RCauth.eu: getting proxies using SSH key AuthN

Mischa Sallé

msalle@nikhef.nl

WLCG Authorization Working Group

28 September 2017

The RCauth.eu Online CA (Pilot ICA 1):

- Motivation: Science Gateways & hiding the certificate. See *https://aarc-project.eu/digital-certificates-behind-the-scenes-the-aarc-cilogon-pilot/*
- IOTA CA, in eduGain (as SP)
- accepts all R&S + Sirtfi IdPs
- produces 11d ($\approx$ 1Ms) certificates

The need for an intermediary

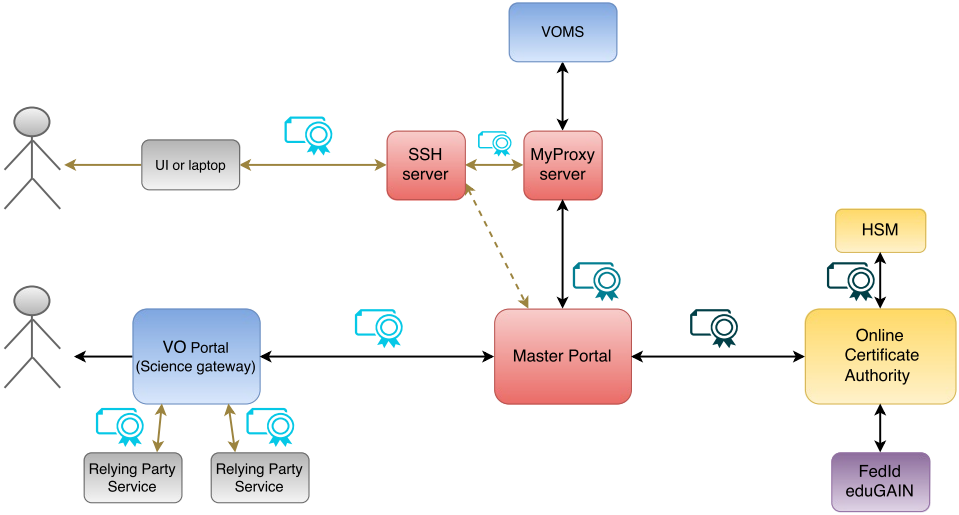
Need more services than only a single Online CA:

- Hierarchical distribution of trust:
  Europe is non-central (unlike US)
- Caching:
  Don't overload the CA

→ Introduce an intermediary: Master Portal

- Retrieves EEC from RCauth.eu
- Stores long-lived proxy in backend MyProxy server
- Provides short-lived proxies for clients:
  - Science Gateways via OIDC (so-called VO-portals)
  - *users e.g. via SSH key authentication*

Architecture overview



Leverage MyProxy store:

- User uploads SSH public key to MasterPortal:
  `https://aai.egi.eu/sshkeys/`
  requires login via RCauth.eu to obtain username
- User makes sure MyProxy has a long-lived proxy, can use 'vo-portal'
  `https://aai.egi.eu/vo-portal/`
  Needs to do this ± once a week
- Obtain a proxy certificate
  `ssh proxy@ssh.aai.egi.eu > /tmp/x509up_u$(id -u)`
  SSH-server contacts MasterPortal to build `AuthorizedKeysCommand`
  SSH-server runs `myproxy-logon`

Open issues

- Currently no VOMS integration for SSH key interface[1], but:
  - ▷ *Vomsify using voms-proxy-init*

    ```
    voms-proxy-init -noregen -voms pvier
    ```
- No automagic enrollment in VO, but:
  - ▷ *Can predict DN from (SAML) attributes, with some restrictions*
  - ▷ *We produce a* `cert_subject_dn` *OIDC claim*

[1] NOTE: the portal scenario does provide transparent VOMS integration

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`
  SSH keys:
  - User info: `https://wiki.nikhef.nl/grid/AARC_Pilot_-_SSH_Key_Portal`
  - API: `https://wiki.nikhef.nl/grid/Master_Portal_sshkey_endpoint`
  - EGI MasterPortal documentation: `https://wiki.egi.eu/wiki/AAI_guide_for_SPs#Integrating_Science_Gateways_with_RCauth_for_obtaining_.28proxy.29_certificates`
- Pilot ICA 1 (e.g. CP/CPS): `https://rcauth.eu/`
- RCauth.eu / MasterPortal based demos: `https://rcdemo.nikhef.nl/`