

Introducing a hundred SPs at once

Automated Shibboleth Service Deployment

Hanspeter Spalinger <h.spalinger@unibas.ch>, 15.05.2019

Agenda.

-
- 1 Why do we want automated Shibboleth Service deployment
 - 2 Challenges we faced
 - 3 Working with the Resource Registry
 - 4 Wishlist for the Resource Registry
 - 5 Questions
-

Agenda.

- 1 Why do we want automated Shibboleth Service deployment
- 2 Challenges we faced
- 3 Working with the Resource Registry
- 4 Wishlist for the Resource Registry
- 5 Questions

Why do we want automated Shibboleth deployment

EasyWeb - Standard CMS for all University websites

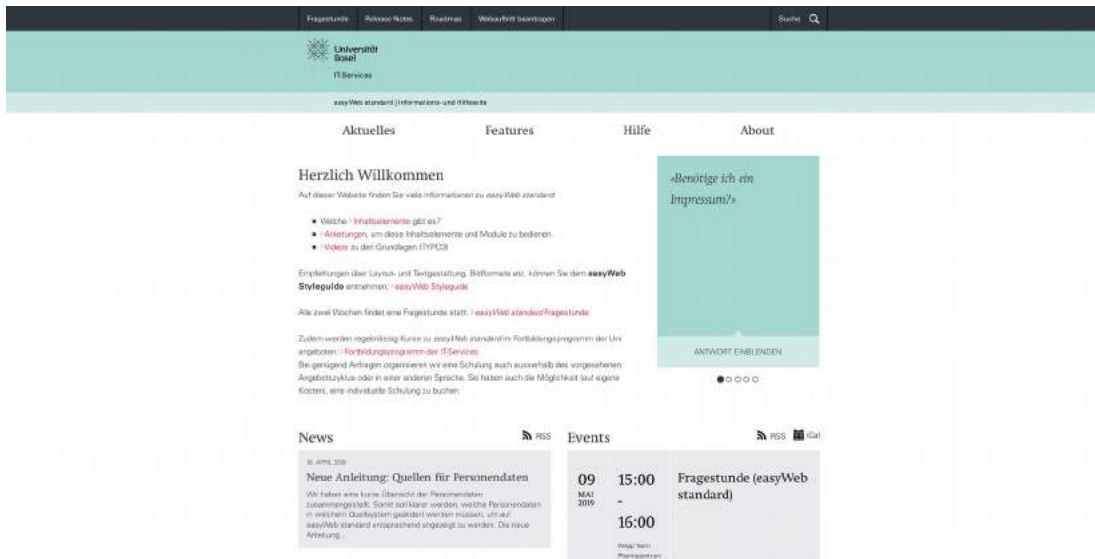
- Typo3 based CMS
- Almost 100% automated deployment system
- Corporated Design mandatory for University Websites
- Centralized User Management

Why do we want automated Shibboleth deployment

Shibboleth - independent authentication

- Uncertain future of Website Hosting Platform (cloud?)
- No dependencies into internal Authentication Services (AD, LDAP, etc)
- But still want use the University Centralized User Management
- No maintenance of user mail/name/surname/etc in CMS itself

Why do we want automated Shibboleth deployment



Login mit Shibboleth

Your user was registered. It needs to be activated. Please contact the responsible site admin so he/she can activate and authorize your account.

As soon as he/she has activated you, you can use the following link to log in: **Login**

Ihr Benutzer wurde registriert und muss noch freigeschaltet werden. Bitte melden Sie sich beim zuständigen Site-Admin, damit dies zeitnah geschieht.

Sobald Sie freigeschaltet wurden, können Sie sich unter folgendem Link anmelden: **Login**

Yes, my account was activated.
Ja, ich wurde freigeschaltet

More about TYPO3



Agenda.

-
- 1 Why do we want automated Shibboleth Service deployment
 - 2 Challenges we faced
 - 3 Working with the Resource Registry
 - 4 Wishlist for the Resource Registry
 - 5 Questions
-

Challenges we faced

LOTS of Sites

- Lots of Departements have their own Websites (~200)
- Each site should have a additional staging instance for testing (x2)
- Filling out the Resource Registry Form can be time consuming
- But all EasyWeb sites have the same settings anyway

Challenges we faced

Home | News | Contact

AAI Resource Registry

Home | Resources | Registration Requests | Home Organizations | Hanspeter Spalinger (unibas.ch) | Logout | Help

↑ About AAI

Home > Resource Administration > Resource Cranio Facial Kinetic Science > Resource Inspector

Resource Inspector for 'Cranio Facial Kinetic Science'

Resource Information for 'Cranio Facial Kinetic Science' (SWITCHaa):

ⓘ Show history

Last change by Hanspeter Spalinger on 3. 4. 2019 14:36

[Edit](#) | [Duplicate](#) | [Request Deletion](#) | [Administrators](#) | [Configuration](#) | [Metadata](#) | [Attribute Release Inspector](#)

Basic Resource Information

Federation

unibas.ch (Switchaa)

EntityID

<https://cranio-facial.weberbildung.unibas.ch/shibboleth>
[\(SAML2\)](#)

Relying Party

Default

Interfederation Enabled

Interfederation support not enabled

GEANT Data Protection Code of Conduct

Not committed to [GEANT Data Protection Code of Conduct](#)

REFEDS R&S Category

Service not compliant with [REFEDS R&S](#)

SWITCH edu-ID Private Identity Enabled

Currently, only SWITCH edu-ID users with one or more [linked identity](#) might access this resource.

REFEDS MFA

Does not require [REFEDS Multifactor Authentication Profile](#) for all users.

Home URL

<https://cranio-facial.weberbildung.unibas.ch/>

Helpdesk URL

<https://its.unibas.ch/>

Valid from

03 April 2019

Valid until

Valid forever.

Public

No
If the Resource is marked as public, it will be visible in public Resource listings.

Resource Admins

Name

[Stefan Keller](#) (unibas.ch) Phone: +41 61 207 22 68

Name

[Dominik Hölter](#) (unibas.ch) Phone: +41 61 207 14 51

Name

[Hanspeter Spalinger](#) (unibas.ch) Phone: +41 61 207 15 24

Name

[Adrian Noller](#) (unibas.ch) Phone: +41 61 207 17 91

Embedded Certificates

Certificate

/ CN=cranio-facial.weberbildung.unibas.ch
Issuer: / CN=cranio-facial.weberbildung.unibas.ch
SHA1 Fingerprint: 36:91:00:5B:51:7D:43:52:A2:57:91:AA:3D:7D:26:4D:98:12:80:83
Expiration Date: Mar 17 00:59:06 2022 GMT

Localized Name and Description

Main Language

English

Language

English

Name

Cranio Facial Kinetic Science

Description

Website Cranio Facial Kinetic Science

Contacts

Type

Administrative

Name

WRPP ITS: wrpp.its@unibas.ch

Type

Support

Name

Support ITS: support.its@unibas.ch

Type

Technical

Name

WSym ITS: wsym.its@unibas.ch

Additional Descriptive Information

Service Locations	
Assertion Consumer Service	https://cranio-facial.weberbildung.unibas.ch/Shibboleth.sso/SAML2/POST Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
Assertion Consumer Service	https://cranio-facial.weberbildung.unibas.ch/Shibboleth.sso/SAML2/Artifact Binding: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Arifact
Assertion Consumer Service	https://cranio-facial.weberbildung.unibas.ch/Shibboleth.sso/SAML2/EC Binding: urn:oasis:names:tc:SAML:2.0:bindings:PAOS
Artifact Resolution Service	https://cranio-facial.weberbildung.unibas.ch/Shibboleth.sso/Artifact/SOAP Binding: urn:oasis:names:tc:SAML:2.0:bindings:SOAP
NameID Formats	
urn:oasis:names:tc:SAML:2.0:nameid-format:transient	
Attribute Usage	
Core Attributes	
E-mail	Required
Reason	User management in easyWeb
Given name	Required
Reason	Display username in easyweb
Surname	Required
Reason	Display username in easyweb
Targeted ID/Persistent ID	Required
Reason	User management in easyWeb
Other Attributes	
Uni Basel personal public id	Required
Reason	Connect the user to other data sources at Uni Basel
Uni Basel specific roles	Required
Reason	User management in easyWeb
Default Intended Audience	
University	-
University of Applied Sciences	-
Hospital	-
Library	-
Professional education and training college	-
Institution on the upper secondary level	-
Virtual Home Organization	-
Other	-
Specific Intended Audience	
unibas.ch	Included
Setup Information	
Service Provider: Shibboleth 2.5.3 XMLSecurity Version: 1.7.2 Xerces Version: 3.1.1 OpenSAML Version: 2.5.5 Last Automatic Update: 07. 05. 2019 06:27:26 (Shibboleth Status Handler accessible)	
Back	

Introducing a hundred SP's at once, Hanspeter Spalinger, 15.05.2019

University of Basel 9

Agenda.

-
- 1 Why do we want automated Shibboleth Service deployment
 - 2 Challenges we faced
 - 3 Working with the Resource Registry
 - 4 Wishlist for the Resource Registry
 - 5 Questions
-

Working with the Resource Registry

Lets talk with SWITCH

- contacted SWITCH in May 2017
- SWITCH implemented changes in August 2017
 - Metadata extensions to add additional information to the Service Description (XML)
 - Metadata Wizard to paste the XML description into the Resource Editor in the AAI Resource Registry

Working with the Resource Registry

Resource Registry > New Resource > Basic Resource Information > Run SAML 2 Metadata Wizard

Resource Menu for 'New Resource'

To create a new Resource Description, first complete the section 'Basic Resource Information' and then the remaining sections.

If you already have SAML2 metadata of your SAML Service provider (e.g. from /Shibboleth.sso/Metadata), run the Metadata Wizard to create or update an existing Resource Description.

The Metadata Wizard can be used to register a new or upgrade an already registered Service Provider. To use it, either paste the SAML2 metadata into the text field or click on the button 'Run SAML 2 Metadata Wizard' to provide an URL to download SAML2 metadata from. To create a complete Resource Description using SAML2 metadata, please also consult the [metadata extension element documentation](#).

 [Run SAML 2 Metadata wizard](#)

- | | |
|---|--|
|  1. Basic Resource Information |  Incomplete |
|  2. Descriptive Information |  Incomplete |
|  3. Contacts |  Incomplete |
|  4. Service Locations |  Incomplete |

Working with the Resource Registry

Setup the Shibboleth SP

- We use ansible for our server setup
- Using Application Overrides for each site
 - we can easily move EasyWeb instances from one server to another
 - each EasyWeb instance has its own certificate

Working with the Resource Registry

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="ew-stage.ius.unibas.ch"
      applicationId="ew-stage.ius.unibas.ch" />
    <Host name="ew-stage.chemie.unibas.ch"
      applicationId="ew-stage.chemie.unibas.ch" />
    <Host name="ew-stage.wvz.unibas.ch"
      applicationId="ew-stage.wvz.unibas.ch" />
    <Host name="ew-stage.theologie.unibas.ch"
      applicationId="ew-stage.theologie.unibas.ch" />
    <Host name="ew-stage.philhist.unibas.ch"
      applicationId="ew-stage.philhist.unibas.ch" />
    <Host name="ew-stage.easyweb.unibas.ch"
      applicationId="ew-stage.easyweb.unibas.ch" />
  </RequestMap>
</RequestMapper>
```

The default settings can be overridden by creating ApplicationOverride elements.
More Information and examples on:
<https://wiki.shibboleth.net/confluence/display/SP3/ApplicationOverride>

```
-->
<ApplicationOverride id="ew-stage.ius.unibas.ch"
  entityID="https://ew-stage.ius.unibas.ch/shibboleth">
  <CredentialResolver type="File"
    keyName="Active"
    key="/etc/shibboleth/ew-stage.ius.unibas.ch.sp-key.pem"
    certificate="/etc/shibboleth/ew-stage.ius.unibas.ch.sp-cert.pem" />
</ApplicationOverride>
<ApplicationOverride id="ew-stage.chemie.unibas.ch"
  entityID="https://ew-stage.chemie.unibas.ch/shibboleth">
  <CredentialResolver type="File"
    keyName="Active"
```

Working with the Resource Registry

Generate the Metadata XML

- Load the basic XML from `https://<easyweb-domain>/Shibboleth.sso/Metadata`
 - Correct settings for this Instance
 - Includes the Certificate
- Add additional Data
 - homeOrganisation, homeURL, federation, etc
 - Requested Attributes
 - Contacts

Working with the Resource Registry

```
<md:Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:alg:support">
<!-- SWITCH RR Metadata Extensions: BEGIN -->
<mdext:SWITCHaaExtensions
  homeOrganization="unibas.ch"
  federation="urn:mace:switch.ch:SWITCHaa"
  isPublic="false"
  homeURL="https://ew-stage.chemie.unibas.ch/"
  helpdeskURL="https://its.unibas.ch/"
  interfederationEnabled="false"
  mainLanguage="en">
  <mdext:Administrator email="h.spalinger@unibas.ch"/>
  <mdext:Administrator email="stefan.keller@unibas.ch"/>
  <mdext:Administrator email="dominik.hofer@unibas.ch"/>
  <mdext:Administrator email="ad.keller@unibas.ch"/>
  <mdext:IntendedAudience type="homeOrganization" audiencePolicy="include">unibas.ch</mdext:IntendedAudience>
  <mdext:RequestedAttributeComment attributeName="urn:oid:0.9.2342.19200300.100.1.3">
    User management in easyWeb
  </mdext:RequestedAttributeComment>
  <mdext:RequestedAttributeComment attributeName="urn:oid:2.5.4.42">
    Display username in easyweb
  </mdext:RequestedAttributeComment>
  <mdext:RequestedAttributeComment attributeName="urn:oid:2.5.4.4">
    Display username in easyweb
  </mdext:RequestedAttributeComment>
  <mdext:RequestedAttributeComment attributeName="urn:oid:1.3.6.1.4.1.22865.10.1.1.93">
    Connect the user to other data sources at Uni Basel
  </mdext:RequestedAttributeComment>
  <mdext:RequestedAttributeComment attributeName="urn:oid:1.3.6.1.4.1.22865.10.1.1.19">
    User management in easyWeb
  </mdext:RequestedAttributeComment>
  <mdext:RequestedAttributeComment attributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.10">
    User management in easyWeb
  </mdext:RequestedAttributeComment>
</mdext:SWITCHaaExtensions>
```


Working with the Resource Registry

```
e.chemie.unibas.ch/Shibboleth.sso/SAML2/POST-SimpleSign" index="6"/>
<!-- SWITCH RR Attribute Data: BEGIN -->
<md:AttributeConsumingService index="1">
  <md:RequestedAttribute
    FriendlyName="email"
    isRequired="true"
    Name="urn:oid:0.9.2342.19200300.100.1.3"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
    FriendlyName="givenName"
    isRequired="true"
    Name="urn:oid:2.5.4.42"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
    FriendlyName="surname"
    isRequired="true"
    Name="urn:oid:2.5.4.4"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
    FriendlyName="unibasChPublicId"
    isRequired="true"
    Name="urn:oid:1.3.6.1.4.1.22865.10.1.1.93"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
    FriendlyName="unibasChRoles"
    isRequired="true"
    Name="urn:oid:1.3.6.1.4.1.22865.10.1.1.19"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
    FriendlyName="eduPersonTargetedID"
```

Working with the Resource Registry

```
<md:Organization>
  <md:OrganizationName xml:lang="en">unibas.ch</md:OrganizationName>
  <md:OrganizationDisplayName xml:lang="de">Universität Basel</md:OrganizationDisplayName>
  <md:OrganizationDisplayName xml:lang="en">University of Basel</md:OrganizationDisplayName>
  <md:OrganizationDisplayName xml:lang="fr">Université de Bâle</md:OrganizationDisplayName>
  <md:OrganizationURL xml:lang="de">http://www.unibas.ch/</md:OrganizationURL>
  <md:OrganizationURL xml:lang="en">http://www.unibas.ch/</md:OrganizationURL>
  <md:OrganizationURL xml:lang="fr">http://www.unibas.ch/</md:OrganizationURL>
</md:Organization>
<md:ContactPerson contactType="support">
  <md:GivenName>Support</md:GivenName>
  <md:SurName>ITS</md:SurName>
  <md:EmailAddress>mailto:support-its@unibas.ch</md:EmailAddress>
</md:ContactPerson>
<md:ContactPerson contactType="technical">
  <md:GivenName>WSyM</md:GivenName>
  <md:SurName>ITS</md:SurName>
  <md:EmailAddress>mailto:wsym-its@unibas.ch</md:EmailAddress>
</md:ContactPerson>
<md:ContactPerson contactType="administrative">
  <md:GivenName>WAPP</md:GivenName>
  <md:SurName>ITS</md:SurName>
  <md:EmailAddress>mailto:wapp-its@unibas.ch</md:EmailAddress>
</md:ContactPerson>
<!-- SWITCH RR Organizational Data: END -->
```

Working with the Resource Registry

Register the Service Provider

- Paste XML into the Wizard on <https://rr.aai.switch.ch/>
- Approve the new Resource providing the Certificate Signature

Agenda.

-
- 1 Why do we want automated Shibboleth Service deployment
 - 2 Challenges we faced
 - 3 Working with the Resource Registry
 - 4 Wishlist for the Resource Registry
 - 5 Questions
-

Wishlist for the Resource Registry

API to Upload Metadata XML

- Copy/Paste of XML is always the same. Could be automated too.
- The Resource is „created by“ the person logged in
 - Can it be a Organization „User“?

Last Changes

 [Hide History](#)

Last change by  [Hanspeter Spalinger](#) on 3. 4. 2019 14:36

Resource Description History

- **3. 4. 2019 14:36:** Resource Description approved by  [Hanspeter Spalinger](#) (unibas.ch)
- **3. 4. 2019 14:36:** Resource Description created by  [Hanspeter Spalinger](#) (unibas.ch)

 [Edit](#) |  [Duplicate](#) |  [Request Deletion](#) |  [Administrators](#) |  [Configuration](#) |  [Metadata](#) |  [Attribute Release Inspector](#)

Agenda.

-
- 1 Why do we want automated Shibboleth Service deployment
 - 2 Challenges we faced
 - 3 Working with the Resource Registry
 - 4 Wishlist for the Resource Registry
 - 5 Questions



University
of Basel

Thank you
for your attention.