EGI: Advanced Computing for Research

www.egi.eu

@EGI_eInfra

EGI Check-in & RCauth Online CA

Use cases & Roadmap

Nicolas Liampotis
& Mischa Sallé

The work of the EGI Foundation
is partly funded by the European Commission
under H2020 Framework Programme

EGI Check-in

Check-in in a nutshell

Identity and Access Management solution that makes it easy to secure access to services and resources

Components

- IdP/SP Proxy
- User enrolment & group management
- IdP Discovery
- Token Translation

Documentation

- Usage guide
- Integration guides

https://wiki.egi.eu/wiki/AAI

Motivation behind Check-in

Single sign-on to services through eduGAIN, social media and other institutional or community-managed identity providers

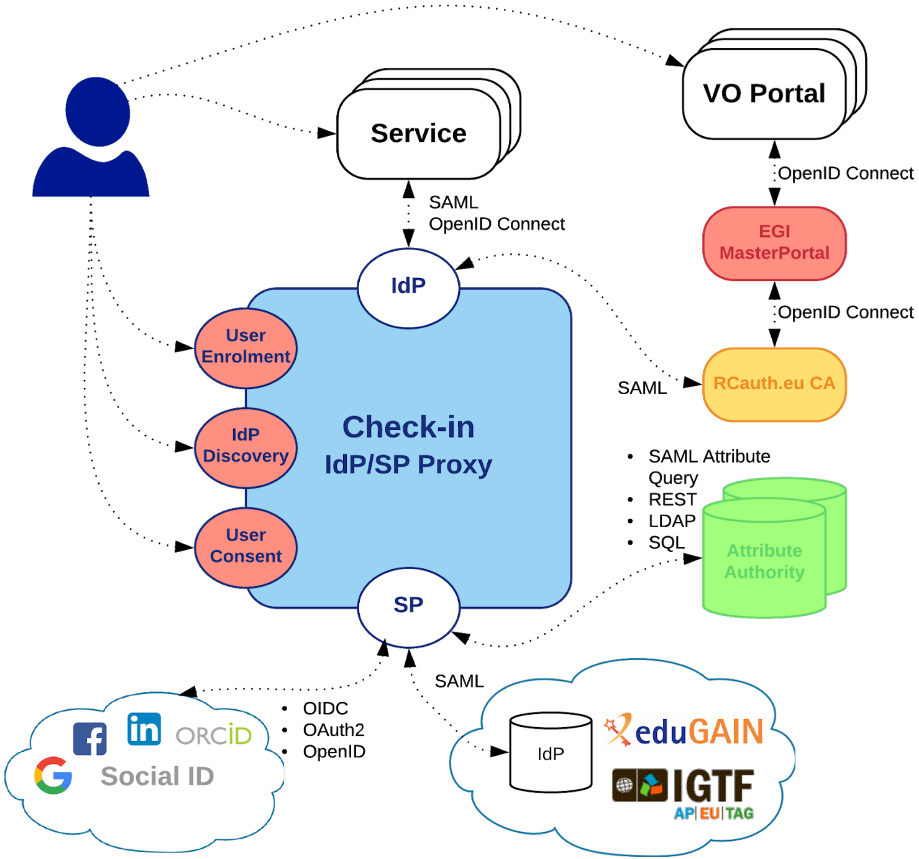
Only one account needed for federated access to multiple heterogeneous (web and non-web) service providers using different technologies (SAML, OpenID Connect, OAuth 2.0, X509)

Access to resources using different login credentials (institutional/social) via identity linking

Expressing the level of trust in the identity assertions

Aggregation and harmonisation of authorisation information (VOs/groups, roles, assurance) from multiple sources

Check-in service architecture and interfaces



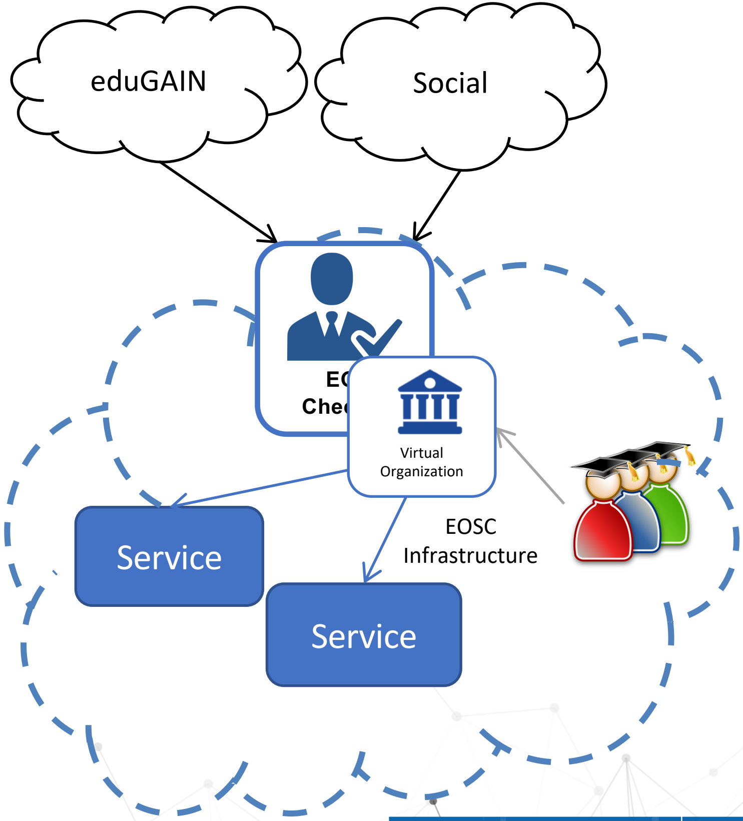
Check-in is an implementation of the AARC blueprint architecture

- Single point of integration for Identity Providers (IdPs) and Service Providers (SPs)
- Registered in eduGAIN as an SP complying with REFEDS Research & Scholarship and Sirtfi security framework
- All connected end-services can have one statically configured IdP
- No need to run an IdP Discovery Service on each end-service
- All connected SPs get harmonised user identifiers and accompanying authorization attribute sets from different IdPs that can be uniformly interpreted

Featured use case – For communities in need of a ready-to-use group management solution

Communities that do not operate their own group management service can leverage the group management capabilities of the Check-in platform to:

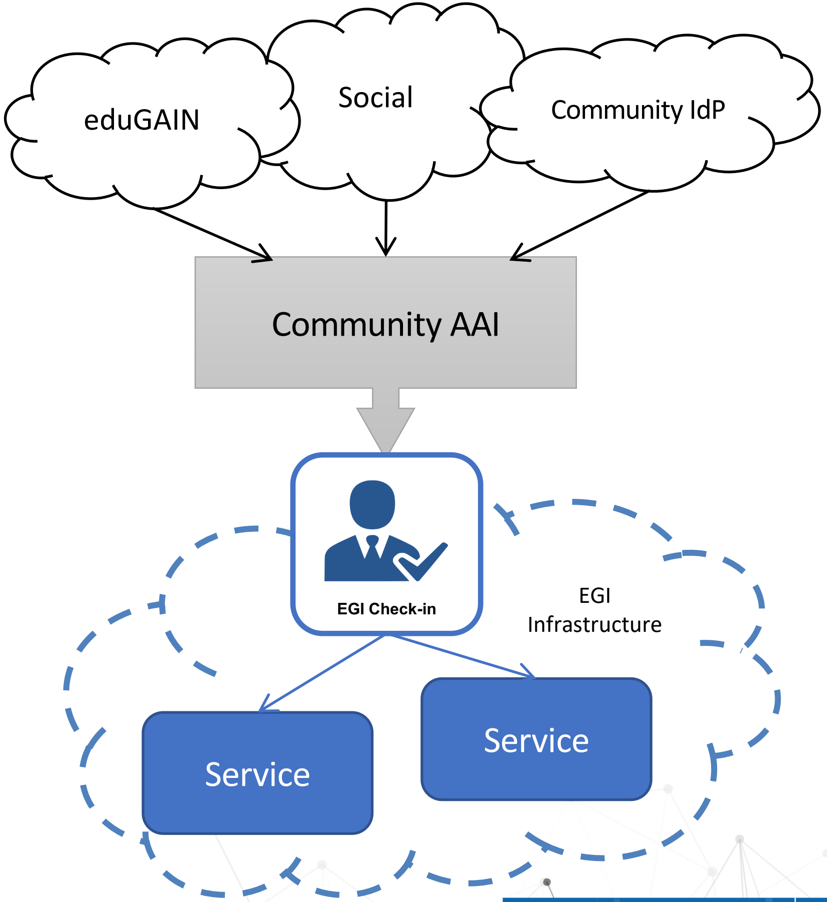
- Avoid overhead of deploying a dedicated group management service
- Allow authorised group admins to manage the information about their users independently
- Enable easy and secure access to resources offered by EGI and other infrastructures participating in EOSC



Featured use case – For communities operating their own AAI

Community AAI connected to Check-in as an IdP Proxy to allow its users to access EGI services & resources

- Community can access EGI services without changing their users' authentication workflow

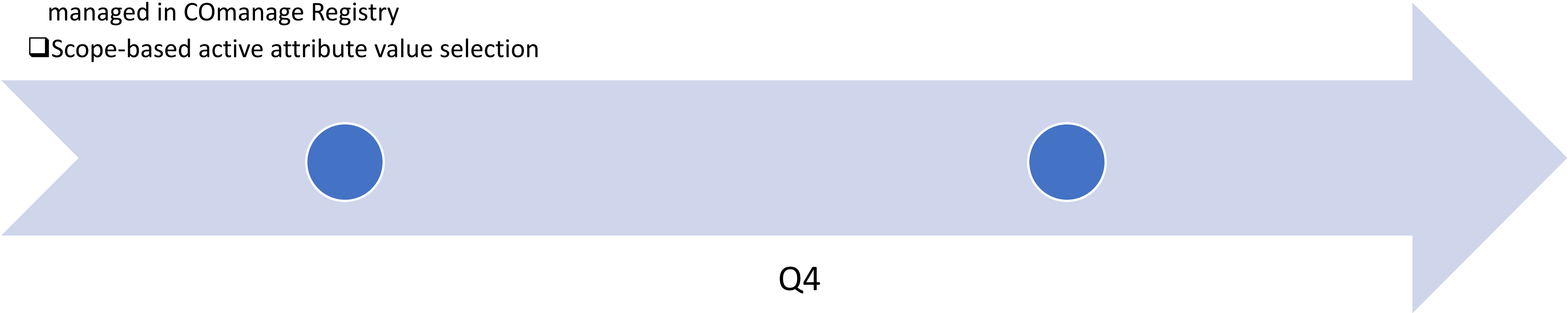


Check-in Roadmap

Short term - 2019

Q3

- □ Adoption of WISE Baseline Acceptable Use Policy (AUP)
- □ Privacy statement compliant with GÉANT Data Protection Code of Conduct v1
- □ Proxy certificate retrieval through SSH key information managed in COmanage Registry
- □ Scope-based active attribute value selection



Q4

- □ Standardised expression of affiliation information (AARC-G025)
- □ Master Portal High Availability Support
- □ Improved integration with EOSC-hub AAI services
- □ User-based active attribute value selection

Check-in Roadmap

Long term – 2020-2021 (1/2)

- Standardised expression of OpenID Connect/OAuth2 claims
  - Research & Education OpenID Connect profile from OpenID RANDE Working Group
- OAuth2 Token validation in multi-AS environment
  - Initial implementation Q4 2019
- Self-service registration and update of OpenID Connect clients
  - Authorised access to OIDC client management interface based on GOCDB roles
- Standardised expression of assurance information (incl. “freshness” of affiliation information) (see AARC-G021, AARC-G026)
  - Compensatory controls for evaluating specific assurance components when users authenticate using IdPs not compliant with REFEDS Assurance Framework (see AARC-G031)
  - Combined evaluation for linked identities (AARC-G031)

Check-in Roadmap

Long term – 2020-2021 (2/2)

- Improved support for (de-)provisioning and continuous update of user account information
- Improved user enrollment and identity linking process
  - Implicit identity linking
- Improved IdP discovery
  - Persistent choice of preferred IdP
  - Support for “IdP hinting” (AARC-G049)
- Technology watch (SATOSA, Keycloak, …)

Check-in Roadmap

Summary

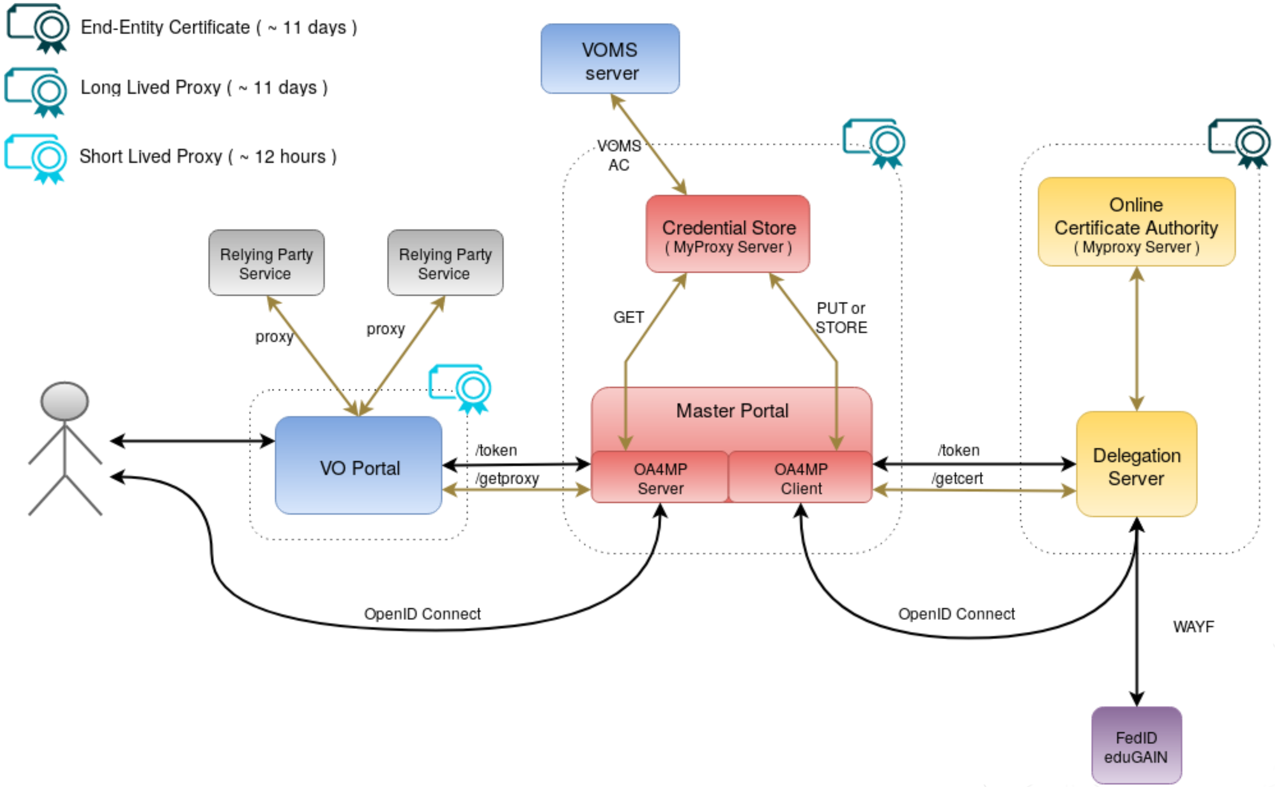
Main areas of focus:

- Adopting AARC/REFEDS/WISE/OpenID RANDE architectural and policy guidelines to enable integration and improve interoperability with EOSC-hub AAI services
- Improving end-user experience (user enrolement, identity linking, IdP discovery)
- Minimising integration effort for service providers
- Technology watch

RCauth.eu Online CA

RCauth Online CA

Overall architecture

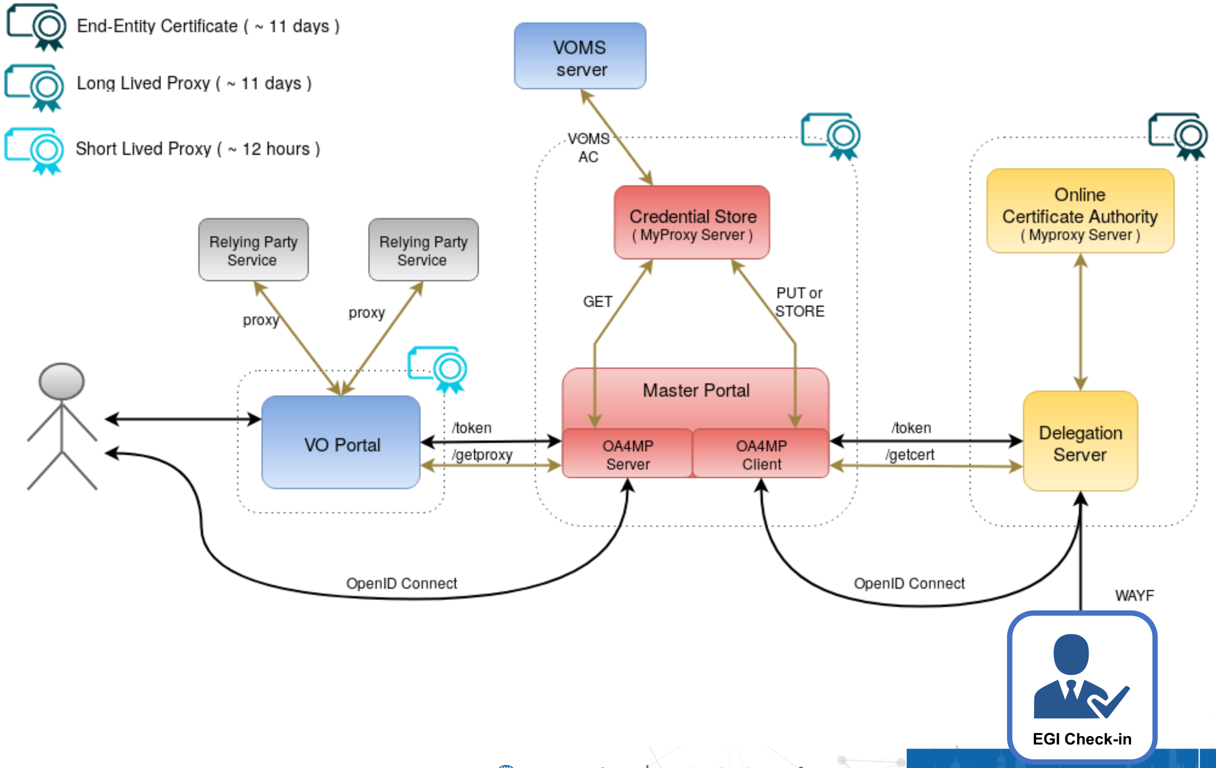


RCauth.eu Online CA - Example use case

EGI Service access – Non-web use cases & delegated access via RCauth Online CA issued certificates

Check-in has been integrated with the production RCAuth.eu Online CA for allowing users to retrieve X.509 proxy certificates using their federated credentials

- Master Portal retrieves end-entity certificate from RCauth.eu
- Long-lived proxy certificate stored in backend MyProxy server
- Short-lived proxies provided via:
  - Science Gateways via OIDC (so-called VO-portals)
  - users e.g. via SSH key authentication

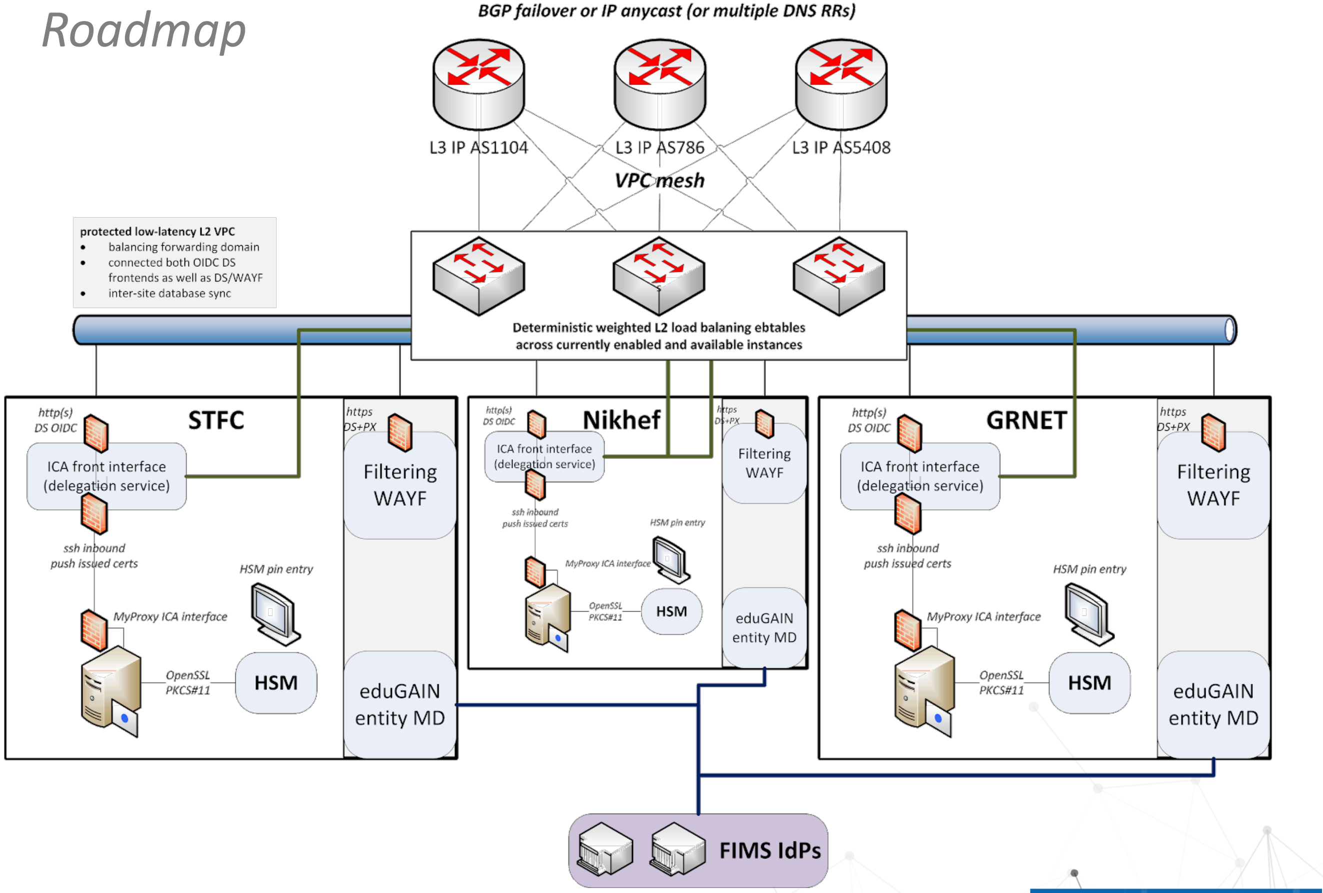


RCauth.eu Online CA

Roadmap

High Availability (HA):

(See §6.5.1 in CP/CPS)



BGP failover or IP anycast (or multiple DNS RRs)
L3 IP AS1104
L3 IP AS786
L3 IP AS5408
VPC mesh
protected low-latency L2 VPC
balancing forwarding domain
connected both OIDC DS frontends as well as DS/WAYF
inter-site database sync
Deterministic weighted L2 load balaning ebtables across currently enabled and available instances
STFC
http(s) DS OIDC
ICA front interface (delegation service)
ssh inbound push issued certs
HSM pin entry
MyProxy ICA interface
OpenSSL PKCS#11
HSM
https DS+PX
Filtering WAYF
eduGAIN entity MD
Nikhef
http(s) DS OIDC
ICA front interface (delegation service)
ssh inbound push issued certs
HSM pin entry
MyProxy ICA interface
OpenSSL PKCS#11
HSM
https DS+PX
Filtering WAYF
eduGAIN entity MD
GRNET
http(s) DS OIDC
ICA front interface (delegation service)
ssh inbound push issued certs
HSM pin entry
MyProxy ICA interface
OpenSSL PKCS#11
HSM
https DS+PX
Filtering WAYF
eduGAIN entity MD
FIMS IdPs

RCauth.eu Online CA

Roadmap (contd.)

See also brief EUGridPMA notes

- key distribution (Q4 2019):
  - most of randomness exchanged: awaiting HSM for GRNET
  - (preliminary) scripts for splitting key / recombining key

- updated CP/CPS (https://rcauth.eu/dev/) (Q3 2019):
  - new governance model accepted https://rcauth.eu/governance/
  - awaiting input from GRNET (and STFC) about local physical config

RCauth.eu Online CA

Roadmap (contd.)

- High Availability (HA) (Q1 2020):
  - backend CA itself (mostly) done:
    - serial numbers increase by 256
    - CRLs (only in case of emergency) would need manual step
    - probably need some work to interact with different HSMs
  - WAYF (Q3 2019)
    - one for each Delegation Server
    - reverse proxy with IP pinning for sso session
  - Delegation server (web frontend), see also MasterPortal (Q1 2020):
    - reverse proxy with IP pinning for web flows e.g. HAProxy
    - multimaster HA database, e.g. Galera cluster
      - ❑ consistent DN
      - ❑ needed for OIDC flow (backend/frontend channel)

RCauth.eu Online CA

Roadmap (contd.)

- High Availability (HA) (Q4 2019):
  - MyProxy server, several options (Q3 2019):
    - shared file system (HA NFS)
    - lsync+rsync
    - (master/slave?)

    needed within one flow (`PUT` MasterPortal and `GET` VO-portal)

  - MasterPortal itself (Q4 2019):
    - behind reverse proxy (NGINX with IP pinning)
    - multimaster HA database, e.g. galera cluster?

      Here only needed for OIDC flows

RCauth.eu Online CA

Other developments

- Reorganised/updated https://github.com/rcauth-eu repositories
  - Updated code to use new and stable upstream code
  - Few new features, many bug fixes and improvements
- Integration with Dirac (latter as VO portal)
  - Work in progress: DIRAC - Check-in integration document
  - Interest from e.g. SKA/AENEAS
- Integration with COmanage/Check-in for SSH keys (see Check-in slides)

www.egi.eu

@EGI_eInfra

Thank you
for your attention.

Questions?

The work of the EGI Foundation
is partly funded by the European Commission
under H2020 Framework Programme