University of Basel

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

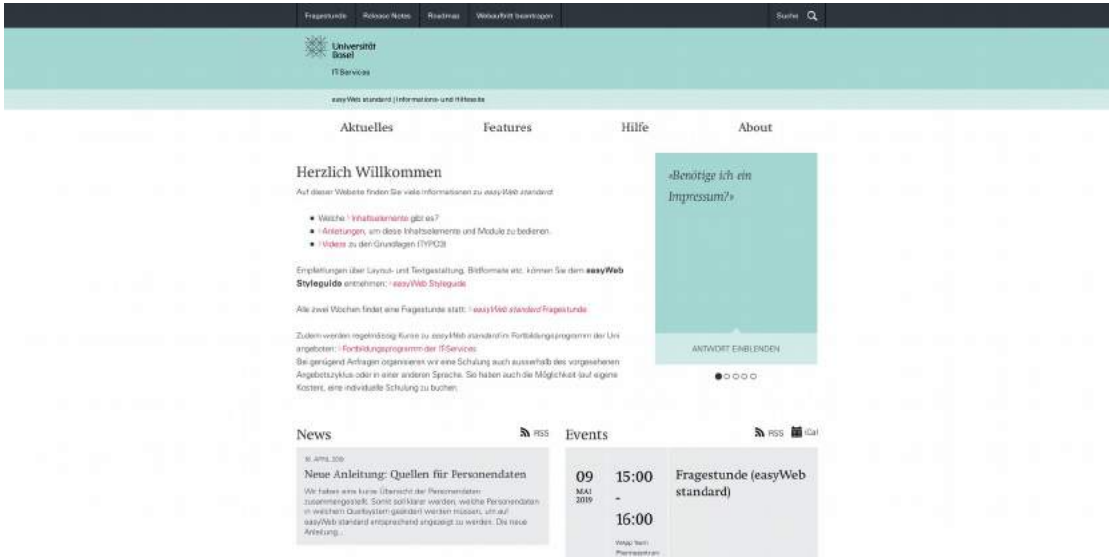
– Uncertain future of Website Hosting Platform (cloud?)

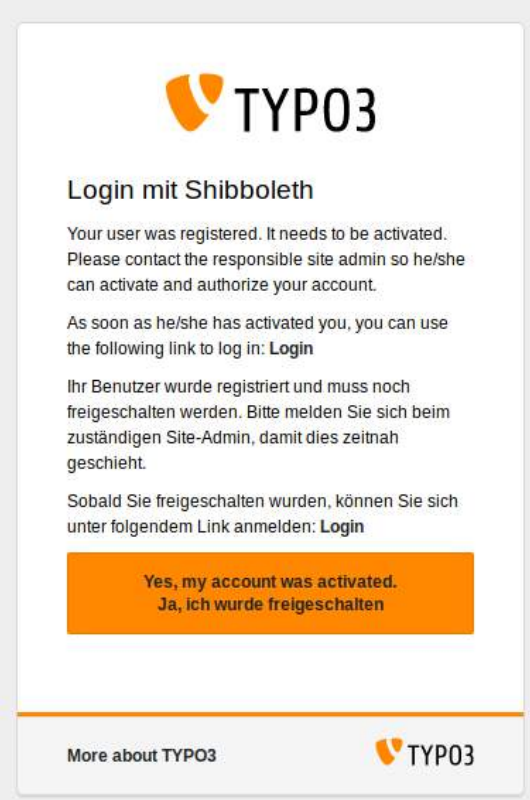
– No dependencies into internal Authentication Services (AD, LDAP, etc)

– 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





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

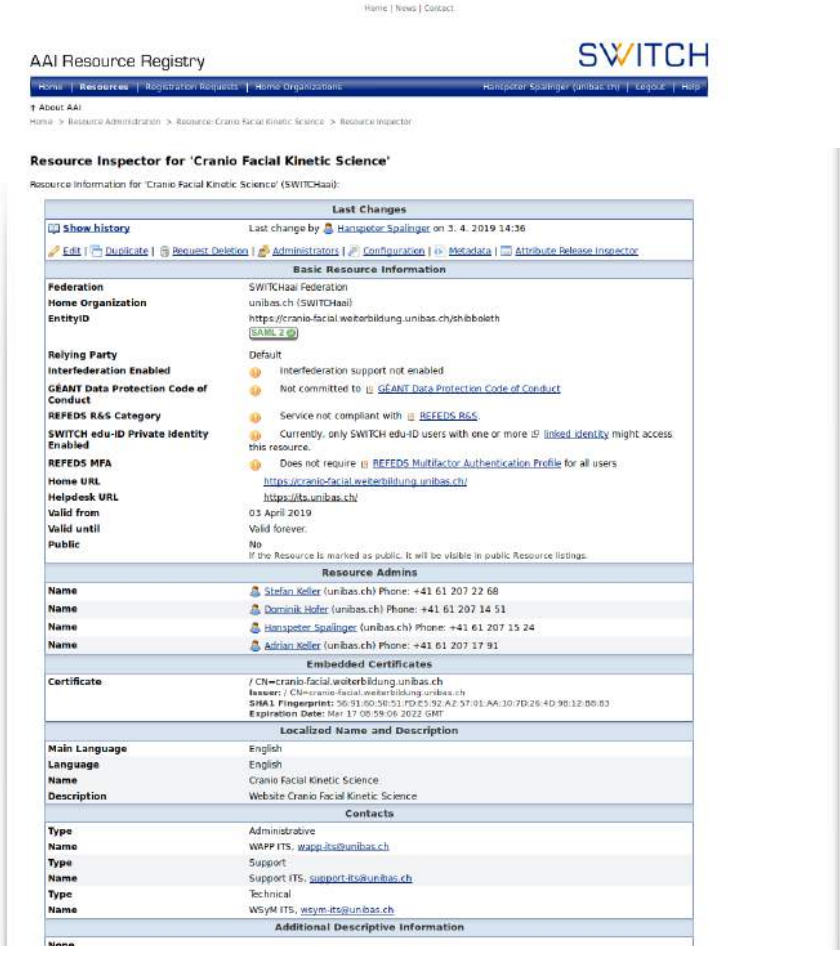
– Lots of Departements have their own Websites (~200)

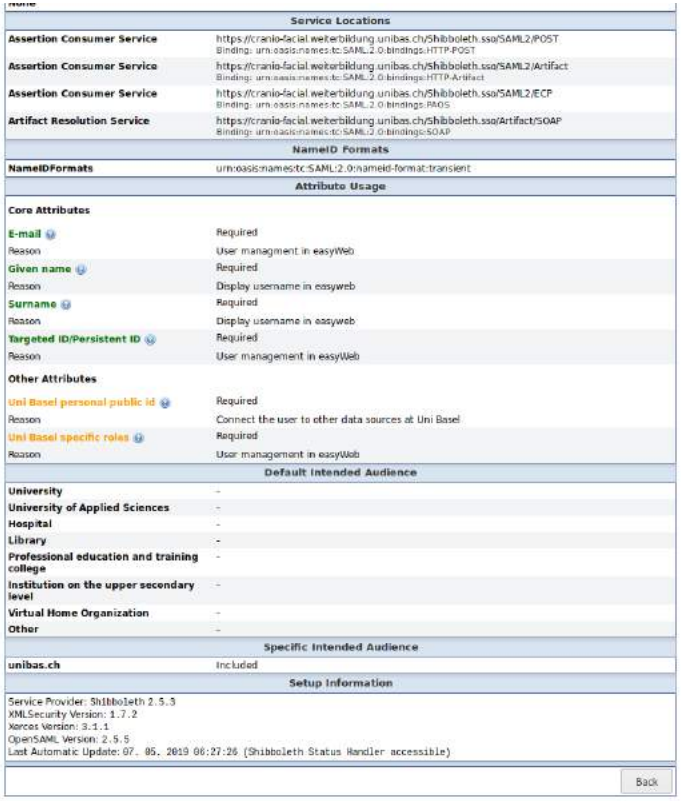
– Each site should have a additional staging instance for testing (x2)

– Filling out the Resource Registry Form can be time consuming

– But all EasyWeb sites have the same settings anyway

Challenges we faced





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

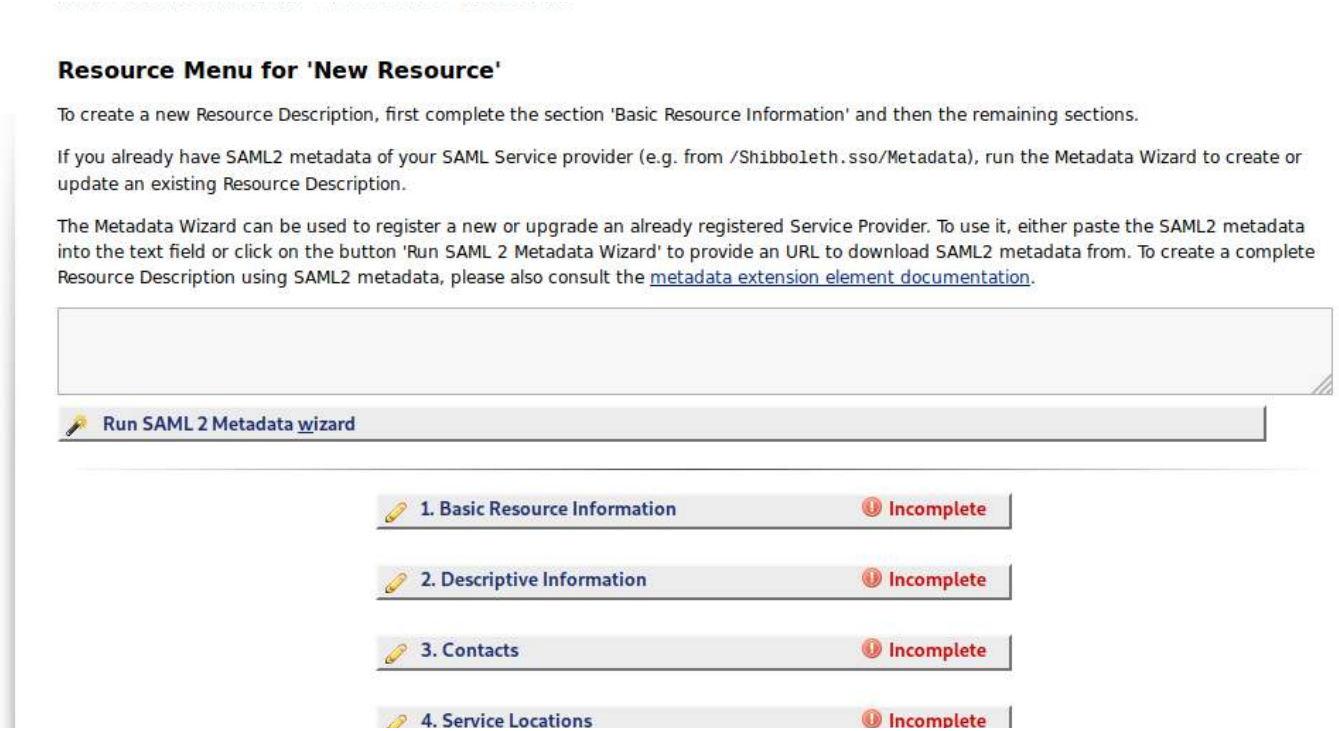
– contacted SWITCH in May 2017

– 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



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.wwz.unibas.ch"
          applicationId="ew-stage.wwz.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:algsupport">
<!-- SWITCH RR Metadata Extensions: BEGIN -->
<mdext:SWITCHaaiExtensions
  homeOrganization="unibas.ch"
  federation="urn:mace:switch.ch:SWITCHaai"
  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 managment 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:SWITCHaaiExtensions>
```

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“?

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.