

GridCertLib

Shibboleth authentication for X.509 certificates and Grid proxies

Riccardo Murri

`<riccardo.murri@uzh.ch>`

Grid Computing Competence Centre,
University of Zurich

<http://www.gc3.uzh.ch/>



e-infrastructure



How to get a Grid proxy
into the portal host?

1. From a command-line UI run `myproxy-init --voms ...`
2. Log in to portal ...
3. set MyProxy server ...
4. and run jobs.
5. When proxy expires, go back to step 1.

This is too distracting to most users.

In addition, resorting to command-line kinda defeats the whole purpose of having a portal. . .

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

- 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

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!)

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

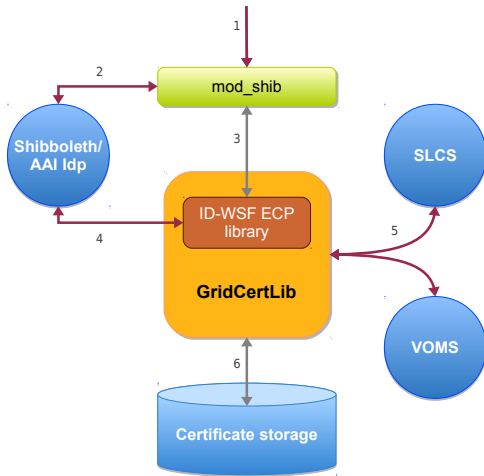
- A *new* certificate at each successful invocation
- *Same* subject DN every time
- Command-line client (Java-based) available in gLite 3.x

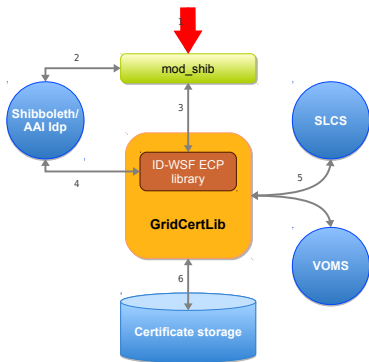
Uses AAI/Shibboleth authentication.

SWITCH SLCS CA is already in the IGTF bundle

- SLCS certificates can be used for normal Grid operations

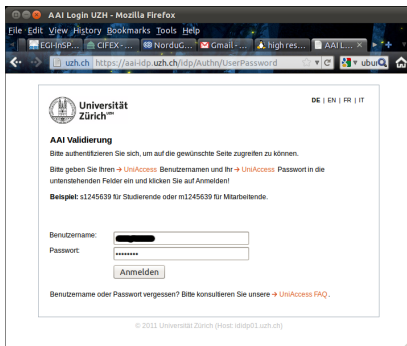
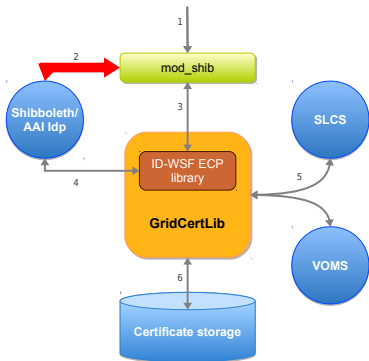
Already in use in SMSCG, the Swiss national Grid infrastructure.





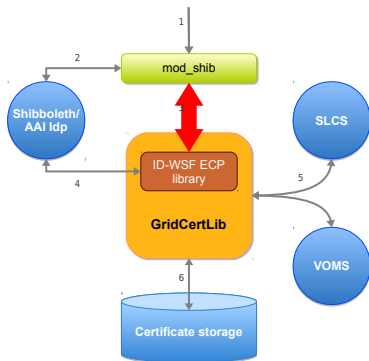
Users log in to the web portal using Shibboleth single sign-on.

GridCertLib operation (2)



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

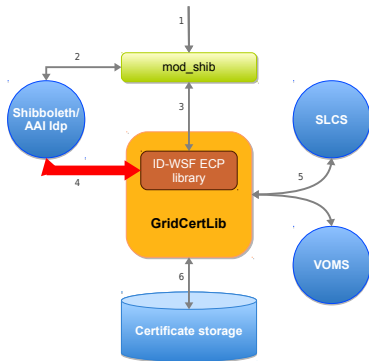
(This is all transparently handled by the Shibboleth software.)



The portal calls GridCertLib.

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

GridCertLib operation (4)



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

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!

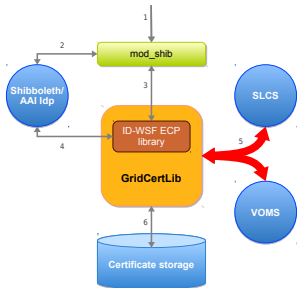
Delegation issue

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

Solution

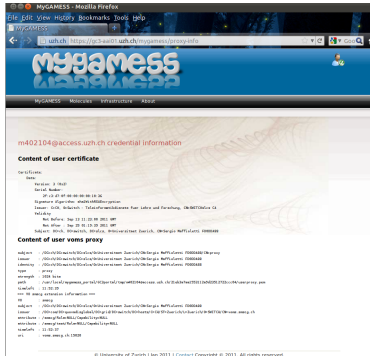
- use pre-production Shibboleth 2.2 IdP *with delegation extension* (at SWITCH)
- register/manage portal user accounts there
- will merge with the production infrastructure eventually

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.



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!)

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)

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

- 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

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(...)
```

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

Come talk to us at the SwiNG booth!
(in Salon Pasteur)

Or write to:
`riccardo.murri@uzh.ch`

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

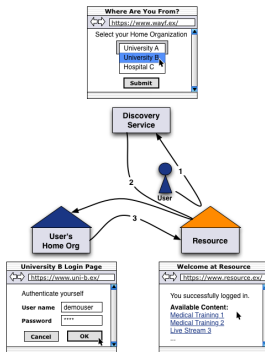
- No user interaction with Grid middleware required at all.
- Once a user has logged in, valid certificate and proxy are available.

Already integrated with P-GRADE and Django

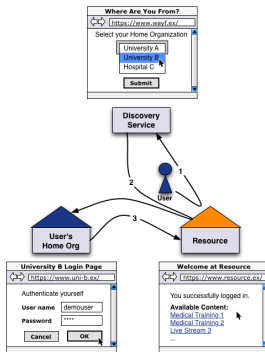
- Example servlets with commented code provided for integration in other portals.

Key ingredients:

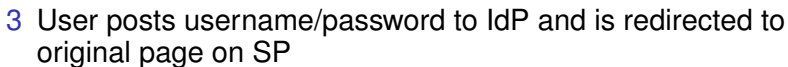
- Shibboleth federated authentication
- SLCS online CA



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



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



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 3
6. Get back signed certificate in response