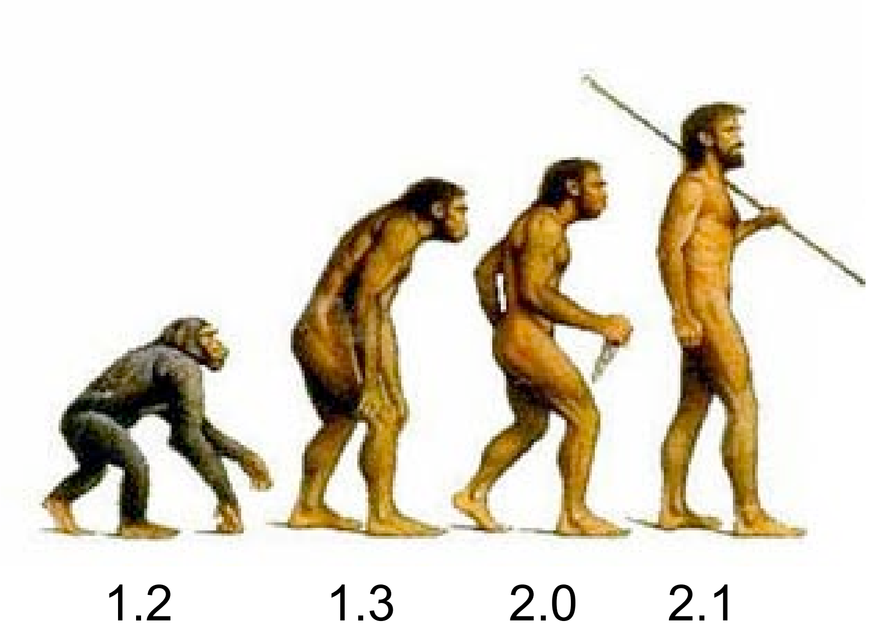
Migrating the SP to 2.1

The necessary steps to get to the next (r)evolutionary level



SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Service Provider Configuration Changes

The Good News:

- Basically, 2.x is just an extension of 1.3
- Same components: shibd and mod_shib web server module
- Not that much will change unless you use new features
- No cronjob/siterefresh needed anymore for updating metadata

The Bad News:

- You cannot just install Shibboleth 2.x over 1.3…
- Configuration file is similar but not compatible with 1.3
  - Modifying the dist `shibboleth2.xml` file from scratch is probably the easiest
  - `AAP.xml` was split up into `attribute-map.xml` and `attribute-policy.xml`
- Attributes are made available to application differently

How Applications Can Access Attributes

- The old Shibboleth 1.3 way (when using Apache): Attributes are put in web server environment as headers

```
HTTP_SHIB_EP_AFFILIATION                staff
HTTP_SHIB_PERSON_SURNAME                Hämmerle
HTTP_SHIB_INETORGPERSON_GIVENNAME       Lukas
HTTP_SHIB_INETORGPERSON_MAIL            lukas.haemmerle@switch.ch
```

- The new Shibboleth 2.x way: Attributes are put in web server environment as variables

```
Shib-EP-Affiliation            staff
Shib-InetOrgPerson-givenName   Lukas
Shib-Person-surname            Hämmerle
Shib-InetOrgPerson-mail        lukas.haemmerle@switch.ch
```

But Shibboleth 2.x also supports the old way above…

How to Migrate an SP

It’s not possible to run a 2.x and 1.3 SP at the same time!

1. Backup old configuration and binaries
2. Also backup the init.d script for `shibd`
3. Disable Apache module (e.g. with `a2dismod shib`)
4. Disable any cronjobs for siterefresh (not needed anymore)
5. Move 1.3 Service Provider out of the way
6. Install new Shibboleth 2.x Service Provider
7. Configure Service Provider
8. Upgrade Service Provider in Resource Registry to SAML 2
   - Run Service Locations Shibboleth 2.x assistant
   - Run Certificate assistant for Shibboleth 2.x
9. Make sure your application still works
   - If not, try using `ShibUseHeaders On` in Apache to re-enable the old behavior regarding the attributes. This is needed for all Java applications!
10. Remove old Service Provider files

Summary

- 2.1 is **easier to install** than 1.3
  - Thanks to more packages, improved guides
- 2.1 is **easier to maintain** than 1.3
  - Metadata update built-in, upgrade via packages
- 2.1 is **more secure** (especially under IIS) than 1.3
  - Attributes are now in web server environment variables
- 2.1 has **more features** like SAML2 support
  - SAML 2 is needed for interoperability with other products
  - **1.3 code basis is not supported anymore!**

🌍 http://www.switch.ch/aai/support/serviceproviders/