GridCertLib
Shibboleth authentication for X.509 certificates and Grid proxies

Sergio Maffioletti
<sergio.maffioletti@gc3.uzh.ch>

Grid Computing Competence Centre,
University of Zurich
http://www.gc3.uzh.ch/

How to get a Grid proxy into the portal host?

What is GridCertLib?

Java library to create an X.509 certificate and a VOMS proxy upon successful login to the portal.

For Users: No interaction with Grid middleware required at all.

For programmers: assures that, once a user has logged in, valid certificate and proxy are available.

Key ingredients:

- Shibboleth federated authentication
- SLCS online CA

Shibboleth

- HTTP-based operation
- User credentials are authenticated by the home organization *Identity Provider* (IdP) server only
  - IdP controls what information about the authenticated user is sent to the *Service Provider* (SP)
  - Passwords and other sensitive data are never disclosed to Service Providers
- *Service Providers* only need to trust the limited number of IdPs for authentication purposes.

Shibboleth login workflow

The SWITCH AAI Infrastructure

Switzerland-wide federated authentication infrastructure.

- Based on Shibboleth 2.x
- “Identity Providers” already operational at every University and several other research centres.
- One login/password to access a variety of services (e.g., e-mail, ... and SLCS!)

Short-Lived Credential Service

Web service to create an X.509 user certificate, valid for 11 days.

- A *new* certificate at each successful invocation
- *Same* subject DN every time
- Command-line client (Java-based) available in gLite 3.x

Uses AAI/Shibboleth authentication.

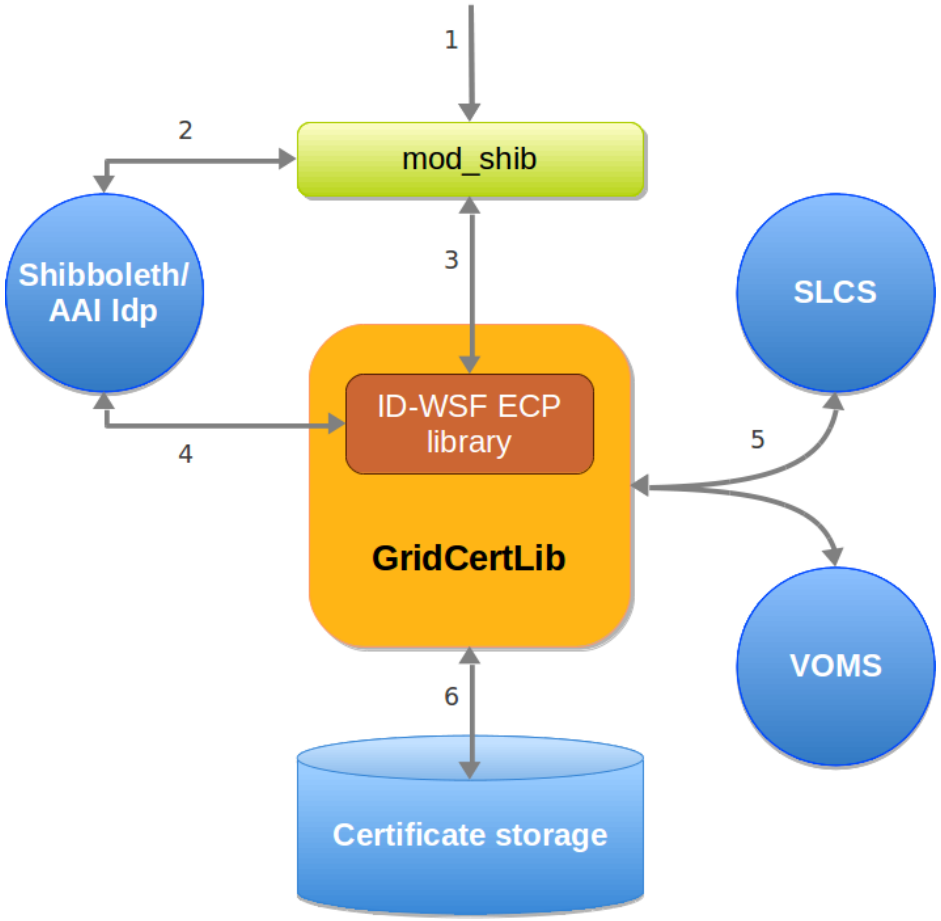
SWITCH SLCS CA is already in the IGTF bundle

- SLCS certificates can be used for normal Grid operations

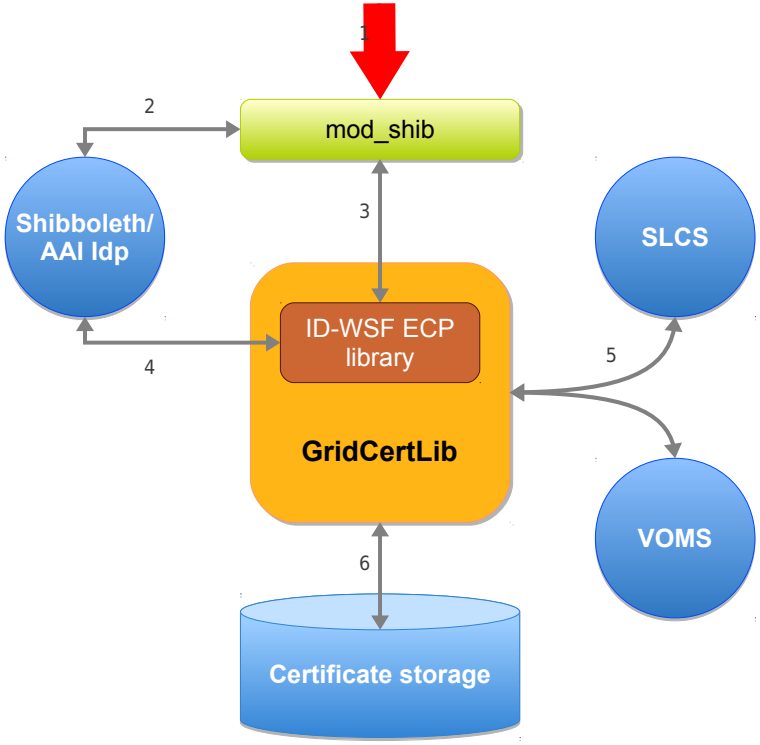
Already in use in SMSCG, the Swiss national Grid infrastructure.

More on SLCS

Architecture

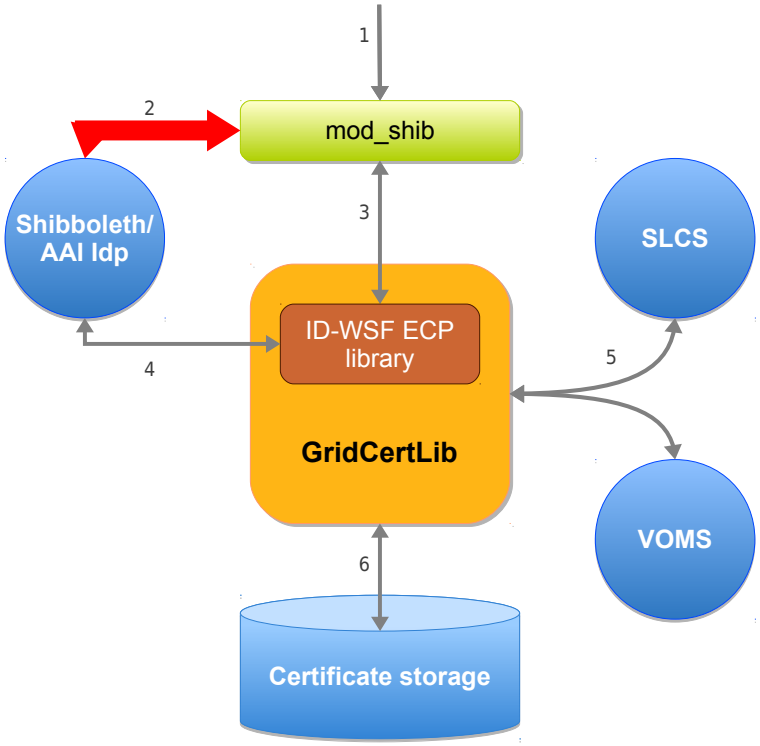


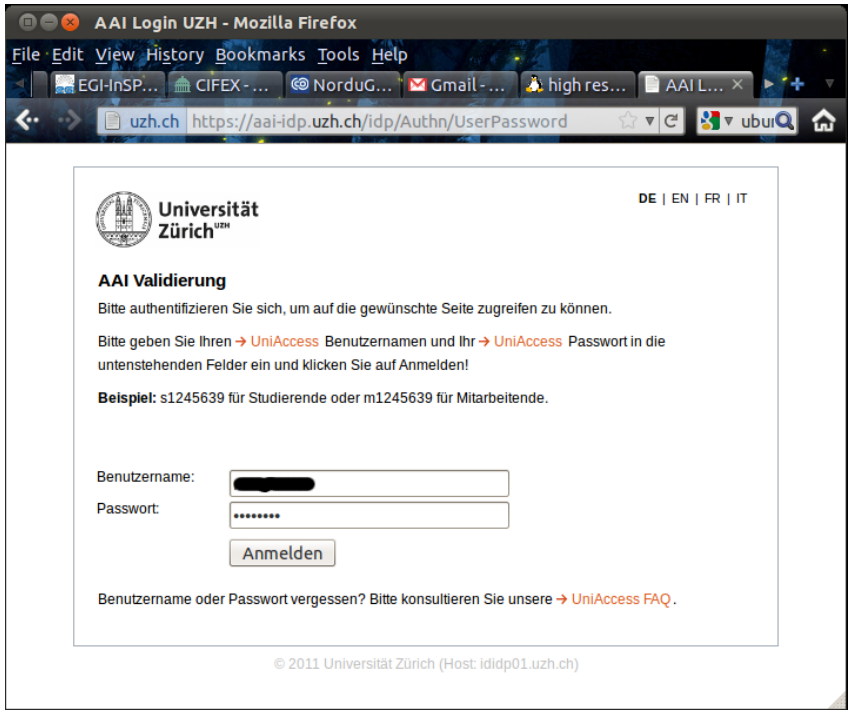
GridCertLib operation (1)



Users log in to the web portal using Shibboleth single sign-on.

GridCertLib operation (2)

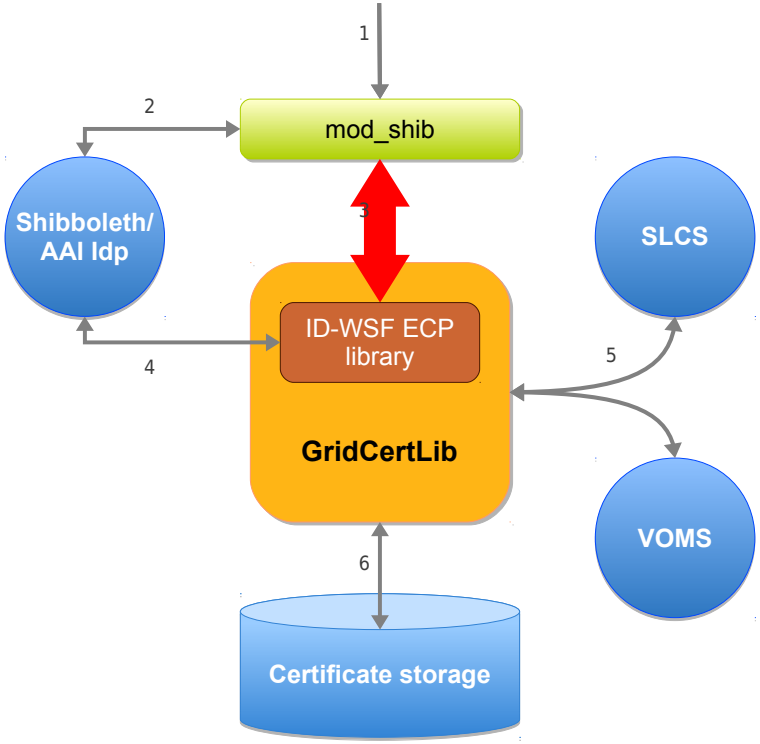




Users are authenticated by their home organization “Identity Provider” (IdP).

(This is all transparently handled by the Shibboleth software.)

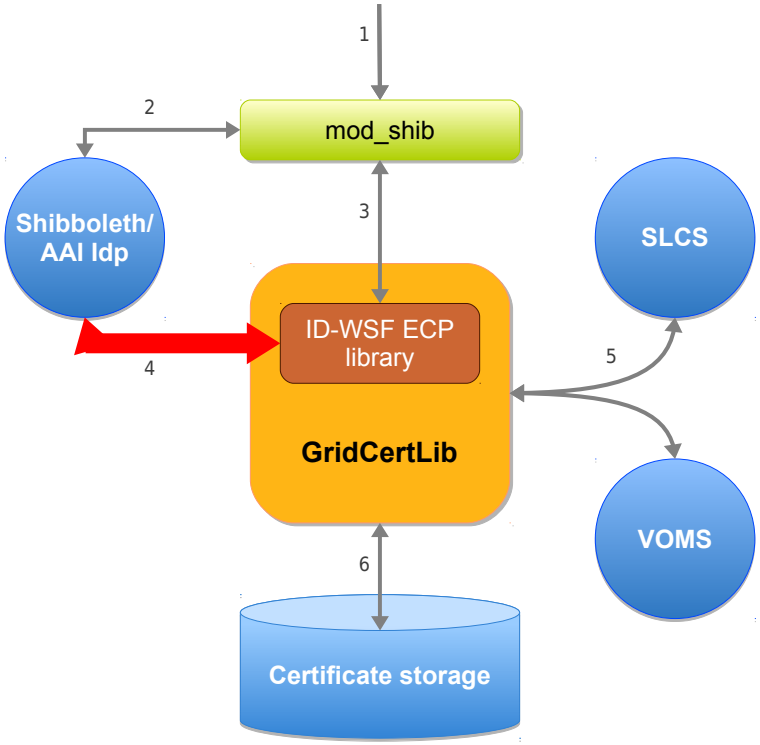
GridCertLib operation (3)



The portal calls *GridCertLib*.

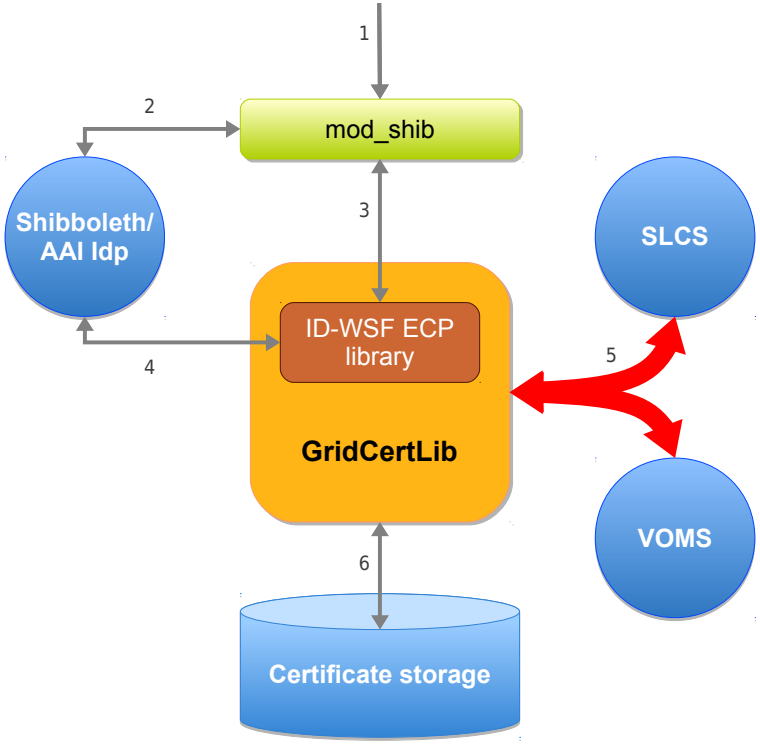
GridCertLib retrieves the SAML2 assertion (Shibboleth login data) from Apache's `mod_shib`.

GridCertLib operation (4)



The portal application code calls *GridCertLib* to obtain a X.509 certificate. This step requires delegation of the Shibboleth credentials (SAML2 assertion)
to the SLCS login service.
done through `Identity Domain - Web Service Framework (ID-WSF) ECP Web Service Client`

GridCertLib operation (5)



GridCertLib generates an X.509 certificate, signs it using SLCS, and then generates a VOMS proxy.

SLCS: Technical issues

Obtaining a user certificate requires delegation of the Shibboleth credentials to the SLCS login service.

- SLCS web service requires Shibboleth authentication...
- ...but AuthN data is only valid towards SP!

Delegation issue

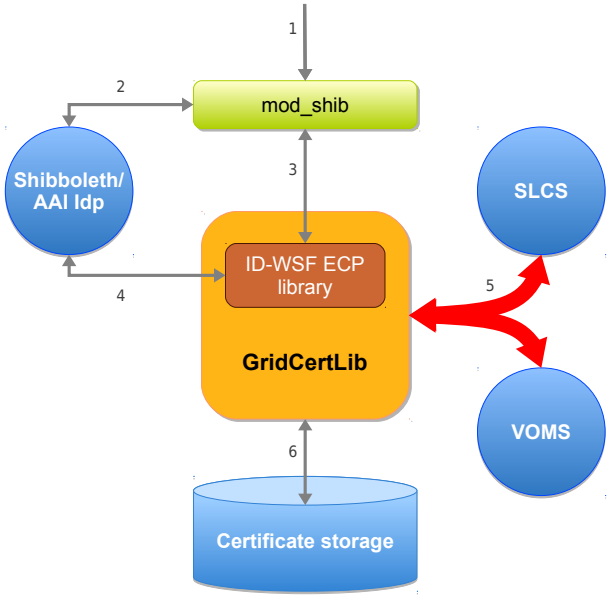
- Shibboleth 2.1.x supports *delegation* of credentials
- but deployed IdP's not (yet) up to that version

Solution

- use pre-production Shibboleth 2.2 IdP *with delegation extension* (at SWITCH)
- register/manage portal user accounts there
- will merge with the production infrastructure eventually

GridCertLib operations (5)

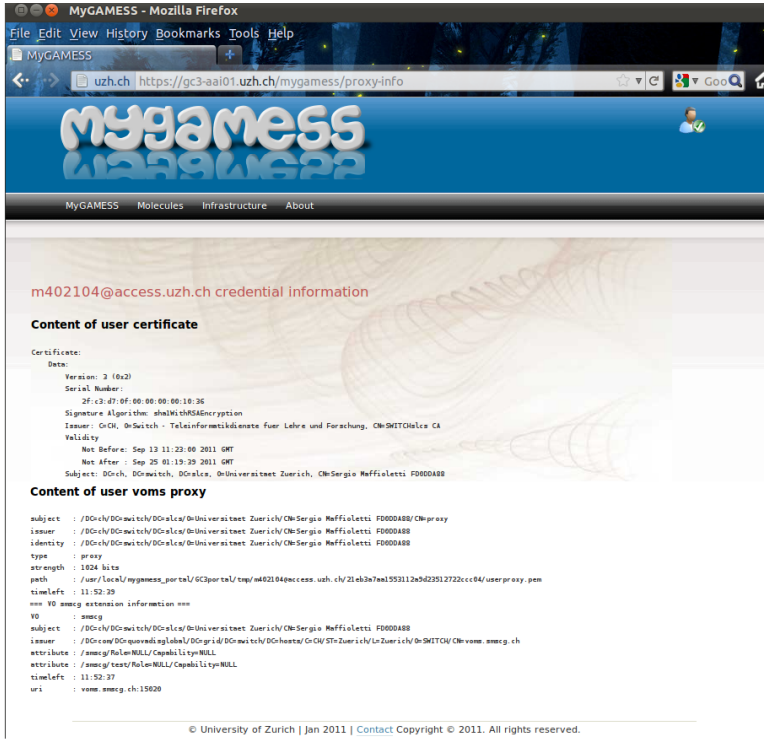
Generate X.509 certificate:



1. Login to SLCS endpoint
2. SLCS server verifies AuthN data with IdP
3. SLCS replies with a “session” token and information to generate a CSR
4. Generate a private key and a CSR
5. Submit CSR to SLCS endpoint
6. Get back *signed certificate* in response

Then, generate proxy and contact VOMS server.

GridCertLib operations (6)



Store certificate and proxy on the disk, ready for use.

(Encrypted with a random password, which is returned by the *GridCertLib* API.)

Users only interact via WWW, and passwords are sent to the IdP only (and only once per login!)

P-GRADE integration

Two main action items:

- Enable Shibboleth login at the GridSphere level
  - Initially done by the Australian MAMS project
  - Requires some lengthy procedure to make login data compatible with the DB storage
- Insert calls to *GridCertLib* into the login code
  - Java code calling Java code, no big issue
- *Disable* P-GRADE's native certificate handling
  - Certificate management is now handled by *GridCertLib*

More on P-GRADE integration

Django integration

Issue: How to bridge Python with Java?

- Run *GridCertLib* servlets in parallel with Django.
- Use HTTP redirects to pass information back and forth.

Use Python decorators to mark view functions that require a certificate and/or Grid proxy.

```
@proxy_required
def submit_job(req):
  # do Grid work
  return HttpResponse(...)
```

Summary

Java library to create an X.509 certificate and a VOMS proxy upon successful login to the portal.

- No user interaction with Grid middleware required at all.
- Once a user has logged in, valid certificate and proxy are available.

Already integrated with P-GRADE and Django

- Example servlets with commented code provided for integration in other portals.

Key ingredients:

- Shibboleth federated authentication
- SLCS online CA

Any questions?

website:

`http://gridcertlib.googlecode.com/`

e-mail:

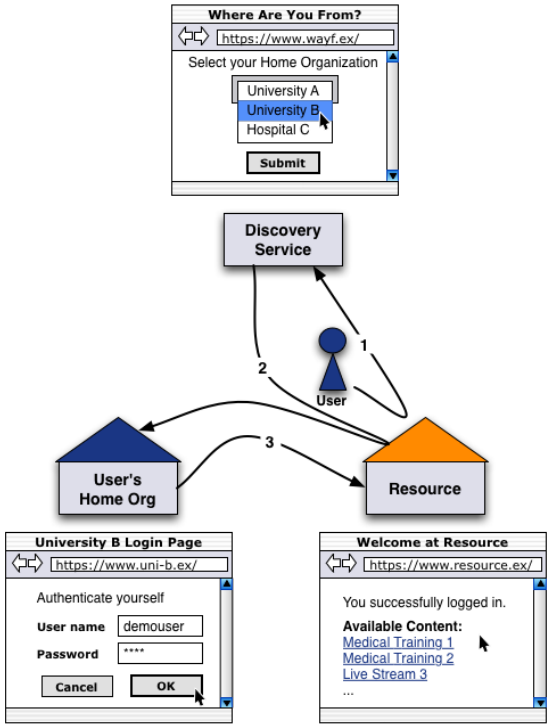
`info@lists.gc3.uzh.ch`

Credits

Peter Kunszt (SystemsX.ch),
Riccardo Murri (GC3/UZH),
Valery Tschopp (SWITCH)

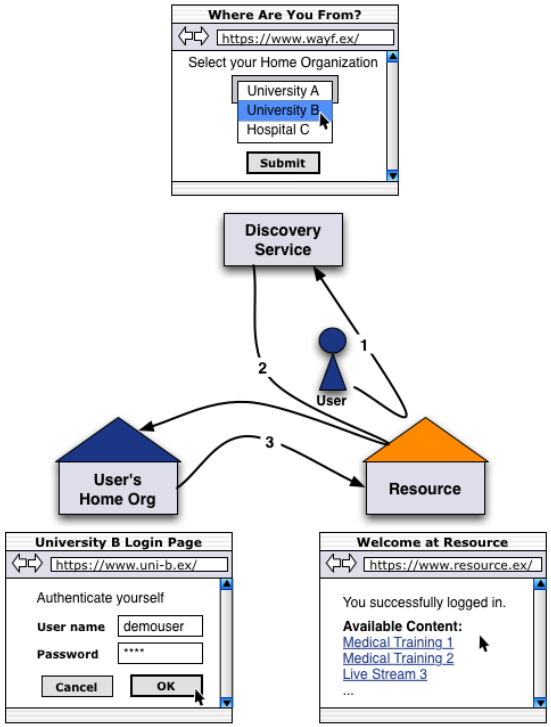
Additional material

Shibboleth login workflow / 1 (Images co



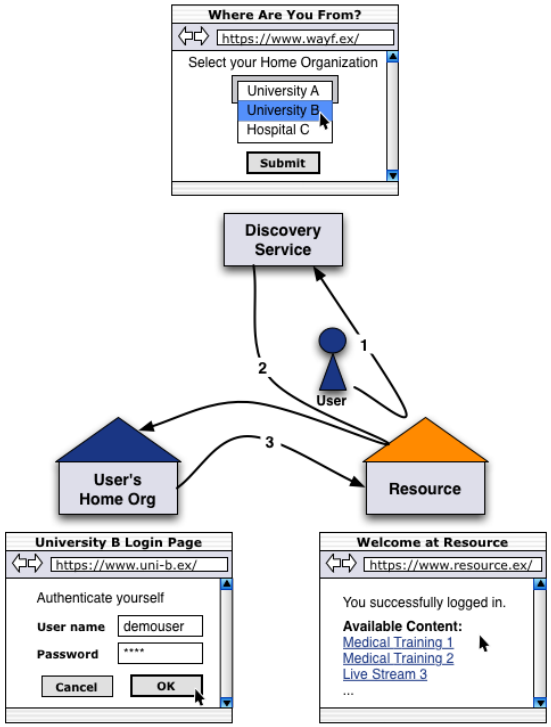
1 User first connects to portal web server (SP) and is redirected to the “Where Are You From?” page (WAYF)

Shibboleth login workflow / 2 (Images co



2 User chooses Home Organisation and is redirected to the IdP AuthN page

Shibboleth login workflow / 3 (Images co



3 User posts username/password to IdP and is redirected to original page on SP

SLCS operations workflow

1. Login to SLCS endpoint
   - HTTP request, using SAML assertion as AuthN data
2. SLCS server verifies AuthN data with IdP
   - Need delegation functionality (Shibboleth 2.1)
3. SLCS replies with a “session” token and information to generate a CSR
4. Generate a private key and a CSR
   - Private key protected by random password known only to the portal
5. Submit CSR to SLCS endpoint
   - Use “session” token from step **??**
6. Get back signed certificate in response

Back to SLCS Intro

More technical issues

Shibboleth authentication data has a limited time validity

- By the time *GridCertLib* is called, it might have expired.

Solution

- Use a “RenewAssertion” servlet
  `http://example.com/RenewAssertion?url=...`
- Forces Shibboleth logout
- Redirects to whatever URL was specified in the initial request
- If the URL is Shibboleth-protected, new login data will be generated.
- No user interaction required until IdP session expires (default 8 hours)

More on P-GRADE integration

- First-time users directed to a page with a single button “sign up”, that only lists their Shibboleth attributes.
- Once they hit the button:
  - Their credentials are stored in the DB but not activated (excluded from login)
  - They are shown a page ’your request is being processed’, the admin gets an email
  - If users try to log in again, they get the ’your request is being processed’ page again
- The admin needs a “Shibboleth” page in the “Administration” section:
  - Here requests can be approved or denied
  - If approved, user can now just log in
  - If denied, user will be removed - can apply again though
  - Users get a notification email either way

Back to P-GRADE integration