Resource Registry News

Some refreshed and some new features

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Bern, 16. September 2009

The five topics

1. X.509 certificate embedding
2. Four-eyes principle
3. Optional 2nd factor authentication with SMS
4. IdP Emergency Disabling
5. IdP & SP version info gathering

X.509 Certificate Embedding

1

- **X.509 certificate must be embedded in metadata**
  This allows to get rid of Root CA certificates.

- **Requirements:**
  Certificate constraints that must be met
  http://www.switch.ch/aai/support/embeddedcerts-requirements.html

- **Migration:**
  How to replace certificates without service disruptions
  http://www.switch.ch/aai/support/certificate-migration.html

X.509 Certificate Requirements

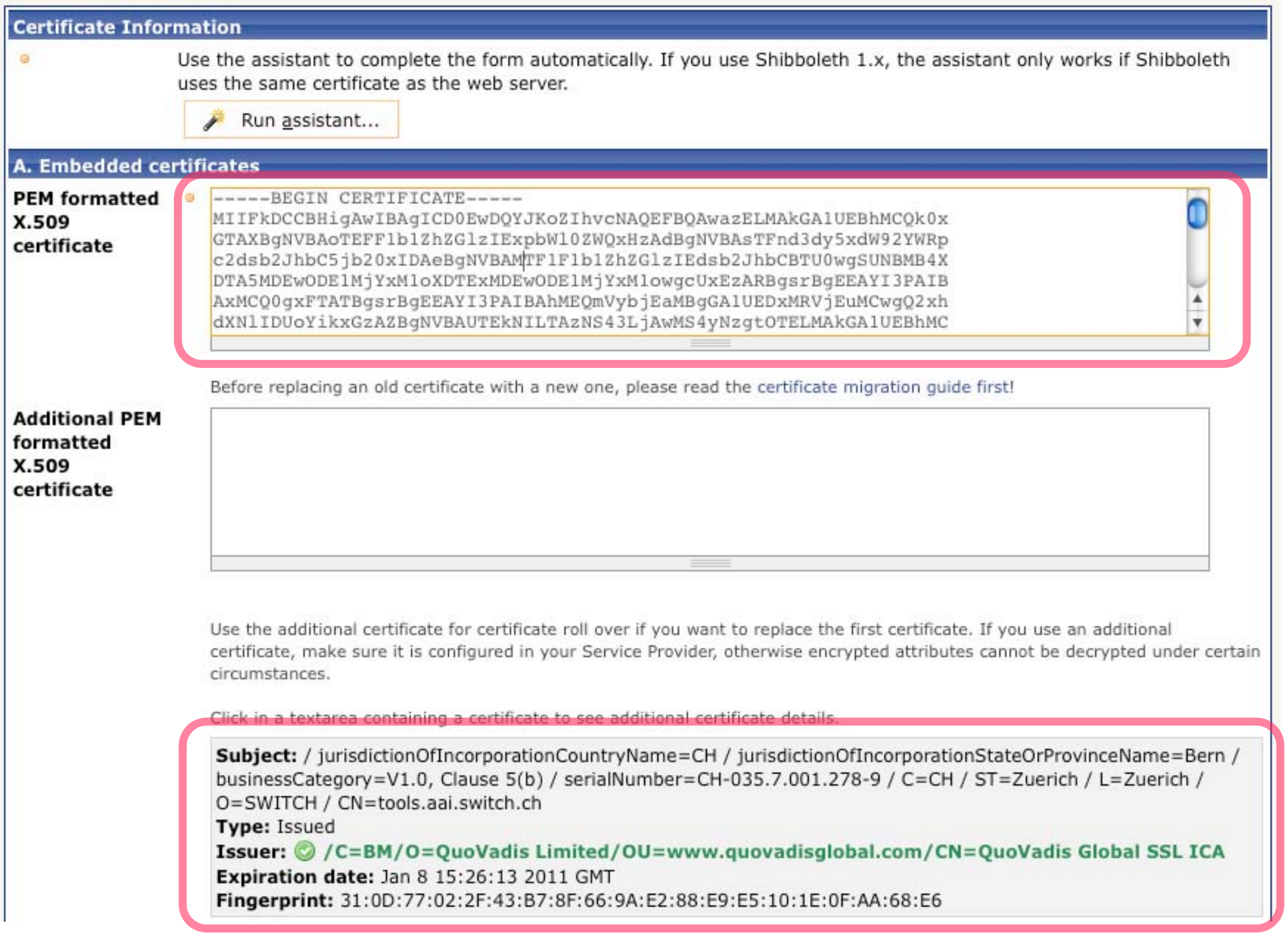
1

The most important requirements

- Max. validity of 3 years
- Key length must be 2048Bit
- Self-signed:
  - As automatically generated by SP/IdP but only 3 years valid
  - Only CN=#Hostname# attribute in subject
  - entityID in subjectAltName
- Issued:
  - No domain validated certificates
  - Only if accepted by Microsoft or Mozilla trust stores

How the embedding looks like

1



Certificate Information

Use the assistant to complete the form automatically. If you use Shibboleth 1.x, the assistant only works if Shibboleth uses the same certificate as the web server.

A. Embedded certificates

PEM formatted X.509 certificate

```
-----BEGIN CERTIFICATE-----
MIIFkDCCBHigAwIBAgICD0EwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbW10ZWQxHzAdBgNVBAsTFnd3dy5xdW92YWRp
c2dsb2JhbC5jb20xIDAeBgNVBAMTF1F1b1ZhZGlzIEdsb2JhbCBTU0wgSUNBMB4X
DTA5MDEwODE1MjYxMloXDTExMDEwODE1MjYxMlowgcUxEzARBgsrBgEEAYI3PAIB
AxMCQ0gxFTATBgsrBgEEAYI3PAIBAhMEQmVybjEaMBgGA1UEDxMRVjEuMCwgQ2xh
dXNlIDUoYikxGzAZBgNVBAUTEkNILTAzNS43LjAwMS4yNzgtOTELMAkGA1UEBhMC
```

Before replacing an old certificate with a new one, please read the certificate migration guide first!

Additional PEM formatted X.509 certificate

Use the additional certificate for certificate roll over if you want to replace the first certificate. If you use an additional certificate, make sure it is configured in your Service Provider, otherwise encrypted attributes cannot be decrypted under certain circumstances.

Click in a textarea containing a certificate to see additional certificate details.

Subject: / jurisdictionOfIncorporationCountryName=CH / jurisdictionOfIncorporationStateOrProvinceName=Bern / businessCategory=V1.0, Clause 5(b) / serialNumber=CH-035.7.001.278-9 / C=CH / ST=Zuerich / L=Zuerich / O=SWITCH / CN=tools.aai.switch.ch
Type: Issued
Issuer: ✓ /C=BM/O=QuoVadis Limited/OU=www.quovadisglobal.com/CN=QuoVadis Global SSL ICA
Expiration date: Jan 8 15:26:13 2011 GMT
Fingerprint: 31:0D:77:02:2F:43:B7:8F:66:9A:E2:88:E9:E5:10:1E:0F:AA:68:E6

Four-Eyes Principle

2

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 should not be usable to change/create (malicious) Resource Descriptions
- Prevent configuration mistakes

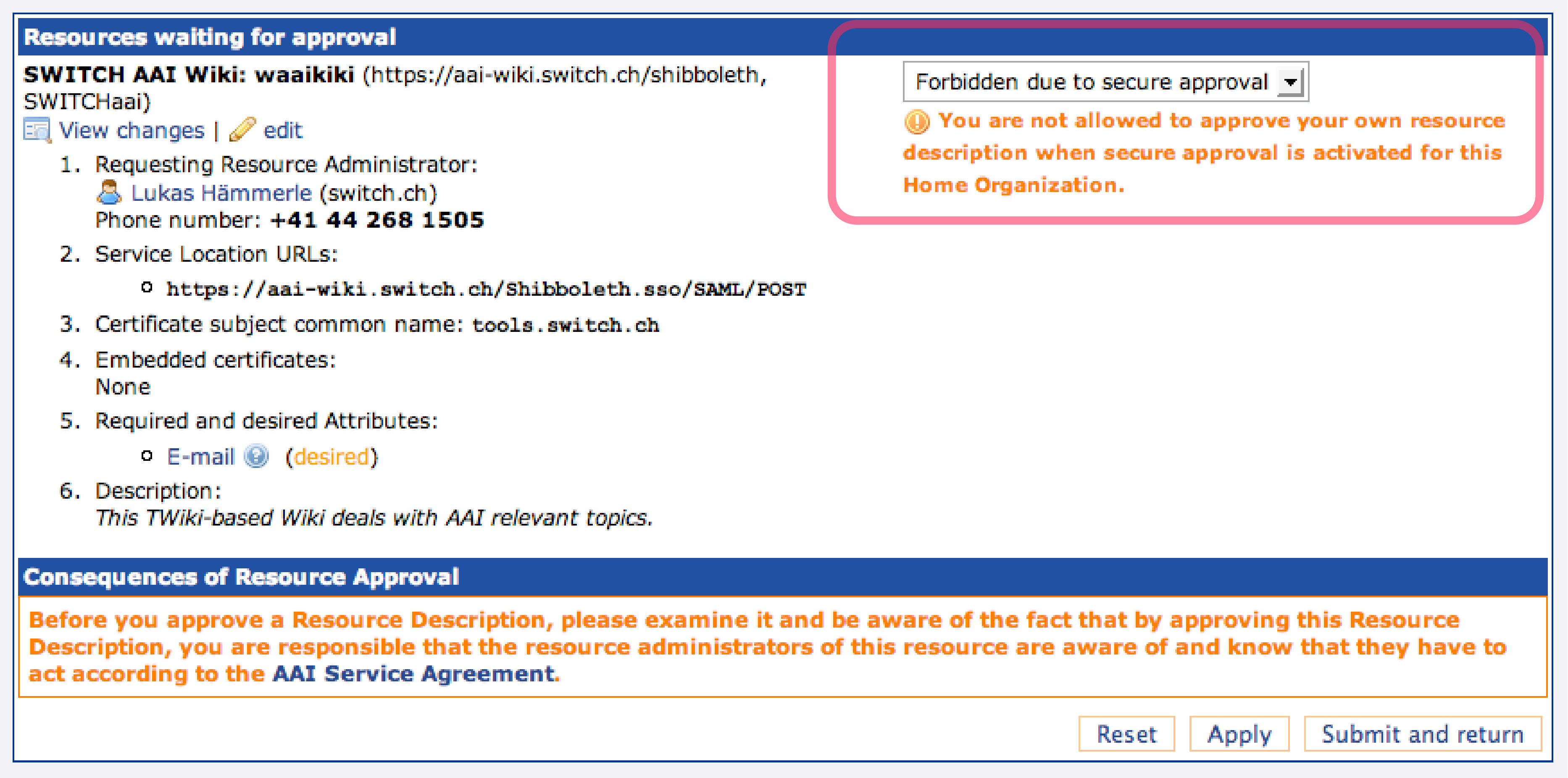
Status:

Has been used by SWITCH and UniL for several months

Four-eyes principle in action

2

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:
   - `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:
   - 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.

2nd Factor Authentication with SMS

3

Threat:
Stolen/phished credentials could be used to change/create malicious Resource Description or sabotage Home Organisation Description.

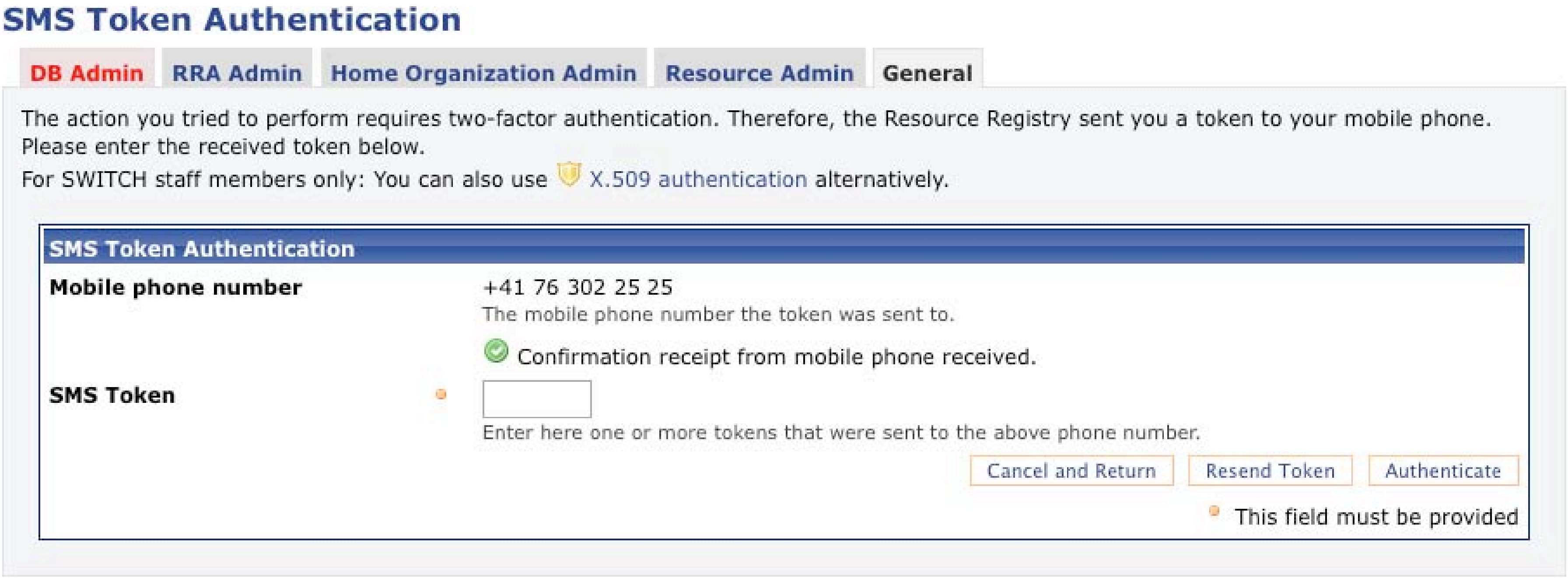
Issue:
Except SWITCH IdP, no other IdP has supported two-factor authentication so far. Therefore, improved security had to be added to Resource Registry directly.

Goal:

Additional security for approving Resource Descriptions or modifying Home Organization descriptions.

How 2nd factor AuthN with SMS looks like 3

- One has to enter a 5 character token (.e.g “8sd46”) that is sent to mobile phone as flash SMS.
- Immediate feedback from SMS provider is displayed
- Up to 3 tokens are sent, all of them valid for 5 minutes
- First correct token invalidates all others that were sent



SMS Token Authentication

The action you tried to perform requires two-factor authentication. Therefore, the Resource Registry sent you a token to your mobile phone. Please enter the received token below.

For SWITCH staff members only: You can also use X.509 authentication alternatively.

SMS Token Authentication

Mobile phone number	+41 76 302 25 25 The mobile phone number the token was sent to. ✓ Confirmation receipt from mobile phone received.
SMS Token ●	□ Enter here one or more tokens that were sent to the above phone number.

● This field must be provided

Requirements and Implementation

3

What is required for SMS Token to be used

User’s mobile phone number must be known

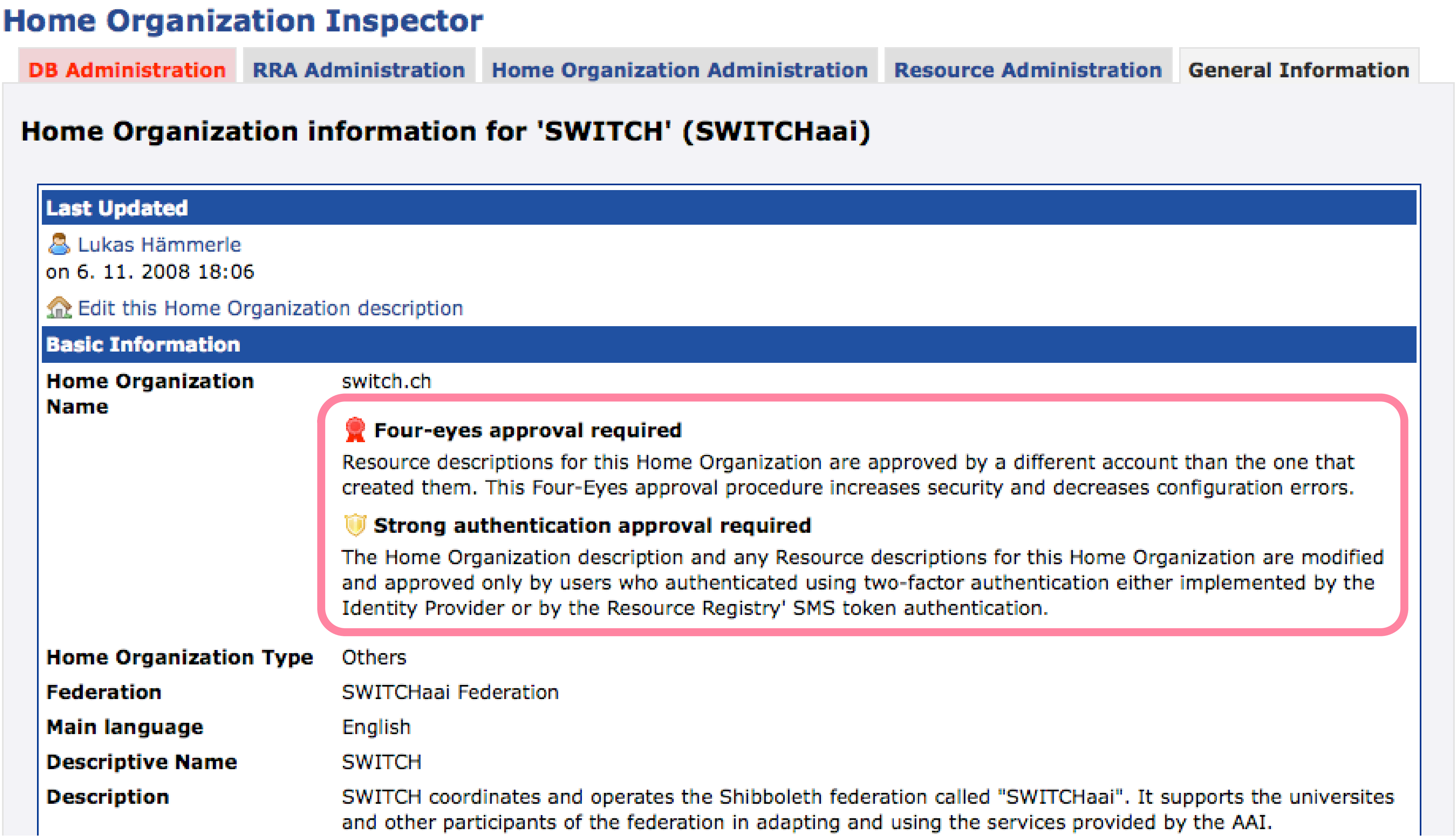
- Identity Provider must be able to release mobile attribute
- or mobile number must be manually added to Resource Registry database

Some words about the implementation

- Implementation to send SMS is very easy
- SMS status feedback requires a bit more effort
- SMS provider clickatell.com is used
  - Many features and APIs, good documentation, low prices
- Code can be requested at aai@switch.ch

Reward for being more secure

2 3



Home Organization Inspector

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 universites and other participants of the federation in adapting and using the services provided by the AAI.

Who would like to test SMS tokens?

Who would like to test Four-Eyes approval?

Image from www.fedcbs.ie

Generally: SMS tokens are recommended for smaller institutions as alternative to four-eyes approval.

Identity Provider Emergency Disabling

4

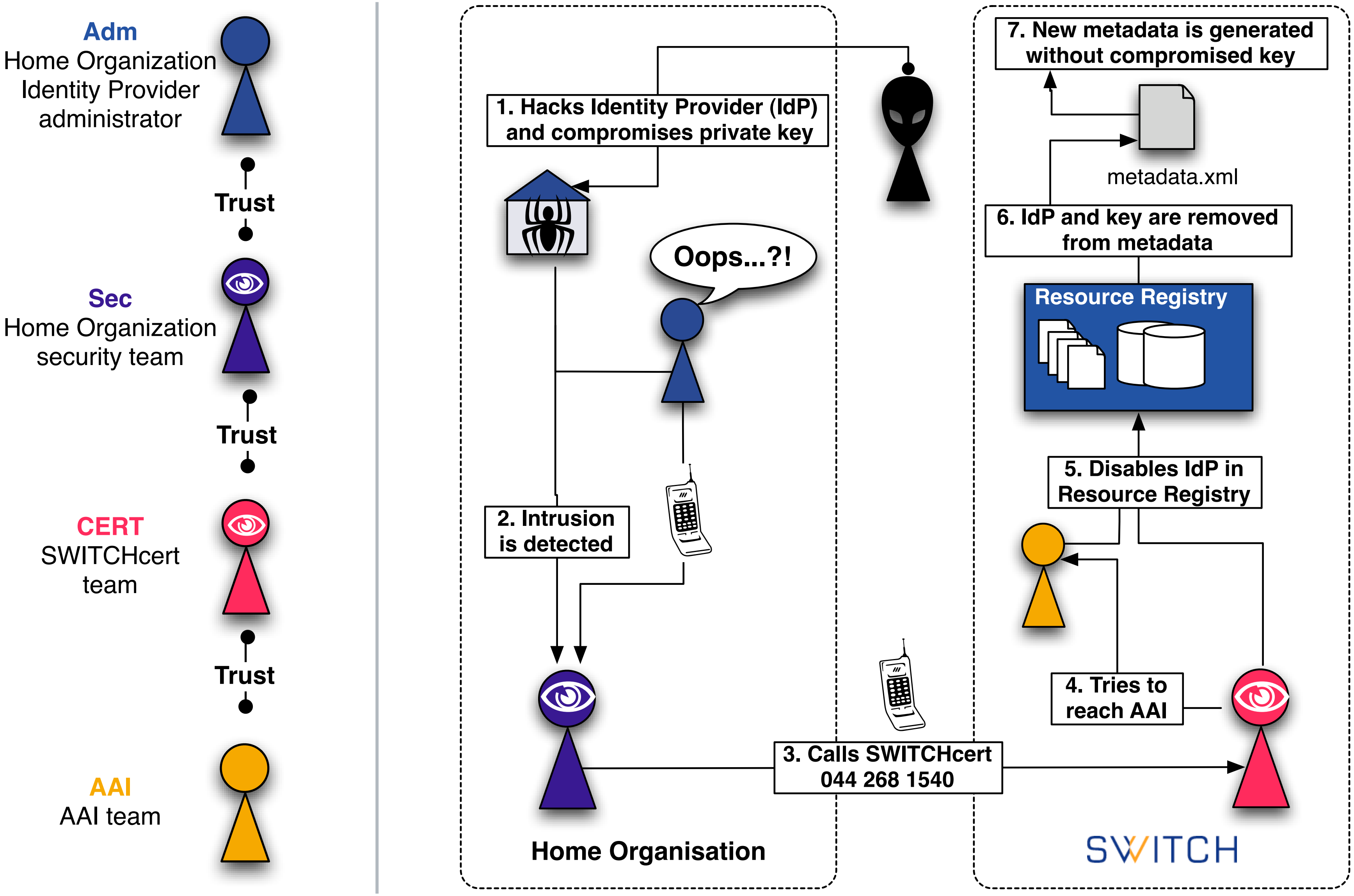
- Procedures for the worst case like...
- A few weeks ago a SWITCHaai IdP was used by spammers due to an Apache misconfiguration
  - Fortunately, this was not the worst case (filesystem access)
- But in the worst case it wouldn’t be enough to just shut down the IdP...

The risk to prevent:

- Potentially stolen private key could be used to issue identity assertions in the name of compromised IdP

IdP Emergency Disabling Procedure

4



Adm
Home Organization Identity Provider administrator

Trust

Sec
Home Organization security team

Trust

CERT
SWITCHcert team

Trust

AAI
AAI team

1. Hacks Identity Provider (IdP) and compromises private key

2. Intrusion is detected

3. Calls SWITCHcert 044 268 1540

4. Tries to reach AAI

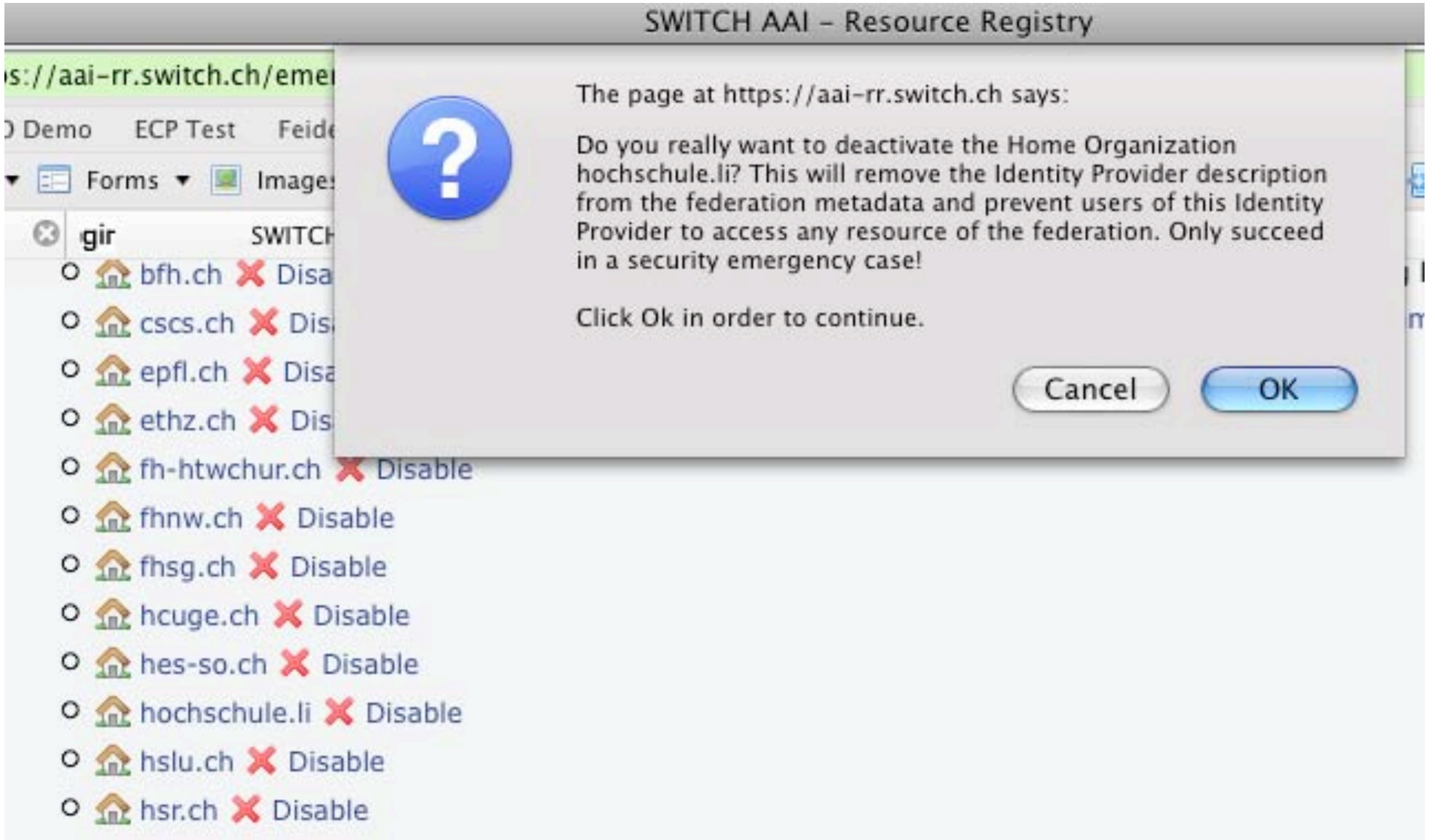
5. Disables IdP in Resource Registry

6. IdP and key are removed from metadata

7. New metadata is generated without compromised key

The red buttons

Page is protected to allow only AAI team members and SWITCHcert team members that authenticated with X.509 certificate



The page at https://aai-rr.switch.ch says:

Do you really want to deactivate the Home Organization hochschule.li? This will remove the Identity Provider description from the federation metadata and prevent users of this Identity Provider to access any resource of the federation. Only succeed in a security emergency case!

Click Ok in order to continue.

What happens if you push the red button

- Description of compromised Identity Provider is removed from metadata within max. 1 hour

- Service Providers download updated metadata within max.1 hour

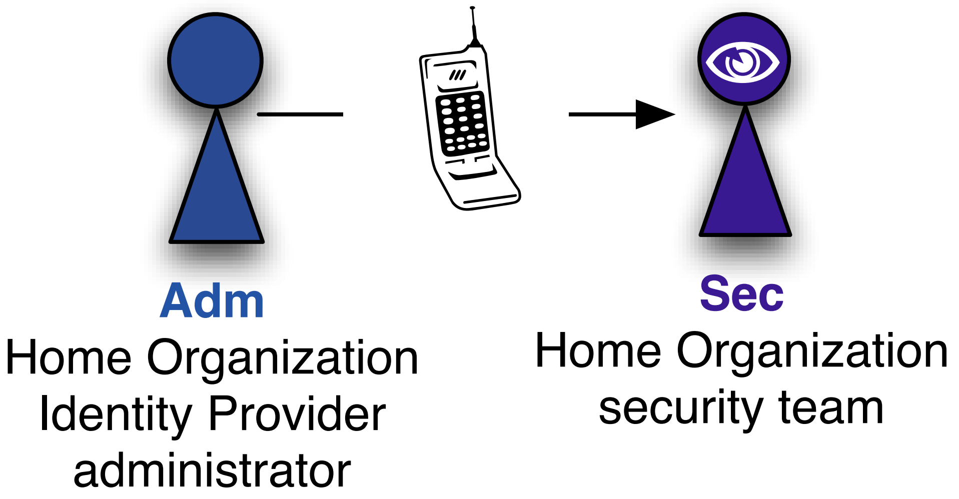
- Assertions using compromised IdP key won’t be accepted anymore after max. 2 hours

What you have to remember

4

If IdP was compromised:

- **Contact your organization security team**
  - Tell them to contact and inform SWITCHcert
- Alternatively,contact AAI team directly during office hours
  - Assuming AAI team knows IdP admin (by voice)



Version Info Gathering

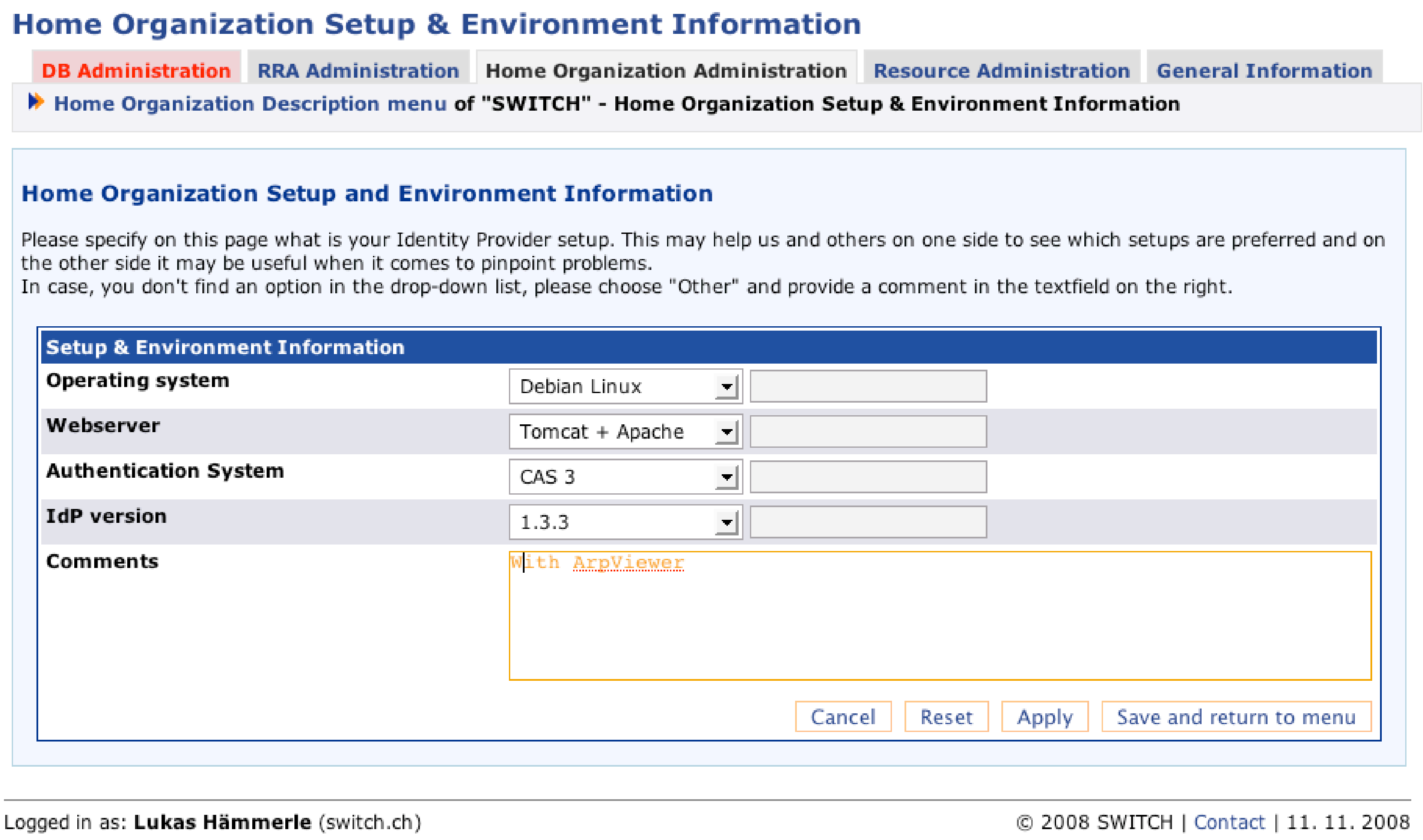
5

- Knowing the setup and version of an SP or IdP in case of security advisories is crucial!
- That's the reason why we provided ...

Setup Information Section

5

... the setup information section



Home Organization Setup & Environment 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

Logged in as: **Lukas Hämmerle** (switch.ch)

© 2008 SWITCH | Contact | 11. 11. 2008

Version Info Gathering

5

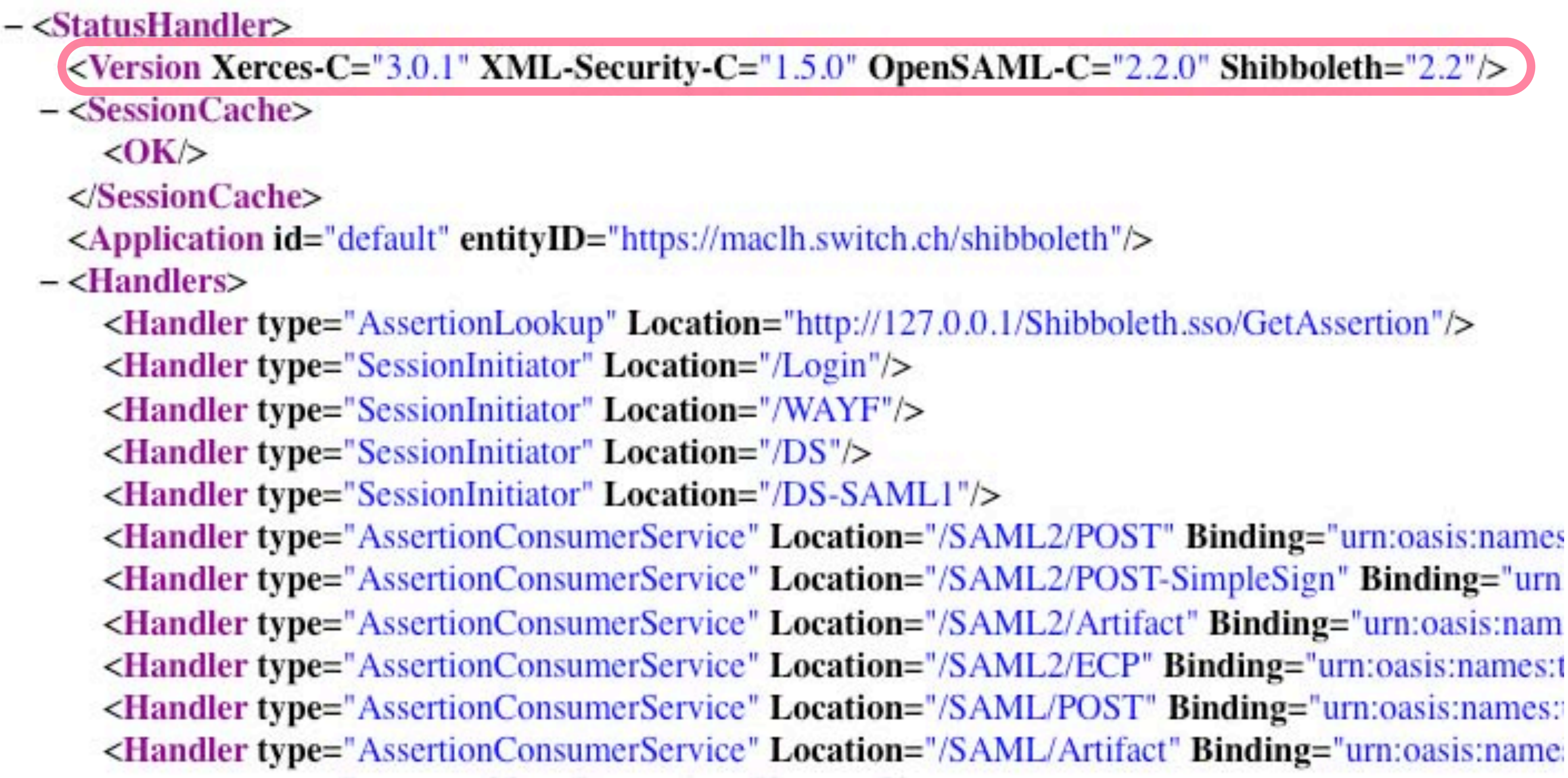
- But filling in and (especially) updating this form is cumbersome and often is forgotten
- Outdated information is not of much use
- But fortunately there is the ...

SP Status Handler and the...

5

Available since Service Provider 2.0

URL: https://*#hostname#*/Shibboleth.sso/Status



```
- <StatusHandler>
    <Version Xerces-C="3.0.1" XML-Security-C="1.5.0" OpenSAML-C="2.2.0" Shibboleth="2.2"/>
  - <SessionCache>
      <OK/>
    </SessionCache>
    <Application id="default" entityID="https://maclh.switch.ch/shibboleth"/>
  - <Handlers>
      <Handler type="AssertionLookup" Location="http://127.0.0.1/Shibboleth.sso/GetAssertion"/>
      <Handler type="SessionInitiator" Location="/Login"/>
      <Handler type="SessionInitiator" Location="/WAYF"/>
      <Handler type="SessionInitiator" Location="/DS"/>
      <Handler type="SessionInitiator" Location="/DS-SAML1"/>
      <Handler type="AssertionConsumerService" Location="/SAML2/POST" Binding="urn:oasis:names
      <Handler type="AssertionConsumerService" Location="/SAML2/POST-SimpleSign" Binding="urn
      <Handler type="AssertionConsumerService" Location="/SAML2/Artifact" Binding="urn:oasis:nam
      <Handler type="AssertionConsumerService" Location="/SAML2/ECP" Binding="urn:oasis:names:
      <Handler type="AssertionConsumerService" Location="/SAML/POST" Binding="urn:oasis:names:
      <Handler type="AssertionConsumerService" Location="/SAML/Artifact" Binding="urn:oasis:name
```

IdP Status Handler

5

Available since Identity Provider 2.1.3
URL: https://*#hostname#*/idp/status

```
### Operating Environment Information
operating_system: Linux
operating_system_version: 2.6.18-6-686
operating_system_architecture: i386
jdk_version: 1.6.0_11
available_cores: 1
used_memory: 46MB
maximum_memory: 508MB
current_time: 2009-09-15T14:48:32Z

### Identity Provider Information
idp_version: 2.1.3
idp_start_time: 2009-09-11T14:49:55Z
attribute_resolver_valid: true

[...]
```

Status Handler Access Restrictions

5

- Both handlers are protected by IP to be accessible only from localhost in the default configuration

- Therefore, we added in the SP default configuration:

```
shibboleth2.xml:
[...]
<Handler type="Status" Location="/Status"
 acl="127.0.0.1 130.59.138.32"/>
[...]
```

Resource Registry IP

- Similar setting for IdP will follow...

Automatic Version Gathering

5

- Thanks to modified access list, Resource Registry can update version information automatically
- This of course also allows monitoring the service
- Access list can manually be disabled by removing the Resource Registry IP: 130.59.138.32 from configuration
- Any suggestions or comments?

Suggestions and Feedback

- Some of the most useful features of the Resource Registry where suggested by you

- If you have ideas for further improvements, let us know :-)

aai@switch.ch