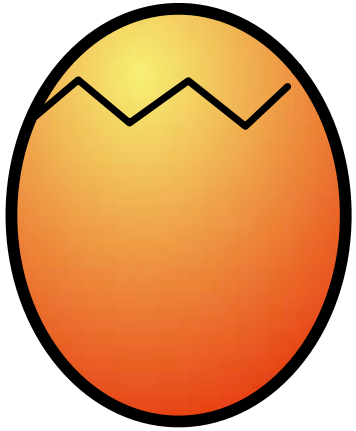
Evolution instead of revolution

Summary of new features of the Shibboleth SP versions newer than 2.2



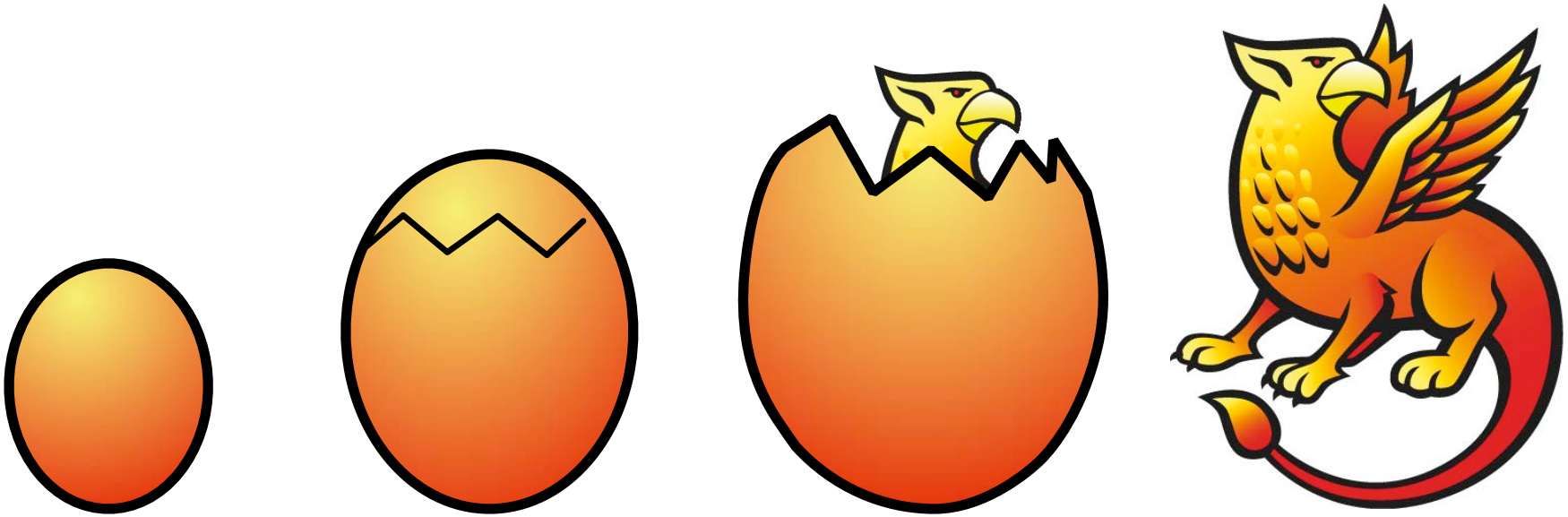
SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Bern, 24. Mai 2011

Service Provider is Maturing



- Shibboleth SP 1.0 was released on July 1, 2003
- Shibboleth SP 1.3 was released on August 26, 2005
- Shibboleth SP 2.0 was released on March 19, 2008

Shibboleth SP Versioning

- Version number: <MAJOR>.<MINOR>.<PATCH>
- **Patch Release**
  - Binary, source, configuration, and protocol compatibility.
  - Forwards and backwards compatible. Pure bug fix releases.
- **Minor Release**
  - May introduce new features and APIs but does **not** remove old APIs.
  - Backwards and forward compatible with respect to protocol behavior.
  - Backward but not necessarily forward compatible source and config
- **Major Release**
  - May make any type of change to protocols, APIs, and configuration.
  - As such, neither backwards nor forwards compatibility is guaranteed.
  - May be treated as if they were a new piece of software.

New Features in 2.2

Most helpful:

- shibd options:
  - -w <int>: Seconds to wait for the background process to fully initialize before returning success or failure to the shell.
  - -f : Keep the process in the foreground (good for debugging)
- Certificates and Keys can now also be loaded from URL
  - Can be downloaded periodically
  - Changes on file system can be reloaded dynamically
- Attributes as raw XML in (webserver) header variable
  - Including friendly name, name format, oid etc
  - Might be useful for multi-valued attributes

New Features in 2.2

- For files loaded from URLs, the <TransportOption> can be used, for example to to bypass proxies
- Multiple <AccessControl> can be chained for a path
- Metadata filter can filter out roles (e.g. all SPs)
  - Saves some memory if metadata file is huge
- SimpleAggregation AttributeResolver
  - Aggregates attributes from multiple Attribute Authoritities
  - Used for VO Platform
- Preserve POST data with postData option
  - Saves POST data across SSO on supported platforms
  - No lost POST messages anymore when session expires

New Features in 2.3

- Mostly a bug fix and patch release
- SPNameQualifier can be set in a request
  - Will be used for Virtual Organization
- defaultACSIndex was renamed to acsIndex
  - Visible as warnings in the shibd.log. Should be fixed in config file.
- SP can request a specific NameIDFormat
  - Available formats: transient (default) or persistent
  - Transient: Random string that expires after a few minutes
  - Persistent: Same value as eduPersonTargetedID attribute. Only rarely needed as NameID. Allows account checking/updating.

New Features in 2.4

- Introduced a simplified configuration file format
  - Only most relevant things have to be configured explicitly
  - But old format still is supported and also required for some options
- Attribute encoding for headers can be set
  - Default still is UTF-8
- CRL can be checked for PKIX metadata validation
  - Revoked metadata signing certificates can be detected
  - Increases metadata security
- Various options to be included in self-generated metadata
  - <ContactPerson>, <RequestedAttribute>, <Organization>, ...

New Features in 2.4

- Discovery Feed Handler
  - Used for Embedded Discovery Service
  - Generates simplified JSON metadata

```
[{ "entityID": "https://aai-logon.switch.ch/idp/shibboleth",
    "DisplayNames": [ { "value": "SWITCH", "lang": "en" } ],
    "Descriptions": [ { "value": "The SWITCH Identity Provider", "lang": "en" },
                      { "value": "Der SWITCH Identity Provider", "lang": "de" }
                    ]
 }
, ... ]
```

- XML Access Control rules can be referenced from .htaccess
  - Non-root users can dynamically create complex access control rules

```
AuthType shibboleth
ShibRequireSession On
ShibRequireAll On
require shibboleth
ShibAccessControl /home/lukas/phpmyadmin-shibacl.xml
```

Likely new Features in (unreleased) 2.5

Currently listed in the roadmap

- Parseable audit.logs
  - Time, IP, user, protocol, binding, authentication context, etc...
- Attribute Requirements
  - SP shows message (using a template) if some attributes are missing