

Resource Registry News

What Santa will bring you (probably) even before Christmas



SWITCH

Serving Swiss Universities

Lukas Hämmerle

lukas.haemmerle@switch.ch

Proposed Christmas Presents

Early Christmas gifts to discuss about:

1.  Resource contact info removal from metadata

2.  Contact/setup information notifications

3. Security improvements



- Optional four-eyes principle (already operational)
- Optional second factor Authentication (being implemented)
- Emergency disabling via CERT (to be implemented)

1. XML Diet for Resource Description



- **Proposal:** Removal of contact information in metadata for Resource Descriptions
- Only concerns resource descriptions
 - Contact information for IdPs won't be touched
- Contact information is technically not necessary
- Information still can be looked up in Resource Registry by people with an AAI account or on



<http://www.switch.ch/aai/participants/allresources.html>

- Are there any objections/reasons against this proposal?

Sample Resource Description

```
<EntityDescriptor entityID="https://econf.switch.ch/shibboleth">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>econf.switch.ch</ds:KeyName>
      </ds:KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <AssertionConsumerService
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
      Location="https://econf.switch.ch/Shibboleth.sso/SAML/POST"
      index="1" isDefault="true" />
  </SPSSODescriptor>

  <ContactPerson contactType="technical">
    <SurName>Fabio Vena</SurName>
    <EmailAddress>vena@switch.ch</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="support">
    <SurName>Fabio Vena</SurName>
    <EmailAddress>vena@switch.ch</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="administrative">
    <SurName>Fabio Vena</SurName>
    <EmailAddress>vena@switch.ch</EmailAddress>
  </ContactPerson>
</EntityDescriptor>
```

Sample Resource Description

```
<EntityDescriptor entityID="https://econf.switch.ch/shibboleth">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>econf.switch.ch</ds:KeyName>
      </ds:KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <AssertionConsumerService
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
      Location="https://econf.switch.ch/Shibboleth.sso/SAML/POST"
      index="1" isDefault="true" />
  </SPSSODescriptor>
</EntityDescriptor>
```

Contact/Setup Notifications



- **Proposal:** Notification email (1 email only) to IdP administrators every 6 months with current setup and contact information
- People join and leave organisations
- IdP software is/should be updated from time to time
- ⇒ Both should be reflected in Resource Registry for the data to be accurate
- Bounced mails also can expose expired accounts
- Is 6 months a reasonable interval?

Example Setup Information

Home Organization Setup & Environment Information

DB Administration RRA Administration Home Organization Administration Resource Administration General Information

▶ Home Organization Description menu of "SWITCH" - Home Organization Setup & Environment Information

Home Organization Setup and Environment Information

Please specify on this page what is your Identity Provider setup. This may help us and others on one side to see which setups are preferred and on the other side it may be useful when it comes to pinpoint problems.

In case, you don't find an option in the drop-down list, please choose "Other" and provide a comment in the textfield on the right.

Setup & Environment Information	
Operating system	Debian Linux <input type="text"/>
Webserver	Tomcat + Apache <input type="text"/>
Authentication System	CAS 3 <input type="text"/>
IdP version	1.3.3 <input type="text"/>
Comments	<input type="text" value="With ArpViewer"/>

Example Contact Information

Home Organization List of contacts

DB Administration RRA Administration Home Organization Administration Resource Administration General Information

▶ Home Organization Description menu of "SWITCH" - Home Organization List of Contacts

List of Contacts

At least one **support and one technical** contact should be provided:

- **Administrative contact:** The person that is generally responsible for AAI.
- **Technical contact:** The person that is responsible for the host and the Shibboleth Identity Provider.
- **Support contact:** The person that is responsible for the user directory, e.g. when users lost their password.

Be aware that all data you provide will be included in the federation metadata and some user helpdesk web pages. Therefore, it will be published online and accessible for all Internet users.

List of contacts

Contact Type	Technical
Contact Name	SWITCHaai Team
E-Mail	aai@switch.ch
Contact Type	Support
Contact Name	SWITCHaai Team
E-Mail	aai@switch.ch
Contact Type	Administrative
Contact Name	Thomas Lenggenhager
E-Mail	lenggenhager@switch.ch

Cancel Reset Apply Save and continue

Security Improvements I



Optional four-eyes principle:

A different account must be used for approving a Resource Description than was used for creating or modifying it.

Goals:

- Stolen RRA admin credentials cannot be used to change/create rogue Resource Description
- Prevent configuration mistakes

Status: Is already operational and has been used by SWITCH. Works well provided there are multiple RRA administrators.

Screenshot of Four-eyes approval

- Resource Descriptions cannot be edited/created and approved with the same AAI account

Resources waiting for approval

SWITCH AAI Wiki: waaikiki (<https://aai-wiki.switch.ch/shibboleth, SWITCHaai>)

[View changes](#) | [edit](#)

1. Requesting Resource Administrator:
Lukas Hämmerle (switch.ch)
Phone number: **+41 44 268 1505**
2. Service Location URLs:
 - o <https://aai-wiki.switch.ch/Shibboleth.sso/SAML/POST>
3. Certificate subject common name: `tools.switch.ch`
4. Embedded certificates:
None
5. Required and desired Attributes:
 - o E-mail ⓘ (desired)
6. Description:
This TWiki-based Wiki deals with AAI relevant topics.

Forbidden due to secure approval ▼

⚠ **You are not allowed to approve your own resource description when secure approval is activated for this Home Organization.**

Consequences of Resource Approval

Before you approve a Resource Description, please examine it and be aware of the fact that by approving this Resource Description, you are responsible that the resource administrators of this resource are aware of and know that they have to act according to the AAI Service Agreement.

[Reset](#) [Apply](#) [Submit and return](#)

Security Improvements II



Optional Second Factor Authentication:

For approving Resource Descriptions or altering Home Organization descriptions, improved authentication security can be required for a Home Organization.

Goal:

Stolen RRA admin credentials cannot be used to change/create rogue Resource Description or alter a Home Organization description.

Status: Except SWITCH, no other IdP supports two-factor authentication. Therefore, Resource Registry will implement SMS token authentication as second factor.

Preview of SMS Token authentication

- Will only be requested if Home Organization decided to use this feature
- Only necessary when changing Home Organization description or approving Resource Descriptions

SMS Token Authentication

DB Administration | RRA Administration | Home Organization Administration | Resource Administration | General Information

The action you tried to perform requires strong authentication. Because your Home Organization cannot yet provide strong authentication, the Resource Registry sent you a Token to your mobile phone. Please enter the received token below.

SMS Token Authentication

Mobile phone number +41 76 302 25 74
The mobile phone number the token was sent to.

SMS Token
Enter here the token you should have received on your mobile phone

This field must be provided

The reward for being a little bit more secure...

Home Organization Inspector

DB Administration

RRA Administration

Home Organization Administration

Resource Administration

General Information

Home Organization information for 'SWITCH' (SWITCHaai)

Last Updated


 Lukas Hämmerle
on 6. 11. 2008 18:06

 Edit this Home Organization description


Basic Information

Home Organization Name

switch.ch

 **Four-eyes approval required**

Resource descriptions for this Home Organization are approved by a different account than the one that created them. This Four-Eyes approval procedure increases security and decreases configuration errors.

 **Strong authentication approval required**

The Home Organization description and any Resource descriptions for this Home Organization are modified and approved only by users who authenticated using two-factor authentication either implemented by the Identity Provider or by the Resource Registry' SMS token authentication.

Home Organization Type

Others

Federation

SWITCHaai Federation

Main language

English

Descriptive Name

SWITCH

Description

SWITCH coordinates and operates the Shibboleth federation called "SWITCHaai". It supports the universities and other participants of the federation in adapting and using the services provided by the AAI.

Example of Home Organization description page in Resource Registry

Security Improvements III



Emergency Disabling of IdP and SP:

SWITCH CERT members could be contacted by their known university security contact person when an IdP's certificate was compromised and has to be removed from metadata.

Goal:

Prevent attacker from creating assertions in the name of a compromised IdP and become aware of phishing IdP.

Status: Is being implemented. CERT members will have a special interface in Resource Registry to disable an IdP.

Emergency Disabling Procedure

