

One small step for the Shib admin, one giant leap for the SAML community?

Some Shibboleth migration tales and recommendations



SWITCH

Serving Swiss Universities

Lukas Hämmerle

lukas.haemmerle@switch.ch

W H O W I L L B E L E F T B E H I N D ?

2010

June 30th

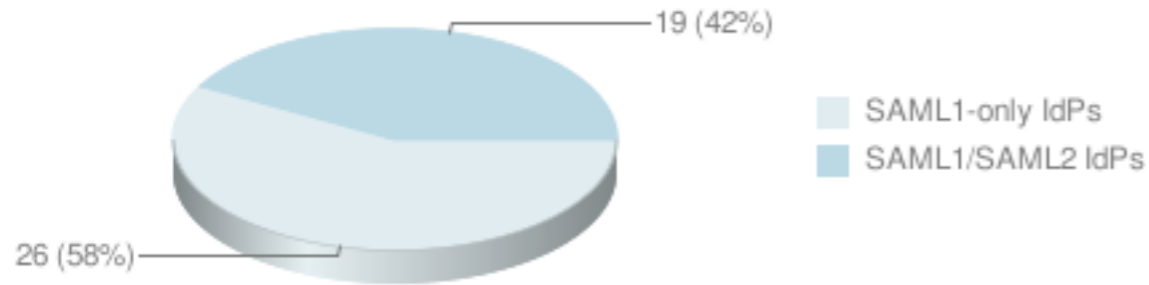
Coming soon to your Shibboleth 1.3
deployment

The end of the world? No, just Shibboleth 1.3

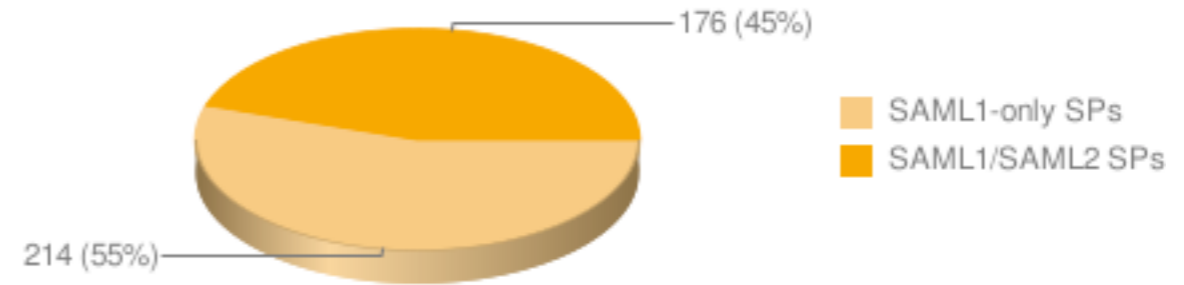
- Shibboleth 1.3 is already half-dead right now :-)
- Any support (including security patches) for 1.3 officially **ends on June 30th 2010**
- Shibboleth 2.x has many useful new features!
- The goal in SWITCHaai is to have migrated all Identity Providers (IdP) and Service Providers (SP) by September 2010!

The clock is ticking...

Identity Provider statistics



Service Provider statistics



45 SWITCHaai IdPs

- 19 Shibboleth 2.x (42%)
- 26 Shibboleth 1.3.x (58%)

390 SWITCHaai SPs

- 176 Shibboleth 2.x (45%)
- 214 Shibboleth 1.3.x (58%)

SP/IdP ratio: ~ 8.7

26 IdPs and 214 SPs to upgrade in the next 7 months!
Only two more semester breaks admins can upgrade.

SP/IdP Upgrade Analysis

Identity Provider Upgrade

- Complex due to changed configuration and endpoints
- Set up new IdP in parallel on other host → soft migration
- Operate both IdPs before and after migration
- Actual migration is just a small change on WAYF/DS

Service Provider Upgrade

- Less complex
- Just replace 1.3 SP in-place (→ short service disruption)
- SAML 1 Endpoints stay the same
- Many SPs → Many upgrades → Many issues

Top 10 Migration Issues (unranked)

- ① Insufficient planning
- ② Insufficient communication
- ③ Insufficient testing
- ④ EntityID change from URN to URL
- ⑤ Duplicate Identity Providers during migration phase
- ⑥ Publisher's SAML implementations
- ⑦ Bookmarks and static login links
- ⑧ X.509 certificate embedding in metadata
- ⑨ Wrong sequence of software and metadata upgrade
- ⑩ Changed attribute names in Apache

General

IdP

-specific

SP

-specific

1 Insufficient planning/communication/testing

Most other issues are tied to these key issues

Planing

Upgrading an IdP that is used daily by thousands of users should be planned carefully!

Communication

Friday 4pm, *“Hello AAI Team, we just upgraded our production IdP in-place and now have problems.”*

Testing

Is essential for a successful migration! Should be allocated enough time depending on number of SPs used by users.

④ EntityID change from URN to URL

Old convention (URN) for entityIDs:

urn:mace:switch.ch:SWITCHaai:unige.ch

New convention (URL):

<https://aai.unige.ch/idp/shibboleth>

- 😊 No URN registry needed anymore
- 😊 URL can return entity's metadata (→ dynamic discovery)
- 😊 New IdP can be set up in parallel (→ soft migration)
- 😞 Problems with bookmarks, login links, outdated metadata

⑤ Duplicate IdP entries in metadata and DS

Change of entityID and soft migration causes multiple entries in metadata. Which one is active/valid?

SWITCH > aai
[About AAI](#) : [About SWITCH](#) : [FAQ](#) : [Help](#) : [Privacy](#)

Select your Home Organisation

In order to access a Resource on host 'aai-viewer.switch.ch' you must select yourself.

HSR – Hochschule für Technik Rapperswil

- SUPSI – Scuola Universitaria Professionale della Svizzera Italiana
- ZHAW – Zürcher Hochschule für Angewandte Wissenschaften
- ZHdK – Zürcher Hochschule der Künste
- University Hospitals**
 - HUG – Hôpitaux Universitaires de Genève
 - Inselspital – Universitätsspital Bern
 - Universitätsspital Zürich
- Virtual Home Organisations and Libraries**
 - Virtual Home Organisation @SWITCHaai
 - Zentral- und Hochschulbibliothek Luzern
- Others**
 - CSCS – Swiss National Supercomputing Centre
 - IDIAP – Idiap Research Institute
 - PSI – Paul Scherrer Institut
 - SWITCH
 - WSL – Eidg. Forschungsanstalt für Wald, Schnee und Landschaft
- Upcoming**
 - NOT YET ACTIVE: Universität Bern
 - NOT YET ACTIVE: ETH Zürich
 - NOT YET ACTIVE: Universitätsspital Zürich

Additional “Upcoming” category with new IdPs that are not yet in production

🙄 Won't work for DS that use metadata to generate drop-down list

⑥ Some Publisher's SAML Implementations...

... for are often hand-made and not using already available and stable implementations.

Therefore, they unfortunately are often:

- **Buggy**
SSO Endpoints in metadata must follow a certain order?!
- **Inflexible**
Bugs cannot be fixed before 2010 due to release cycles
- **Not (yet) SAML 2 compatible**

Of course, it's not only the publishers but mostly...

⑦ Bookmarks and static login links

IdP's hostname and entityID change

→ bookmarks and login links have to be adapted!

Again, some Publishers seem to have a hard time to update such login links... even if asked multiple times

Hint:

Monitor your old IdP's log files after the migration to spot users with bookmarks and SPs with login links. Add a note to your old IdP's login page and urge users to delete bookmark.

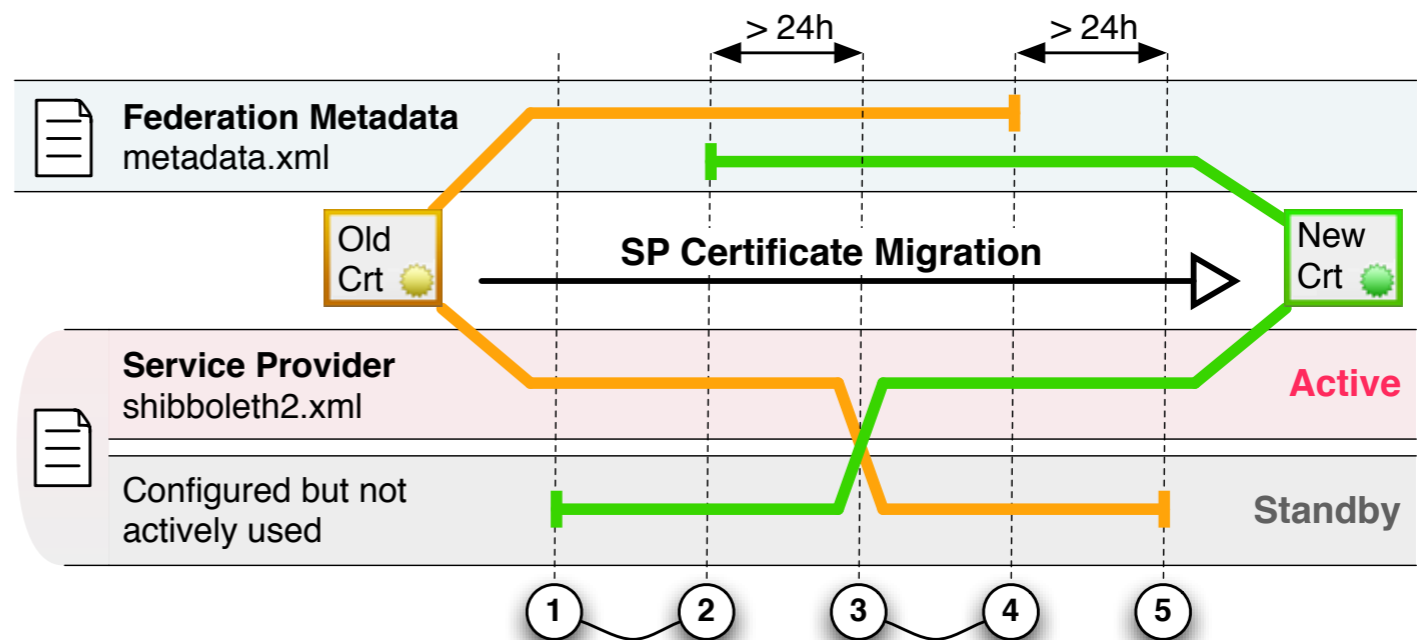
⑧ X.509 Certificate Embedding in Metadata

SAML 2 encrypted assertions require certificates (public key) to be embedded in metadata!

- 😊 X.509 requirements can be enforced → better security
- 😊 Admins can be notified when their certs expire
- 😊 Self-signed certificates can be used → greater flexibility
- 😞 Certificates have to be renewed with roll-over procedure

Also see <http://www.switch.ch/aai/support/certificate-migration.html>

Example for SP
certificate roll-over
procedure



⑨ Wrong Sequence of Upgrade

Problem:

SP is upgraded before metadata is “upgraded”

- SP uses SAML 2 if user authenticates at SAML 2 IdP
- IdP doesn't know SAML 2 endpoints of SP
- IdP issues a cryptic error message

Solution:

SP should be forced to use SAML 1 or

SP admin should first change metadata and add SAML 2 endpoints and certificates there. After that software of SP can be upgraded.

⑩ Changed attribute names in Apache

SP 2.x changed default way to make attributes available to web apps. SP header variables → Environment variables

Problem:

HTTP_SHIB_EP_AFFILIATION → Shib-EP-Affiliation

Some applications have hard-coded names!

Solution:

Use the ShibUserHeaders directive for old behaviour.

```
<Location /my-application>
  AuthType shibboleth
  ShibRequireSession On
  ShibUseHeaders On
  require valid-user
</Location>
```

General Recommendations

- Increase awareness of support/security dead-line
- Create migration guidelines! Examples:
 - SP: <http://www.switch.ch/aai/docs/shibboleth/SWITCH/2.0/sp/migration-sp-2.0.html>
 - IdP: <http://www.switch.ch/aai/support/identityproviders/idp-migration.html>
- Assist the organizations that upgrade
 - On-site support often is not needed
 - TeamViewer/Skype and phone work well
- Some subtle naming & shaming as seen on the right :-)

