SA1 CILogon pilot - motivation and setup

Tamas Balogh & Mischa Sallé

tamasb@nikhef.nl
msalle@nikhef.nl

AARC General Meeting, Milan

4 November 2015

Outline

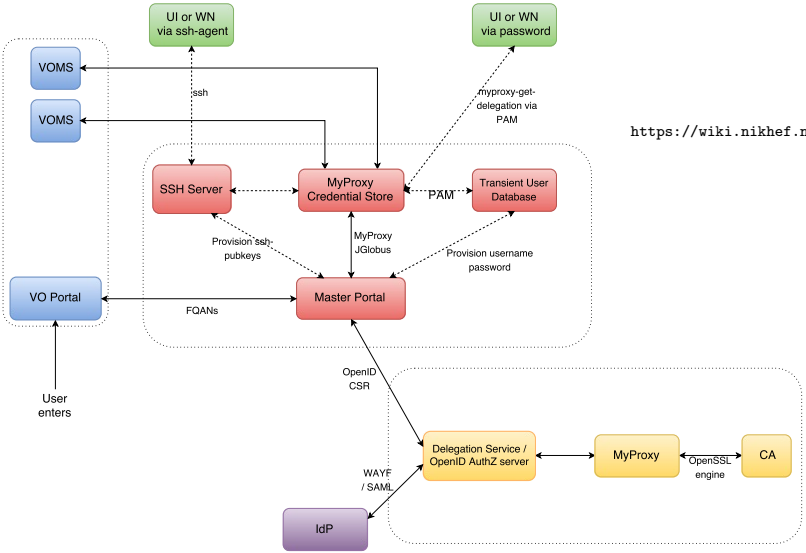
Typical Setup: wishlist

- Science Gateway
- typical user does not see any certificate
- jobs run with personal user certificate (traceability)
- some users need command line usage
- Science Gateway adaptations must be simple

CILogon Pilot

- CILogon widely used in US
- Different portals for OpenID-Connect/OAuth-for-MyProxy
  - TCS/DigiCert portal-like: PKCS12 download
  - *portal delegation* ←
  - ...
- Actually OAuth-for-MyProxy (OA4MP) pilot
- OA4MP essentially a frontend for MyProxy server
- MyProxy server: online CA or credential store (or both)

Pilot Setup



https://wiki.nikhef.nl/grid/CILogon_Pre-Pilot_Work

Main features

- certificate hidden from user
- safe and cached storage of credentials (private key is safe)
- flexible online CA: easily moved to HSM
- modular (European/Global, NGI, SG)
- already or to be standardised protocols
- VOMS integration: *attribute provider*
- SSH backdoor for *non-web*: next slide

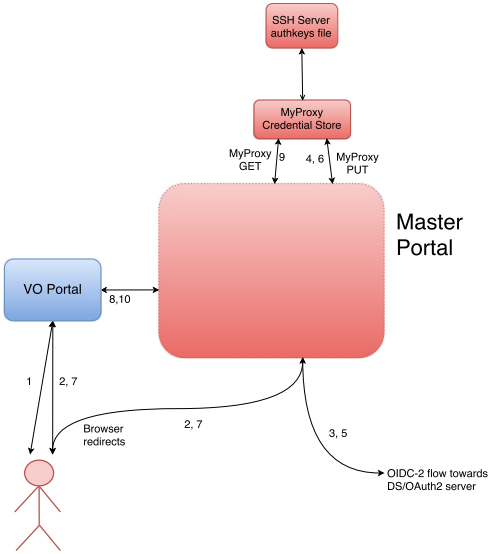
SSH backdoor

- VO Portal can upload user's SSH pubkey to Master Portal
- Master Portal can store in e.g. LDAP
- SSH Server runs cron job and creates `authorized_keys` file: special account, runs `myproxy-logon` wrapper
- SSH-agent forwarding: workernode, UI, laptop retrieves proxy
- wrapper to save proxy: similar to kerberos ticket

→ No need for either extra password, ECP, Moonshot etc.

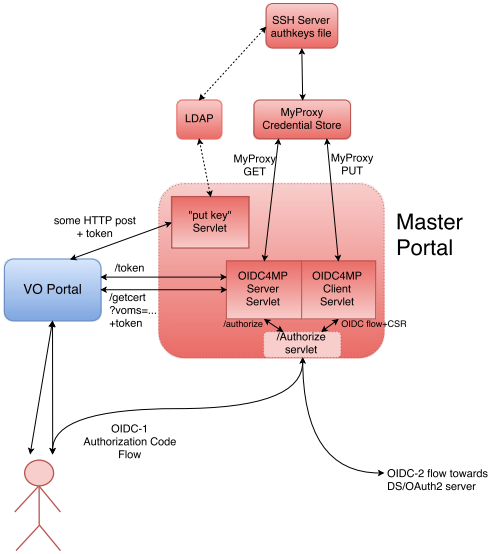
→ Very similar to GitHub, CERN, etc.

Master Portal: heavy lifting - high level



1. entry point
2. redirect to Master Portal
3. redirect to DS/CILogon
   receive code, token, userinfo
4. * initiate MyProxy PUT
5. * request certificate
6. * store certificate
7. redirect back to VO portal
8. request VOMS proxy
9. MyProxy GET for proxy
10. retrieve VOMS proxy

Master Portal: heavy lifting - details



1. user enters VO portal
2. VO portal starts authZ flow
3. `/authorize` endpoint:
   1. server servlet needs authZ
   2. client servlet: initiate authZ flow
4. redirect to DS
5. back to `/authorize` endpoint
   1. client $\rightarrow$ $\texttt{/token}_{\texttt{DS}}$
   2. client $\rightarrow$ $\texttt{/userinfo}_{\texttt{DS}}$
   3. * client initiates PUT
   4. * client $\rightarrow$ $\texttt{/getcert}_{\texttt{DS}}$
   5. * client finalises PUT
   6. server returns his code
6. return to VO portal
7. VO-p. $\rightarrow$ $\texttt{/token}_{\texttt{MP}}$
8. VO-p. $\rightarrow$ $\texttt{/getcert}_{\texttt{MP}}$
9. server servlet retrieves proxy
10. VO-p. receives VOMS proxy

Open issues and next (pilot) steps

- Further implement Master Portal (interface with VO portal):
  - `/authorize` servlet and integrating OIDC servlet
  - API endpoint for uploading SSH keys
- Small extensions to profile `http://goo.gl/VnMKXS`
  - `/getcert` without CSR for proxies
  - `/getcert` with VOMS-string request parameter
- Need to adapt OIDC servlet (upstream)
- build an online CA

- perhaps look at alternative: Unity-IdM (EUDAT scenario): also OIDC + Online CA
- look at integration with DigiCert portal
- EGI pilot: Master Portal as a Token Translation Service

Conclusion

Work in progress but looking good!

Some References

- Our setup: `https://wiki.nikhef.nl/grid/CILogon_Pre-Pilot_Work`
- OpenID Connect for MyProxy: `http://goo.gl/VnMKXS`
- CILogon docs: `http://www.cilogon.org/portal-delegation`
- MyProxy: `http://grid.ncsa.illinois.edu/myproxy/`
  - OA4MP: `http://grid.ncsa.illinois.edu/myproxy/oauth/`
  - protocol: `http://grid.ncsa.illinois.edu/myproxy/protocol/`
- VOMS: e.g. `http://italiangrid.github.io/voms/`
- ssh `authorized_keys`: `man sshd`

Extra: (VOMS) Proxy Certificates

- Authentication standard for Grid, PRACE, ...
- Standard:
  - RFC3820
  - end-entity (user) certificate functions as 'mini CA'
- used as delegated authentication token
- can embed e.g. Attribute Certificates:
  - RFC3281, updated to RFC5755
  - used by VOMS: bind attributes to proxy (e.g. roles and groups)
- VOMS proxy certificates can be verified off-line