RCauth Online CA service and MasterPortal Token Translation Service

RCauth operations team

eosc-hub.eu
@EOSC_eu

Dissemination level: Public

EOSC-hub receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 777536.
RCauth - status

- RCauth is an IGTF accredited online CA (of the IOTA / DOGWOOD class)
  - Online credential conversion
  - Connected to eduGAIN (R&S+Sirtfi) plus direct e.g. EGI Check-in

- EOSC Hub is implementing a High Availability setup across three sites
  - Private key is to be cloned and hosted in Hardware Security Modules (HSM) at each site
  - Cloning is done by XORing key with random strings
  - Randomness exchanged using different means (usually in-person)
  - => key is 3-of-3 encrypted
    - Any part, or any two of the three, will have no information about the key
Why RCauth?

- Easy issuance of certificates to Check-In users
  - Assuming their Level of Assurance is sufficient

- Certificates can -
  - Drive FTS / GridFTP transfers - high performance managed data transfer
  - Enable command line access
  - Carry VOMS attributes
  - Interface to anything (through secure sockets, TLS)

- Ease of use
  - Portals can abstract the certificate management (browsers are not great at managing client certificates)
  - Users don’t even need to know they are using certificates
First of its kind - a CA run by three different organisations

Lots of interesting technology enables this to happen

will reuse for making the MasterPortal also HA

User experience improves:
- lower latency to nearest node
- higher reliability
- improved performance
Detailed CA Layout / relation to MasterPortal
MasterPortal Demo

Proxy X.509 certificate retrieval using SSH key authentication
Proxy X.509 certificate retrieval using SSH key authentication

- EGI MasterPortal also allows users to authenticate using their SSH key pair to retrieve proxy certificates issued by the RCauth Online CA
Proxy X.509 certificate retrieval using SSH key authentication

- Users need to first upload the public key via a self-service portal, [https://aai.egi.eu/sshkeys/](https://aai.egi.eu/sshkeys/)
Proxy X.509 certificate retrieval using SSH key authentication

• Users can then obtain a proxy certificate by doing:

```
ssh proxy@ssh.aai.egi.eu
```
Proxy X.509 certificate retrieval using SSH key authentication

- About once a week users need to follow a web-flow to ensure a long-lived proxy certificate is present in MasterPortal
- Demo VO Portal: https://aai.egi.eu/vo-portal/
Thank you for your attention!

Questions?

Contact
RCauth Operations team
ops-management(AT)rcauth.eu

eosc-hub.eu  @EOSC_eu

This material by Parties of the EOSC-hub Consortium is licensed under a Creative Commons Attribution 4.0 International License.