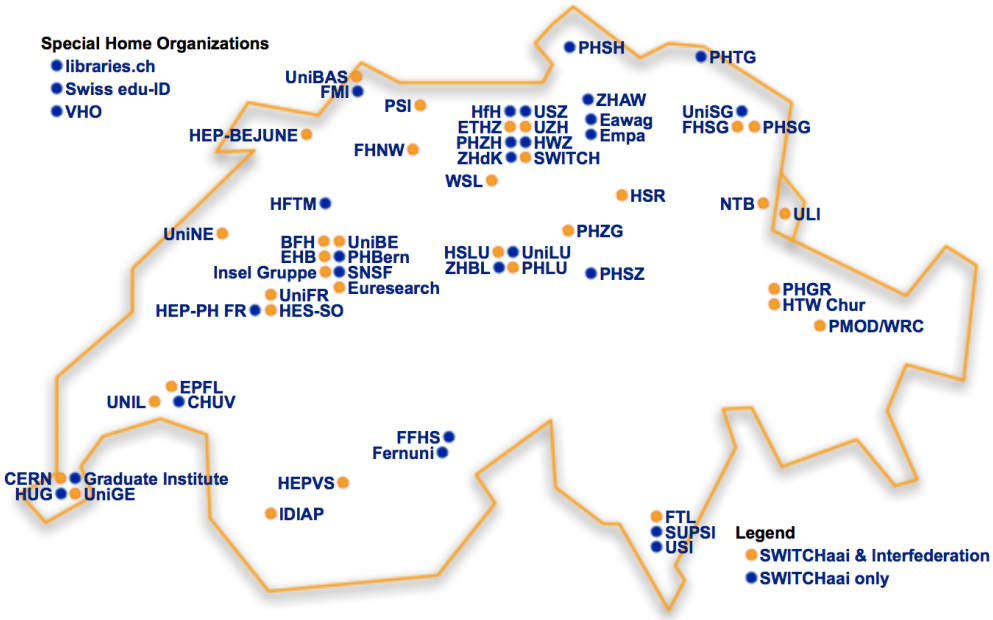
SWITCHaai Status Update

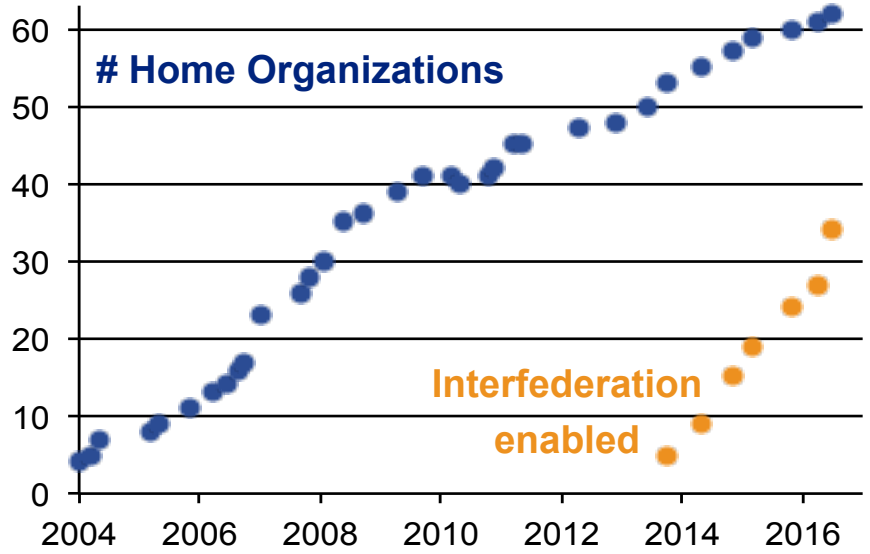
SWITCH

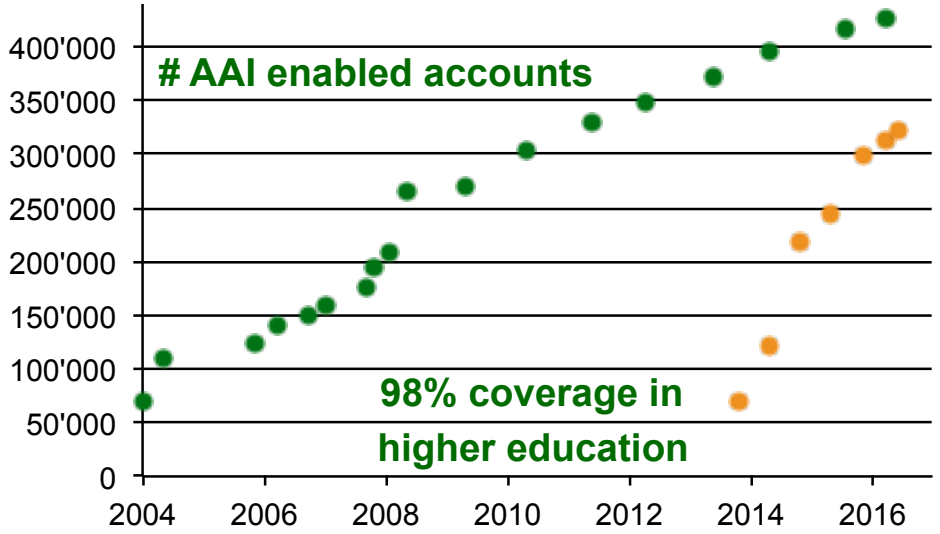
Thomas Lenggenhager
aai@switch.ch

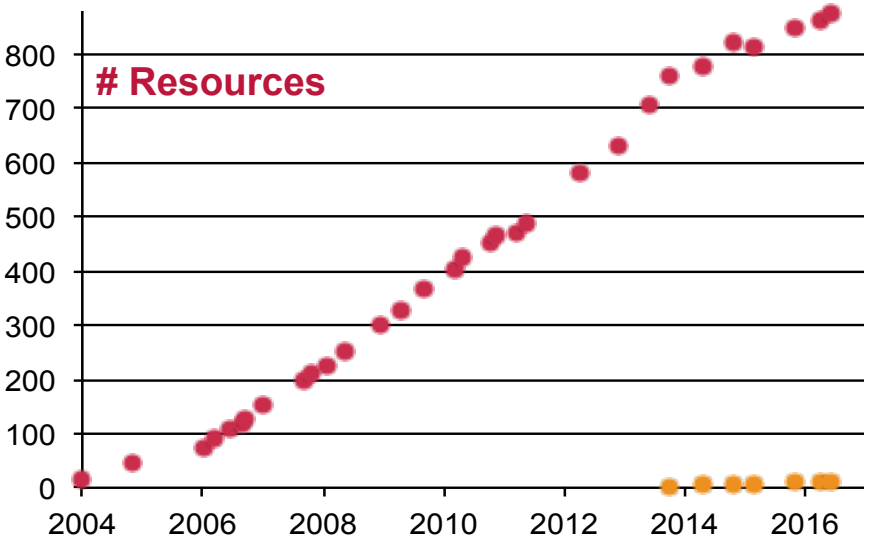
Berne, 30. June 2016

SWITCHaai Federation Summer 2016

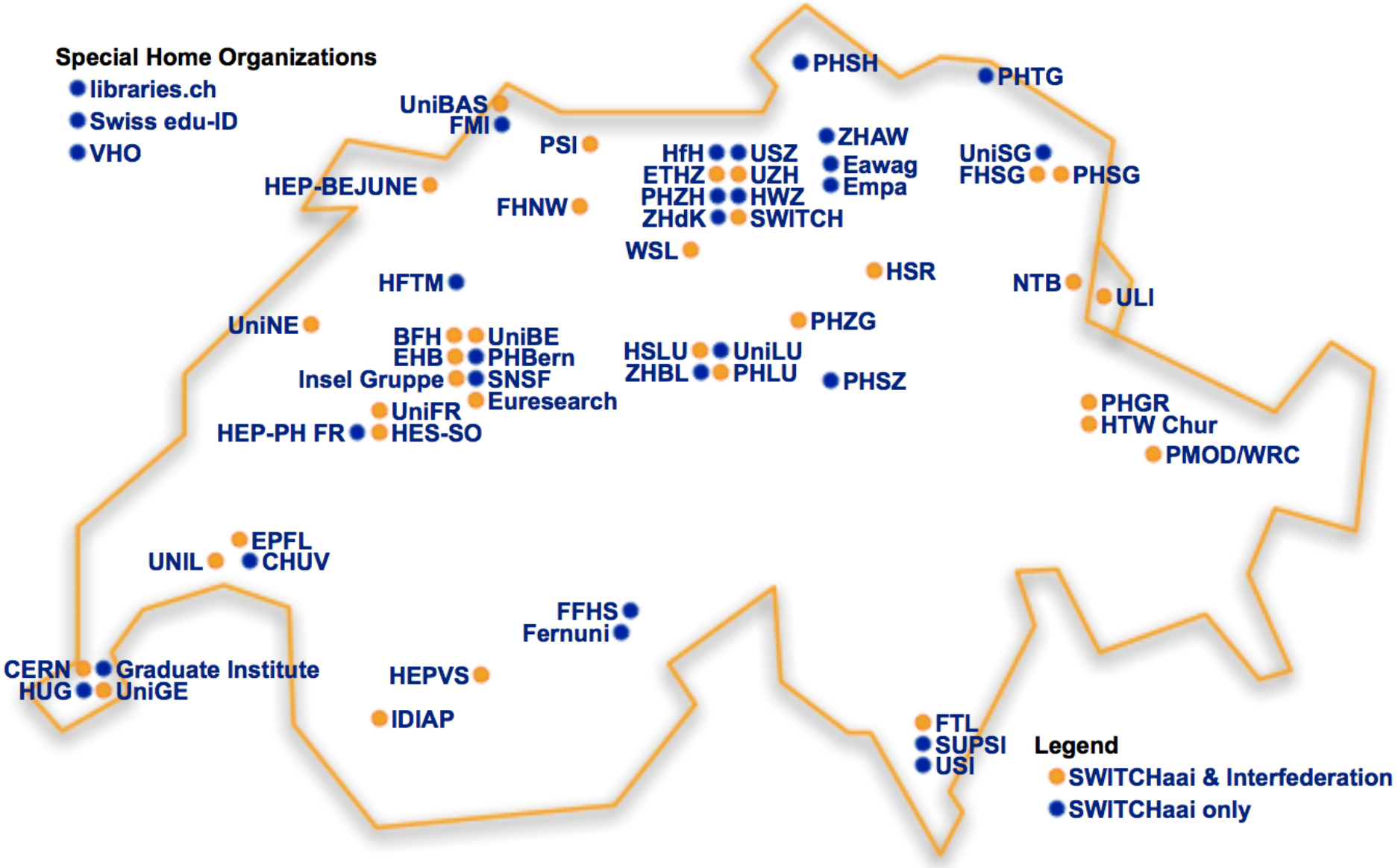








SWITCHaai Federation Summer 2016



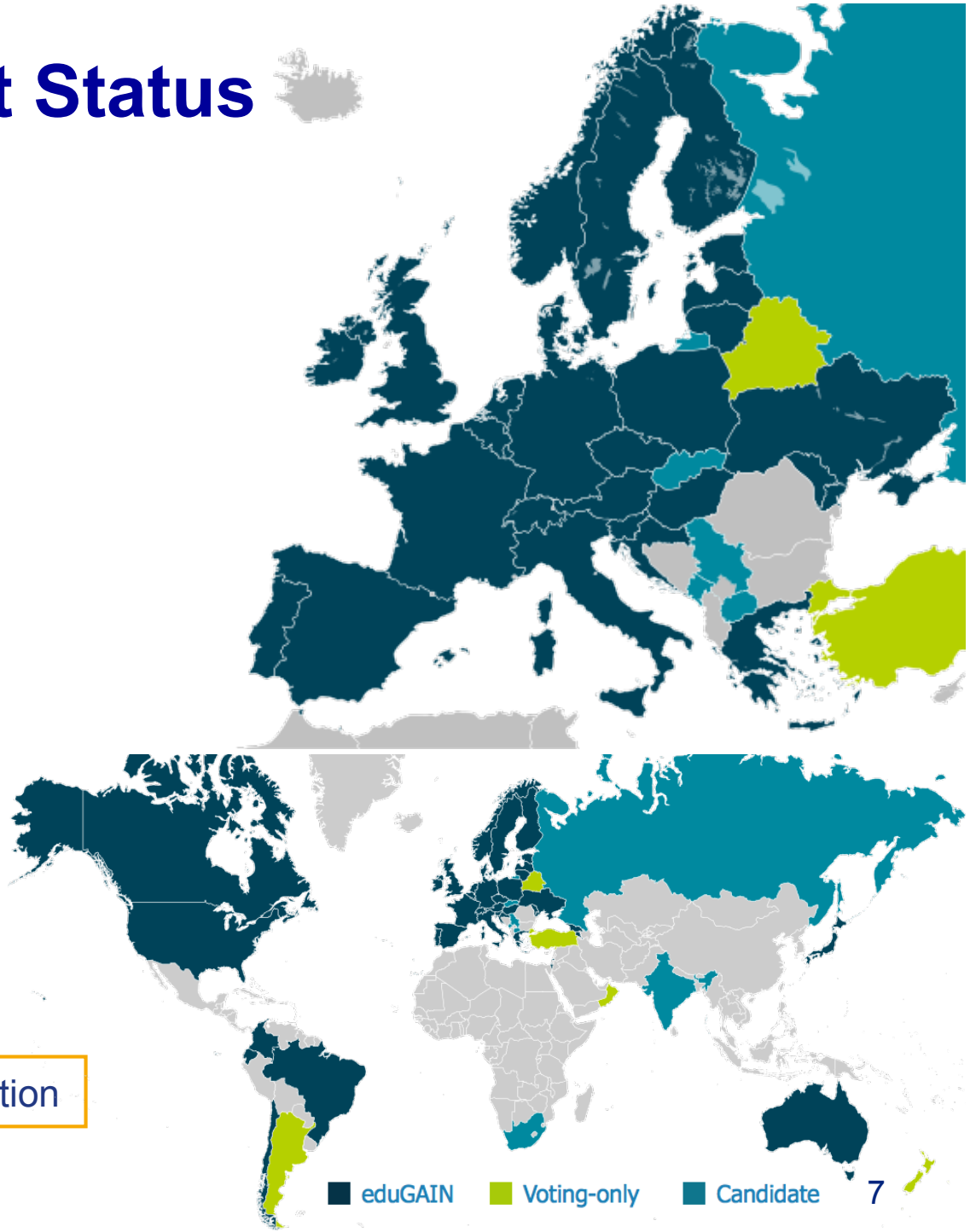
eduGAIN: Current Status

- eduGAIN in Total
  - 2140 IdPs, 1224 SPs

https://technical.edugain.org/status

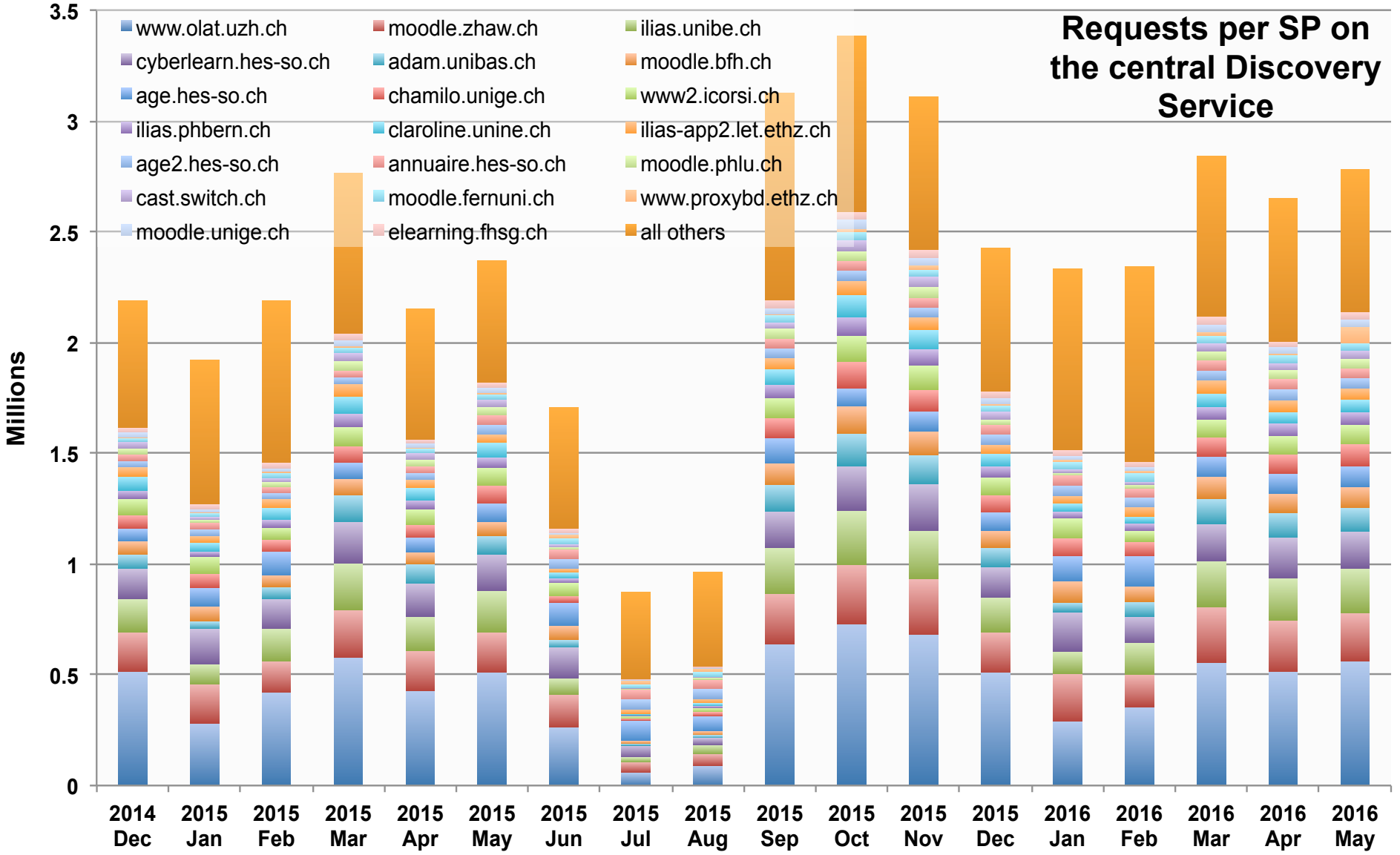
- Status in CH
  - 34 IdPs enabled
    ~ 76% off all AAI accounts
  - 10 SPs enabled
  - 51 institutions signed
    the Interfederation
    Access Declaration

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



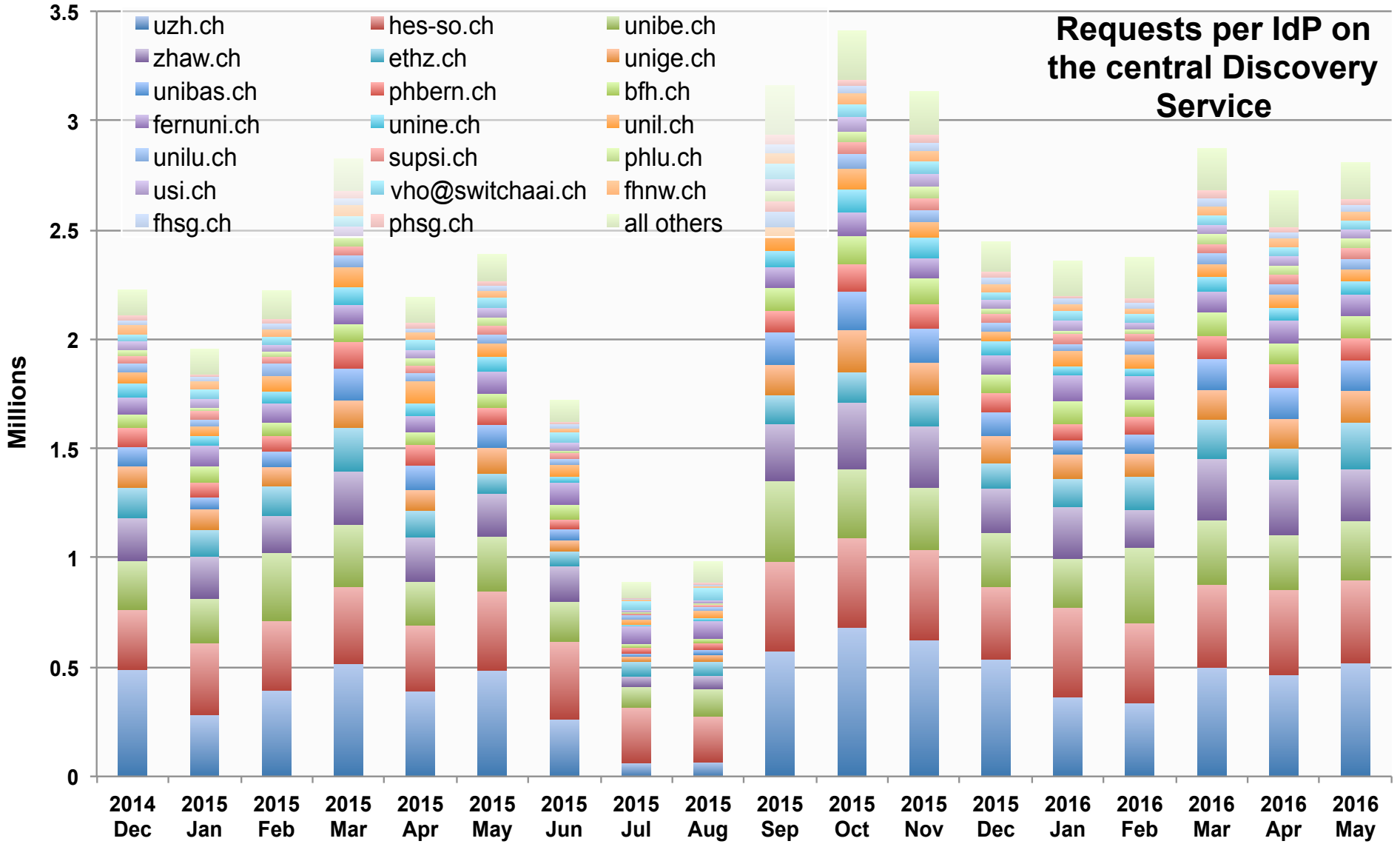
AAI User Authentication Requests

Dec 14 - May 16



AAI User Authentication Requests

Dec 14 - May 16



Next on the Shibboleth Roadmap

- SP 2.6 29 June 2016
  - Attribute Query Handler included
  - Many fixes and several new features

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPReleaseNotes

- IdP 3.3 planned for Q4 2016
  - Fix for logout flow and many more
  - More scripted attributes possibilities

https://wiki.shibboleth.net/confluence/display/IDP30/ReleaseNotes

FHNW OpenID Connect pilot

The (SAML) World is not enough …

Agenda

- Business use case
- Technical requirements
- OpenID Connect (OIDC)
- SAML vs. OIDC vs. Oauth
- Implicit Flow
- Architecture
- Implementation
- Demo

Business use case

- Webbased registration for any kind of «events» managed in administration system «Evento», e.g. certificate courses, conferences, information events, sports activities, …
- Required information during registration is very diverse between various event types and target groups (eg. catering options, workshop sign-up, etc.)
- Authentication via AAI (existing FHNW students/staff) and
  Swiss edu-ID must be possible, as well as unauthenticated registration (guest)
- Flexible web application that can be easily integrated in any kind of
  web page, CMS, infrastructure, etc. (e.g. SharePoint-based intranet).

Technical requirements

- Solution based on JavaScript-Webclient and REST-Services
- Strategic technologies AngularJS and ASP.NET (WebApi)
- Lightweight authentication and authorization protocol with good support for untrusted clients and delegated access scenarios
- Generic approach and infrastructure

OpenID Connect (OIDC)

«A Simple Identity layer on top of OAuth 2.0»

From the website (http://openid.net):

- OIDC is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. It uses straightforward REST/JSON message flows with a design goal of «making simple things simple and complicated things possible». It's uniquely easy for developers to integrate, compared to any preceding Identity protocol.
- OIDC allows for clients of all types, including browser-based JavaScript and native mobile apps, to launch sign-in flows and receive verifiable assertions about the identity of signed-in users.

SAML vs OIDC vs OAuth

Simply said:

- SAML: single sign-on for enterprise users
- OAuth: API authorization between applications
- OIDC: single sign-on for consumers + API access

Token format:

- SAML: XML
- OIDC: JWT (JSON web token)

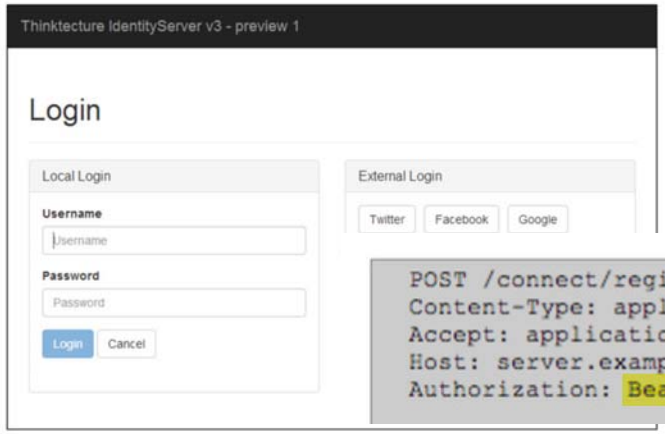
The whole story:

«Unifying Authentication & Delegated API Access for Mobile, Web and the Desktop with OpenID Connect and OAuth2 by Dominick Baier», https://vimeo.com/113604459

Implicit Flow

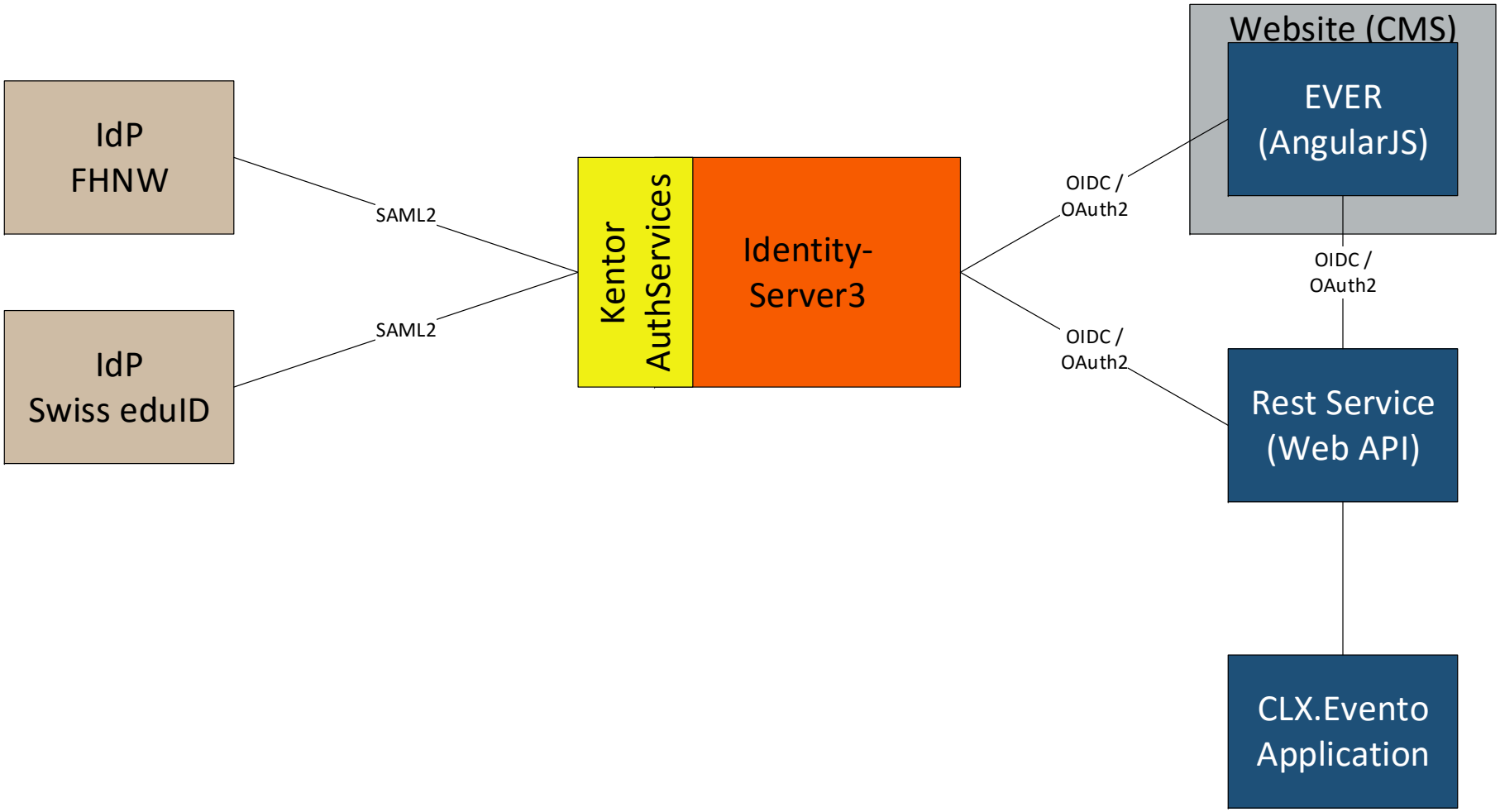
- One of multiple flows (processes) defined in the specification
- Specifically designed for «untrusted clients» such as JavaScript apps
- Key steps:
  - Client sends the request to the Authorization Server.
  - Authorization Server authenticates the End-User, obtains consent, sends him/her back to the Client with an ID Token and, if requested, an Access (Bearer) Token.
  - Client validates the tokens and retrieves the End-User's Subject Identifier.
  - Client uses the Access Token for calls to Backend Web Services

```
GET /authorize
?client_id=app1
&scope=openid profile
&redirect_uri=https://app.com/cb
&response_type=id_token token
&state=af0ifjsldkj
&nonce=n-0S6_WzA2Mj
```




```
POST /connect/register HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: server.example.com
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJ ...
```

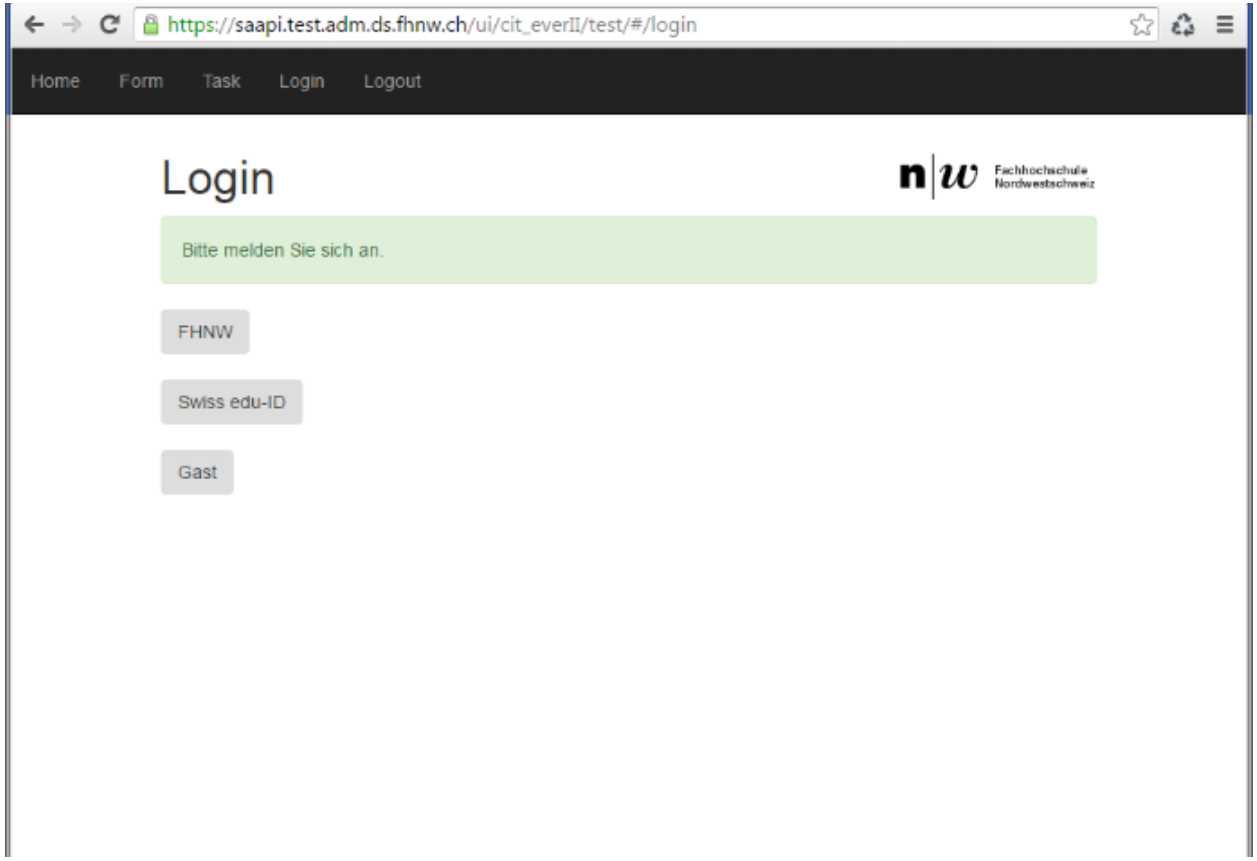
Architecture



Implementation

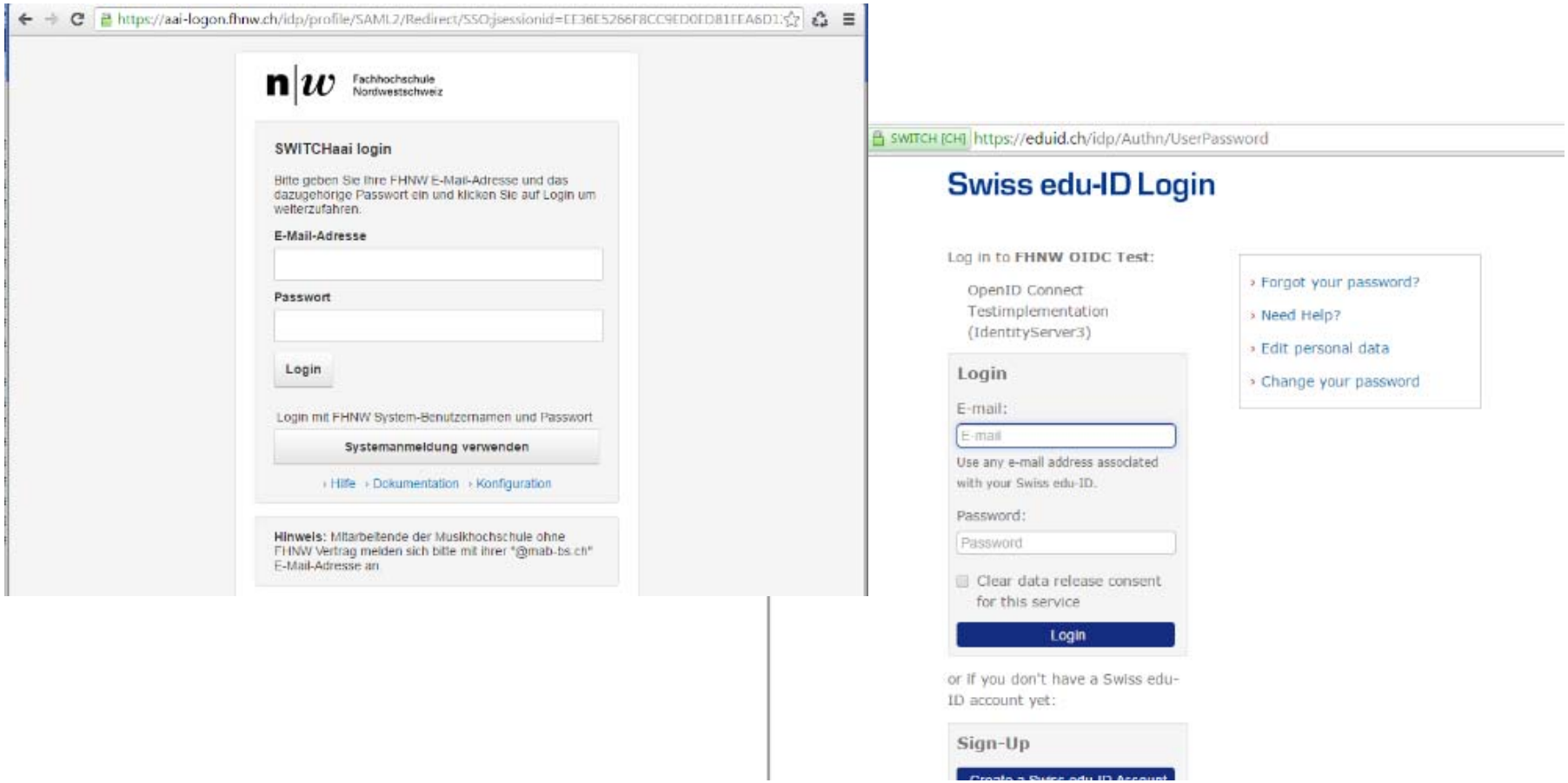
- **IdentityServer3**
  - OpenID Connect Provider and OAuth 2.0 Authorization Server Framework
  - Certified OpenID Connect implementation
  - Open Source
  - Based on ASP.NET web framework
  - https://github.com/IdentityServer/IdentityServer3
- **Kentor Authentication Services**
  - SAML2 Authentication services for ASP.NET
  - Open Source
  - https://github.com/KentorIT/authservices
- some extension code developed in-house

Demo (1/5)



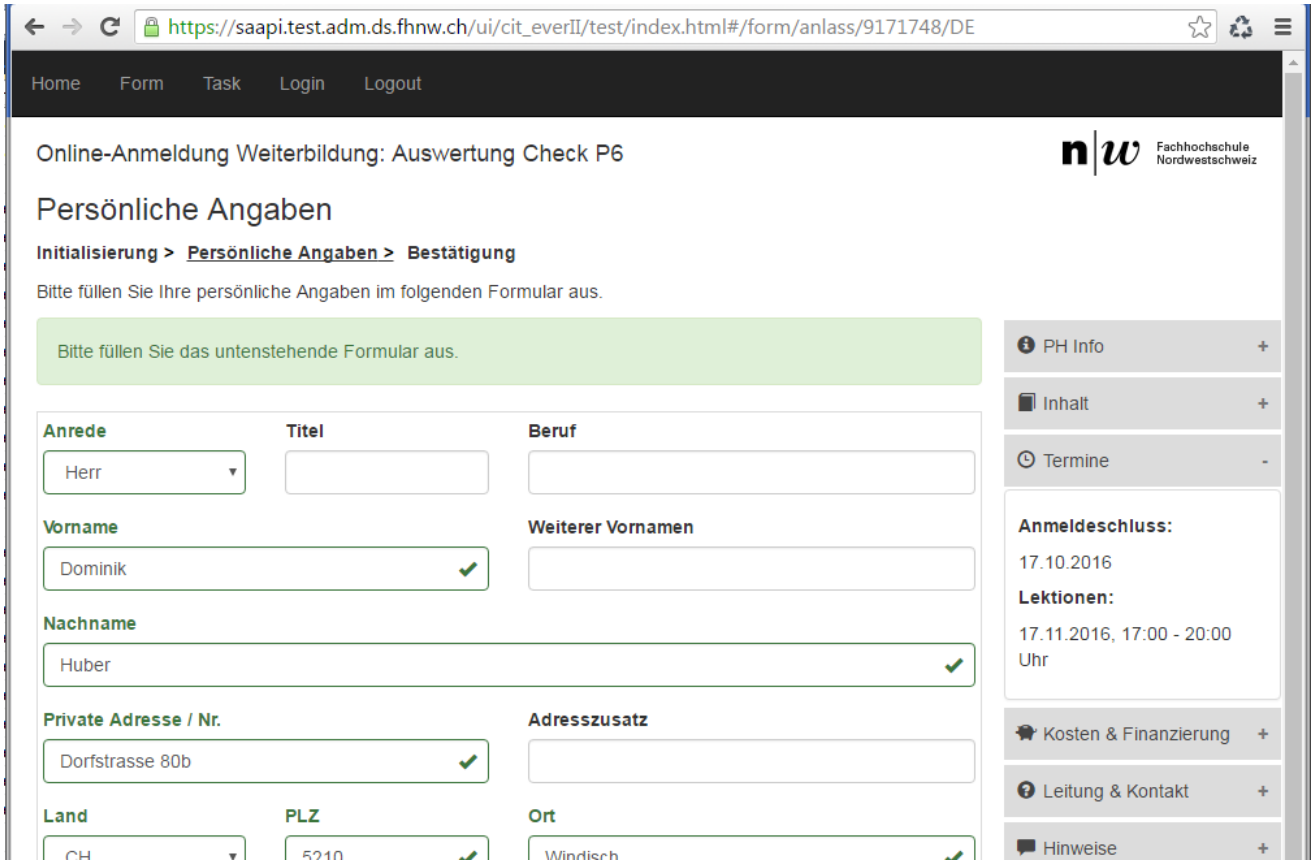
Discovery (to be integrated in application logic later)

Demo (2/5)



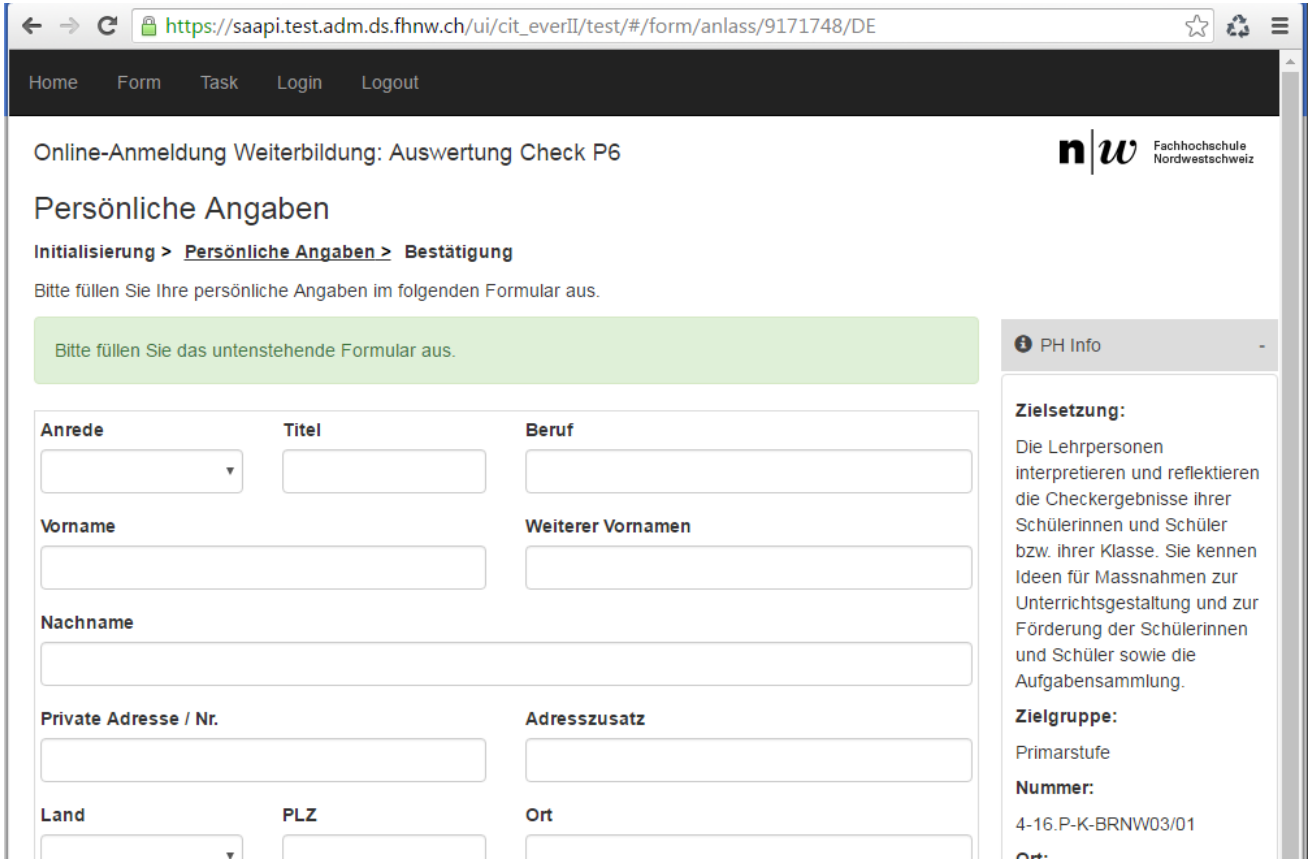
Login (AAI FHNW or Swiss edu-ID)

Demo (3/5)



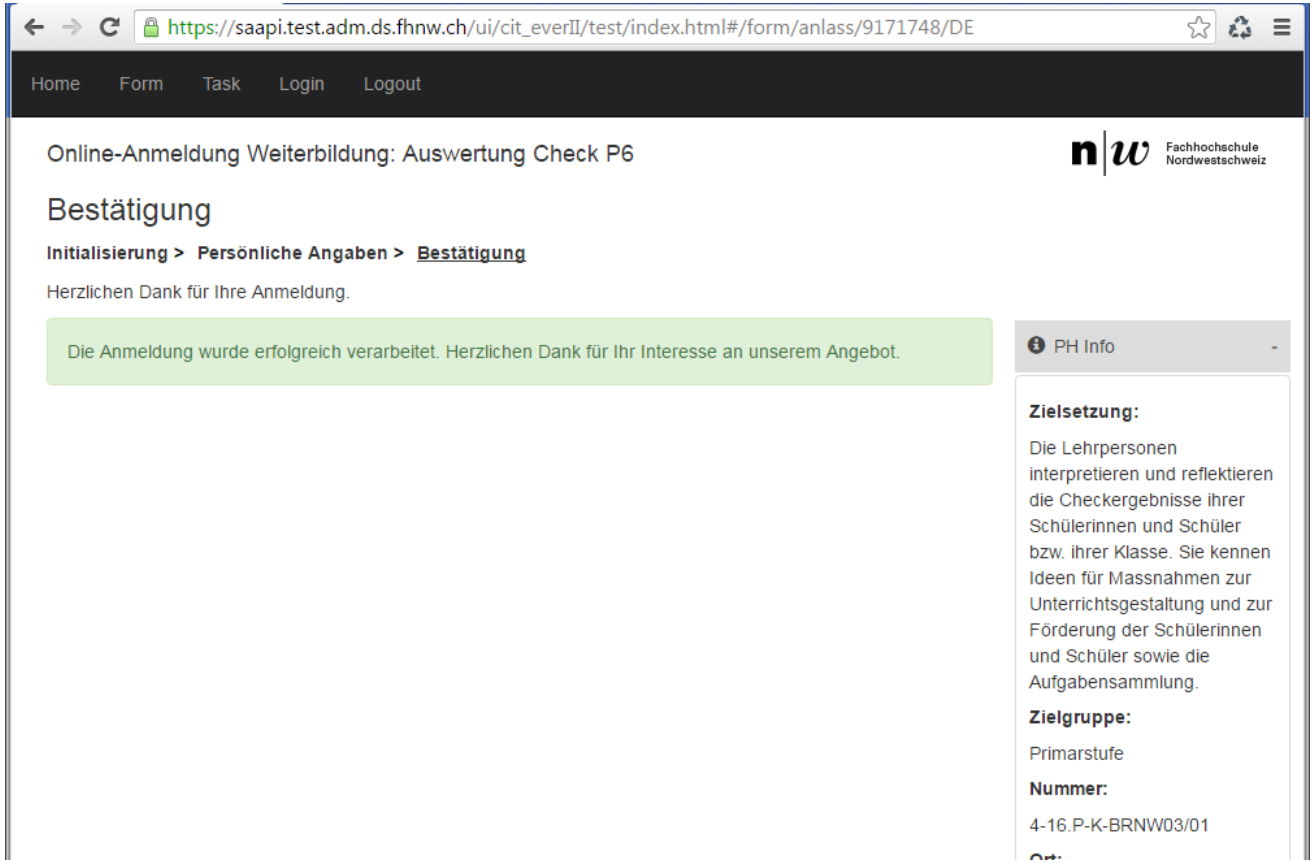
Personal data (authenticated)

Demo (4/5)



Personal data (unauthenticated)

Demo (5/5)



Confirmation

Questions?

Contact:

– Michael Hausherr, Enterprise Architect
T: +41 56 202 71 56, E: michael.hausherr@fhnw.ch
– Dominik Huber, Application Developer
T: +41 56 202 70 27, E: dominik.huber@fhnw.ch

OpenID Connect for Swiss edu-ID

SWITCH

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

What is OpenID Connect?

- OAuth 2.0: authorisation protocol for applications
- Adds “simple identity layer” on top of OAuth 2.0
- Easy solution for delegating access to protected resources
- Reinvents the wheel with JSON (see JW*)
- OpenID Connect 1.0 finalised early 2014
- Popular with web and mobile developers

Meanwhile, in our community...

- Very few concrete use cases for OAuth or OIDC so far
- SAML isn't going away soon
- Bridging SWITCHaai and OIDC is technically possible, see our example mobile proxy (https://www.switch.ch/aai/support/tools/aai-for-apps/)

Operate SAML and OIDC together

- Ask each institution to operate an OIDC service?
  ⇒ rollout too slow
- One IdP with OIDC for the whole federation
  ⇒ the Swiss edu-ID IdP!

Pilot IdP with OpenID Connect

- Shibboleth IdPv3 addon (https://github.com/uchicago/shibboleth-oidc) developed by the University of Chicago and Unicon
- Successfully tested by another team @SWITCH
- Open for other testers
- Manual client registration
- Contact us if you want to try

Other interesting projects

- Mapping eduPerson attributes to OIDC claims
  REFEDS OIDCre WG
  (https://wiki.refeds.org/display/GROUPS/OIDCre)
- OpenID Connect Federation draft
  (https://github.com/rohe/pyoidc/blob/master/oidc_fed/oidcfed.txt)

University of Zurich[UZH]

Zentrale Informatik – Business Applications

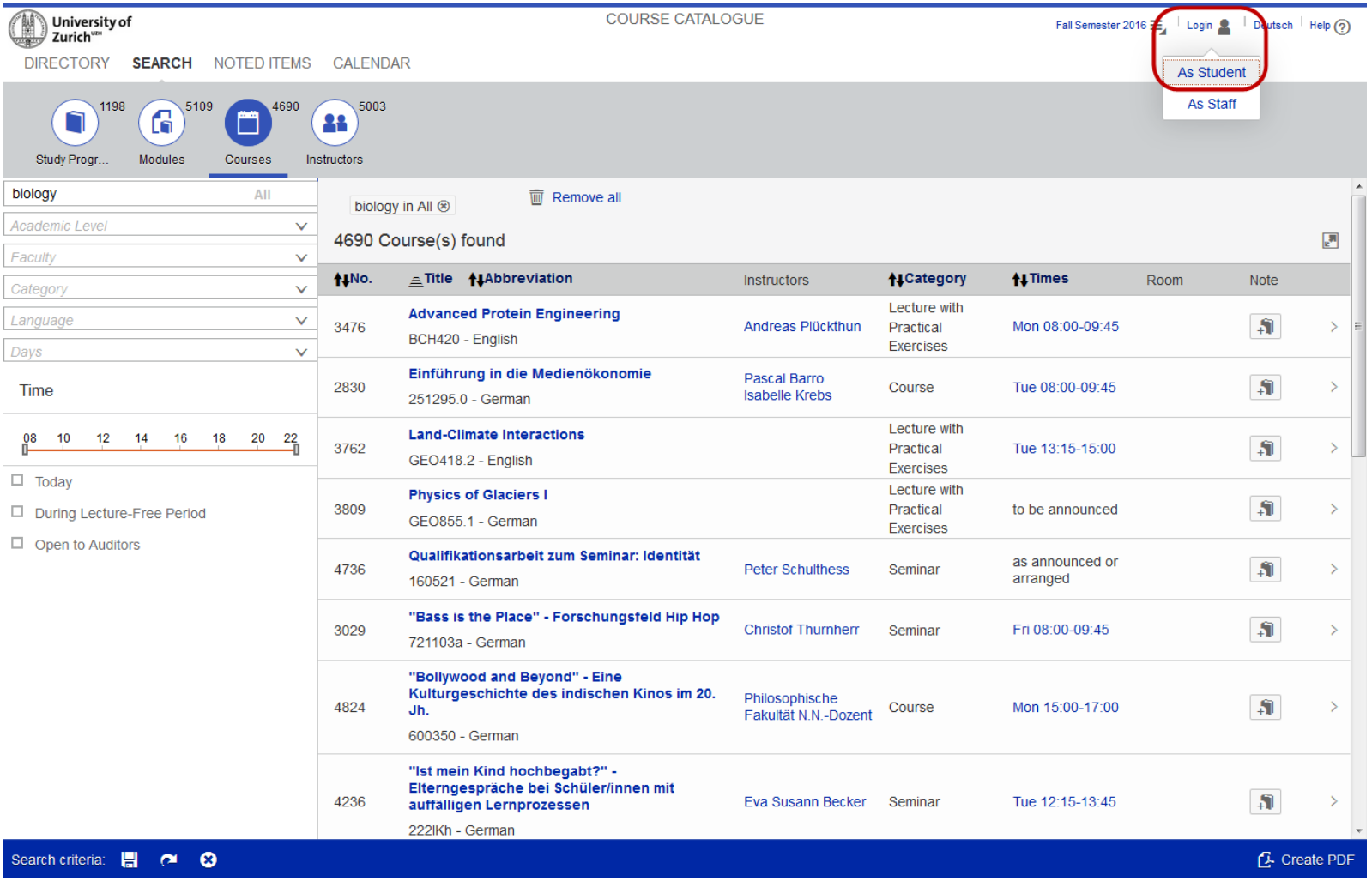
AAI & SAP SAML2 for Fiori / UI5

SAP NetWeaver Application Server ABAP as SAML service provider

Daniel Emch

University of Zurich

Trigger: new course catalog



Current Situation

The UZH is using the shibboleth service provider (mod_shib, shibd) to protect the SAP online services for students (www.students.uzh.ch/en.html)

All these UZH SAP online services (self-developed BSP-applications) will be replaced within the next two years

The login functionality for these UZH SAP online services is a self-developed BSP-application, which cannot be used without modification for Fiori authentication

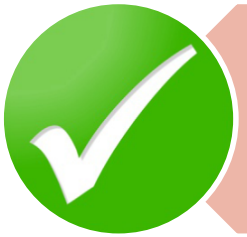
The first self-developed UZH SAPUI5 application is the new course catalog (www.courses.uzh.ch), which is available since June 2016

The UZH plans to use the Fiori Launchpad to present the SAP UI5 online services to the students

Goals of the AAI authentication for Fiori / UI5

The authentication technology should be based on well known industry standards

The implementation should be possible without any modifications on SAP and IdP side



It has to be fully integrated in the AAI Federation & Resource Registry

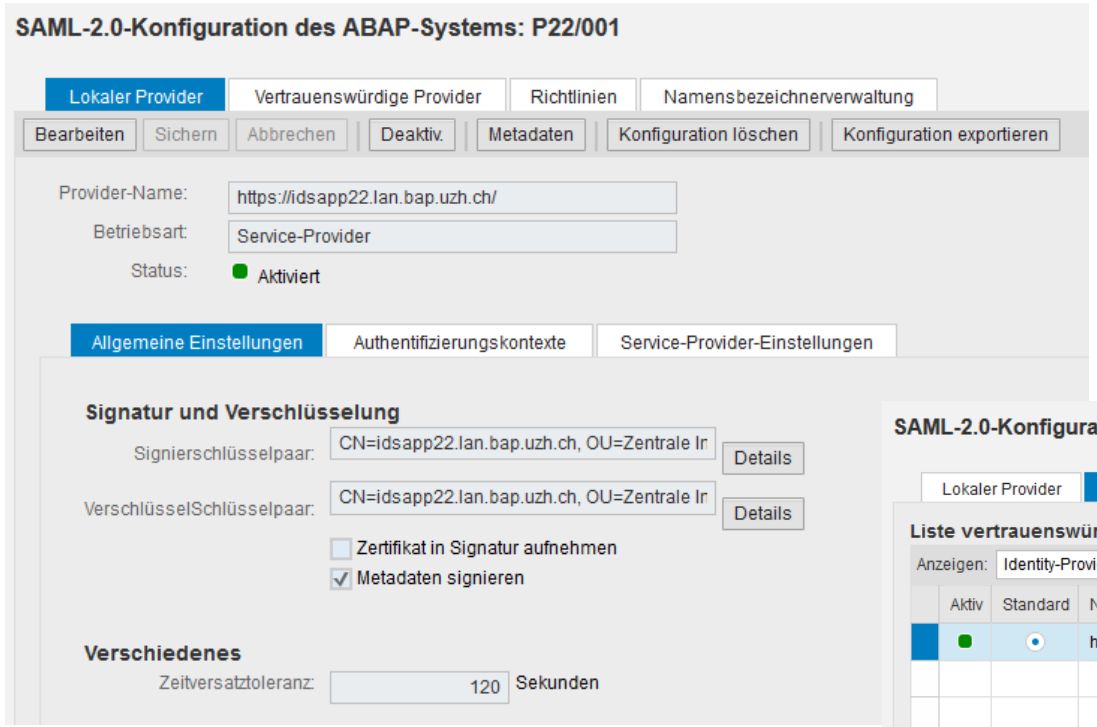
Solution

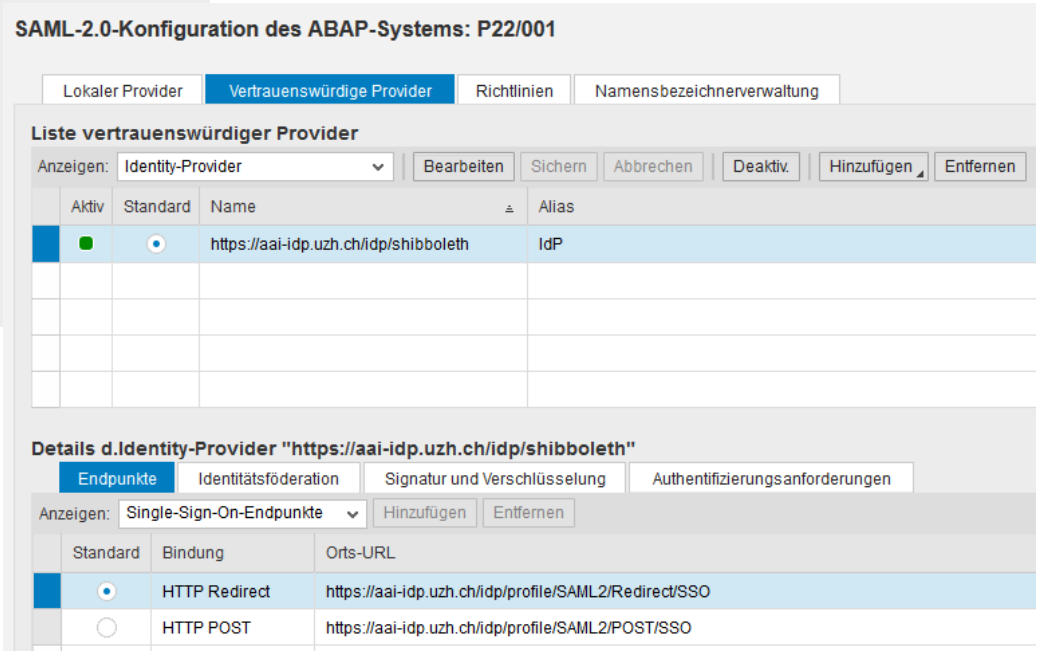
1. Configuration of the SAP NetWeaver Application Server ABAP to operate as a SAML service provider (SAP transaction SAML2)

2. Create service provider in the AAI Resource Registry (https://rr.aai.switch.ch/)

3. Set the logon procedure of the corresponding SAP service to «Alternative Logon Procedure» (SAP transaction SICF)

1. SAP SAML2 transaction

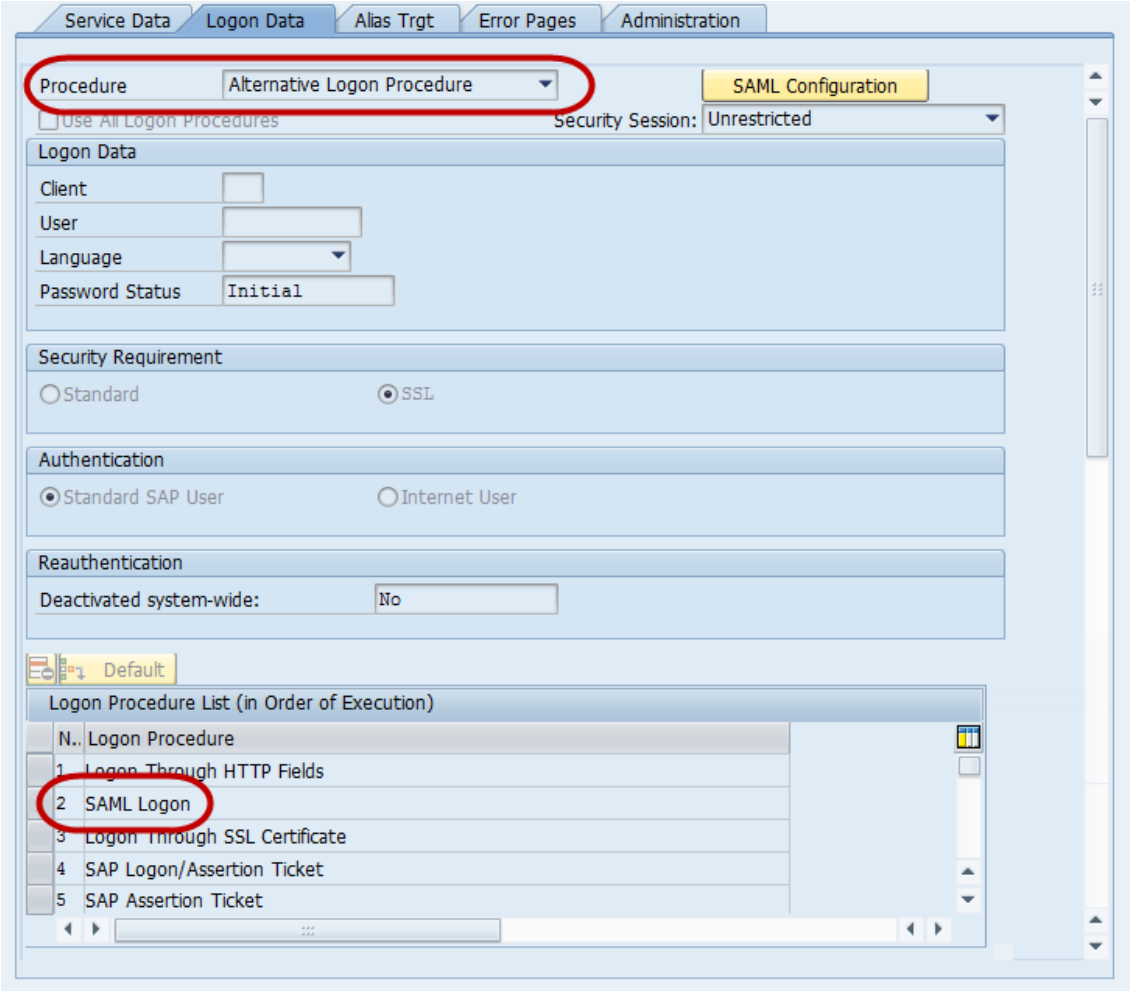




2. AAI Resource Registry

Basic Resource Information	
Federation	SWITCHaai Federation
Home Organization	uzh.ch (SWITCHaai)
EntityID	https://idsapp22.lan.bap.uzh.ch/ SAML 2
Relying Party	Default
Interfederation Enabled	Interfederation support not enabled
GÉANT Data Protection Code of Conduct	Not committed to GÉANT Data Protection Code of Conduct
REFEDS R&S Category	Service not compliant with REFEDS R&S.
Home URL	https://studentservices.uzh.ch/
Helpdesk URL	
Valid from	27 April 2016
Valid until	Valid forever.
Public	Yes If the Resource is marked as public, it will be visible in public Resource listings.
Embedded Certificates	
Certificate	/ C=CH / ST=Zuerich / L=Zuerich / O=Universitaet Zuerich / OU=Business Applications / OU=Zentrale Informatik / CN=idsapp22.lan.bap.uzh.ch **Issuer:** / C=BM / O=QuoVadis Limited / CN=QuoVadis Global SSL ICA G2 **SHA1 Fingerprint:** 20:E4:07:64:4D:DD:5C:98:54:49:83:29:C0:82:87:37:4F:98:FD:AB **Expiration Date:** Apr 8 15:02:54 2019 GMT
Service Locations	
Assertion Consumer Service	https://studentservices.uzh.ch/sap/saml2/sp/acs/001 Binding: urn:oasis:names:tc:SAML:2.0:bindings:PAOS
Assertion Consumer Service	https://studentservices.uzh.ch/sap/saml2/sp/acs/001 Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact
Assertion Consumer Service	https://studentservices.uzh.ch/sap/saml2/sp/acs/001 Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

3. Alternative Logon Procedure (SAP transaction SICF)



Multi-Factor Authentication

Pilot Project Update

SWITCH

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

Project members

- University of Geneva
- Swiss edu-ID
- developer: me :)

University of Geneva

Goal

Stronger authentication for a HR web application handling personal data of university staff

Second factors

- Google Authenticator (OATH-TOTP)
- SMS OTP

Authentication server with RADIUS interface to verify OTPs

Swiss edu-ID

Goal

Offer stronger authentication methods on the edu-ID IdP

Second factors

- First demo with Google Authenticator
- Add more as required

Project links

- SWITCH toolbox (https://toolbox.switch.ch/en/combos/idpv3-mfa)
  - wiki (meeting notes)
  - mailing list (announcements)
  - Discourse (forum)
- SWITCH Forge (https://forge.switch.ch/projects/idpv3-mfa)
  - issue tracking, roadmap
  - source code (git://git.switch.ch/idpv3-mfa.git) (public read access)

Project links

- Public demo IdP & SP in AAI Test federation
  https://mfa-dev.ed.switch.ch/index.html (https://mfa-dev.ed.switch.ch/index.html)

IdP 3.3 enhancements for MFA

IDP-962 (https://issues.shibboleth.net/jira/browse/IDP-962)

- Orchestrator flow to combine login flows
- Execute several authentication methods and aggregate results
- Attribute resolution during authentication
- Transition logic

The SAML & MFA horror scenario

1. SP wants “MFA”
2. SP requests a particular AuthnContext
3. IdP does not support this AuthnContext
4. Failure!

How can SPs request MFA and IdPs indicate that MFA was used, without getting too precise about the actual authentication method?

⇒ The InCommon MFA interoperability profile working group (https://spaces.internet2.edu/display/MIPWG) tackled this problem and published two profiles to help solve it

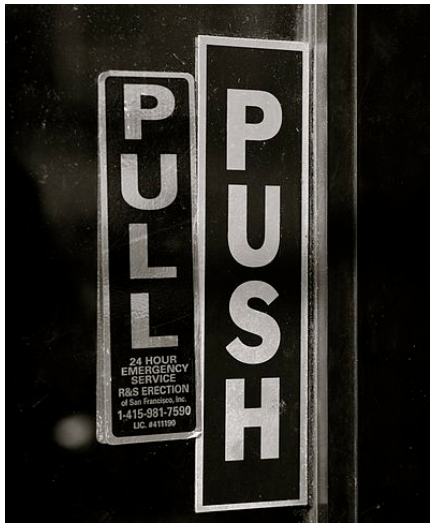
MFA interoperability profiles

InCommon MFA profile

- AuthnContext
  `http://id.incommon.org/assurance/mfa` says "MFA was used"
- Factors must be independent
- Combination of factors mitigates single-factor-only risks related to non-real-time attacks: phishing, offline cracking, online guessing, theft
- Limited to authentication: nothing about registration or identity proofing
- Not technology-specific

SAML Attribute Query

Pulling attributes from an IdP



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

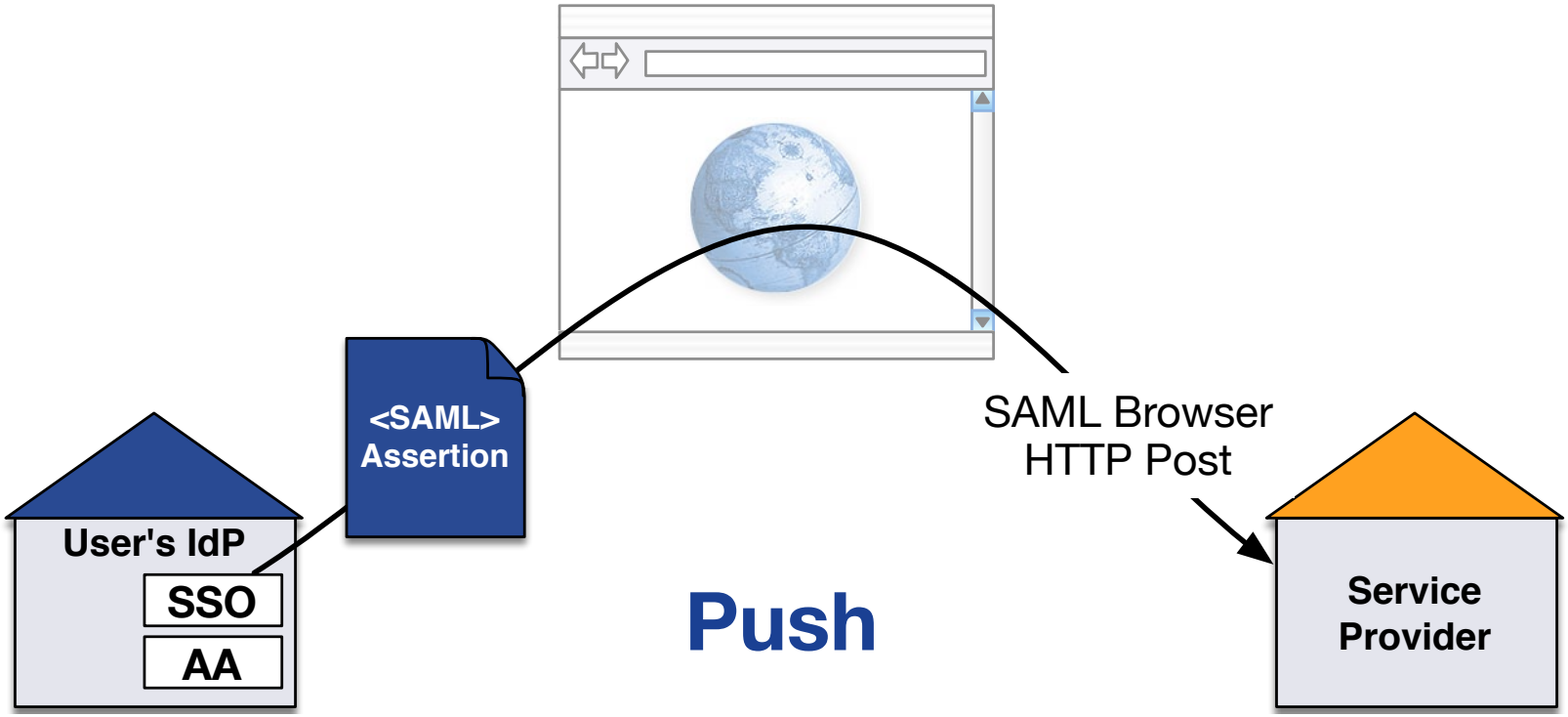
Berne, 30. June 2016

SAML Attribute Query

- What is it?
- For what is it useful?
- How to use it?
- How can my IdP support it?

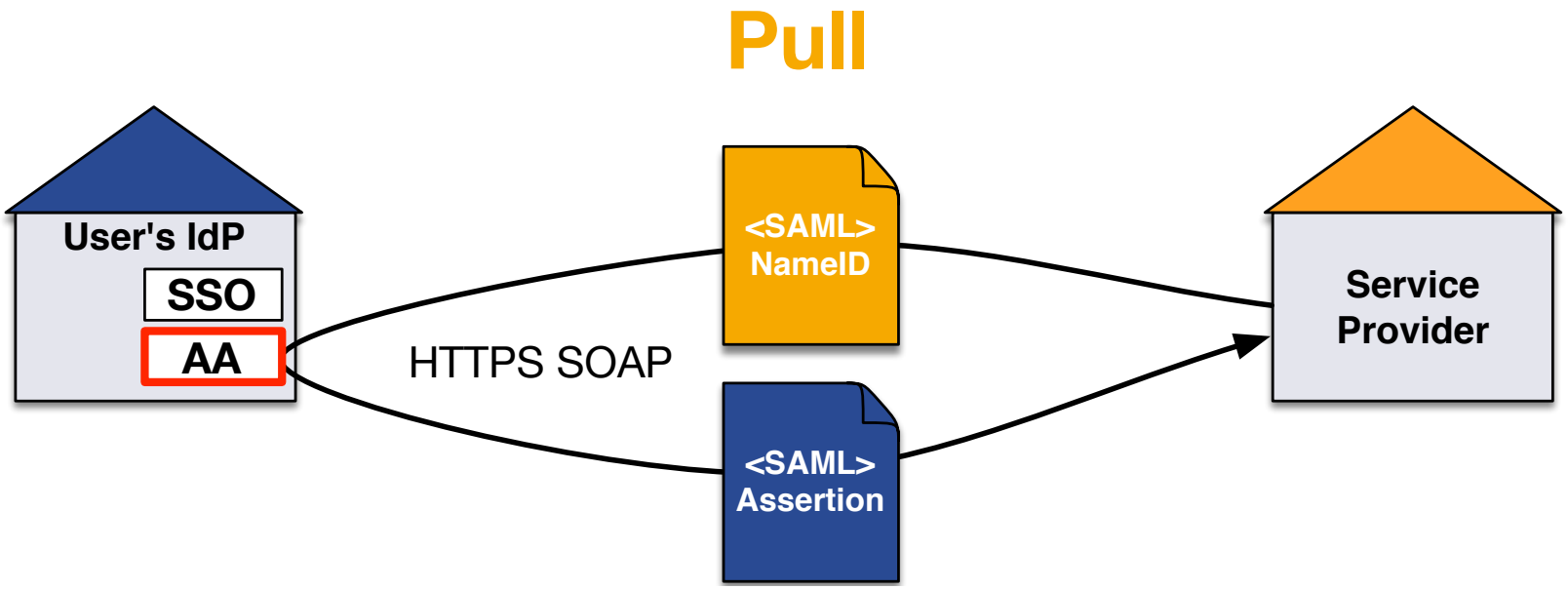
Attribute Query in greater detail:
https://www.switch.ch/aai/support/presentations/techupdate-2014/04_Account_Checking.pdf

Normal AAI Login



- Assertion sent via web browser to SP
- Requires user and his web browser

SAML Attribute Query



- SP queries IdP Attribute Authority (AA) asking for assertion
- SAML PersistentID/eduPersonTargetedID needed by SP
- No user involvement or web browser needed

So why are Attribute Queries useful?

Get **up-to-date** user **attributes** at any time **without user involvement** from IdP!

- Only possible if user at least once accessed SP (and gave consent to release attributes to this SP)
- Update user account data on request
- Detect if user still has an account at IdP
  (no personal attributes probably means no account anymore)
- Easy to use:

```
curl -k 'https://localhost/Shibboleth.sso/AttributeQuery?
entityID=#IdP#&nameId=#PersistentID#'
```
➔ Attributes as JSON data

- Needed for **Swiss edu-ID** to keep user data up-to-date!

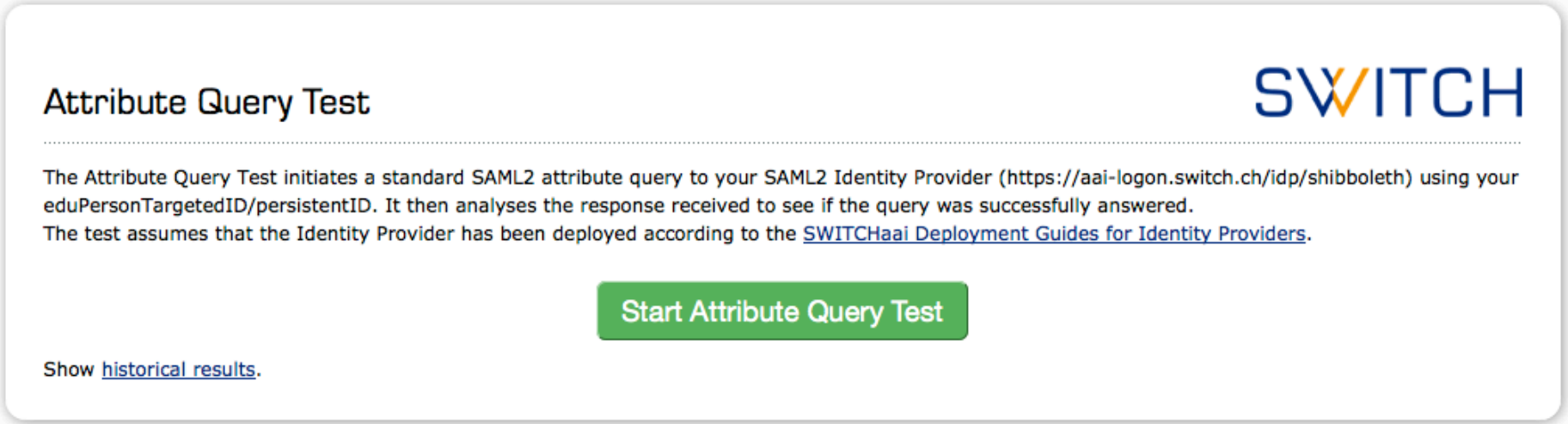
How to Perform an Attribute Query

- Shibboleth SP `resolvertest` binary
  - Bundled since Shibboleth SP 2.x
  - Slow and only for testing
  - Non standard form for returning attributes
  - Usage information in Shibboleth Wiki

- Shibboleth Attribute Query Plugin
  - Was plug-in but is now bundled with SP 2.6 (**released yesterday!**)
  - Developed by Japanese GakuNin federation
  - Very fast!
  - Accessible via URL (`/Shibboleth.sso/AttributeQuery?nameID=XY`)

Does it work for my IdP?

- Yes, it should if you used the SWITCHaai IdP guides!
- Test it: https://av.aai.switch.ch/aai/attribute-query-test/



- 31 (49%) of 63 IdPs successfully took the the test (29.6.2016)

Attribute Query Test

SWITCH

The Attribute Query Test initiates a standard SAML2 attribute query to your SAML2 Identity Provider (https://aai-logon.switch.ch/idp/shibboleth) using your eduPersonTargetedID/persistentID. It then analyses the response received to see if the query was successfully answered.
The test assumes that the Identity Provider has been deployed according to the SWITCHaai Deployment Guides for Identity Providers.

Test successfully passed!

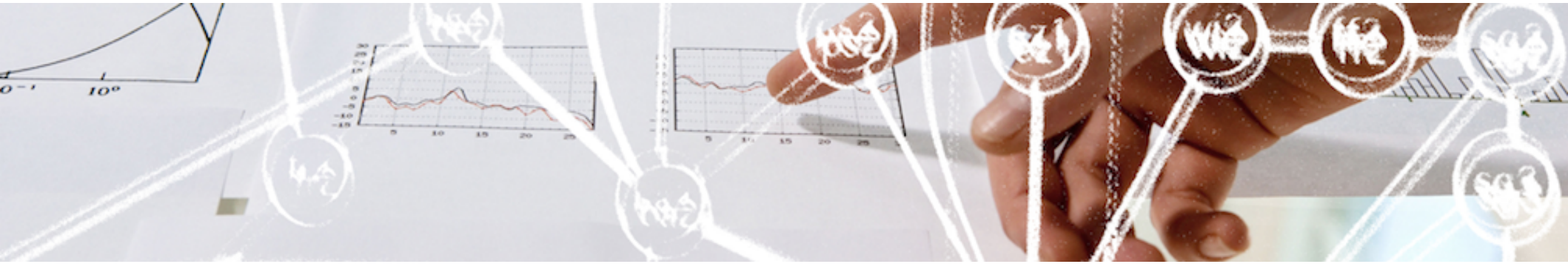
```
2016-06-22 17:07:05 INFO: Testing AttributeQuery with inexistent persistentID
2016-06-22 17:07:05 INFO: Querying URL https://localhost/Shibboleth.sso/AttributeQuery?entityID=https%3A%2F%2
2016-06-22 17:07:05 WARN: IdP returns attributes for inexistent targetedIDs
2016-06-22 17:07:06 INFO: Testing with real persistentID yrVdvdAmohZY+cE6dcGvqu/Dubc=
2016-06-22 17:07:06 INFO: Querying URL https://localhost/Shibboleth.sso/AttributeQuery?entityID=https%3A%2F%2
2016-06-22 17:07:06 INFO: IdP returns more attributes for existing than inexistent targetedID
2016-06-22 17:07:06 INFO: Personal attributes (givenName, surname, displayName, cn, mail, uniqueID, principal
2016-06-22 17:07:06 INFO: Attributes received as Header Array
(
    [mobile] => +41 [redacted]
    [displayName] => Lukas Haemmerle
    [postalAddress] => SWITCH$Werdstrasse 2$CH-8004 Zürich
    [telephoneNumber] => +41 44 268 15 64
    [isMemberOf] => https://toolbox.switch.ch/earlyadopters;https://toolbox.switch.ch/earlyadopters/.admin;ht
    [mail] => lukas.haemmerle@switch.ch
    [persistent-id] => https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shib
    [schacHomeOrganizationType] => urn:schac:homeOrganizationType:int:NREN;urn:schac:homeOrganizationType:ch:
    [gender] => 1
    [dateOfBirth] => [redacted]
    [cn] => Lukas Haemmerle
    [homeOrganizationType] => others
    [uniqueID] => [redacted]
    [homeOrganization] => switch.ch
    [schacHomeOrganization] => switch.ch
    [preferredLanguage] => en
    [givenName] => Lukas
    [scoped-affiliation] => staff@switch.ch;member@switch.ch
    [surname] => Hämmerle
    [principalName] => [redacted]
    [affiliation] => member;staff
    [eduPersonUniqueId] => [redacted]
    [uid] => haemmer
)
2016-06-22 17:07:06 INFO: AttributeQuery to IdP https://aai-logon.switch.ch/idp/shibboleth was successful!
```

Repeat Attribute Query Test

Show historical results.

SAML Single Logout

with the Shibboleth IdPv3



SWITCH

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

Sessions, sessions, sessions!

- IdP session
- SP1 session
- application1 session
- SP2 session
- application2 session
- etc.

SLO is harder than SSO

- *Single*: terminate all sessions in one operation
- Does it make sense for the user?
- What happens when only one session is terminated?
- How do you cleanly terminate all those sessions?


NUKE IT FROM ORBIT
ITS THE ONLY WAY TO BE SURE
memegenerator.net

Availability with Shibboleth

- Already implemented in SP (simplified configuration since 2.4)
- SP can notify protected application
- Available since IdP 3.2.0, with some bugs in logout flow and view: IDP-956 (https://issues.shibboleth.net/jira/browse/IDP-956), IDP-924 (https://issues.shibboleth.net/jira/browse/IDP-924)
- Works on IdP 3.2.1 with those fixes applied
- Bindings: *front-channel* (HTTP-Redirect, HTTP-POST) and *back-channel* (SOAP)

Availability with Shibboleth

- Back-channel propagation not yet available on IdP, but planned for 3.3 (https://issues.shibboleth.net/jira/browse/IDP- 964)

- Administrative logout is *not supported*

Implementation in IdPv3

IdP- and SP-initiated logout sequences

Logout views

Configuration overview

Configuration details

Fixes for IdP 3.2.0 and 3.2.1

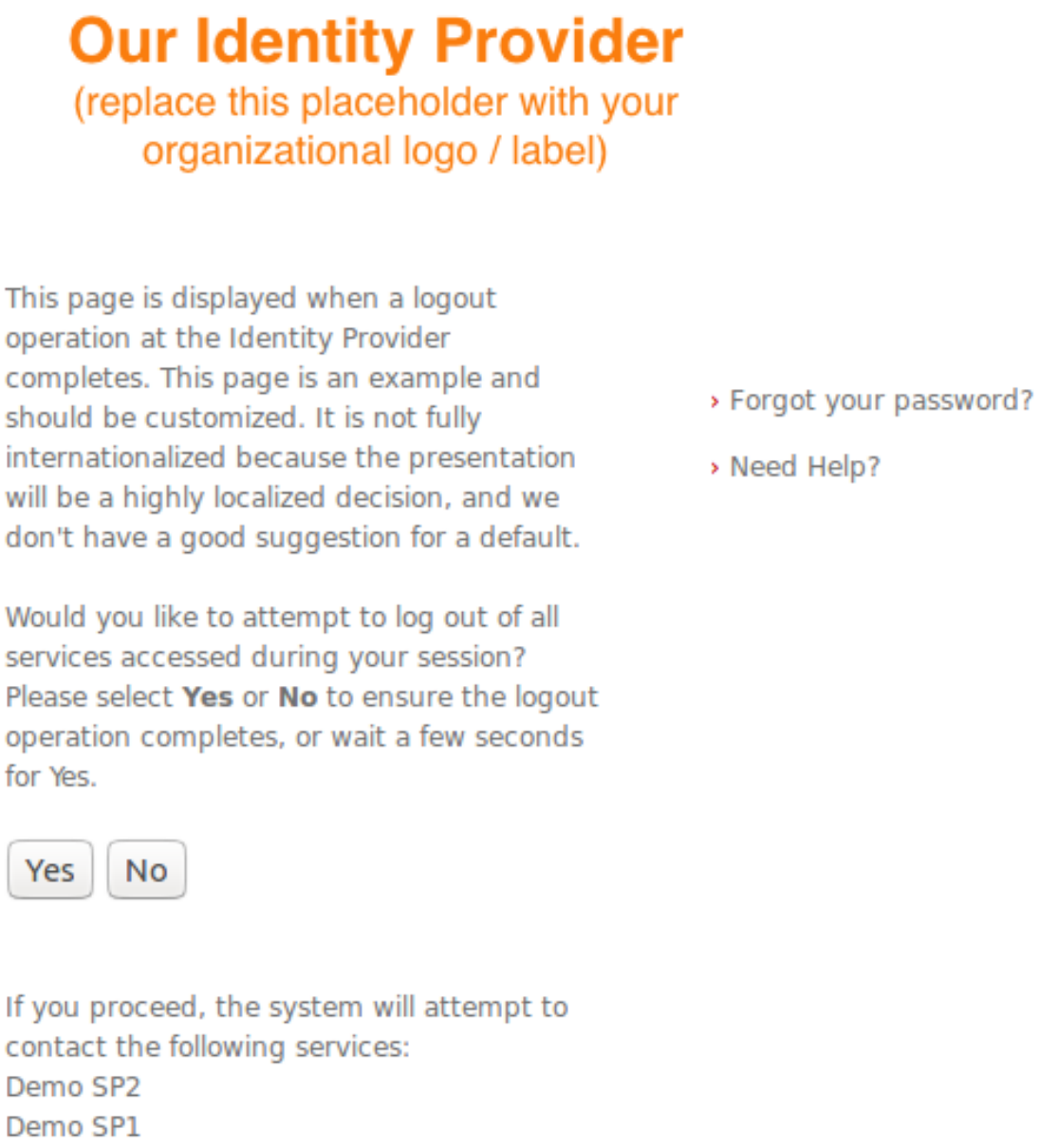
IdP-initiated (proprietary) logout

1. HTTP GET on `/idp/profile/Logout` with session cookie
2. End IdP session
3. Log out of other services? If yes, proceed
4. Propagate logout to accessed SPs
5. Display result (flow always ends at IdP)

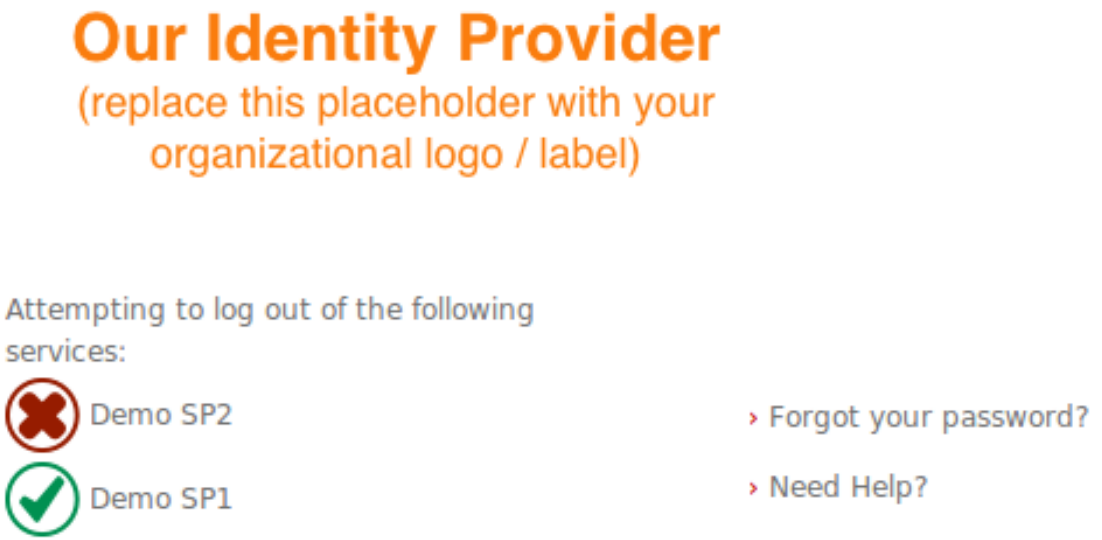
SP-initiated (SAML) logout

1. HTTP GET on `/Shibboleth.sso/Logout`
2. *(if notify)* Redirect to application logout notification endpoint
3. *(if notify)* Redirect to `/Shibboleth.sso/Logout`
4. Redirect to IdP with SAML LogoutRequest
5. Same as IdP-initiated logout (flow always ends at IdP)

IdPv3 logout views (1)

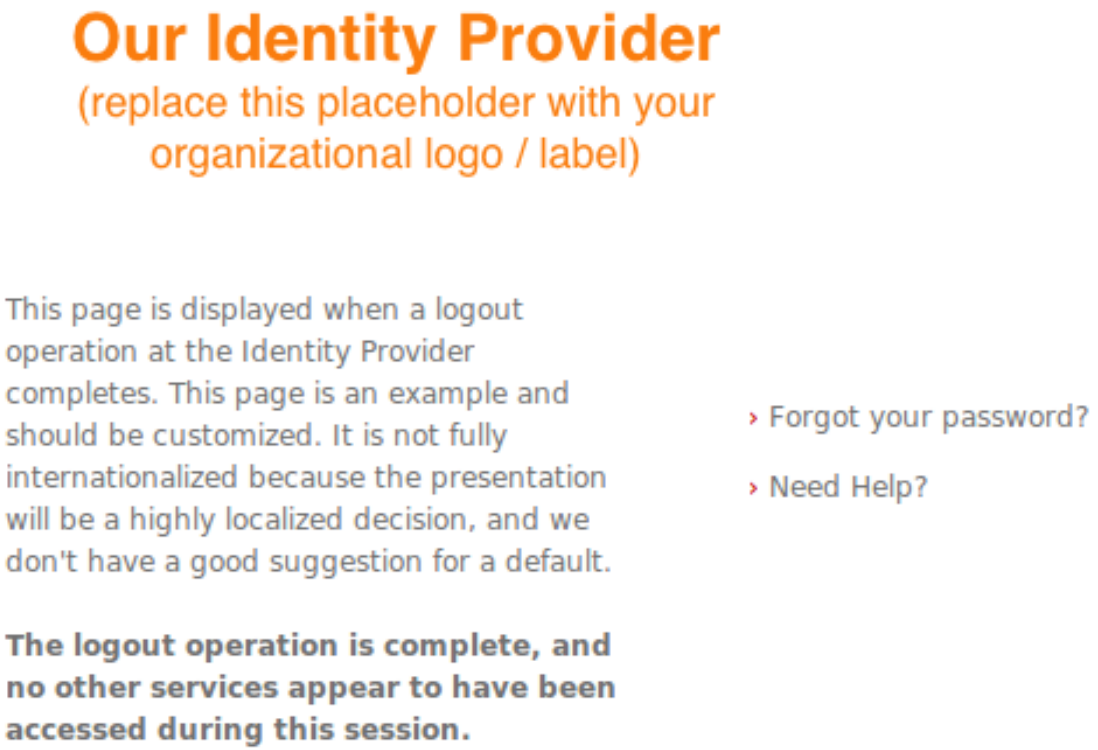


IdPv3 logout views (2)



- Shows list of SPs with logout status
- One hidden iframe per SP ⇒ each sends one SAML logout request
- Uses jQuery (https://jquery.com/)

IdPv3 logout views (3)



- No propagation question when the only SP in the session sends the logout request

Configuration overview

1. Enable SLO on your IdP (properties)
2. Publish IdP SLO endpoints in metadata (Resource Registry)
3. Enable SLO on your SP
4. If your SP-protected application has its own sessions:
   - Enable application notifications on your SP
   - Program your application to respond to logout notifications
5. Publish SP SLO endpoints in metadata (Resource Registry)
6. Test!

Configuration: IdP properties

Required to enable SLO

- Track SPs logged into
  `idp.session.trackSPSessions = true [false]`
- Enable receiving SAML logout requests from SPs
  `idp.session.secondaryServiceIndex = true [false]`

Reference: LogoutConfiguration
(https://wiki.shibboleth.net/confluence/display/IDP30/LogoutConfiguration)

Configuration: IdP properties

Optional tweaks

- Display SP information from metadata

  `idp.logout.elaboration = true [false]`

- How long does the IdP remember SPs? It cannot know the real SP session duration!

  `idp.session.defaultSPlifetime = PT2H [PT2H]`

  `idp.session.slop = PT0S [PT0S]`

- Require logout requests/responses be signed/authenticated, better leave it enabled

  `idp.logout.authenticated = true [true]`

Configuration: IdP SLO endpoints

Publish `SingleLogoutService` endpoints in metadata

	Single Logout Service
SAML2 HTTP Redirect binding	https://xenos.switch.ch/idp/profile/SAML2/Redirect/SLO Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect **Only partially supported by Shibboleth Identity Provider.**
SAML2 HTTP POST binding	https://xenos.switch.ch/idp/profile/SAML2/POST/SLO Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST **Only partially supported by Shibboleth Identity Provider.**
SAML2 SOAP binding	https://xenos.switch.ch/idp/profile/SAML2/SOAP/SLO Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:SOAP **Only partially supported by Shibboleth Identity Provider.**

Configuration: SP logout service

Add “SAML2” inside the `Logout` element (in `shibboleth2.xml`)

```
<Logout>SAML2 Local</Logout>
```

Reference: NativeSPServiceLogout
(https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPServiceLogout)

Configuration: SP logout notifications

Add a `Notify` element (in `shibboleth2.xml`)

```
<Notify Channel="front"
        Location="https://sp.example.org/app/logout-notify"/>
```

and program your application to respond at the given URL

References: NativeSPNotify (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPNotify), SLOWebappAdaptation (https://wiki.shibboleth.net/confluence/display/SHIB2/SLOWebappAdaptation)

Configuration: SP SLO endpoints

Publish `SingleLogoutService` endpoints in metadata

Single Logout Service	
SAML2 SOAP binding	https://xenos.switch.ch/Shibboleth.sso/SLO/SOAP Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:SOAP
SAML2 HTTP Redirect binding	https://xenos.switch.ch/Shibboleth.sso/SLO/Redirect Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
SAML2 HTTP POST binding	https://xenos.switch.ch/Shibboleth.sso/SLO/POST Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
SAML2 HTTP Artifact binding	Binding URN: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact

Fixes for IdP 3.2.0 and 3.2.1 (1)

```
--- system/flows/logout/logout-flow.xml    2016/01/20 19:57:55    8080
+++ system/flows/logout/logout-flow.xml    2016/04/01 14:23:58    8190
@@ -73,7 +73,7 @@
 <view-state id="LogoutView" view="logout">
-    <on-entry>
+    <on-render>
         <evaluate expression="WriteAuditLog" />
         <evaluate expression="environment" result="viewScope.environme
         <evaluate expression="opensamlProfileRequestContext" result="v
@3,7 +83,7 @@
         <evaluate expression="flowRequestContext.getExternalContext().
         <evaluate expression="flowRequestContext.getExternalContext().
         <evaluate expression="flowRequestContext.getActiveFlow().getAp
-    </on-entry>
+    </on-render>
     <transition on="proceed" to="LogoutCompleteView" />
     <transition on="end" to="LogoutCompleteView" />
     <transition on="propagate" to="LogoutPropagateView" />
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/system/flows/logout/logout-flow.xml?r1=8080&r2=8190&pathrev=8190&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (2)

```
--- system/flows/logout/propagation/cas-flow.xml    2015/10/14 15:50:01
+++ system/flows/logout/propagation/cas-flow.xml    2016/04/01 14:23:58
@@ -3,12 +3,12 @@
       xsi:schemaLocation="http://www.springframework.org/schema/webflo

 <view-state id="ShowServiceLogoutView" view="cas/logoutService">
-    <on-entry>
+    <on-render>
         <set name="viewScope.logoutPropCtx"
              value="opensamlProfileRequestContext.getSubcontext(T(net.
         <set name="viewScope.messageID" value="T(java.util.UUID).rando
         <set name="viewScope.issueInstant" value="DateFormatter.print('
-    </on-entry>
+    </on-render>
     <transition on="proceed" to="proceed" />
 </view-state>
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/system/flows/logout/propagation/cas-flow.xml?r1=7822&r2=8190&pathrev=8190&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (3)

```
--- views/logout.vm    2016/01/05 12:57:59    8067
+++ views/logout.vm    2016/02/18 17:39:36    8095
@@ -65,10 +65,8 @@
 </ol>
 #else
 <p><strong>#springMessageText("idp.logout.complete", "The logout opera
-<!-- If SAML logout with no extra work to do, complete the flow by add
-#if ( $profileRequestContext.getProfileId().contains("saml2/logout") )
-<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
-#end
+<!-- Complete the flow by adding a hidden iframe. -->
+<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
 #end

 </div>
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/views/logout.vm?r1=8067&r2=8095&pathrev=8095&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (4)

```
--- views/logout-complete.vm    2015/10/28 16:17:35    7896
+++ views/logout-complete.vm    2016/02/18 17:39:36    8095
@@ -44,7 +44,7 @@

 <!-- If SAML logout, complete the flow by adding a hidden iframe. -->
 #if ( $profileRequestContext.getProfileId().contains("saml2/logout") )
-<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
+<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
 #end

 <footer>
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/views/logout-complete.vm?r1=7896&r2=8095&pathrev=8095&diff_format=u)

Fixes for IdP 3.2.0 and 3.2.1 (5)

```
--- system/views/logout/propagate.vm    2015/11/06 20:22:32    7958
+++ system/views/logout/propagate.vm    2016/02/18 17:39:36    8095
@@ -99,5 +99,5 @@

 <!-- If SAML logout, complete the flow by adding a hidden iframe. -->
 #if ( $profileRequestContext.getProfileId().contains("saml2/logout") )
-<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
+<iframe style="display:none" src="$flowExecutionUrl&_eventId=proceed">
 #end
```

original diff from svn.shibboleth.net

(http://svn.shibboleth.net/view/java-identity-provider/trunk/idp-conf/src/main/resources/system/views/logout/propagate.vm?r1=7958&r2=8095&pathrev=8095&diff_format=u)

SIRTFI

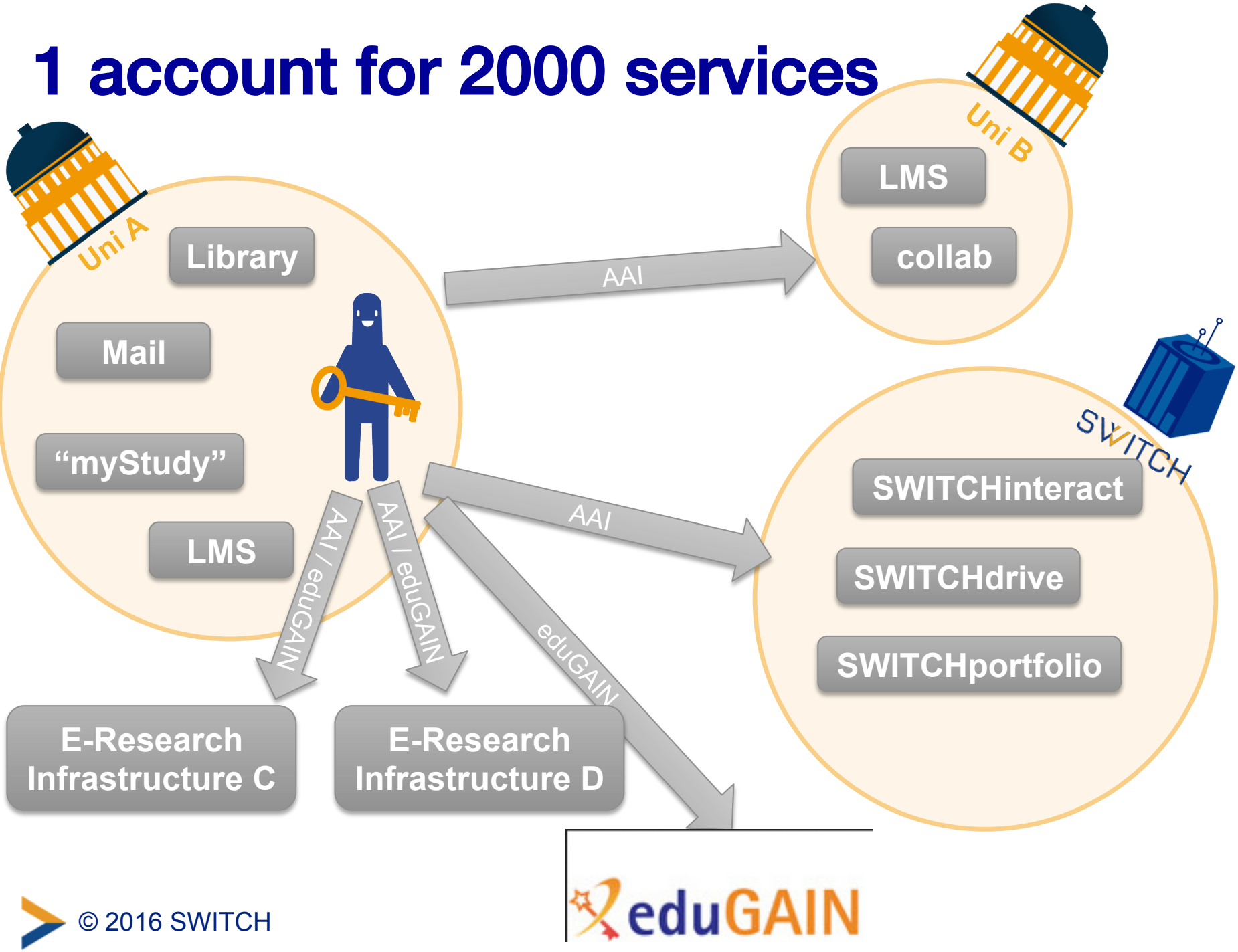
How to handle compromised AAI accounts

SWITCH

Thomas Bärecke
thomas.baerecke@switch.ch

Bern, June 30th, 2016

1 account for 2000 services



SIRTFI - coordinated incident response

A Security Incident Response Trust Framework for Federated Identity

- Operational Security
- Incident Response
- Traceability
- Participant Responsabilities

Operational Security

- Regular patches
- Processes for vulnerability management
- Intrusion detection and information protection
- Possibility of timely user rights changes
- Established contacts for service owners and users
- Security Incident Response

Incident Response

- Security incident response contact information
- Timely reply to other SIRTFI members
- Collaborate in management of security incidents
- Respect SIR procedures of own organisation
- Respect user privacy
- Respect Traffic Light Protocol

Traceability and participants responsibilities

Keep accurate logs of all relevant information available for handling security incidents

Acceptable use policy (AUP)

User consent to AUP

Next steps

SWITCH

- Implement processes to add security contact information
- Publish security contact information in metadata where available

SP and IdP operators

- Read the document at https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf
- Decide whether you wish to participate

Attribute Release Update

Upcoming changes for IdP administrators

SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 30. June 2016

IdP Attribute Release Changes

1. eduGAIN SPs without <RequestedAttributes>
2. R&S Changes
3. PersistentID NameFormat Changes

On the Changes

- All changes planned to become active in August 2016
- Separate announcement on aai-operations list will follow
- Generally, no actions required by SP and IdP administrators

1. eduGAIN SPs without <RequestedAttributes>

- Many eduGAIN SPs don't declare attributes they need ☹
- So far Resource Registry assigned such SPs a default set of "requested" unpersonal attribute:
  - schacHomeOrganization (e.g. "switch.ch")
  - schacHomeOrganizationType (e.g. "urn:schac:homeOrganizationType:int:NREN")
  - eduPersonScopedAffiliation (e.g. "staff@switch.ch")
  - eduPersonAffiliation (e.g. "staff")
  - eduPersonTargetedID (e.g. "yrV12dAmohZY+cE6dc34qu/Dubc=")
- Planned change: **No default attribute set anymore**
  - **No action needed from IdP admins**
  - **Low impact expected**

2. R&S Changes

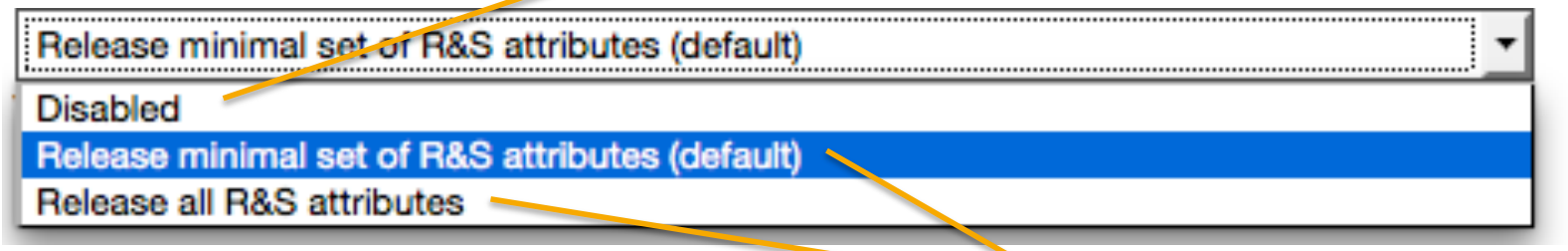
- REFEDS Research & Scholarship category
  - Federations can "tag" research and education SPs
  - https://refeds.org/category/research-and-scholarship
  - Allows easier/safer attribute release
  - Initial specification (2014) ➔ clarification proposal (2016)

- SWITCHaai was early adopter ➔ a few changes
  - No distinction anymore between minimal and full R&S attribute set

- Planned Change: **Clarification-conform implementation**
  - **No action needed by IdP admins. R&S Service Providers will additionally get affiliation and eduPersonTargetedID attribute**

Proposed Change in Resource Registry

- Current:



No eduGAIN-enabled IdP has chosen the "Disabled" option since 2014

Difference between default and full R&S set is only the "unpersonal" affiliation and the opaque eduPersonTargetedID attributes

- Future:

3. PersistentID NameIDFormat Changes

- transientID is default NameIDFormat for SWITCHaai SPs
  - Some SAML implementations require persistentID format
  - SAML2int.org also profile recommends persistentID format

- Planned Change (August):
  Support for using SAML2 persistent NameID
  - **No changes needed at IdPs**
  - **Better interoperability with non-Shib SAML implementations**

- Implications
  - AAI Resource Registry to support declaration of NameIDFormat
  - New SPs to use persistentID format by default
  - eduPersonTargetedID contains same value like persistentID
  - Eventually, migration from existing SPs to persistentID

Questions

Attribute Release Problem

- Most federations don't have a scalable attribute management like SWITCHaai has

  ➔ Many login problems, helpdesk requests, frustrated users, ...

- Solution was to create a metadata "flag" for SPs to whom a fixed set of attributes should be released

  ➔ REFEDS Research & Scholarship entity category

R&S Entity Category

- **REFEDS Research & Scholarship (R&S) Entity Category**
  - https://refeds.org/category/research-and-scholarship
  - To tag SPs that "enhance the research and scholarship"

- **Facilitates attribute release to R&S SPs**
  - Federation operators (like SWITCH) set and control which SPs get R&S flag
  - R&S SPs: non-commercial SPs used for research and education, e.g. SPs from CERN, LIGO, ...
  - Easy configuration, no/less privacy issues

- **For SWITCHaai IdPs only relevant in context of eduGAIN**
  - Has been in place since 2014

So what changes?

- R&S specification (from 2014) leaves too much room for interpretation ☹
  - SWITCHaai was early-adopter of this category
  - Today: Better consensus about implementation
  - (For SPs back-wards) compatible R&S Clarification Proposal

R&S Clarification Proposal

"The *R&S attribute bundle* consists (abstractly) of the following required data elements:

- *shared user identifier*
- *person name*
- *email address*

and one optional data element:

- *affiliation*

To be on the safe side, we propose to release both attributes because some SWITCHaai orgs cannot ensure that uniqueID/principal name never is reassigned

where *shared user identifier* is a persistent, non-reassigned, non-targeted identifier defined to be either of the following:

- eduPersonPrincipalName (if non-reassigned)
- eduPersonPrincipalName + eduPersonTargetedID

and where *person name* is defined to be either (or both) of the following:

- displayName
- givenName + sn"

Impact on Attribute Release

Number of attributes released to R&S SPs changes!

Compared to current default setting for IdPs:

+ Scoped Affiliation released
e.g. `staff@empa.ch`, `student@unige.ch`, `faculty@uzh.ch`

+ eduPersonTargetedID released
e.g. `yrVdvdAmohZYocE6dcGvqu/Dubc=`

+ Complete R&S attribute set released independent of `<RequestedAttributes>` element in metadata

Impact on IdPs

- **No action needed by IdP admins!**
  - Unless your organisation is not comfortable with R&S attributes being released to research and scholarship SPs
    - R&S-based attribute release has been in place since 2014 for all SWITCHaai Interfederation-enabled IdPs
    - No problems known of any SWITCHaai organisations
    - Default setting can be changed by Home Organisation administrator in Resource Registry
- **Benefit:**
  - **Better interoperability with R&S Service Providers in eduGAIN**
  - **(Slightly less helpdesk requests due to missing attributes)**