## Resource Registry News

What Santa will bring you (probably) even before Christmas







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</pre>
          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



## **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**

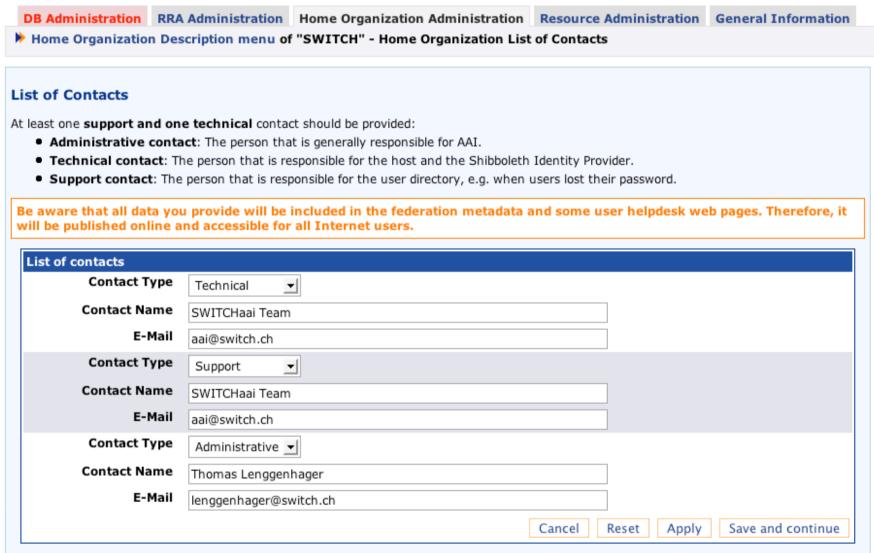
DB Administration RRA Administration Home Organization Administration Resource Administration General Information ▶ Home Organization Description menu of "SWITCH" - Home Organization Setup & Environment Information Home Organization Setup and Environment Information Please specify on this page what is 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 Webserver Tomcat + Apache **Authentication System** CAS 3 IdP version **▼** 1.3.3 Comments With ArpViewer Cancel Reset VlqqA Save and return to menu



Logged in as: Lukas Hämmerle (switch.ch)

## **Example Contact Information**

#### **Home Organization List of contacts**



## **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.

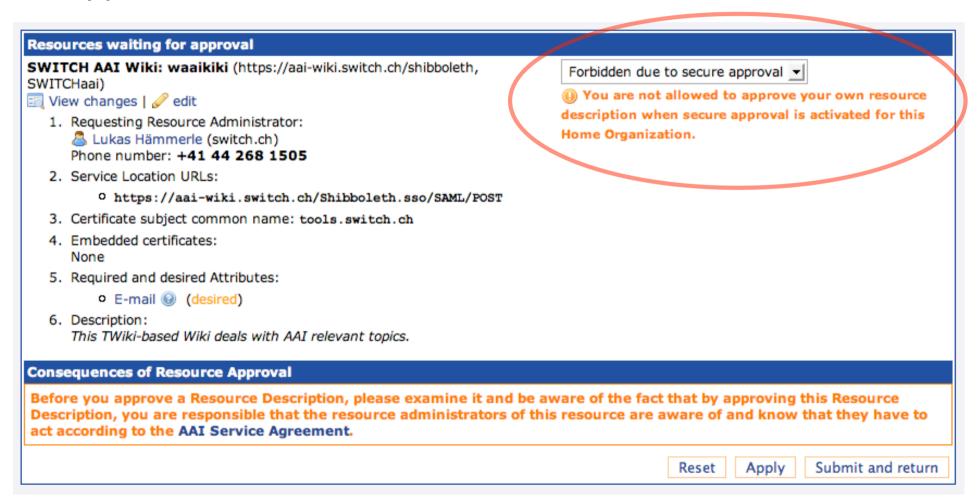
#### Goals:

- 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



## **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:

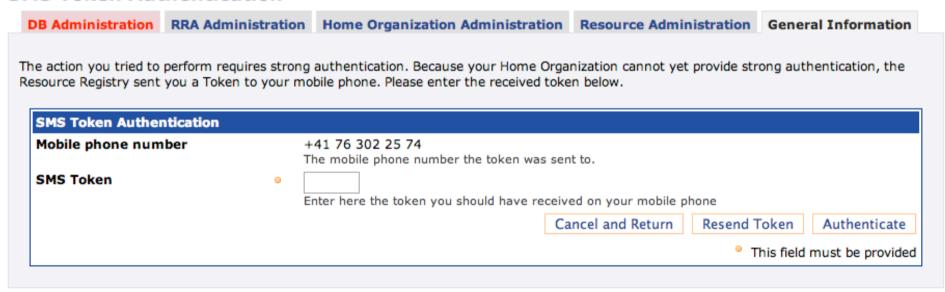
Stolen RRA admin credentials cannot be used to change/create rogue Resource Description or alter a Home Organization description.

**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
- Onle necessary when chaning Home Organization description or approving Resource Descriptions

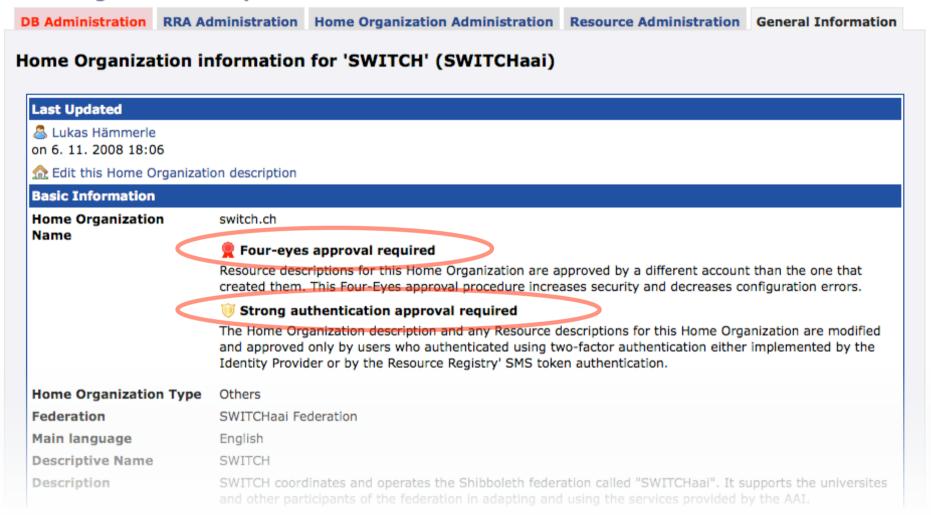
#### **SMS Token Authentication**





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

#### **Home Organization Inspector**



#### 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

