

AARC-SA1 CILogon pilot: user certificates behind the scenes

Mischa Sallé

Tamas Balogh David Groep

`msalle@nikhef.nl`

3rd AARC face-to-face meeting, Utrecht

25 May 2016



Scenarios:

1 Science gateways

Running pre-defined workflows, limited permissions, often federated access
→ single account / limited traceability

2 Grid and supercomputers

Arbitrary workload, or even interactive access, certificate based access
→ per-user account / good traceability

Both face challenges

Scenarios:

① Science gateways

Running pre-defined workflows, limited permissions, often federated access
→ single account / limited traceability

② Grid and supercomputers

Arbitrary workload, or even interactive access, certificate based access
→ per-user account / good traceability

Problems for Science gateways

- want more complicated flows
- one service contacts the next
- access to other resources

Problems for commandline access

- user cert + private key difficult
- steep learning curve
- user misplaces key

Scenarios:

① Science gateways

Running pre-defined workflows, limited permissions, often federated access
→ single account / limited traceability

② Grid and supercomputers

Arbitrary workload, or even interactive access, certificate based access
→ per-user account / good traceability

Problems for Science gateways

- want more complicated flows
- one service contacts the next
- access to other resources

Problems for commandline access

- user cert + private key difficult
- steep learning curve
- user misplaces key

Wishlists

Science gateways:

- improved traceability:
personal credentials
- inter-operable credentials
- service to service ('delegation')

Commandline access:

- simpler to handle cert+key
- based on federated / social login

Number of attempts, so far non ideal ...

Science gateways:

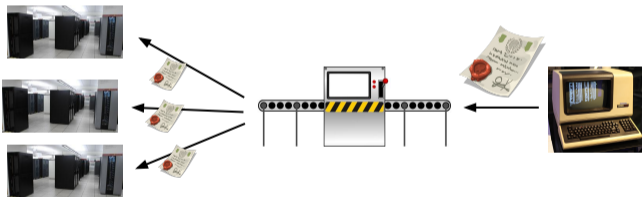
- EUDAT:
online CA (Token Translation Service),
not inter-operable
- (EGI:
Per-User Sub-Proxies: interim
solution, leave out for now)

Commandline access:

- TCS:
makes easier to obtain a cert+key, can
still lose it (VM, internet cafe), not
pan-European
- SWITCH: SLCS Grid CA for
Switzerland (discontinued)
- CILogon:
online CA, primarily for downloading
cert, but wait ...

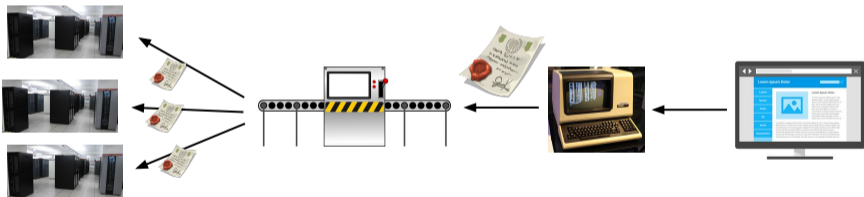
We like to get the best of both, solve it for the whole of Europe:

Extend the commandline access setup . . .



We like to get the best of both, solve it for the whole of Europe:

Extend the commandline access setup . . . into



First note: X.509 certificates are everywhere:

- https
 - server to server
 - SAML metadata
 - OS signing (secure boot)
- well supported, fast, security model understood



First note: X.509 certificates are everywhere:

- https
 - server to server
 - SAML metadata
 - OS signing (secure boot)
- well supported, fast, security model understood



Username
Enter your username

Password [Forgot your password?](#)
Enter your password

Keep me logged in (for up to 30 days)

Log in



Problems with alternatives authN mechanisms:

- username/password → no delegation
- OpenID Connect → no multi-step delegation
- SSH-keys → bootstrap problem, difficult
- SAML-ECP → not-yet widely available, ...?

We want it all:

- A single, fully IGTF accredited online CA
- Federated access via eduGAIN
- Hidden personal user certificates
- Easy integration with Science Gateways
- Scalable trust model (certs are powerful!)

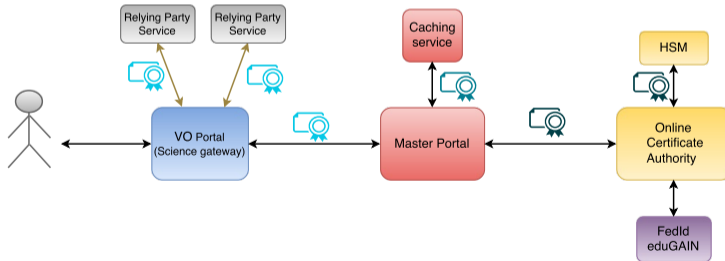
Plus: commandline access (with still mostly hidden cert+key)

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**

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**



Online CA

- CILogon based, MyProxy CA with HSM (eToken...)
- Produces user certificates, delegated to service via OpenID-Connect
- Via WAYF into eduGAIN (almost there)
- Single one in Europe: white label
- IGTF accredited!!!

→ [kaasvat eh ...pilot-ca1.rcauth.eu](https://kaasvat.eh...pilot-ca1.rcauth.eu)

Science gateway / VO portal

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

Online CA

- CILogon based, MyProxy CA with HSM (eToken...)
- Produces user certificates, delegated to service via OpenID-Connect
- Via WAYF into eduGAIN (almost there)
- Single one in Europe: white label
- IGTF accredited!!!

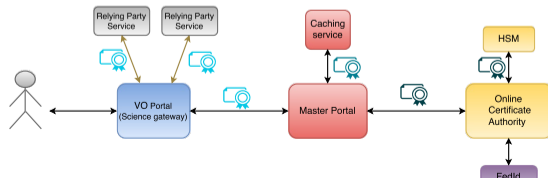
→ kaasvat eh ... pilot-ca1.rcauth.eu

Science gateway / VO portal

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




Master Portal

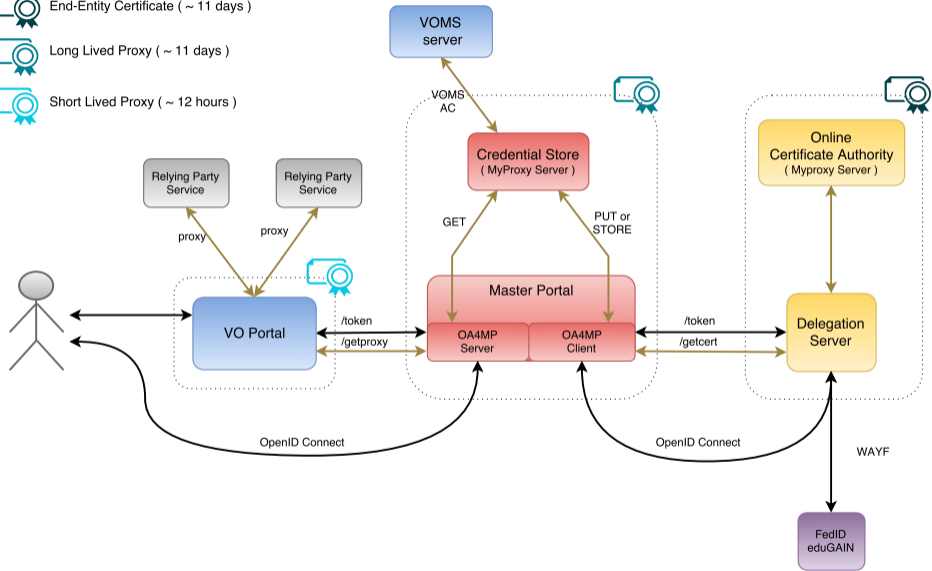
- Handles complexity
- Trusted component (see David's talk)
- OpenID Client to online CA, OpenID server to VO portal
- "Caches" incoming certificate as a proxy in MyProxy store
- VOMS integration
- Typically one per e-infrastructure
- Few running: EGI, ELIXIR



Can use credential caching server also for commandline access:

- Allow proxy download based on SSH-agent
think github, svn, GlobusOnline
- Custom “client portal” for uploading SSH public keys
- ssh-ing to the server will return a proxy certificate
- Can use as opaque token, similar to Kerberos tokens

-  End-Entity Certificate (~ 11 days)
-  Long Lived Proxy (~ 11 days)
-  Short Lived Proxy (~ 12 hours)



- Our setup: https://wiki.nikhef.nl/grid/CILogon_Pre-Pilot_Work
- Pilot ICA 1: <https://www.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/>
- ssh `authorized_keys`: `man sshd`