AARC-SA1 CILogon-based pilot: user certs behind the scenes

Mischa Sallé

msalle@nikhef.nl

3^{rd} *AARC face-to-face meeting, CERN*

30 November 2016

Motivation

- Access to X.509 resources
- Hide X.509 credentials for user
- User uses federated access: need token translation: SAML → X.509

→ pilot e.g. CILogon *software*

https://aarc-project.eu/digital-certificates-behind-the-scenes-the-aarc-cilogon-pilot/

Use case description

Science Gateway scenario:

- use from web-browser via SSO
- run workflows or access storage elements
- gateway developers have no special security know-how
- like personalised user credentials (traceability)

→ portal needs a user credential, via a simple API

Question:

How to get (personal) X.509 certs on a Science Gateway ?

Ingredients

Starting points:

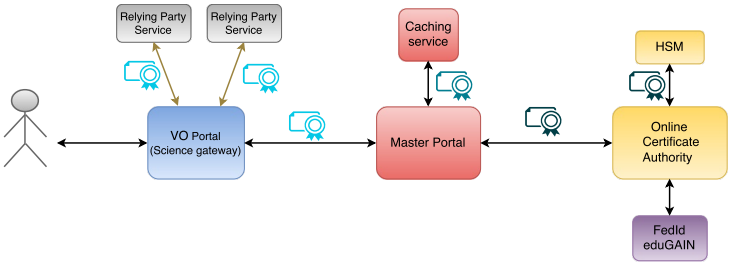
- A single, fully IGTF accredited online CA: *RCauth.eu*
- Scalable trust model (certs are powerful!): *Master Portal*
- Trustworthy federated access: *eduGAIN* + *R&S* + *Sirtfi*
- Easy integration with Science Gateways: *OIDC authorization flow*
- Hidden personal user certificates
- Integration with VO-run attribute authorities: *VOMS*

Basic building blocks

Start from CILogon *software*: federated online CA with web frontend + delegation

→ produces end-entity certificates:
need caching plus trusted service to handle them.

→ new component: Master Portal



Basic building blocks

Online CA: RCauth.eu

- CILogon-software based, MyProxy CA with HSM (eToken...)
- Produces user certificates, delegated via OpenID-Connect
- Via filtering WAYF into eduGAIN (only R&S and Sirtfi IdPs)
- Single one in Europe: white label
- IGTF accredited

Science gateway / VO portal

- Straightforward OpenID Connect client
- Uses `/getproxy` call to obtain (VOMSified) proxy certificates
- $O(\text{many})$ in Europe

Basic building blocks

Online CA: RCauth.eu

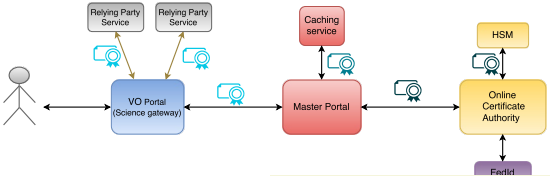
- CILogon-software based, MyProxy CA with HSM (eToken...)
- Produces user certificates, delegated via OpenID-Connect
- Via filtering WAYF into eduGAIN (only R&S and Sirtfi IdPs)
- Single one in Europe: white label
- IGTF accredited

Science gateway / VO portal

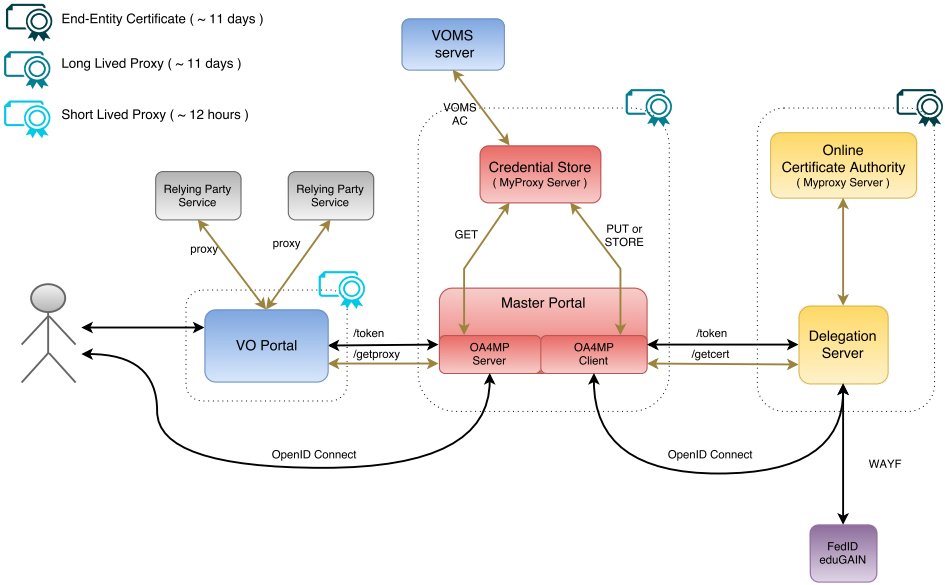
- Straightforward OpenID Connect client
- Uses `/getproxy` call to obtain (VOMSified) proxy certificates
- $O(\text{many})$ in Europe

Master Portal

- Handles complexity
- Trusted component
- OpenID Client to online CA, OpenID server to VO portal
- “Caches” incoming certificate as a proxy certificate in MyProxy store
- transparent VOMS integration (no specific VO)
- Typically one per e-infrastructure
- Few running: EGI, ELIXIR



Putting it all together



Status update

- Lots of documentation (wiki, thanks to Tom)
- New semi-permanent demos (next slide, thanks to Paul Millar and David)
- Work on VOMS *provisioning* (with EGI)
- EGI towards production, HA Master Portal setup
- EUDAT integration? INDIGO integration?
- IOTA software support for EGI (e.g. Argus integration)
- We need more R&S + Sirtfi IdPs!
- Support for OIDC IdPs?
- Next step hopefully ssh key access (non-web)

https://rcdemo.nikhef.nl/

- Basic demo: Show OIDC authorization flow + demo portal integration code:
  1. front-channel (browser redirect) to `/authorize` endpoint
  2. back-channel token request to `/token` endpoint
  3. back-channel getproxy request to `/getproxy` endpoint
- GSIFTP demo: Browse a dCache storage element:
  1. login either with or without additional VOMS attributes
  2. browse, upload etc. a dCache storage element

Some References

- Blog post:
  `https://aarc-project.eu/digital-certificates-behind-the-scenes-the-aarc-cilogon-pilot/`
- Our setup: `https://wiki.nikhef.nl/grid/AARC_Pilot`
- Pilot ICA 1 (e.g. CP/CPS): `https://rcauth.eu/`
- CILogon / MyProxy:
  - 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/`