

GRNET Introduction + SYNTHESYS+ AAI with Check-In

Kostas Koumantaros (GRNET)

GRNET: Greek Research and Technology Network



- Is the Greek Research and Education Network (NREN) and e-infrastructure provider for research and academia.
- We utilize state-of-the-art networking technologies to offer advanced, high-speed interconnection services to the Greek research and education community.
- We undertake initiatives for creating e-infrastructures and services that can facilitate organizing, describing and promoting digital content of educational, research, geospatial, environmental and cultural topics.
- We provide innovative public IaaS cloud services
- We are member of GEANT association, EGI Foundation, EUDAT CDI and PRACE
- We supply the Federated Authorisation and Authentication solutions for EOSC Portal, EOSC-HUB, EGI Federation, OpenAIRE, OpenMinTeD & VI-SEEM

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>

What benefits does Check-in bring?



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

Creates a **Unique Persistent Identifier** for All Users that allows for better integration of Service 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)

Identity linking enables access to resources using different login credentials (institutional/social)

Assurance information associated to each authenticated identity

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

Check-in Community AAI service options



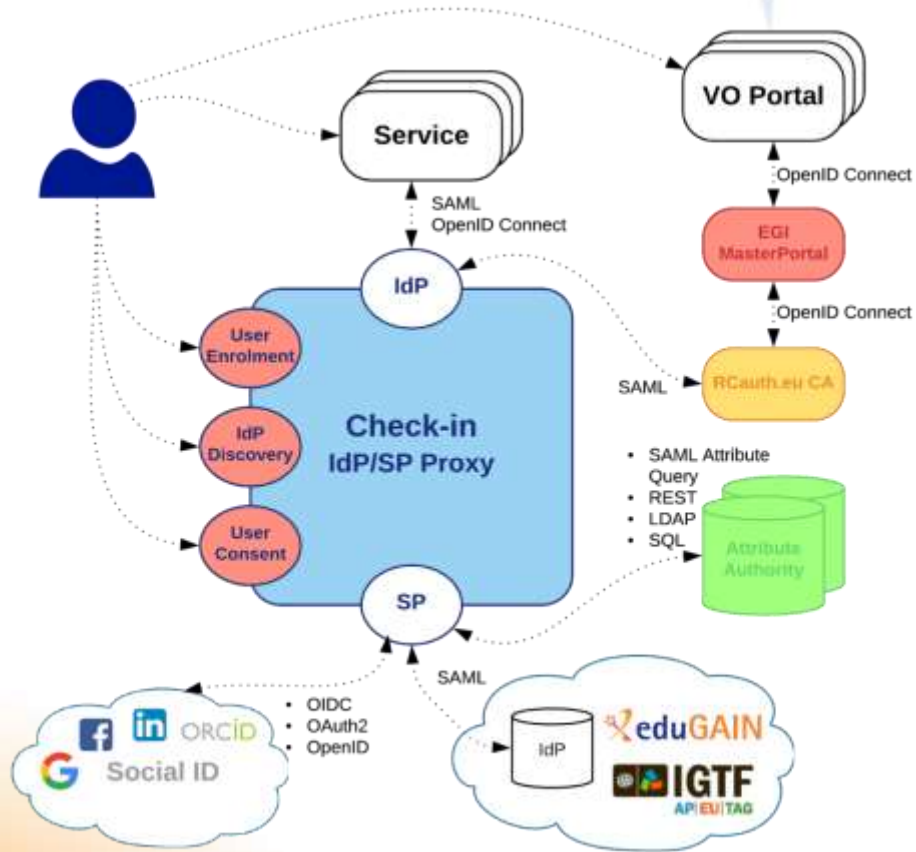
Multi-tenant service

- All the standard Check-in authentication options
- Community management using CManage or Perun
- Basic customisation of user-facing interfaces (e.g. community-specific themes for enrolment flows, group management)
- Basic customisation of AAI proxy behavior

Dedicated service (individual components or AAI service as a whole)

- Customisation of user-facing interfaces: WAYF, enrolment, group membership UI
- Customisation of AAI proxy behaviour (e.g. attribute aggregation rules, service entitlements/capabilities)
- Integration with the EOSC-hub AAI e-Infrastructure SP Proxies for accessing EOSC services and resources

IdP/SP Proxy

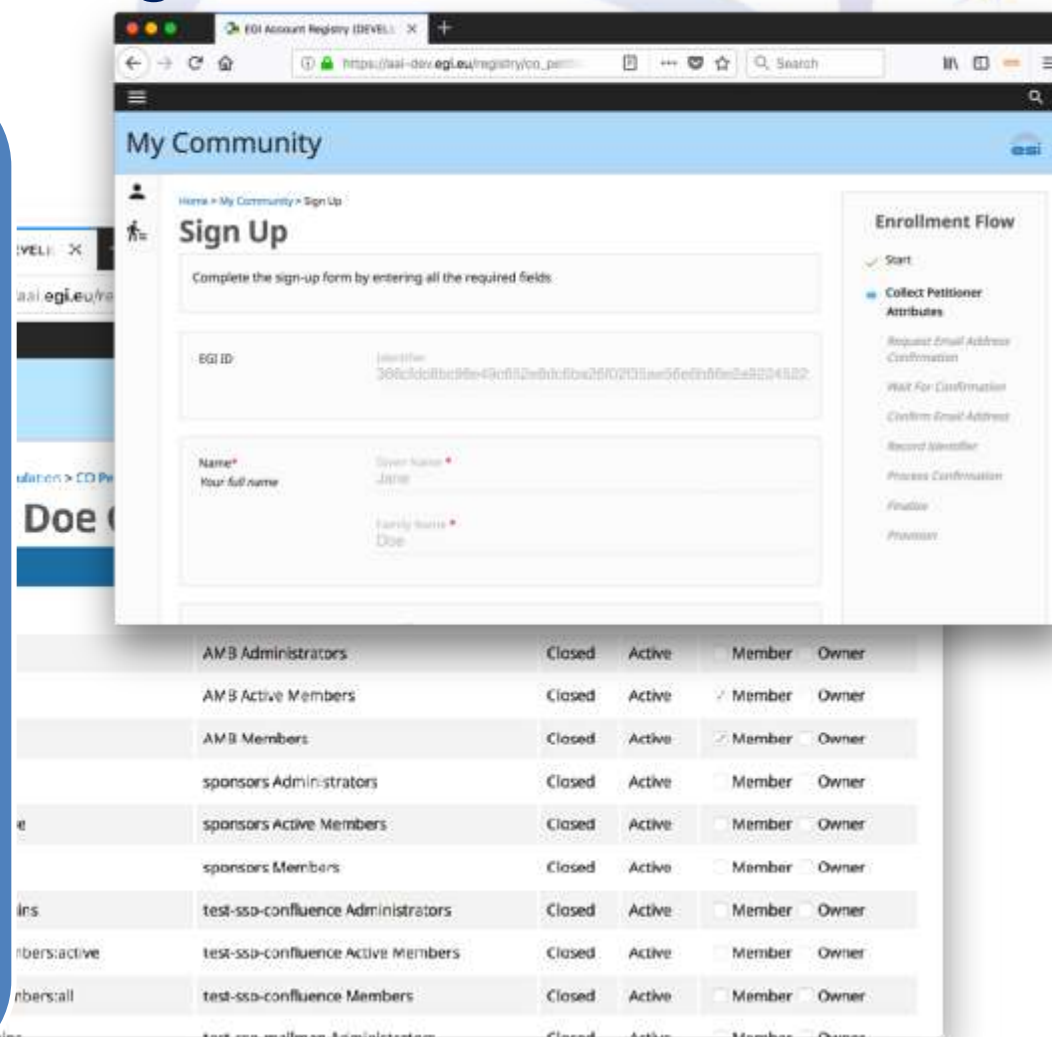


- Implementation of the AARC blueprint architecture
- Registered in eduGAIN as an SP complying with REFEDS Research & Scholarship and Sirtfi
- All community SPs can have one statically configured IdP
- No need to run an IdP Discovery Service on each community SP
- Connected SPs get consistent/harmonised user identifiers and accompanying attribute sets from different IdPs/AAs that can be interpreted in a uniform way for authorisation purposes

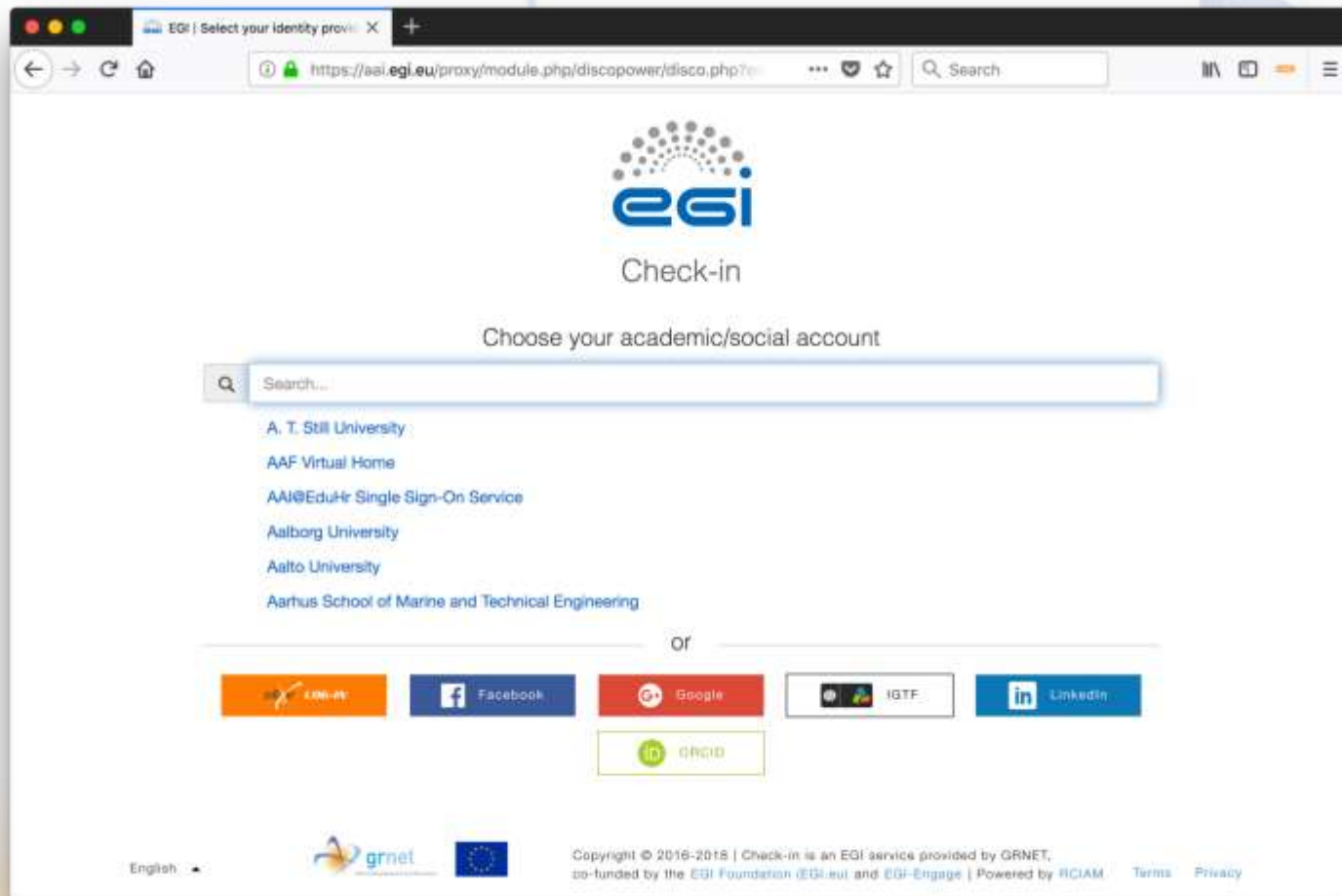
User enrolment & group management



- Ability to create enrolment flows specific to a community's requirements
- Support for organizing users in hierarchical groups
- Ability to associate certificate and ssh key information to researcher's federated identity
- Ability to enrich researcher's identity with community-specific attributes
- Direct (de)provisioning of information into an LDAP directory or VOMS

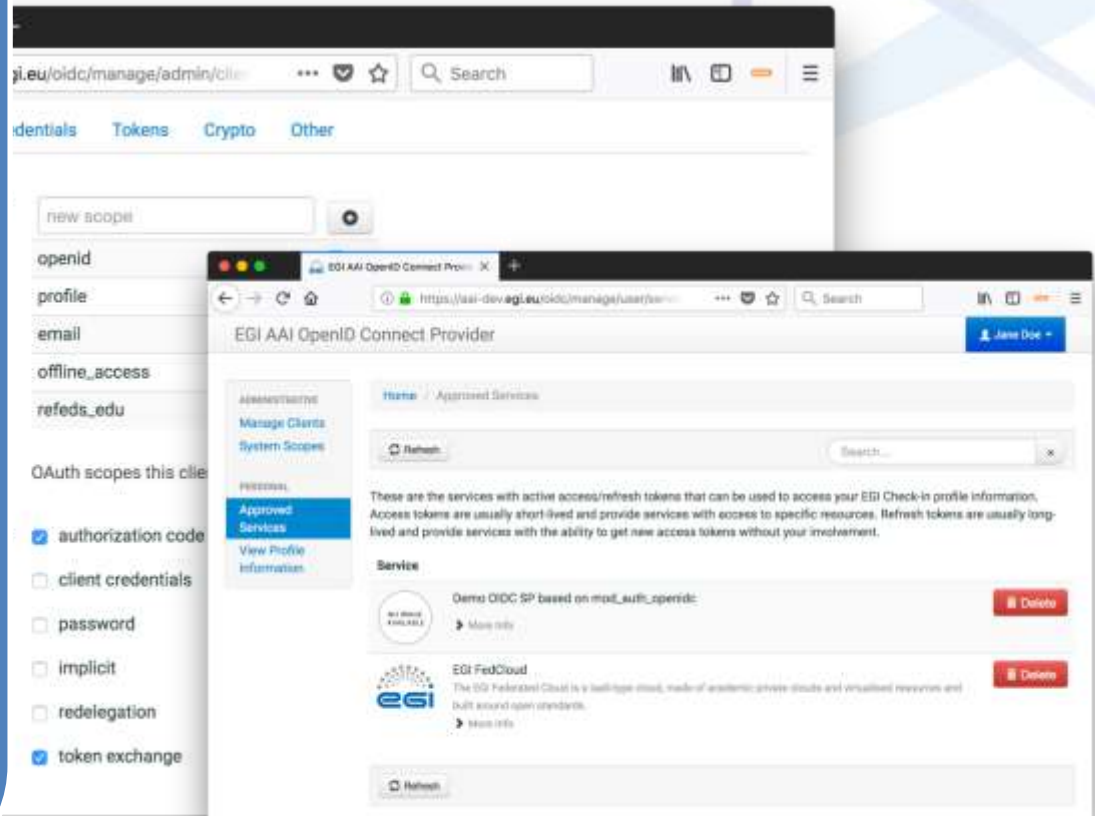


IdP Discovery



Non-web use cases & delegated access via OpenID Connect/OAuth 2.0

- Friendly UI for managing/testing OpenID Connect/OAuth 2.0 clients
- Provides overview of OpenID Connect/OAuth 2.0 services authorised to access their identity
- Allows users to see the specific permissions (e.g. read email, offline access, etc.) granted to each service
- Enables users to manage access/refresh tokens associated with each service:
 - ⑩ Revoke access for individual tokens or service as a whole
 - ⑩ Retrieve access/refresh tokens to be used for federated access to CLI tools/APIs
- Multipath delegation via OAuth 2.0 Token Exchange (*)
 - ⑩ Support for attenuation of rights/scopes



Authorisation

- Supports authorisation decisions based on the combination of different types of information:
 - **identity attributes** asserted by the IdP of the user's home organisation;
 - **VO/group membership and role** information aggregated from one or more community-managed attribute authorities;
 - **assurance** information associated with the authenticated identity
- Provides two types of attributes/claims that can be used by SPs to control access to resources:
 - Entitlements expressing:
 - rights/capabilities of the user to access specific services/resources, or
 - VO/group membership and role information in support of group- and/or role-based access control by SPs
 - Attributes carrying assurance information can be used by SPs to decide how much to trust the assertions made by Check-in and its attribute sources

Group membership and role information



Use of URN-formatted entitlement values based on AARC guidelines:

```
urn:mace:egi.eu:group:<group>[:<subgroup>*][:role=<role>]#<group-authority>
```

- **<group>** is the name of a VO, research collaboration or a top level arbitrary group; unique within a given <namespace>
- optional list of **<subgroup>** components represents the hierarchy of subgroups in the **<group>**
- optional **<role>** component indicates particular position of the user; scoped to the rightmost (sub)group
- **<group-authority>** indicates the authoritative source for the group membership and role information

Thank you for your attention!

**For more info e-mail
faai@grnet.gr**