

RCauth.eu / MasterPortal update

Mischa Sallé

`msalle@nikhef.nl`

5th AARC face-to-face meeting, Αθηνα

21 March 2017



- Access to X.509 resources made easy¹
 - Science Gateway scenario (browser-central)
need *simple* api to get user certificates
 - Compared to US Europe decentralized/multi-federated:
need layered setup
- intermediaries: MasterPortals
- between central CA and O(many) science gateways
 - similar position as IdP/SP proxies in eInfras/ResearchInfras

¹ <https://aarc-project.eu/digital-certificates-behind-the-scenes-the-aarc-cilogon-pilot/>

Single RCauth.eu


- single, fully IGTF accredited online CA
- *eduGAIN + R&S + Sirtfi*

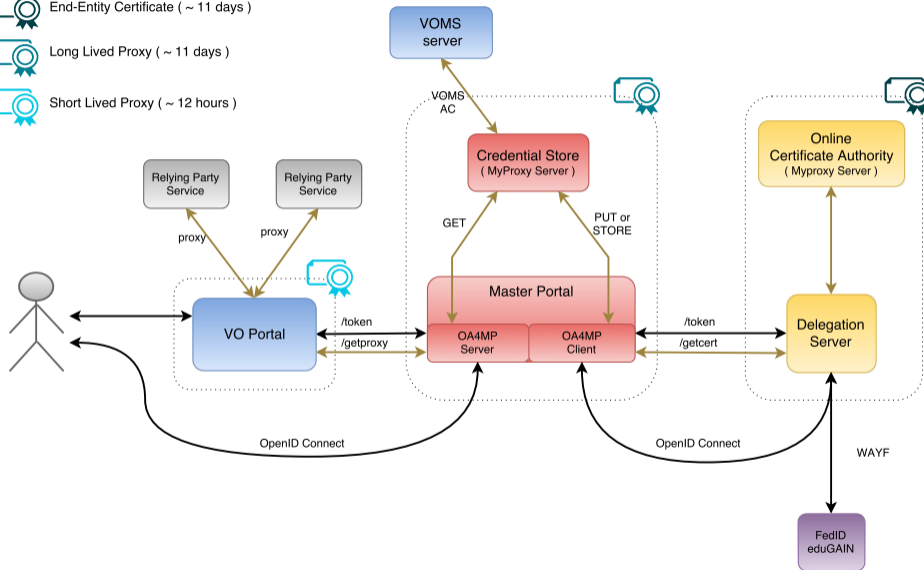
Few Master Portals

- Scalable trust model
- Handling the complexity (end-entity-cert to proxy-cert)
- Caches the credentials
- VOMS integration

Many Science gateways / VO portals

- Easy integration using OIDC authZ flows access

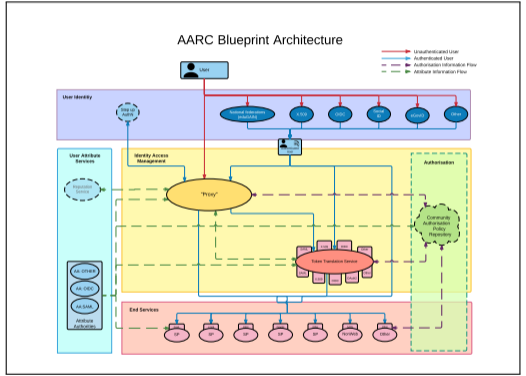
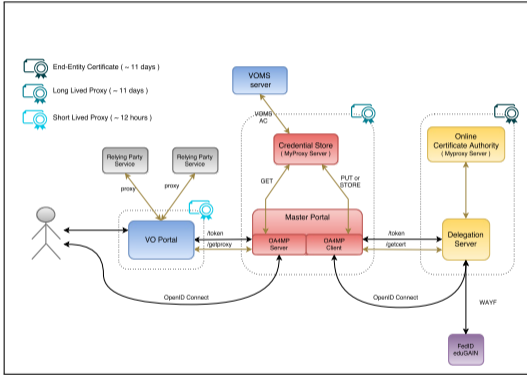
-  End-Entity Certificate (~ 11 days)
-  Long Lived Proxy (~ 11 days)
-  Short Lived Proxy (~ 12 hours)



- Use new upstream code, now (also) on github (used both in MasterPortal and RCauth.eu itself)
- Upstream has improved OIDC support (towards Cllogon-2)
 - signed id_token
 - `/.well-known/openid-configuration`
- Generic MasterPortal ansible scripts now also on github

→ <https://github.com/rcauth-eu/>

- Software support: Try to push back our patches
- **joint RCauth proposal** (EGI, EUDAT, GÉANT...?): e.g. HA setups
- Integration Master Portals (next slides)
- Training in AARC2?



MasterPortal \approx TTS, close to or inside IdP/SP proxy

- Infra Integrations (order of appearance):
 - ELIXIR is running our implementation of a MasterPortal
 - EGI is also running our implementation: next to CheckIn, looking e.g. at HA
 - INDIGO is integrating MasterPortal within WaTTS²
 - EUDAT is testing our implementation, considering integration within Unity-IdM³
 - PRACE: ongoing discussions, need to look at the use-cases.

²Demo/talk Uros

³Demo from Shiraz/Nicolas

- MasterPortal can already return VOMS proxies, but user must be **provisioned**
- Need user attributes, but also DN
 - IdP/SP proxy is ideal location
 - acting as OIDC client to RCauth (like a MasterPortal) → get cert_subject_dn
- VOMS provisioning @IdP/SP proxy: create e.g. a **COmanage plugin**
 - useful discussions and planning with Benn, Peter, Nicolas at plugfest
 - basic provisioning/deprovisioning plugin planned soon (before end AARC1?)
 - no changes needed to existing VOMS servers, but do need VO-admin
 - mapping of e.g. Role is not yet fully clear

How to deal with multiple identities in RCauth?

(Different IdP gives different DN: "ePUId" ↔ DN token translation)

- could link DNs at every SP (bad)
- could link DNs inside VOMS (ok but depends on how)
- could link all ePUIds (or similar) in central IdP/SP proxy:
 - use *preferred* IdP as default `idphint` for RCauth
 - can do VOMS provisioning for *all* identities
- alternative: linking in MasterPortal: 'idphint-per-user' list
 - multiple identities are known and sufficient for returning proxy cert
 - but one is preferred and used for end-entity cert creation

- **Demos:** <https://rcdemo.nikhef.nl/>
→ email me your RCauth DN for provisioning into `rcdemo.aarc-project.eu` test VO
- Blog post:
<https://aarc-project.eu/digital-certificates-behind-the-scenes-the-aarc-cilogon-pilot/>
- Our setup: https://wiki.nikhef.nl/grid/AARC_Pilot
→ also contains links to CILogon code, MyProxy protocol etc.
- Pilot ICA 1 (e.g. CP/CPS): <https://rcauth.eu/>
- VOMS: e.g. <http://italiangrid.github.io/voms/>

- Need IOTA support on production X.509 resources:
 - compute: EMI: LCMAPS ok, Argus unofficially ok, ARC: needs to implement
 - storage: dCache partially, DPM needs to implement
- Might need support for OIDC IdPs at central RCauth CA