2 IdPs	Use of central MSSQL-cluster
Uni Genève (IdPv2)	F5 BIG-IP Loadbalancer (sticky)		MySQL DB Cluster
Uni Lausanne (IdPv2)	HW load balancer (active-passive)	2 IdPs (active-passive)	external MySQL-DB (also HA: Heartbeat + DRBD)
Uni Zürich (IdPv2)		3 IdPs	external MySQL database
HES-SO Fr (IdPv2)		2 IdPs active-active	
Uni Marburg (IdPv2)	NGINX Loadbalancer	2 IdPs, memcached,	1 external PostgresDB server
SWITCH (IdPv2)	Anycast address	2 IdPs active-passive	Local MySQL-DB, replicated by cron

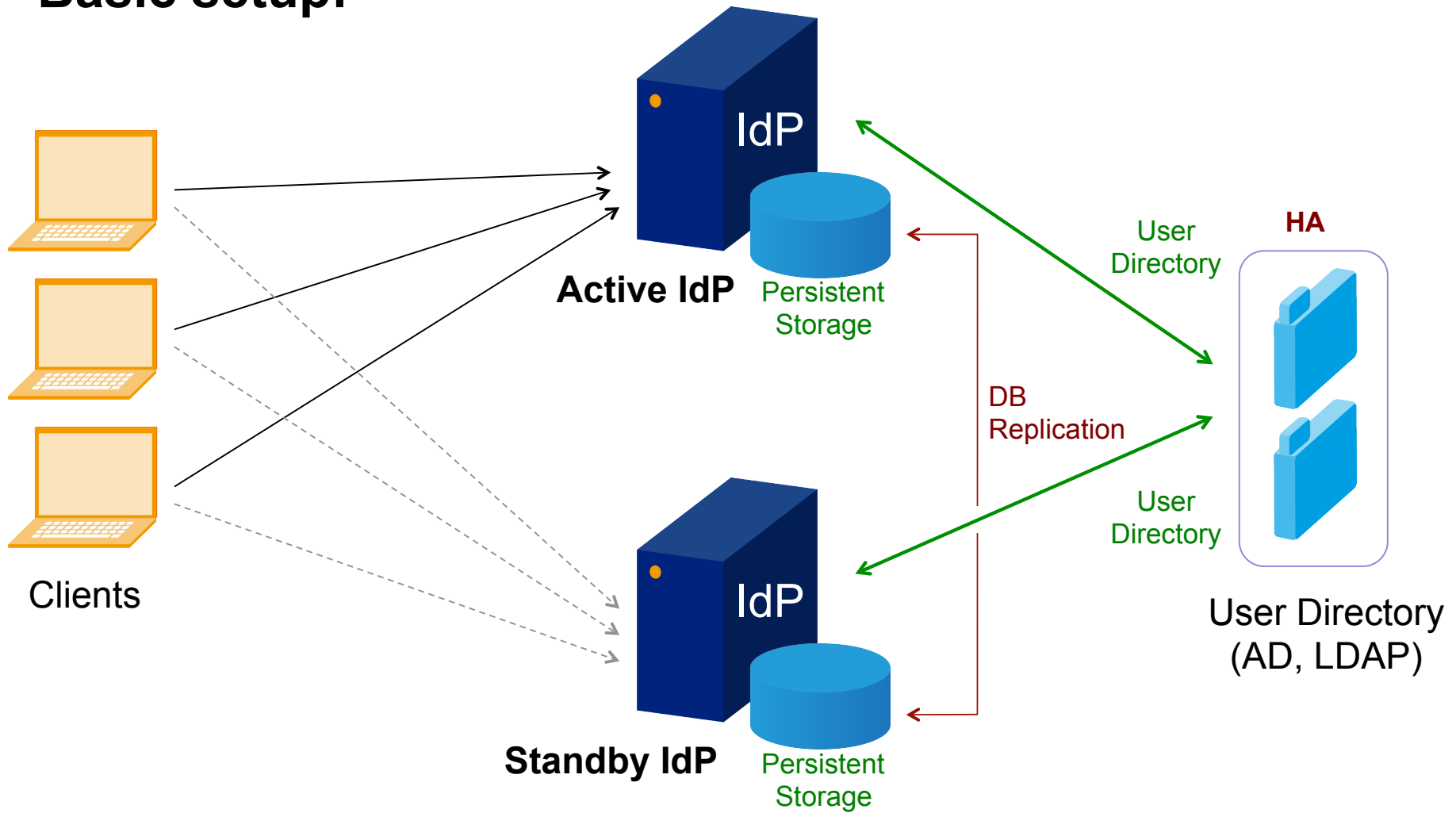
Example Environment

Full-featured setup:



Example Environment

Basic setup:



References

Documentation

- **Clustering**
<https://wiki.shibboleth.net/confluence/display/IDP30/Clustering>
- **Secret Key Management**
<https://wiki.shibboleth.net/confluence/display/IDP30/SecretKeyManagement>
- **Storage**
<https://wiki.shibboleth.net/confluence/display/IDP30/Storage>
- **Discussion on Persistence**
<https://wiki.shibboleth.net/confluence/display/IDP30/Persistence>

Thanks to

- **Dominique Petitpierre**
- **Manuel Haim**
- **Michael Pfister**
- **Daniel Lutz**
- **Lukas Hämmerle**
- **Many others**

Multi-Factor Authentication and Shibboleth IdPv3

New flexibility, same old questions



SWITCH

Etienne Dysli-Metref
etienne.dysli-metref@switch.ch

Multi-factor authentication

Authenticate with factors picked from two (or more) of the following categories.

Something you:

- know (password)
- have (token)
- are (biometrics)

Do you want MFA?

- Does your SP ask for something better than username+password?
- Do you already have a multi-factor authentication solution deployed (without Shibboleth)?

Swiss edu-ID “Processes” WG, December 2014

Many institutions wish they had MFA but no one really knows how to introduce or implement it.

Problem landscape

- What do you want to gain from MFA? What are the risks and expected quality levels?
- Who is going to use it?
- How much are you willing to pay? What hardware can you rely on? (mobile/smart phones)
- Is it only for the IdP or should it work with other systems too?

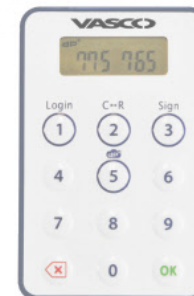
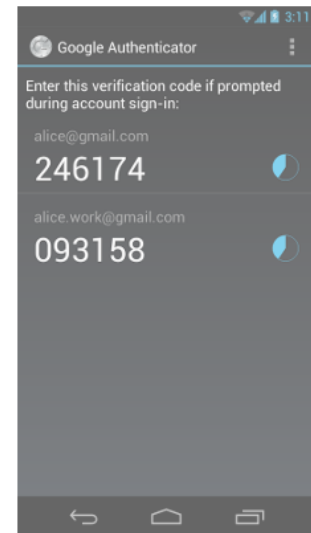
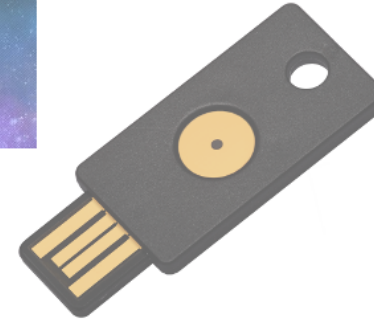
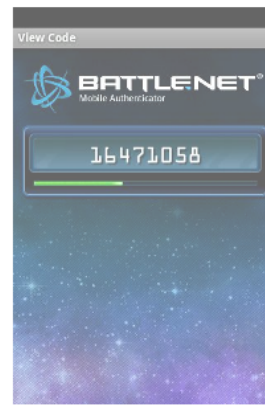
So many tokens!

Categories

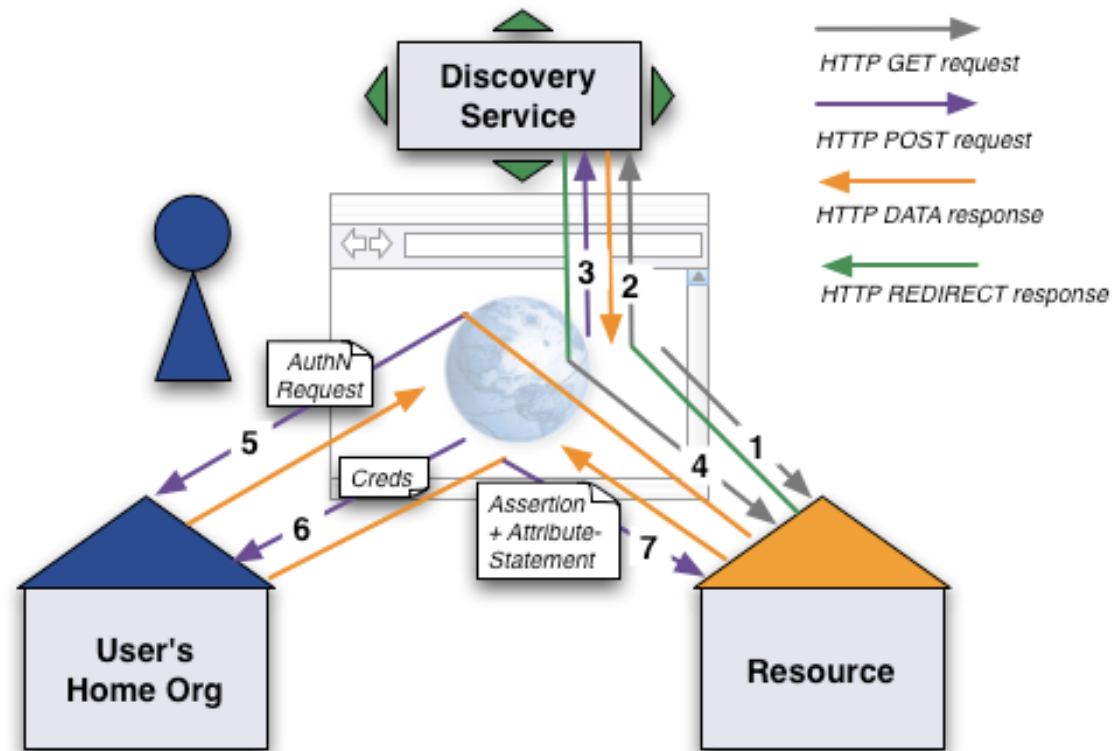
- hardware | software
- event-based | time-based | challenge-response | out of band OTP
- standard | proprietary

Standards

- OATH: HOTP, TOTP, OCRA
- X.509 certificate, smartcards



Implementation in Shibboleth



(<https://www.switch.ch/aai/demo/medium/>)

MFA happens in steps 5, 6 and 7

Implementation in Shibboleth

1. SP requests a specific *authentication context class*
2. IdP selects and runs a *login flow* that satisfies this class
3. IdP replies with an authentication assertion containing the class actually used

Authentication context classes

Login flows

Assembling the pieces

SAML authentication contexts

- OASIS standard (<http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>) (2005)
- XML Schema to describe the authentication context
 - identification, authentication method
 - technical protection, operational protection
 - governing agreements
- Provides a list of authentication context *classes* for SAML (namespace `urn:oasis:names:tc:SAML:2.0:ac:classes`)

SAML authentication context classes

Which class to use?

- Completely define your own
 - ⇒ not interoperable with other institutions
- Pick one from the OASIS list that fits your needs
 - ⇒ better for interoperability
- Or one from IETF's [Level of Assurance profiles registry](https://www.ietf.org/assignments/loa-profiles/) (https://www.ietf.org/assignments/loa-profiles/)
 - ⇒ for example [InCommon Bronze or Silver](https://incommon.org/assurance/) (https://incommon.org/assurance/)

SAML authentication context classes

List of classes from the OASIS standard

Internet Protocol, Internet Protocol Password, Kerberos, Mobile One Factor Unregistered, Mobile Two Factor Unregistered, Mobile One Factor Contract, Mobile Two Factor Contract, Password, **Password Protected Transport**, Previous Session, Public Key - X.509, Public Key - PGP, Public Key - SPKI, Public Key - XML Digital Signature, Smartcard, Smartcard PKI, Software PKI, Telephony, Telephony (“Nomadic”), Telephony (Personalized), Telephony (Authenticated), Secure Remote Password, **SSL/TLS Certificate-Based Client Authentication**, Time Sync Token, **Unspecified**

Authentication context classes

Login flows

Assembling the pieces

Login flows



New technology in IdPv3

- The IdPv3 uses **Spring Web Flow** (<http://projects.spring.io/spring-webflow/>) to implement various authentication methods as login flows
- Child project of the Spring Framework
- Allows implementing the “flows” of a web application
- Sequence of steps for user interaction e.g. forms
- State machine described in XML

```

<!-- Examples extracted from system/flows/authn/authn-flow.xml -->
<flow xmlns="http://www.springframework.org/schema/webflow"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.springframework.org/schema/webflow
http://www.springframework.org/schema/webflow/spring-webflow.xsd"
  parent="authn.abstract">
  <action-state id="AuthenticationSetup">
    <evaluate expression="PopulateAuthenticationContext" />
    <evaluate expression="PopulateSessionContext" />
    <evaluate expression="'proceed'" />
    <transition on="proceed" to="TestForSession" />
  </action-state>
  <decision-state id="TestForSession">
    <if test="opensamlProfileRequestContext.getSubcontext(...) != null"
      then="SessionExists" else="FilterFlows" />
  </decision-state>
  <!-- ...more states... -->
  <subflow-state id="CallAuthenticationFlow" subflow="#{currentEvent.id"
    <input name="calledAsSubflow" value="true" />
    <transition on="proceed" to="CallSubjectCanonicalization" />
    <transition on="ReselectFlow" to="SelectAuthenticationFlow" />
  </subflow-state>
  <!-- ...more states... -->
  <bean-import resource="authn-beans.xml" />
</flow>

```

IdPv3 login flows

Tools you get out of the box

- Built-in login flows for:
 - Password
 - X.509 client certificate
 - IP address
- Each login flow states what authentication context classes it supports
(configured in `conf/authn/general-authn.xml`)

IdPv3 login flows

Tools you get out of the box

- A flow may call another flow as *subflow*
- Optional *initial flow*: always runs first
 - ⇒ fetch user attributes before another flow runs
 - when there is no session
 - regardless of what the SP requests
- **But** there is no generic way of chaining flows

Login flows and MFA

Combining flows (1): the big one

Write one flow to implement both first and second factors

```
Please enter your credentials
Username: [_____]
Password: [_____]
OTP:      [_____]

```

- Completely customised to your needs
Example: if OTP field left empty then send OTP via SMS and reprompt
- Likely to duplicate most of the password flow

Login flows and MFA

Combining flows (2): the initial glue

Write one flow for the second factor and “glue” it after an existing first factor *initial* flow

```
Please enter your credentials
Username: [_____]
Password: [_____]

```

```
Please enter your one-time password
OTP:      [_____]

```

- Can easily replace one flow with another
- SFA + SFA =? MFA

Login flows and MFA

Combining flows (3): the subflow explosion

Offer the user a choice of second factors after an *initial* password flow

```
Please enter your credentials
Username: [_____]
Password: [_____]

```

```
Please pick your authentication method
token1 | token2 | token3
token4 | token5 | token6

```

```
Please enter your one-time password
tokenX:  [_____]

```

Authentication context classes

Login flows

Assembling the pieces

Migrating version 2 extensions

- Unfortunately, IdPv2 login handlers can't be reused “as is” in v3
- New name: *login handler* → *login flow*
- Code changes are needed because the API is different
- Reimplement them as flows if possible
⇒ much more flexible than servlets
- Like in v2, you need someone with Spring skills

Pieces to configure

- Choose one authentication context class
- SP must request authentication with that particular class
- IdP must have a login flow for that class, enabled
- Implement that flow
- Have something to verify each authentication factor
 - inside the IdP process or external system?

Non-technical pieces

Administrative processes

- Registration of new users and distributing tokens (enrolment)
 - identity verification?
- Replacement of forgotten, lost, stolen or expired tokens
- Revocation

Summary

- Planning and deploying MFA is still as difficult as before (same old questions)
- IdPv3 offers greater flexibility thanks to flows

References

- OATH: Initiative for Open Authentication (<http://openauthentication.org/>)
- OASIS: Authentication Context for SAML2 (<http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>)
- IETF: Level of Assurance Profiles registry (<https://www.ietf.org/assignments/loa-profiles/>)
- IETF: RFC 6711: An IANA Registry for Level of Assurance (LoA) Profiles (<https://tools.ietf.org/html/rfc6711>)

References

- InCommon Assurance Program
(<https://incommon.org/assurance/>)
- Spring Web Flow project (<http://projects.spring.io/spring-webflow/>)
- Shibboleth wiki: IdPv3 Authentication Configuration
(<https://wiki.shibboleth.net/confluence/display/IDP30/AuthenticationConfig>)

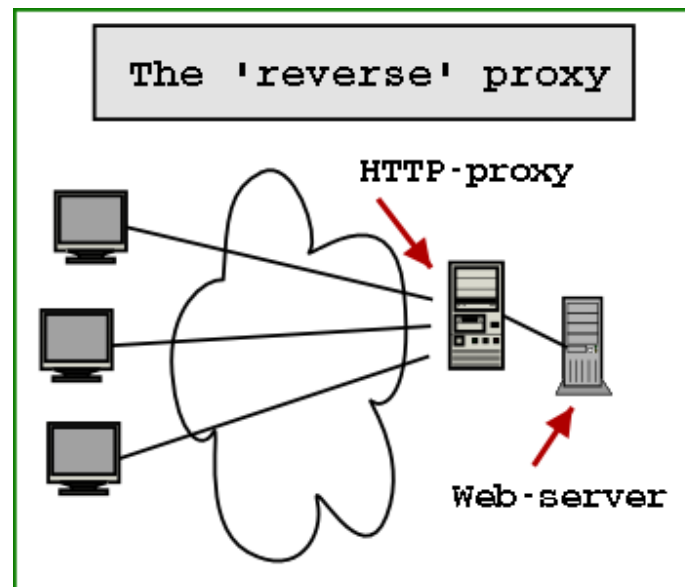
SWITCHaai & Swiss edu-ID Update 2015

SP REVERSE PROXY SERVER AT ZHAW

- What are we talking about?
- Why we operate one at ZHAW?
- Why this could be interesting for others, too.
- How it's done.
- Getting help.

SP Reverse Proxy Server at ZHAW

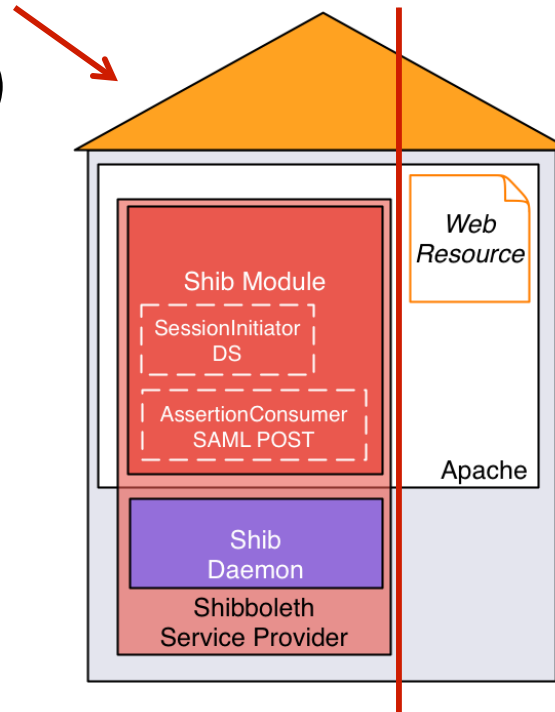
Reverse Proxy 101



SP Reverse Proxy Server at ZHAW

How to reverse proxify a Shibboleth SP?

**HTTP-proxy
(with mod_shib)**



Web-server

SP Reverse Proxy Server at ZHAW

But why?

In 2011, only one reason:

Compiling library dependencies on Solaris 

Moving web server to another OS 

Split the SP functionality and the web server 

SP Reverse Proxy Server at ZHAW

It's a good thing...

Pros:

- Less time to add new SPs
- Reduced complexity on web servers
- No need to update 23958 systems on a new SP version
- Option to use different web servers
- Security
- Easy to set up

SP Reverse Proxy Server at ZHAW

... but it has its drawbacks.

Cons:

- Easy to upset: Single Point of Failure
- Debugging web traffic involves (at least) two systems
- May get difficult to use with load balancing / clustering
- Configuration may get complex if every SP has other settings
- Security

SP Reverse Proxy Server at ZHAW

Configuration overview – Shibboleth

- ApplicationOverrides

```
<ApplicationOverride
```

```
  id="webtools"  
  entityID="https://webtools.zhaw.ch/shibboleth">
```

```
  <CredentialResolver
```

```
    type="File"  
    key="/etc/pki/tls/private/webtools.zhaw.ch.key"  
    certificate="/etc/pki/tls/certs/webtools.zhaw.ch.crt.pem"/>
```

```
</ApplicationOverride>
```

SP Reverse Proxy Server at ZHAW

Configuration overview – HTTPD

- Authentication

```
<Location />  
    AuthType shibboleth  
    ShibRequestSetting requireSession 1  
    ShibRequestSetting applicationId webtools  
    ShibUseHeaders On  
    Require valid-user  
</Location>
```

SP Reverse Proxy Server at ZHAW

Configuration overview – HTTPD

- Reverse Proxy directives

```
SSLProxyEngine On  
ProxyRequests Off  
ProxyPass / http://webtools-intern.zhaw.ch/  
ProxyPassReverse / http://webtools-intern.zhaw.ch/  
ProxyPreserveHost On
```

SP Reverse Proxy Server at ZHAW

Configuration overview – HTTPD

- Authentication for subdirectories

```
# The Shibboleth handler shall process all HTTPS requests...
```

```
<Location />  
    AuthType shibboleth  
    ShibRequestSetting applicationId webtools  
    ShibUseHeaders On  
    Require shibboleth  
</Location>
```

```
# ...but only enforce a session for the locations below.
```

```
<Location /secure>  
    AuthType shibboleth  
    ShibRequestSetting requireSession 1  
    ShibRequestSetting applicationId webtools  
    ShibUseHeaders On  
    Require valid-user  
</Location>
```


SP Reverse Proxy Server at ZHAW

Where can I get help?

Shibboleth Wiki:

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

SWITCH AAI Wiki:

<https://wiki.aai.switch.ch/twiki/bin/view/AAIResources/ShibbolethReverseProxy>

aai@switch.ch

How the SAMLtrace Firefox add-on can be useful



SWITCH

Thomas Lenggenhager
thomas.lenggenhager@switch.ch

Berne, 13 August 2015

Motivation

- What really happens after...
 - ...picking the Home Organisation in the Discovery Service and the IdP presenting the login screen?
 - Some HTTP redirects and the SP issues a SAML authentication request
 - ...providing user consent and getting into the web application?
 - The IdP posts a SAML authentication assertion to the SP and the SP redirects you to the web application

In action...

The screenshot shows a web browser window titled "SAML tracer". The interface includes a toolbar with "Clear", "Autoscroll", and "Filter resources" buttons, and "Export" and "Import" icons. A list of HTTP requests is displayed, with the third request highlighted in orange and labeled "SAML".

The selected request is a GET request to `https://aai-logon.vho-switchaai.ch/idp/profile/SAML2/Redirect/SSO?SAMLRequest=jZJdT8IwFib%2FytL7rduQDxtGgnAhCQph0wtvTNsdWJPSzp4O9N87GBq8IV737fOc87Zj5Htds2njK7...`. Below the request list, a detailed view of the SAML request is shown, with tabs for "http", "Parameters", and "SAML".

The SAML request details include the following headers:

```
GET https://aai-logon.vho-switchaai.ch/idp/profile/SAML2/Redirect/SSO?SAMLRequest=jZJdT8IwFib%2FytL7rduQDxtGgnAhCQph0wtvTNsdWJPSzp4O9N87GBq8IV737fOc87Zj5Htds2njK70BjwbQB597bZCdDzLSOMMsR4XM8D0g85Ll06clS6OY1c56K60mwRQRnFfWzKzBZg8uB3dQE142y4xU3tfIKOXeOyUaD%2BFBwRFcxLmK8Ki8rCJZ0bxSQLgNvooQLT1ZUrpe5QUJ5ulYyvCT4ArHVajtzproUNmw45yILUqVNW2H2yoNF84GSuVAeprnKxIs5h15H0pIkt6Ap3x0z2MxFOVgC1sQcTmsQxGLNobYwMKg58ZnJI2TfhiPwiQtKh7r37079IOE60sHD8qUyuxuFya6ELLHoliH3W6v4PC8Vxsgk%2FGpdnYWu6uHuI3lP%2B2TyT%2B7xt%2Bux%2FTK2Ol9twqFvO1lUp%2BBVOt7XHmgHvISELopLvy99NMvgE%3D&RelayState=cookie%3A1439387982_8877 HTTP/1.1
Host: aai-logon.vho-switchaai.ch
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

The SAML request body is shown in the "SAML" tab:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://attribute-viewer.aai.switch.ch/Shibboleth.sso/SAML2/POST"
  Destination="https://aai-logon.vho-switchaai.ch/idp/profile/SAML2/Redirect/SSO"
  ID="_7cell36a2a89a0b7bd6fefeb0d8c7b0b"
  IssueInstant="2015-08-12T13:59:42Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://attribute-viewer.aai.switch.ch/shibboleth</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

Spotting SAML related errors...

```
http Parameters SAML
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://attribute-viewer.aai.switch.ch/Shibboleth.sso/SAML2/POST"
  Destination="https://aai-logon.vho-switch.ch/idp/profile/SAML2/Redirect/SSO"
  ID="_7ce1136a2a89a0b7bd6fefeb0d8c7b0b"
  IssueInstant="2015-08-12T13:59:42Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://attribute-viewer.aai.switch.ch
/shibboleth</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- Without access to the IdP or SP log files, e.g.
 - AssertionConsumerServiceURL=
"https://attribute-viewer.aai.switch.ch/Shibboleth.sso/SAML2/POST"
must match with SP metadata
 - IssueInstant="2015-08-05T13:26:32Z"
must be within 3 minutes of actual time

Where to get it?

- UNINETT in Norway wrote SAMLtracer
 - <https://github.com/UNINETT/SAML-tracer/>
 - <https://github.com/UNINETT/SAML-tracer/releases/download/samltracer-0.3/samltracer-0.3.xpi>
- No magic involved 😊
SAMLtracer can't decrypt the EncryptedAssertion of a SAML response

eduGAIN – An Opportunity for Research Collaborations



SWITCH

SWITCHaai Team
aai@switch.ch

Agenda

- Why eduGAIN?
- Status
- GÉANT Data Protection Code of Conduct
- Scalable Attribute Release

Why Interfederation?

- Federations are mostly of national scope
 - Services may need to register in multiple 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

Interfederation Status

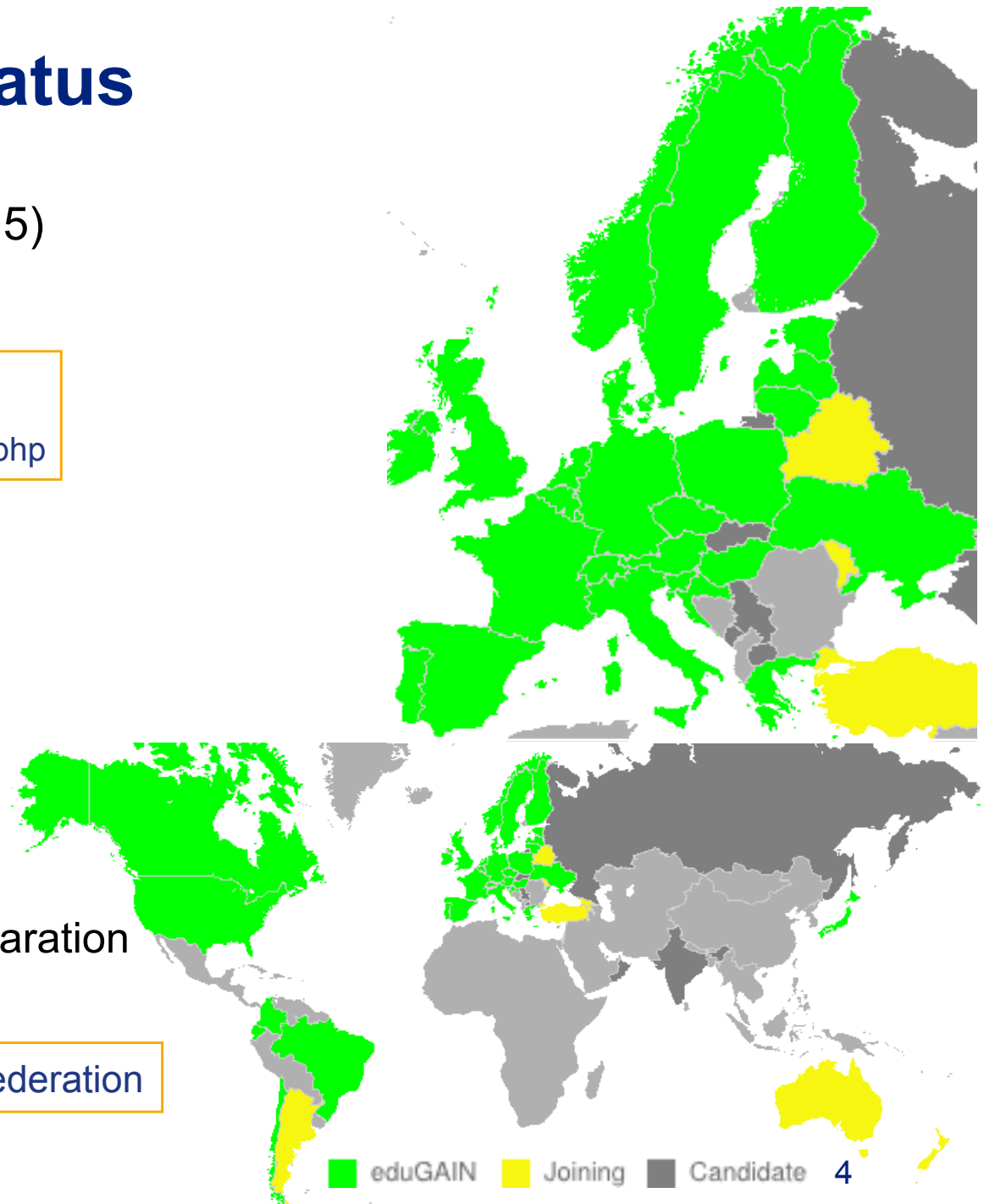
- eduGAIN in Total (Aug. 2015)
 - 1406 IdPs, 959 SPs

<http://www.edugain.org>

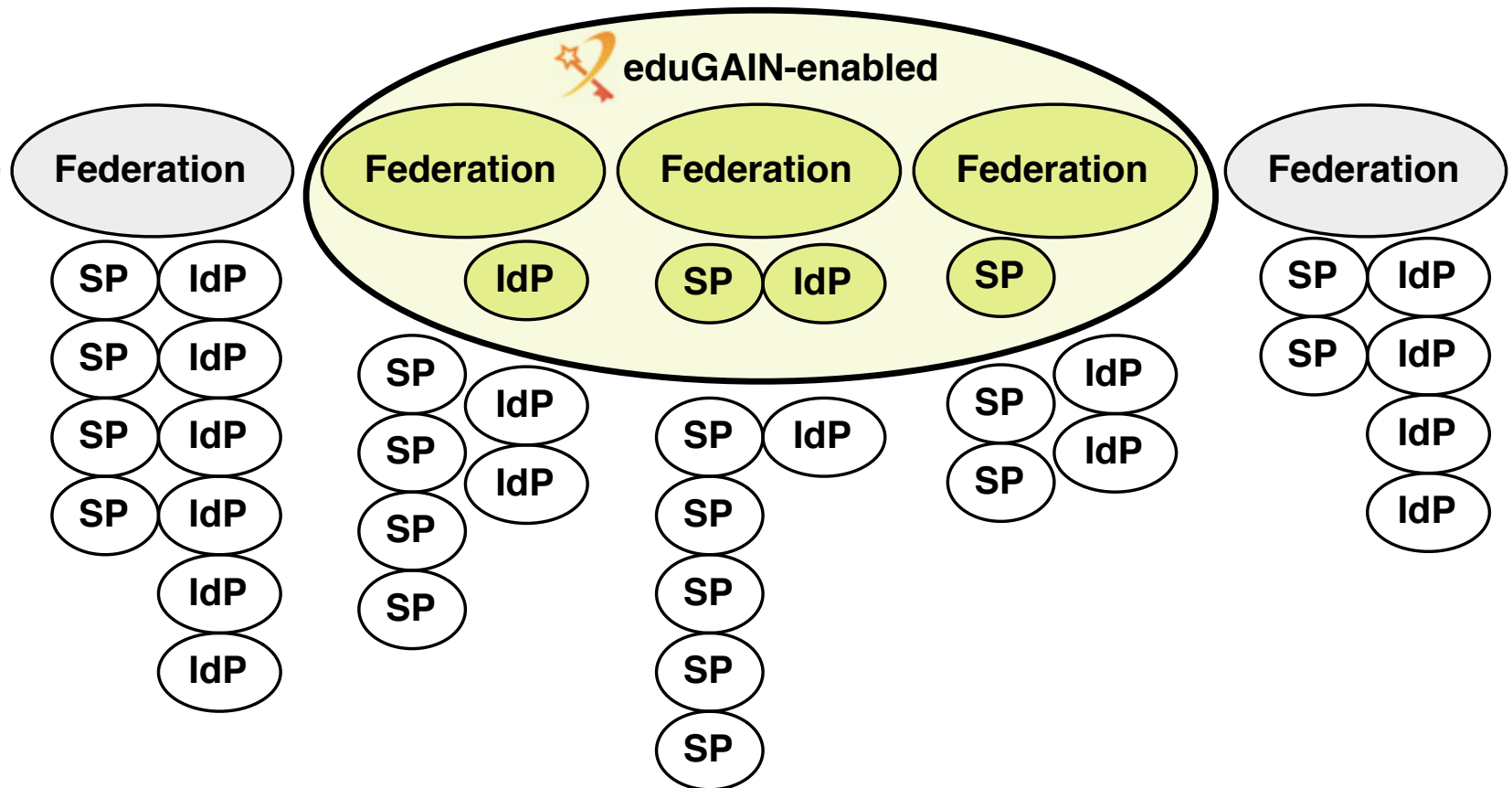
<https://technical.edugain.org/status.php>

- Status in CH
 - 20 IdPs enabled
 - ~ 52% of the accounts
 - 8 SPs enabled
 - 31 institutions signed the Interfederation Access Declaration

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



eduGAIN Adoption Width vs. Depth

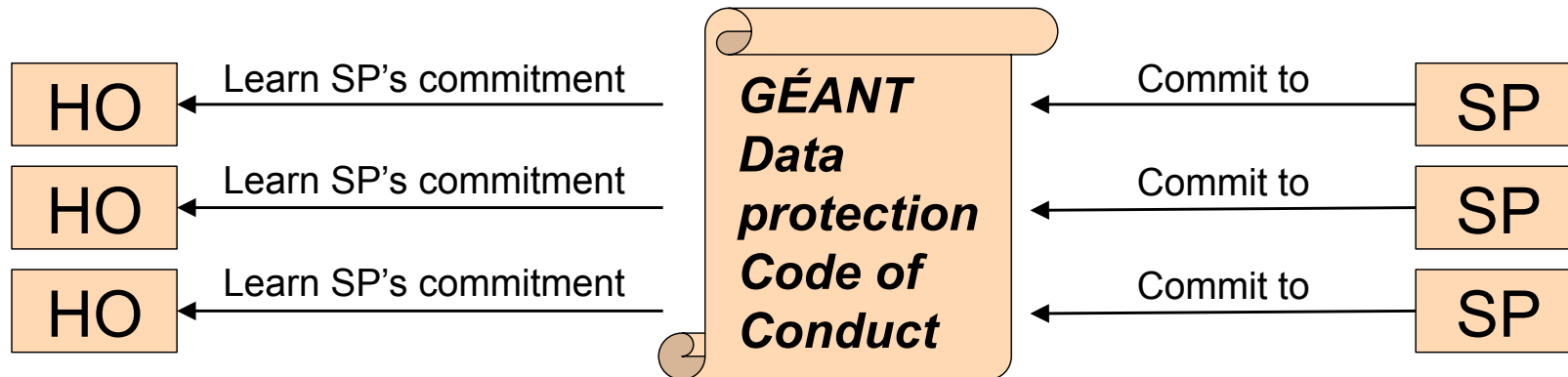


- Good federation adoption (Width)
- Entity Adoptions (Depth) is growing for IdPs (150% increase from 2014 to 2015)
- Not every SP and IdP has requirements to interfederate

GÉANT Code of Conduct – Data Protection within eduGAIN

We need to increase the trust in Service Providers (SPs)

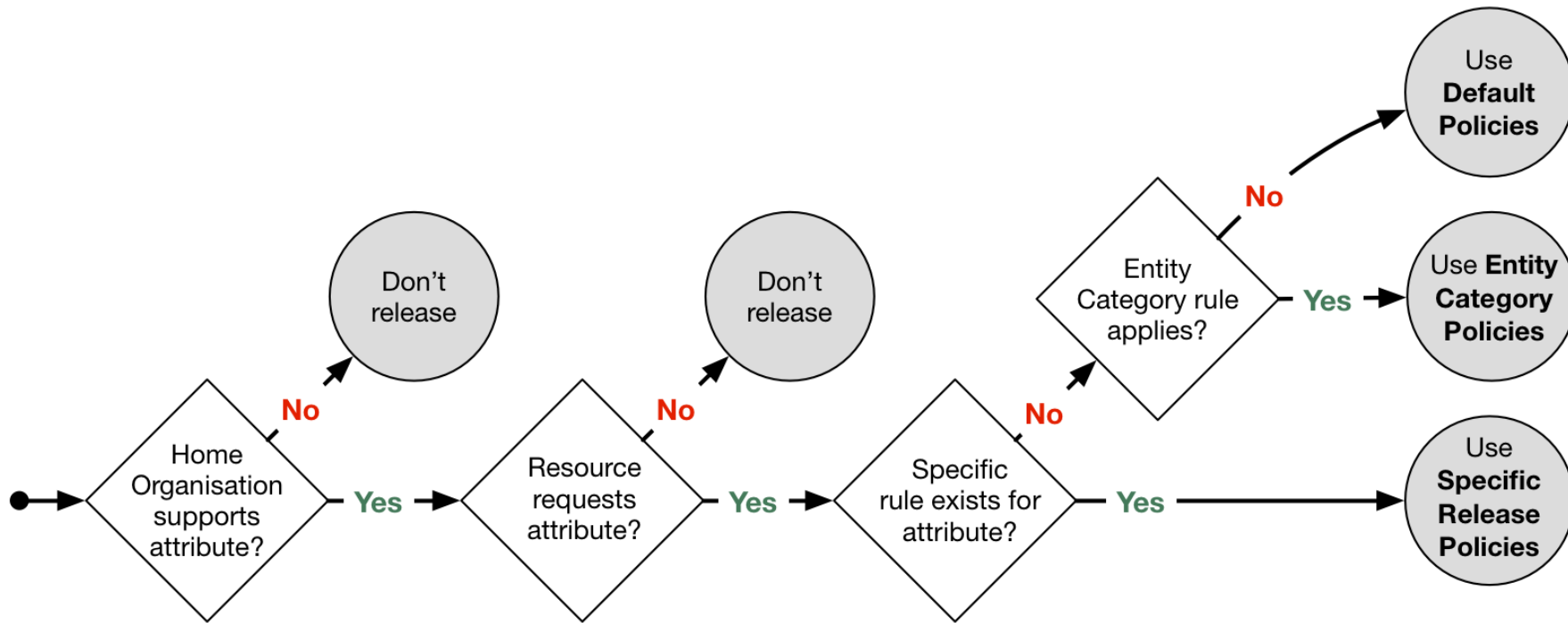
- The method is based on the EU Data Protection directives
- That will encourage the Home Organisation IdP to release attributes



Code of Conduct Toolkit

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

Attribute Release Rules



1
2
3

Attribute Release Settings (1)

Resource Registry –
Edit Home Organization Description –
Attribute Release Settings

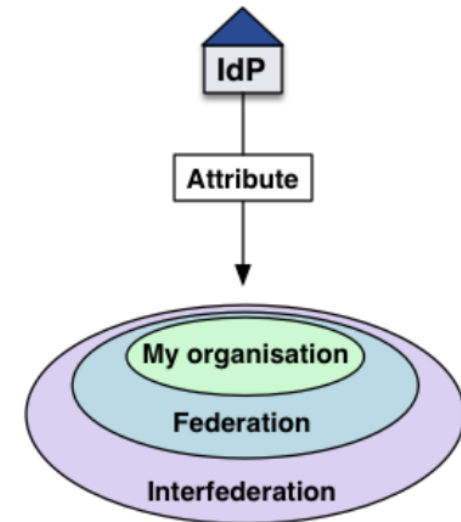
1. Default Policies for Individual Attributes

Individual default Attribute Release Policy rules apply if no Resource Specific Attribute Release Policy rule exists and if the Service Provider is not in one of the above Entity Categories. Only [supported attributes](#) are listed below.

Release Scopes

The release policy rules for individual attributes allow to set one of the following release scopes to which to release an attribute by default. Release attribute to:

- **Nobody**: The attribute is never released except if there is a Resource Specific Attribute Release Policy rule, which overrides all other rules.
- Resources of **My organization** (SWITCH): The attribute is released only to [resources of SWITCH](#), excluding Federation Partner resources.
- Resources in the (SWITCHaai) **Federation**: The attribute is released to all [SWITCHaai resources](#).
- **Interfederation** (e.g. [eduGAIN](#)) resources: The attribute is released to [all interfederation resources](#) as well as to all Resources from the enclosed release scopes. The following attributes are recommended to be released to interfederation resources if they are required:
 - Principal Name (unique identifier)
 - Targeted ID (unique identifier)
 - Affiliation (e.g. staff, student, faculty, affiliate)
 - Scoped affiliation (same as affiliation but domain name appended)
 - E-Mail
 - Display Name (full name)
 - Common Name (same as display name but can be multi-valued)
 - SCHAC Home Organisation (like Swiss Home Organization)
 - SCHAC Home Organisation Type (similar like Swiss Home Organization Type)



Release ...

... required attributes to

... desired attributes to

Have a look at the diagram above in order to understand the effects of the different policy choices below.

SWITCHaai Attributes

Affiliation (**core**) ⓘ

interfederation resources ▾

SWITCHaai resources ▾

Attribute Release Settings (2)

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.

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.

3. Resource Specific Policies

Resource Specific Attribute Release Policy rules have always precedence over all other attribute release policies. Set or review the specific rules: [Resource Specific Attribute Release Policy rules](#).

Why should you care?

There are 8176 international projects with participants from Switzerland in the CORDIS [1] database of the European Commission



Probably some researchers from your institution are participating in one of them

[1] Community Research and Development Information Service

One example

DARIAH

- Digital Research Infrastructure for the Arts and Humanities

Cooperating Swiss partners

- University of Basel
- University of Bern
- University of Geneva
- University of Lausanne
- University of Zurich
- Swiss Academy of Humanities and Social Sciences

eduGAIN Access Check

Also a Topic of Interest for SWITCHaai?



SWITCH

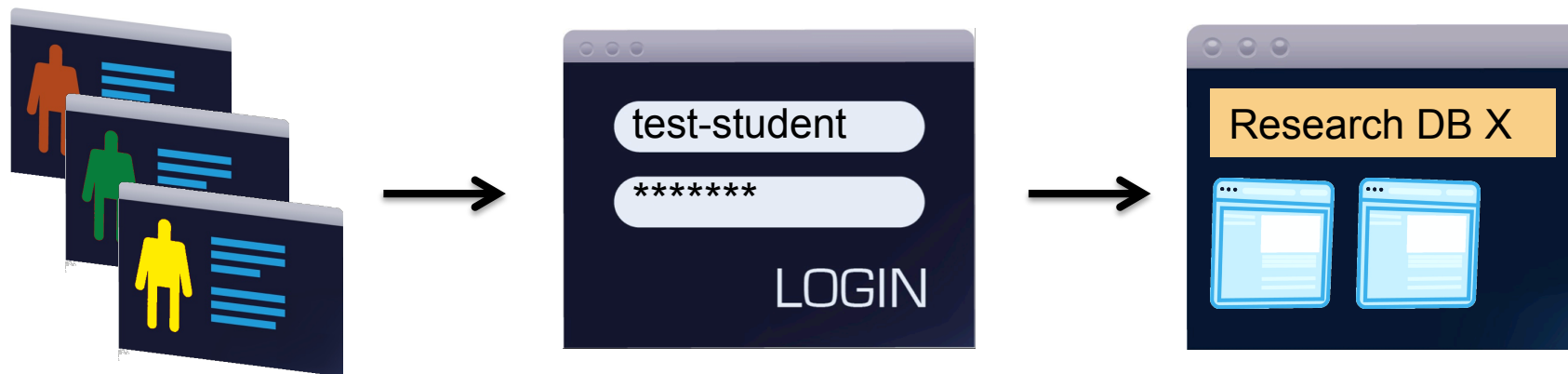
Lukas Hämmerle
lukas.haemmerle@switch.ch

Bern, 13. August 2015

What is this presentation about?

- SWITCH is sometimes asked by (commercial) SP admins:
"Can I get a test account in AAI to test my service?"
- **Why do some SP admins need test accounts?**
 - To validate their SP's behavior also in production environment
- **What's the problem with this request?**
 - (Test) accounts which are not linked to real persons are not allowed in AAI
 - Organisations don't create test identities for people outside their organisation
 - VHO accounts are of limited use for tests and not easy to get
- **Even greater need in Interfederation/eduGAIN context**
 - Federation Partners and their suppliers, cloud providers and research communities often don't have AAI accounts (yet) to test AAI login on their own AAI services
 - GÉANT "Enabling Users" task (led by SWITCH) decided to build **eduGAIN Access Check** service to provide a solution

The eduGAIN Access Check Basics



Create service-specific **test accounts** with different profiles

Use them for login on **own service only**

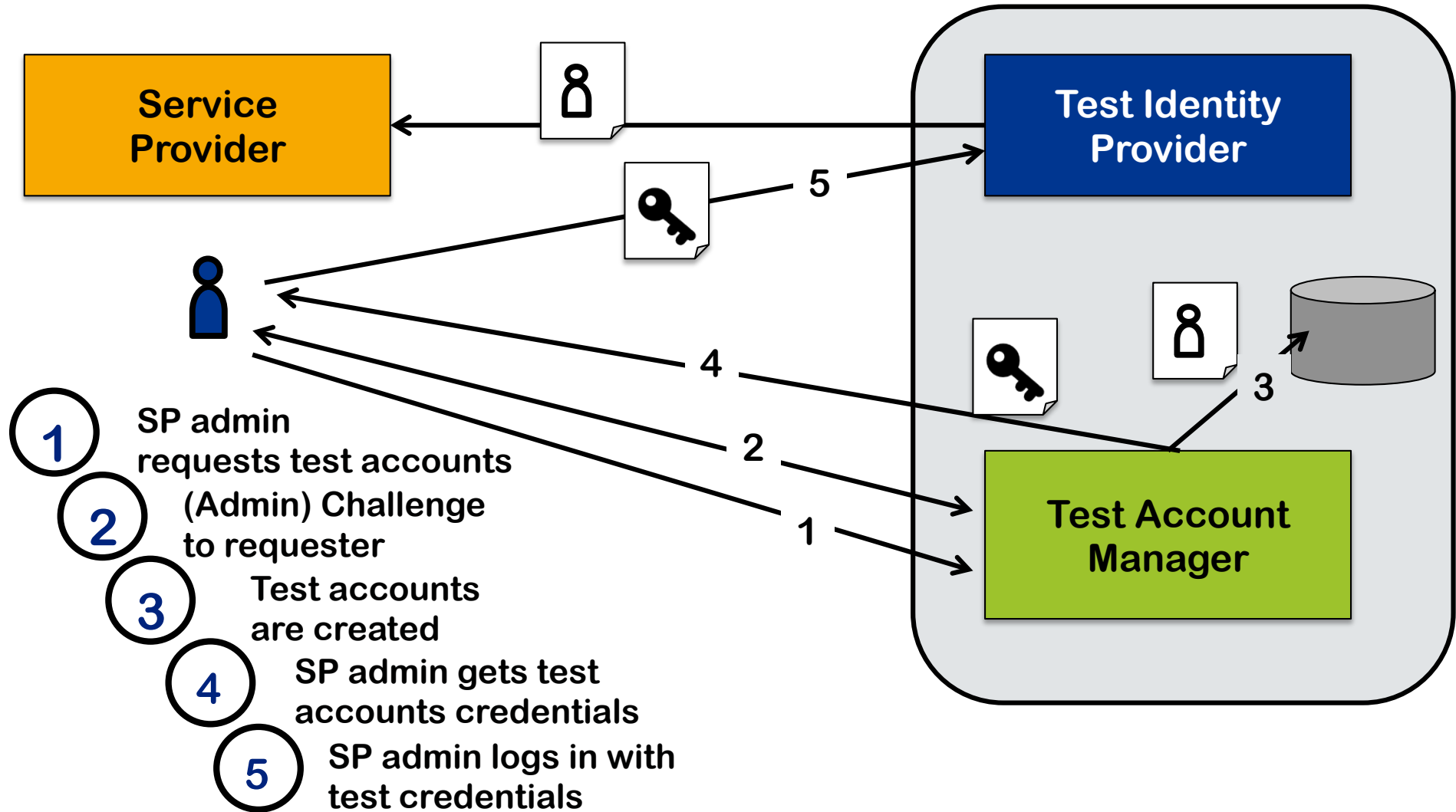
Check if access works and attributes are available

- **eduGAIN Access Check acts as Identity Provider** in eduGAIN
- Mainly useful for service operators without an own AAI/federated login (e.g. commercial cloud providers) but generally for AAI SP admins

Purpose of eduGAIN Access Check

- **A self-service test account provider within eduGAIN to help test access/attribute release to an own federated service**
- **Multiple test accounts with varying attribute sets**
 - with different profiles to simulate real users (incl. non-ascii characters)
 - with different release policies to simulate different IdP behaviors (R&S/CoCo support, missing attributes, all attributes)
- **Restricted use**
 - Validated SP admins can use test accounts to access own service only
 - Test account credentials (currently) expire after a few days
 - Attribute set is fixed and values cannot be changed
 - Identities are clearly marked as test identities

How does Access Check work?



Access Check Screenshots



eduGAIN Access Check

eduGAIN Access Check?

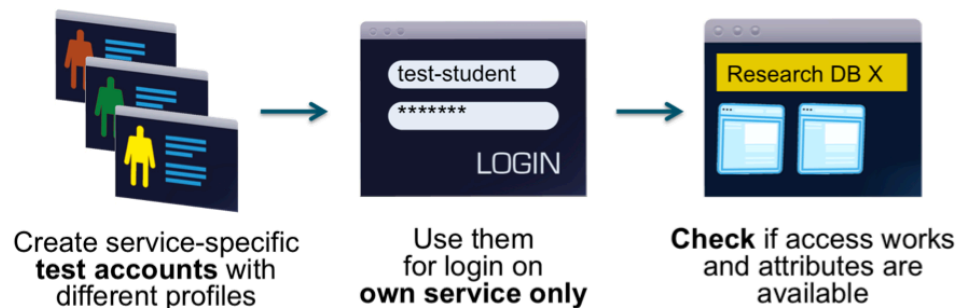
eduGAIN Access Check allows administrators of a Service Provider (SP) registered in [eduGAIN](#) to create test accounts with different profiles to validate the behaviour and test federated login. The test accounts can only be used to access own services. [Learn more about this service...](#)

Start testing your eduGAIN service

To start testing your own eduGAIN service, start by selecting the Service Provider you are administrator for.

[Go on testing the service](#)

eduGAIN Access Check basics



<https://access-check.edugain.org/>

Step 1: Select an AAI Service



eduGAIN Access Check

1. Select your Service Provider

2. Send email challenge

3. Complete Email Challenge

4. Test Accounts

Select your Service Provider

Please search and select the Service Provider that you want to test in the list below. You must be an administrator of that Service Provider to continue afterwards.

Type the SP name or entityID to search for it.

Note that only Service Providers are in the list which are included in the eduGAIN metadata.

▼

- AAI Attributes Viewer (<https://attribute-viewer.aai.switch.ch/shibboleth>)
- AAI Viewer Interfederation Test (<https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth>)
- Haka Attribute Test Service (<https://rr.funet.fi/attribute-test>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) Calendar Server (<https://calendar.larpp.internet2.edu/shibboleth>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) List Manager (<https://list-manager.larpp.internet2.edu/shibboleth>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) Registry (<https://registry.larpp.internet2.edu/shibboleth>)
- Lifestyles of the Attribute Rich and Privacy Preserved (LARPP) Wiki (<https://wiki.larpp.internet2.edu/shibboleth>)

Step 2a: Send (Admin) Challenge

eduGAIN Access Check

1. Select your Service Provider

2. Send email challenge

3. Complete Email Challenge

4. Test Accounts

Send email challenge

Before you can create test accounts at this Identity Provider, we need to ensure you are a legitimate administrator of "AAI Attributes Viewer".

Select your email address

The email addresses below have been extracted from your SP SAML metadata.

Please select the email address where an email challenge can be sent to validate your identity

aai@switch.ch

Previous

Next

Step 2b: Email Challenge

From eduGAIN Access Check <edugain-access-check@geant.net> ☆
Subject eduGAIN Access Check - Test accounts request 15:55
To SWITCHaai Support ☆

This is an email challenge automatically sent to you by eduGAIN Access Check.
viewer.aai.switch.ch/shibboleth.
The address aai@switch.ch is mentioned in the eduGAIN metadata as a contact f
To complete the creation of test accounts, paste the following validation tok

Validation token: 3515c026f6752e8711b3

eduGAIN Access Check: <https://access-check.edugain.org/accountmanager>

If the creation of test accounts was not initiated by you or a fellow adminis
integration@geant.net to inform them about a potential abuse of the eduGAIN A

Best Regards
eduGAIN Access Check Bot

Step 2c: Enter Challenge One Time Token



eduGAIN Access Check

1. Select your Service Provider

2. Send email challenge

3. Complete Email Challenge

4. Test Accounts

Complete Email Challenge

An email challenge including a validation token has been emailed to you at aai@switch.ch. Please copy and paste the validation token in the form below to prove that you are administrator of this service.

Validation Token

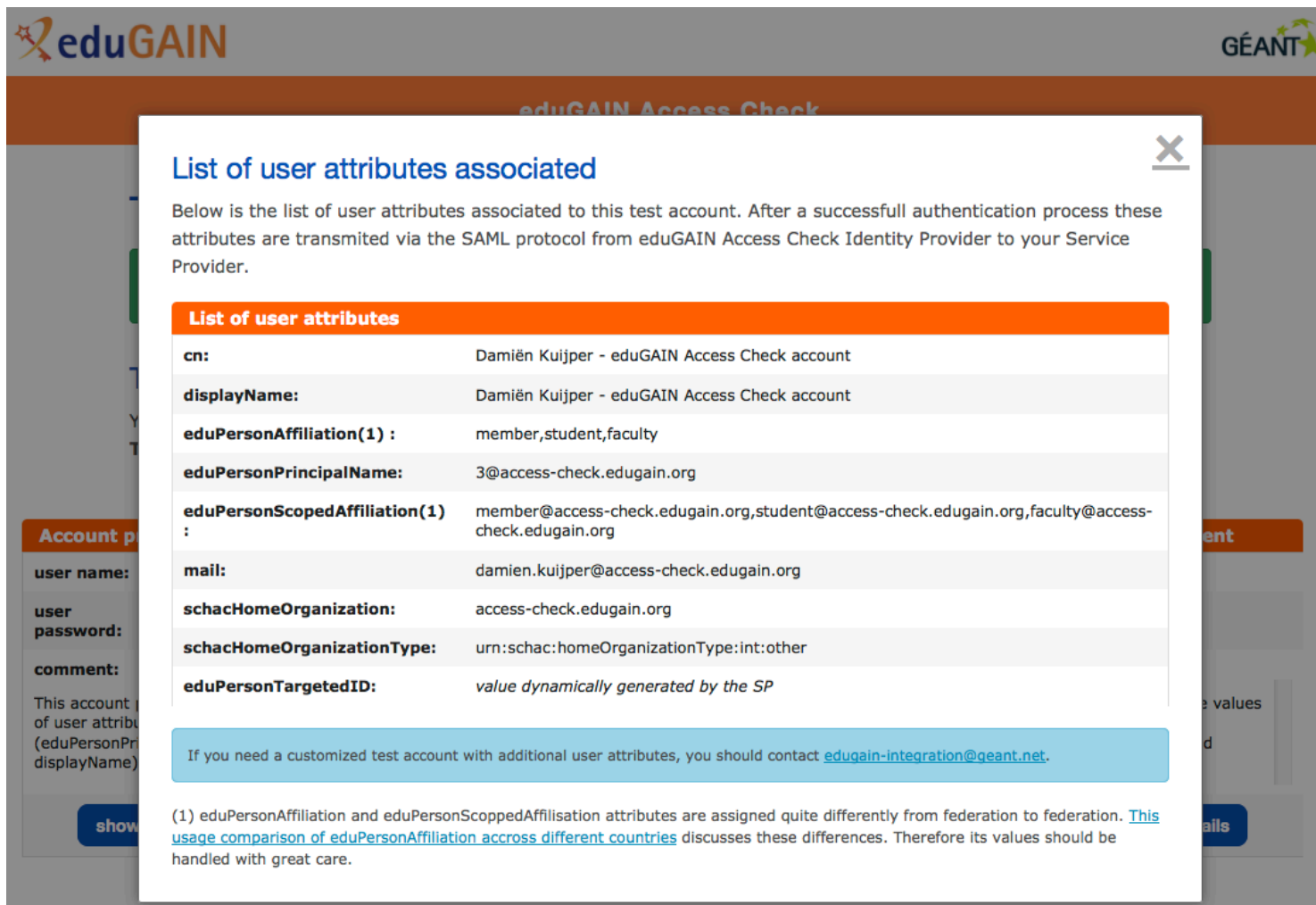
Please provide the validation token here:

3515c026f6752e8711b3

Previous

Next

Step 3: Inspect Test Account Profiles



The screenshot shows the eduGAIN Access Check interface. A modal window titled "List of user attributes associated" is displayed. The modal contains a list of user attributes for a test account. The attributes are as follows:

List of user attributes	
cn:	Damiën Kuijper - eduGAIN Access Check account
displayName:	Damiën Kuijper - eduGAIN Access Check account
eduPersonAffiliation(1) :	member,student,faculty
eduPersonPrincipalName:	3@access-check.edugain.org
eduPersonScopedAffiliation(1) :	member@access-check.edugain.org,student@access-check.edugain.org,faculty@access-check.edugain.org
mail:	damien.kuijper@access-check.edugain.org
schacHomeOrganization:	access-check.edugain.org
schacHomeOrganizationType:	urn:schac:homeOrganizationType:int:other
eduPersonTargetedID:	<i>value dynamically generated by the SP</i>


Below is the list of user attributes associated to this test account. After a successful authentication process these attributes are transmitted via the SAML protocol from eduGAIN Access Check Identity Provider to your Service Provider.

If you need a customized test account with additional user attributes, you should contact edugain-integration@geant.net.

(1) eduPersonAffiliation and eduPersonScopedAffiliation attributes are assigned quite differently from federation to federation. [This usage comparison of eduPersonAffiliation across different countries](#) discusses these differences. Therefore its values should be handled with great care.

Step 4: Initiate Login to Your Service

AAI Attribute Viewer



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

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

Login with: > AAI

eduGAIN Access Check

Remember selection for this web browser session. Login

Alternatively, log in [using an AAI Test Home Organisation](#) or the [Shibboleth Embedded Discovery Service](#).

Use the links below to display the Embedded WAYF in another language.

Display the Embedded WAYF on this page in:
[In English](#) | [In French](#) | [In German](#) | [In Italian](#)

Test central WAYF:
[In English](#) | [In French](#) | [In German](#) | [In Italian](#)

Step 5: Login with Test Account



eduGAIN Access Check

[English](#) | [Bokmål](#) | [Nynorsk](#) | [Sámegiella](#) | [Dansk](#) | [Deutsch](#) | [Svenska](#) | [Suomeksi](#) | [Español](#) | [Français](#) | [Italiano](#) | [Nederlands](#) | [Lëtzebuergesch](#) | [Čeština](#) | [Slovenščina](#) | [Lietuvių kalba](#) | [Hrvatski](#) | [Magyar](#) | [Język polski](#) | [Português](#) | [Português brasileiro](#) | [Türkçe](#) | [日本語](#) | [简体中文](#) | [繁體中文](#) | [русский язык](#) | [eesti keel](#) | [עברית](#) | [Bahasa Indonesia](#) | [Srpski](#) | [Latviešu](#) | [Românește](#) | [Euskara](#)

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

The login form is enclosed in a red rounded rectangle. It contains two input fields: 'Username' with the value 'user1' and 'Password' with masked characters '.....'. A blue 'Login' button is positioned below the password field. A yellow key icon is located to the left of the password field.

Help! I don't remember my password.

Too bad! - Without your username and password you cannot authenticate yourself for access to the service. There may be someone that can help you. Consult the help desk at your organization!

eduGAIN Access Check open Beta 1 - [contact us](#)

Test Account Profiles

- eduGAIN Test IdP creates sets of test accounts with:
 - different user profiles (faculty, student, staff),
 - varying set of attributes and values (including non-ascii chars)
- eduGAIN Test IdP will behave like an average IdP regarding attribute release (CoCo, R&S)
- Test accounts profile customization
 - requester should have the ability to customize attribute values
 - planned for phase II of the service

Access Check also for SWITCHaai?

- Currently eduGAIN Access Check can only be used by SWITCHaai services that enabled Interfederation/eduGAIN support
- **Should localized version of Access Check also be included in SWITCHaai?**
 - Access Check IdP metadata would be in SWITCHaai metadata
 - Would not be shown in WAYF/Discovery Service by default due to standardized "Hide-from-Discovery" entity category in metadata. Manually enable in Embedded WAYF or use login link.
 - Would provide SWITCHaai-specific attributes (e.g. uniqueID)