Secure Access Management with EGI Check-in: Latest Advancements and Future Direction

Nicolas Liampotis

GRNET

June 21, 2023

EGI Conference 2023

TLP: GREEN Limited disclosure

Check-in

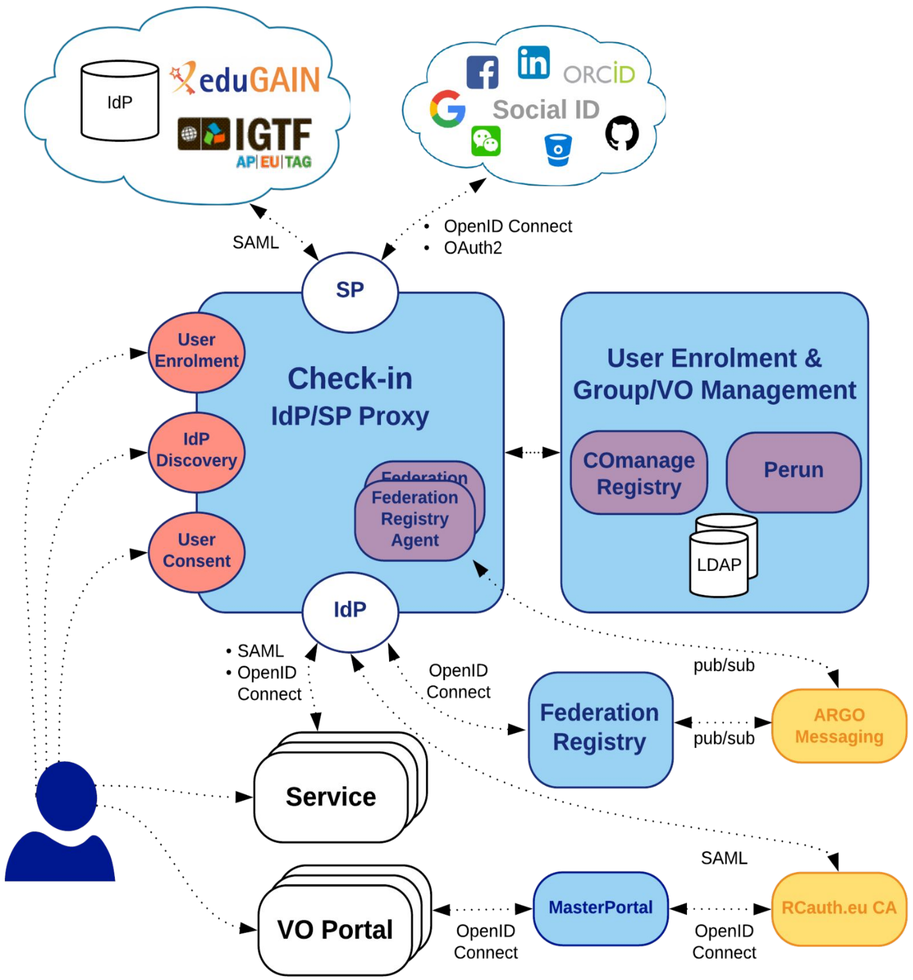
In a nutshell

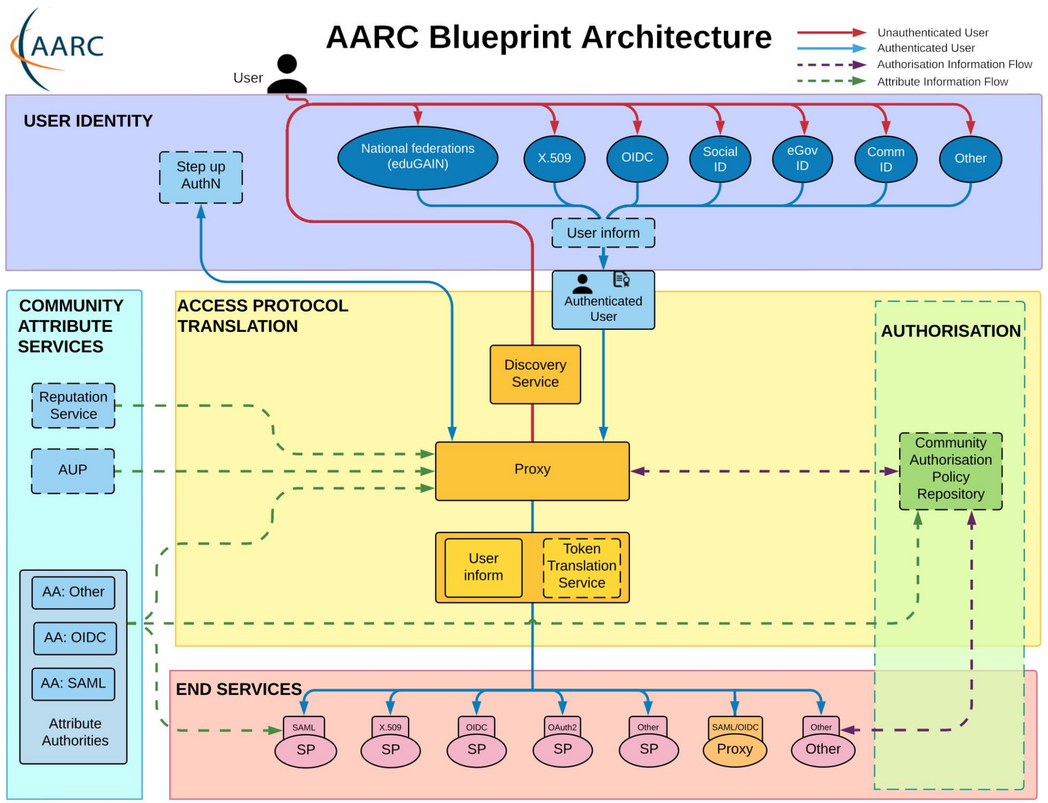
- Identity and Access Management solution that makes it easy to secure access to services and resources
- Single sign-on to services using existing credentials:
  - Academic (e.g. eduGAIN, ORCID)
  - Social media (e.g. Google, Facebook, LinkedIn)
  - Community-managed identities (e.g. Research Infrastructures)
- Federated access to multiple heterogeneous (web and non-web) services using different technologies (SAML, OpenID Connect/OAuth 2.0, X.509)
- Aggregation and harmonisation of authorisation information (groups, roles, assurance) from multiple sources
- Identity linking for accessing resources using different login credentials (institutional/social)
- Expressing the level of trust in the identity assertions (assurance)

Check-in

Architecture

Implementation of the
AARC Blueprint Architecture

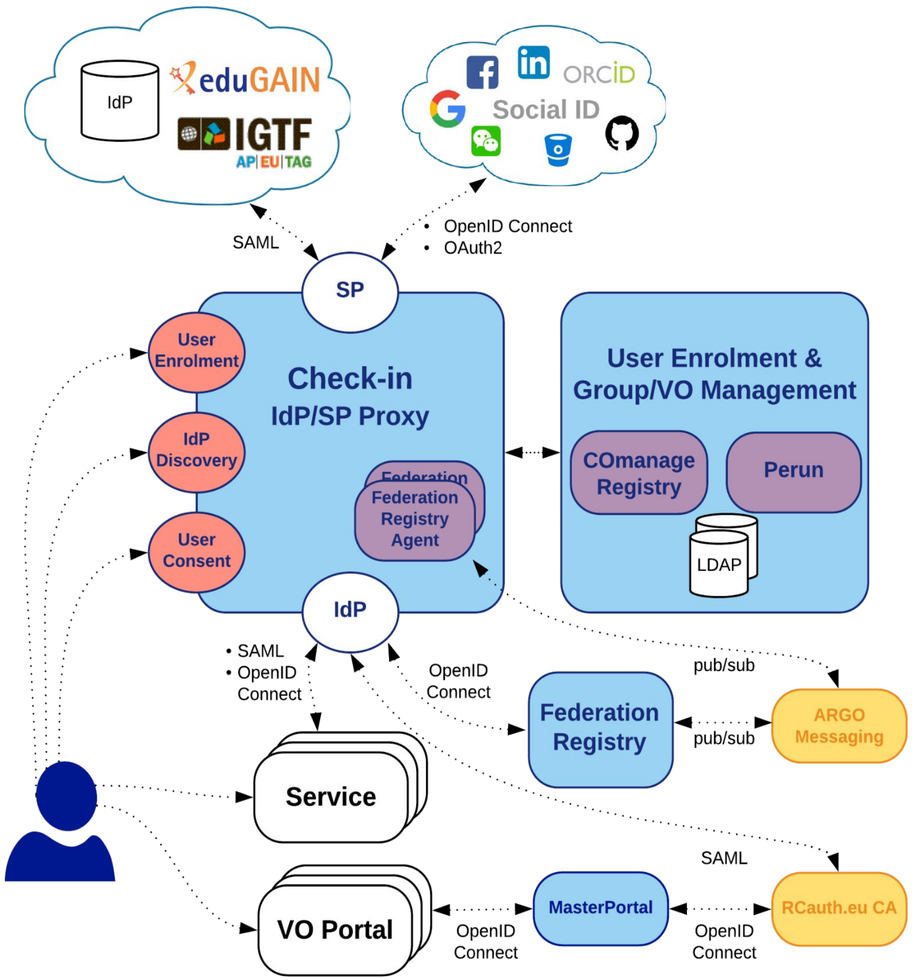


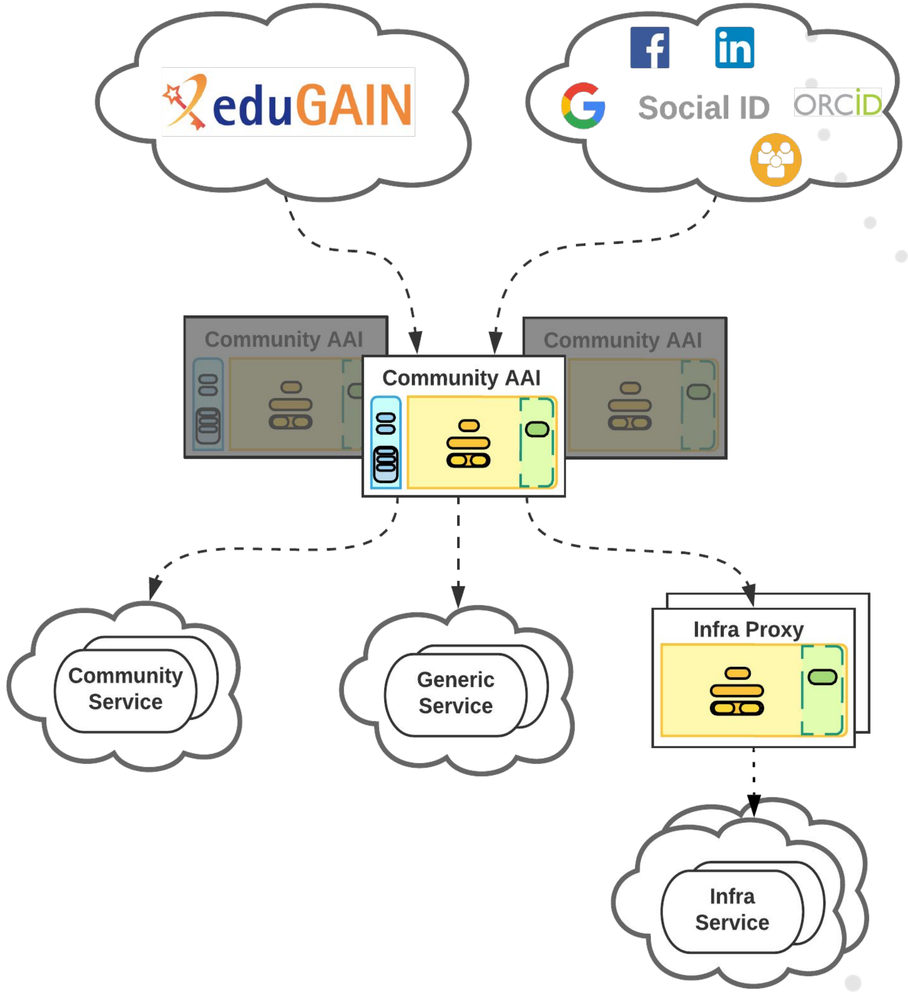


Check-in

Architecture

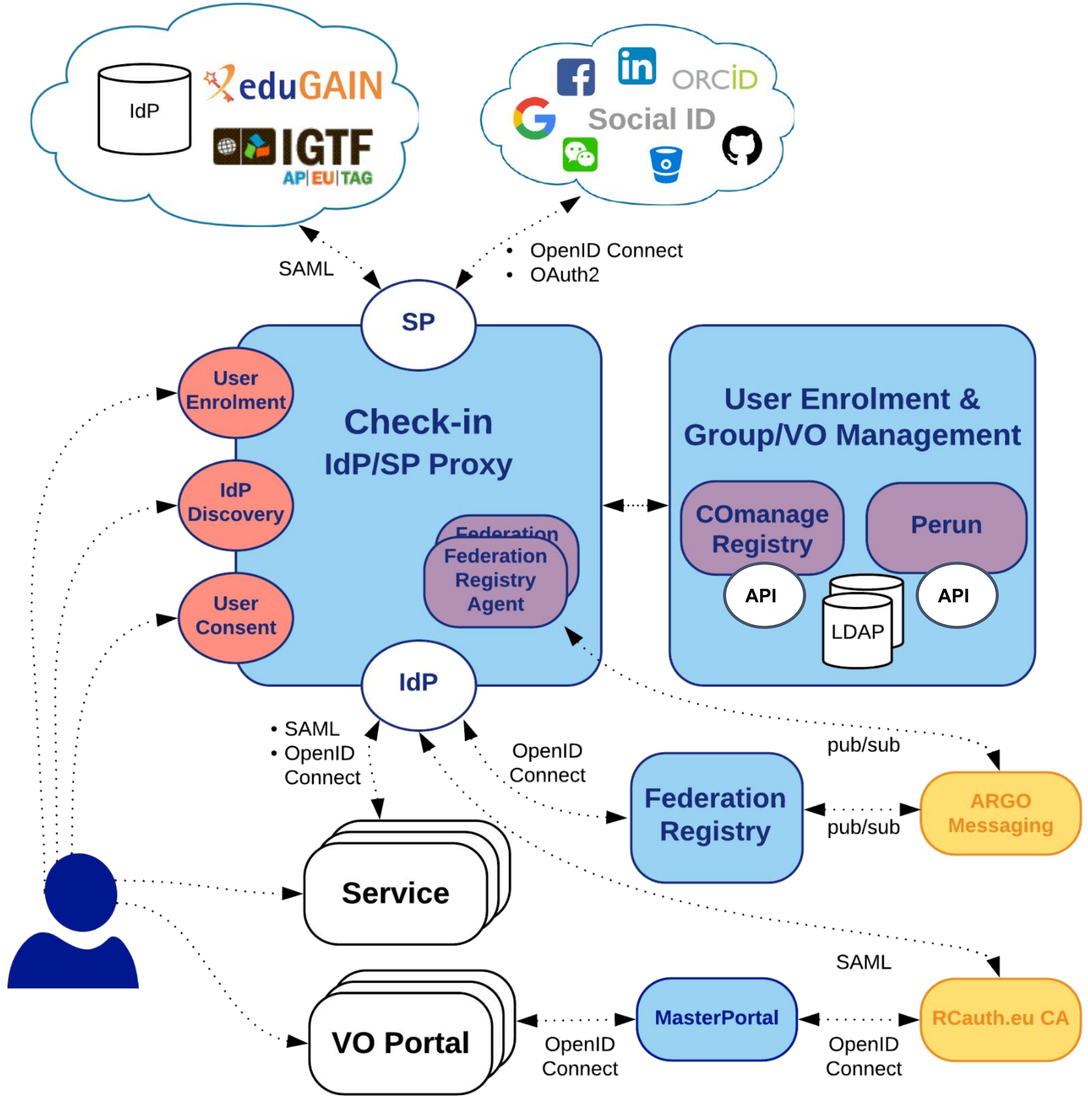
Implementation of the
AARC Blueprint Architecture



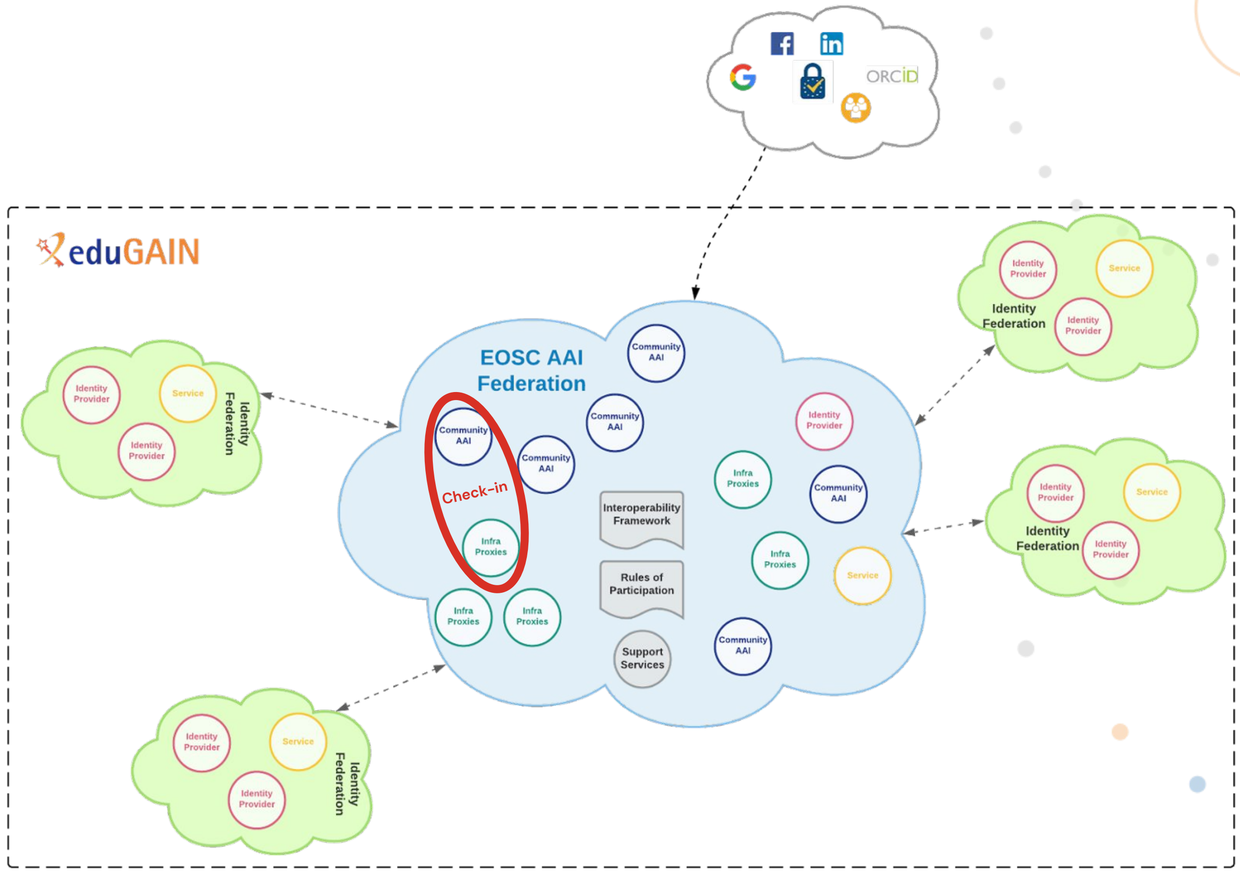


Check-in

Architecture

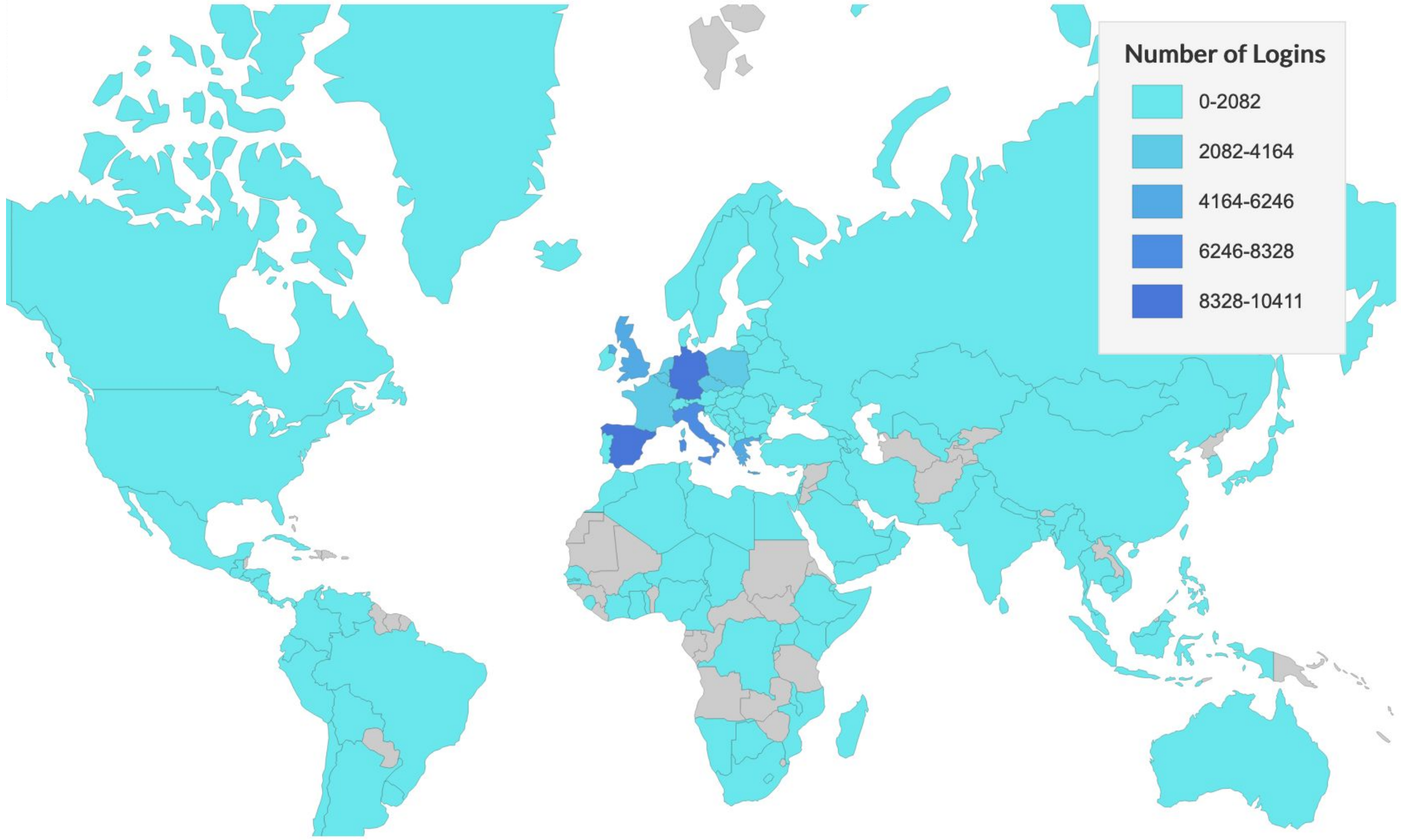


Interoperability with EOSC AAI Federation



Check-in

In numbers



150+

Services

800

Identity Providers

70K+

Logins

Latest advancements

Federated AuthN/AuthZ with Keycloak

Keycloak

Improved compliance with OpenID Connect / OAuth 2.0 standards

- **Completed Phase I of Keycloak migration**
  → Keycloak as OpenID Provider for OIDC relying parties and OAuth 2.0 clients/protected resources
  - Improved compliance with OIDC, SecBCP, RFC6749, RFC6750, RFC8628, RFC7636, RFC6819, RFC7523

A+ EGI Check-in - PROD/DEMO

4,2%

Fail rate

B EGI - MITREid

20,2%

Fail rate

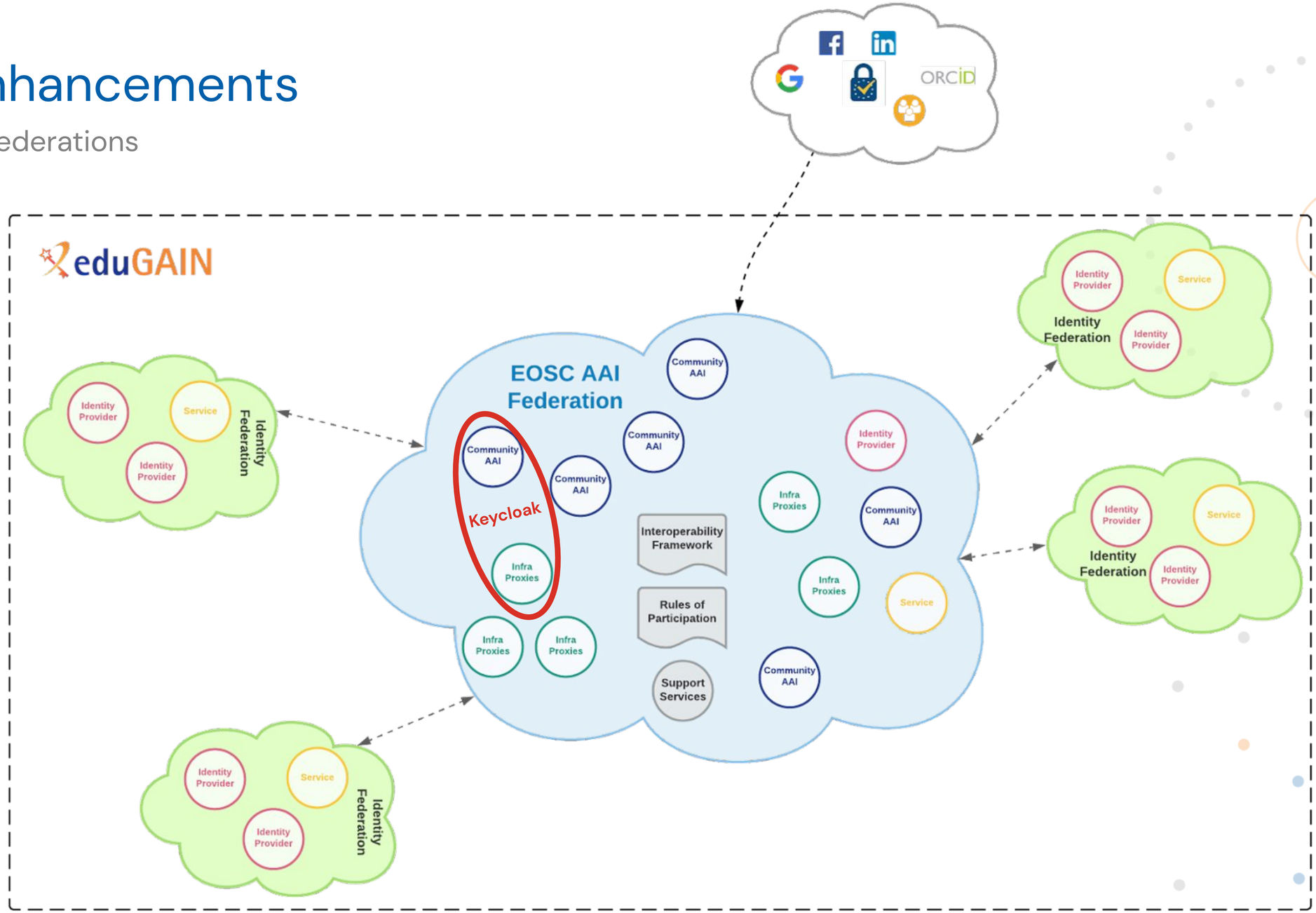
Keycloak Enhancements

- Support for SAML Federations
- Service Registration & Configuration Management
- Advanced Group Management
- Metrics
- New OpenID Connect / OAuth 2.0 flows

Keycloak Enhancements

Support for SAML Federations

- Support for **SAML IdP Federations** (e.g. 5200+ IdPs from eduGAIN)
- Support for **SAML SP Federations** (e.g. EOSC AAI Federation)



Keycloak Enhancements

Support for SAML Federations

- Challenge
  - Upstream reluctant to accept current implementation:
    - Enterprise use cases assume low number of IdPs
    - Requires lots of changes (including account/admin console) for handling large number of IdPs
- Solution → Alternative implementation as a **Keycloak extension**

Keycloak Enhancements

Support for SAML Federations: Keycloak extension

- Proof-of-concept implementation that works on Keycloak v16
  - Extends the logic of keycloak SAML Identity Provider implementation → New SAML Aggregate Identity Provider uses the remote IdP descriptor info selected through a custom where-are-you-from page dynamically during login/link flows
    - Custom broker resource manages the authenticated responses
    - Custom keycloak theme for discovery
  - The linked identities are stored in a db extension in order to allow multiple identities to be linked to the same Identity Provider
  - Issues:
    - Still tightly coupled to Keycloak codebase (a big part of keycloak logic has been replicated in the extension)
    - Lack of administrator interface for showing the linked identities,
    - Lack of advanced interface for setting default values for all the federated IdPs
    - Only supports HTTP-POST binding

Keycloak Enhancements

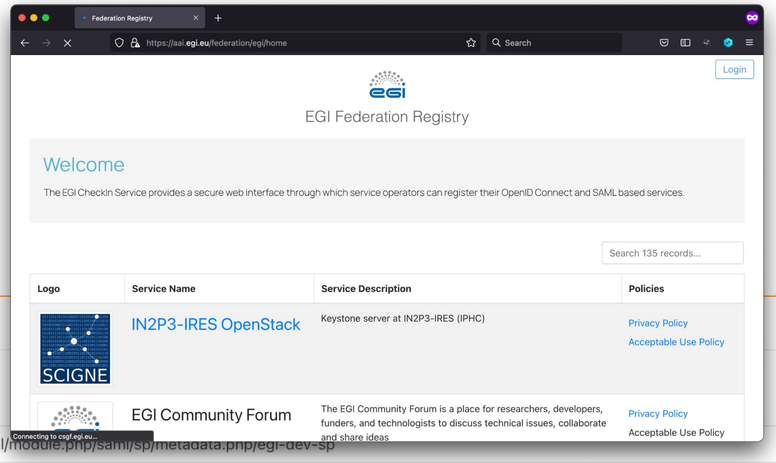
Support for SAML Federations: Keycloak extension

- Ongoing migration to latest Keycloak v21
  - Pros:
    - Refactoring will allow to rely less on Keycloak core code base:
      - by implementing the SAML federation support only through authenticators
      - by using temporary SAML Identity Providers (from kc core code base) in order to manage login/link phases
  - Cons:
    - Refactoring takes time:
      - the extension of the template engine is not supported,
      - admin pages have been totally refactored, etc.

Keycloak Enhancements

SAML Service Registration & Configuration Management

- Support for managing the registration & reconfiguration of SAML Service Providers in Keycloak through the [Federation Registry]
  - Service owners can customise the attribute release
    - Support for customising the attribute OID
- SAML SPs in Demo migrated to Keycloak ✔



General | Protocol Specific

Select Protocol * SAML Service

Entity ID * https://demo.rciam.grnet.gr/saml/module.php/saml/sp/metadata.php/egi-dev-sp

Unique identifier for a SAML service.

Metadata URI * https://demo.rciam.grnet.gr/saml/module.php/saml/sp/metadata.php/egi-dev-sp Load

⚠ Could not find any Requested Attributes from this Metadata Url.

Metadata URI for a SAML service

Requested attributes (see here)

Friendly Name	Attribute Name	Required	
voPersonID	urn:oid:1.3.6.1.4.1.25178.4.1.6	Yes No	☑
displayName	urn:oid:2.16.840.1.113730.3.1.241	Yes No	☑
givenName	urn:oid:2.5.4.42	Yes No	☑
sn	urn:oid:2.5.4.4	Yes No	☑
mail	urn:oid:0.9.2342.19200300.100.1.3	Yes No	☑
voPersonVerifiedEmail	urn:oid:1.3.6.1.4.1.25178.4.1.14	Yes No	☑
uid	urn:oid:0.9.2342.19200300.100.1.1	Yes No	☑
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	Yes No	☑
voPersonExternalAffiliation	urn:oid:1.3.6.1.4.1.25178.4.1.11	Yes No	☑
sshPublicKey	urn:oid:1.3.6.1.4.1.24552.500.1.1.1.13	Yes No	☑
eduPersonOrcid	urn:oid:1.3.6.1.4.1.5923.1.1.1.16	Yes No	☑
voPersonCertificateDN	urn:oid:1.3.6.1.4.1.25178.4.1.3	Yes No	☑
voPersonCertificateIssuerDN	urn:oid:1.3.6.1.4.1.25178.4.1.4	Yes No	☑
isServiceUser	urn:mace:egi.eu:attribute-def:isServiceUser	Yes No	☑
eduPersonAssurance	urn:oid:1.3.6.1.4.1.5923.1.1.1.11	Yes No	☑

List of SAML attributes this SAML service is allowed to receive. See here for more information

https://aai.egi.eu/federation

Keycloak Enhancements

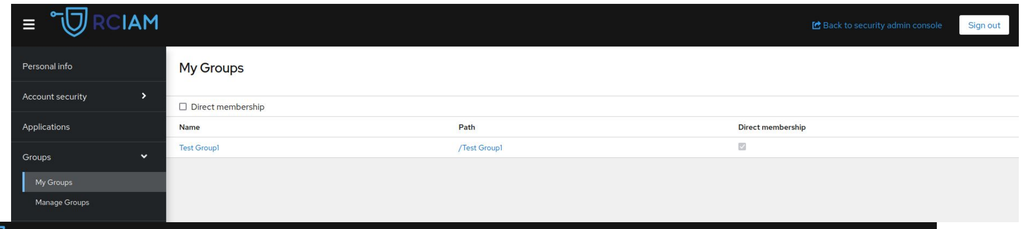
Advanced Group Management

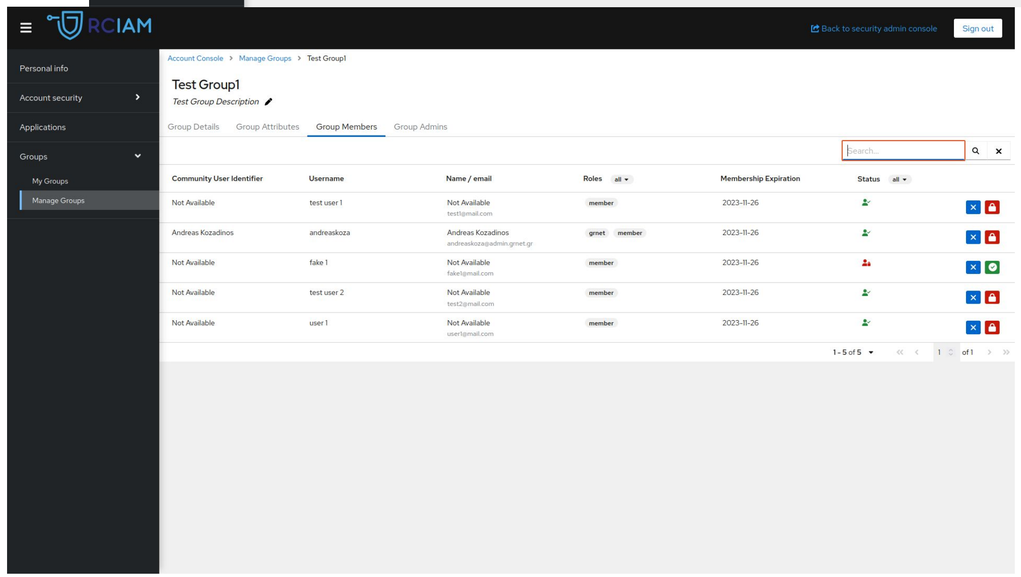
https://github.com/rciam/keycloak-group-management

- User-driven group enrollment flows:
  - Users can request membership in groups
    - Accept group Terms & Conditions
    - Provide comment/justification
  - Membership requests are reviewed by group managers
  - Multi-group enrollment flows

- Time-based group membership:
  - Automatic expiration of group membership beyond a configurable time period after joining the group
  - Membership renewal process

- Roles within groups



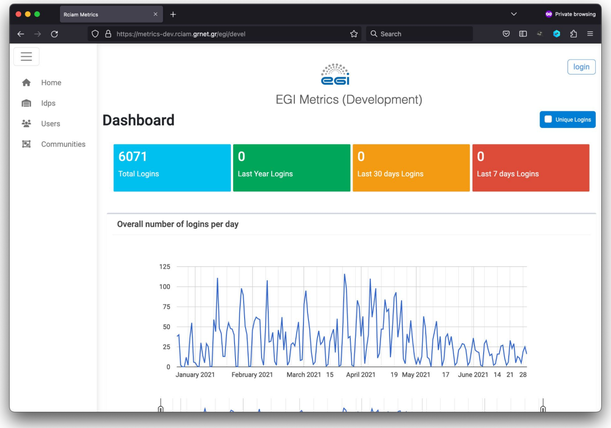


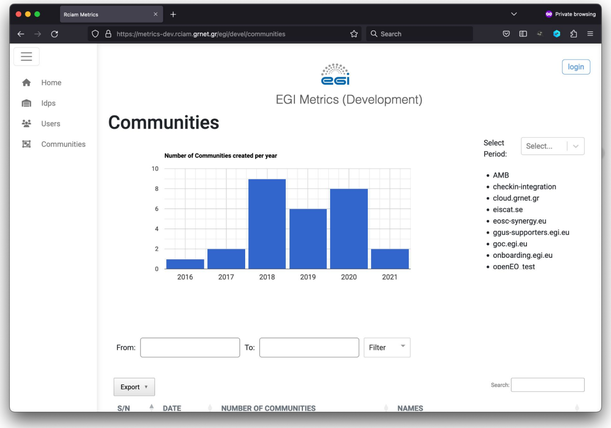
Keycloak Enhancements

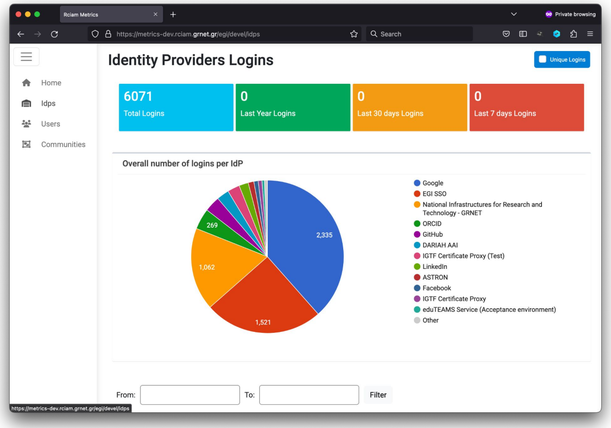
New Metrics Engine & Dashboard

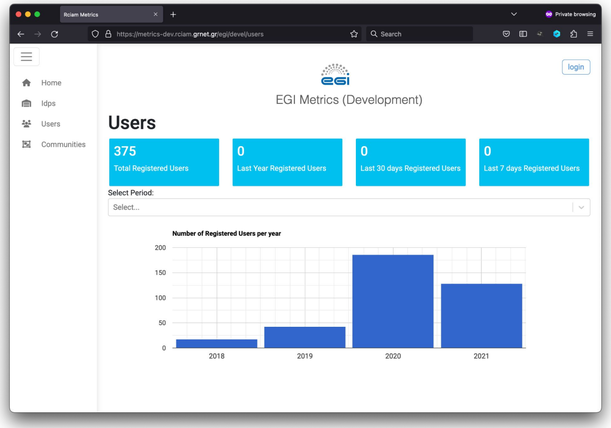
https://github.com/rciam/rciam-authmetrics

- Logins
  - Total
  - Unique
  - Per Identity Provider & Service
  - Geographic distribution
- User registrations
- Communities/groups created
  - Member status
  - Geographic distribution









Keycloak

New OpenID Connect / OAuth 2.0 flows

- **Resource Indicators for OAuth 2.0** (RFC8707) for allowing clients to signal to the authorization server where they intend to use the access token using the **`"resource"`** parameter
- **Remote OAuth 2.0 Proxied Token Introspection** from trusted external Authorization Servers (AARC-G052)
- Scope-based mechanism for allowing clients to **request specific Claim values** (e.g. to filter groups/roles)
- **Scope policies** for enabling control over whether the scope (e.g. **`compute.*`**) should be included in the access token requested by the client
- **OpenID Connect Federation** (OIDCFed) (PoC implementation)

Keycloak

Roadmap

Metrics	Advanced Group Management	OpenID Connect Federation	Self-Sovereign Identities (SSI)
Q3 2023	*Q4 2023*	*Q4 2023*	*Q1 2024*

What's next

- Extend Federation Registry:
  - Improve registration process for Resource Providers
  - Improve registration process for Client Credentials clients → **Service accounts**
  - Support connection / reconfiguration of:
    - Individual Identity Providers
    - IdP/SP Federations
- Support **OpenID Connect Federation** (OIDCFed) (PoC implementation)

Thank you

Nicolas Liampotis

nliam@grnet.gr | check-in@egi.eu

www.egi.eu

This work is partially funded by the EU research and innovation programme