



Community AAI with Check-In

Matthew Viljoen, EGI Foundation

Check-In slides from Nicolas Liampotis (GRNET)



eosc-hub.eu



[@EOSC_eu](https://twitter.com/EOSC_eu)



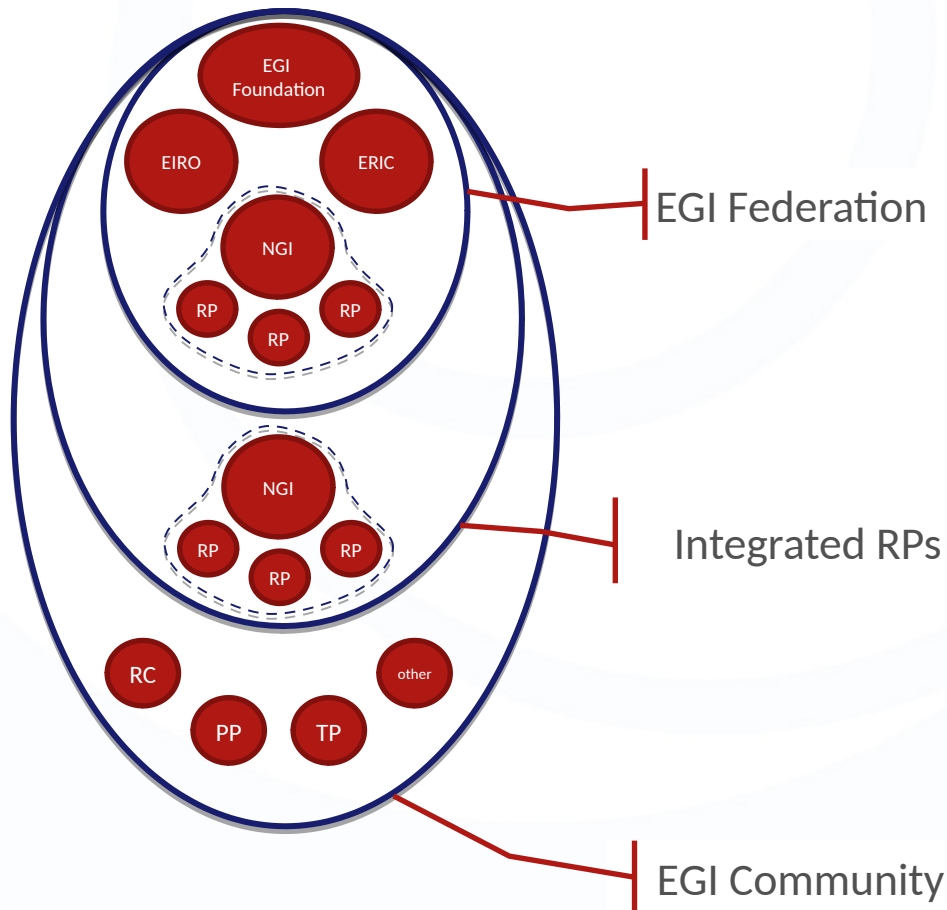
EGI is a federation of over 260 computing and data centres spread across 40+ countries in Europe and worldwide

EGI delivers services to support researchers, international projects, research infrastructures and

47 Countries	61,000 users industry	22,000 Publications
12 Integrated e-Infrastructures	31 large-scale research collaborations	11 Business cases



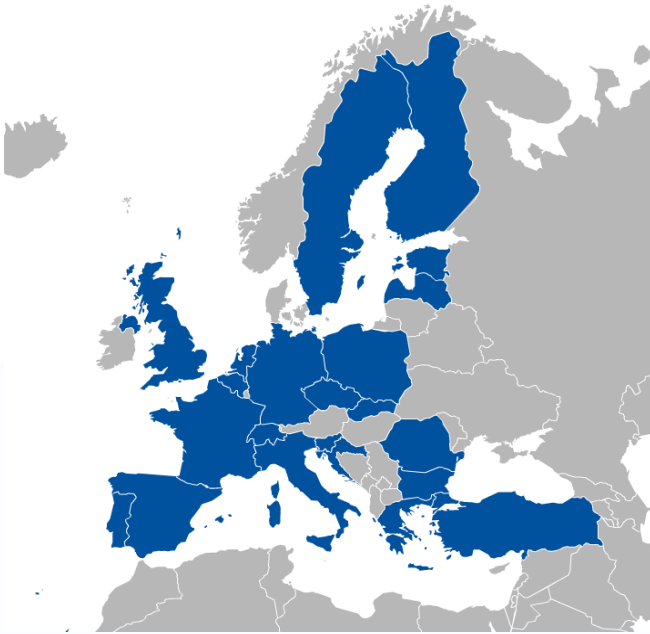
EGI - Some relevant terms



Term	Definition
EGI Foundation	The legal entity whose objective is to coordinate and develop, in collaboration with its Participants, an e-infrastructure that provides distributed compute and storage resources for performing research and innovation activities
EGI Federation	EGI Foundation, EGI Foundation Participants and Associated Participants, their linked organisations (e.g. service and resource providers) represented within EGI Foundation that contribute to the objectives of the foundation
EGI Infrastructure	The federated e-infrastructure composed national and intergovernmental computing and data centres from the EGI federation providing advanced computing services for research and innovation
EGI Community	EGI Federation plus the served research communities (RC), the technology providers (TP), partners in projects (PP) and all other organisations having agreements with EGI.eu
EGI	Can be used as a short version of "EGI Infrastructure" or "EGI Federation"

GI Foundation - Participants

- 22 Countries
- 1 EIRO: **CERN**



www.egi.eu/about/egi-foundation/





EGI - A global system of e-Infrastructures

Africa-Arabia, Asia and Pacific region, China, Europe, India



Europe



China:
Institute of HEP,
Chinese Academy of Sciences



Africa and Arabia:
Council for Scientific and
Industrial Research, South Africa



Latin America:
Universida de Federal do
Rio de Janeiro



India:
Centre for Development of
Advanced Computing

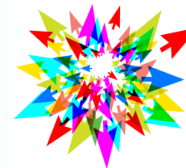


Ukraine:
Ukrainian National Grid



Open Science Grid

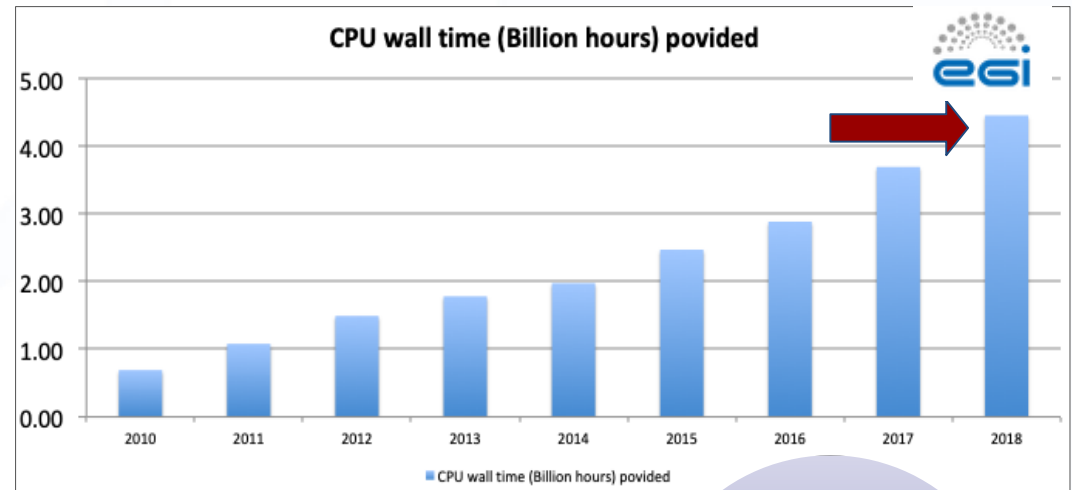
USA



compute | calcul
canada | canada

Canada

- 4.4 Billion CPU core wall time delivered in 2018
- > 1 Million computing cores for the first time in the EGI history
- 356 PB disk & 380 PB tape storage
- 1170 open access publications / year
- 31 large scale ESFRI projects/landmarks supported



+20%
utilization
of
computing
in 2018

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?

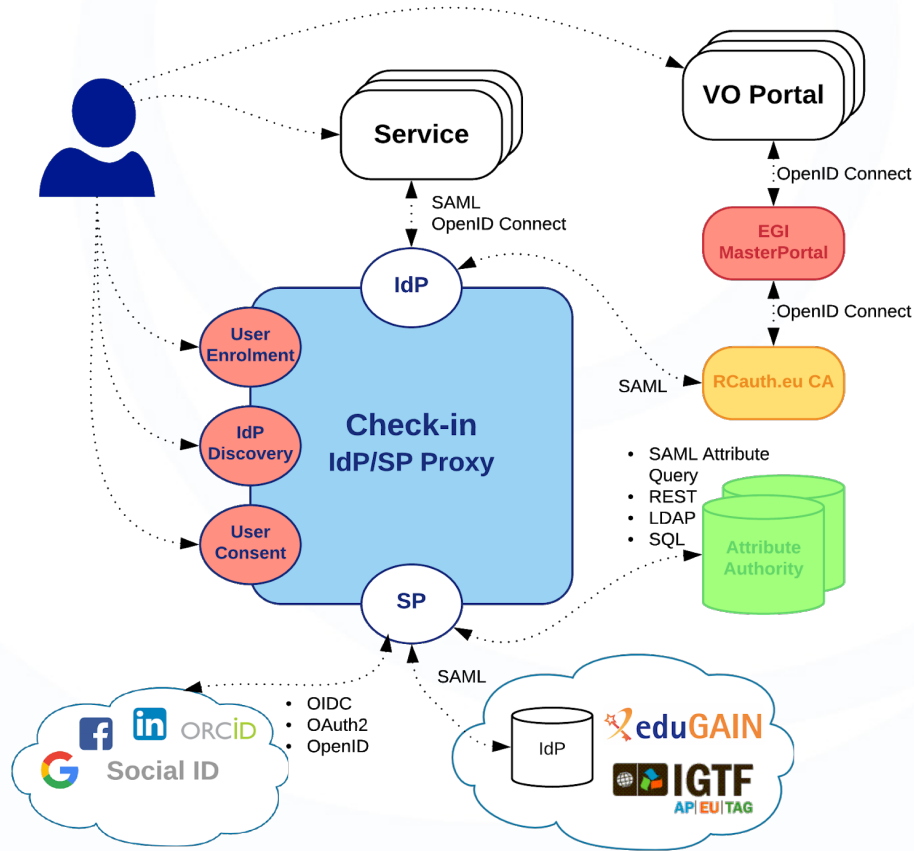
Single sign-on to services through eduGAIN, social media and other institutional or community-managed identity providers

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)

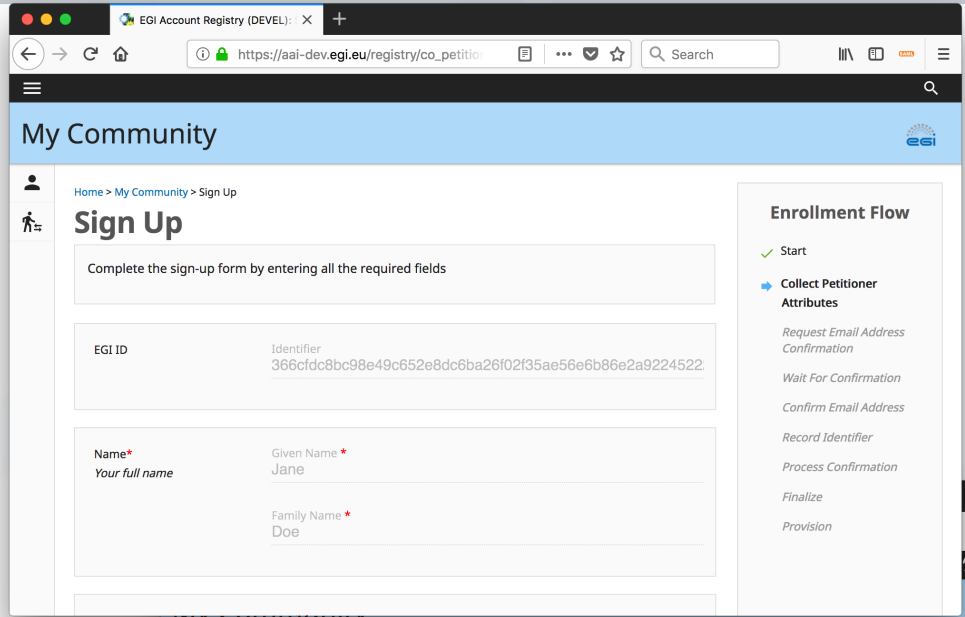
Assurance information associated to each authenticated identity

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

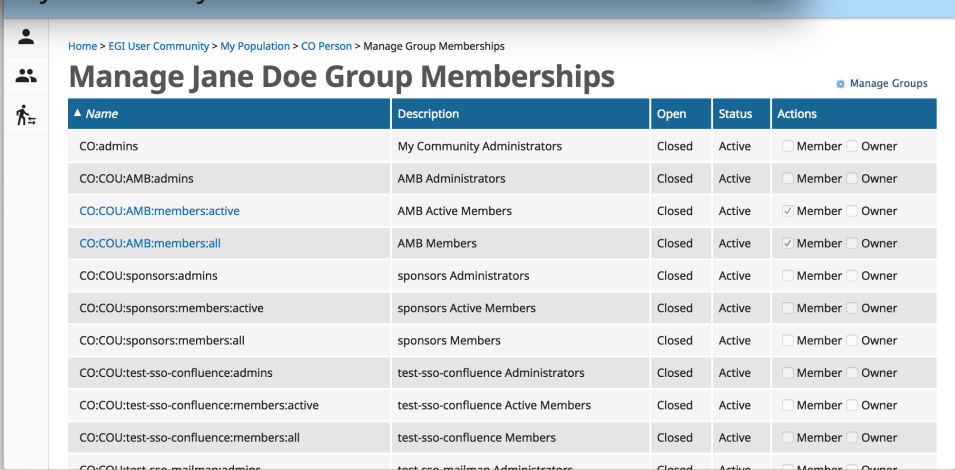


- Implementation of the AARC blueprint architecture
- Registered in eduGAIN as an SP complying with REFEDS Research & Scholarship and Sirtfi
- All community SPs can have one statically configured IdP
- No need to run an IdP Discovery Service on each community SP
- Connected SPs get consistent/harmonised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

- Ability to create enrolment flows specific to a community's requirements
- Support for organising 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

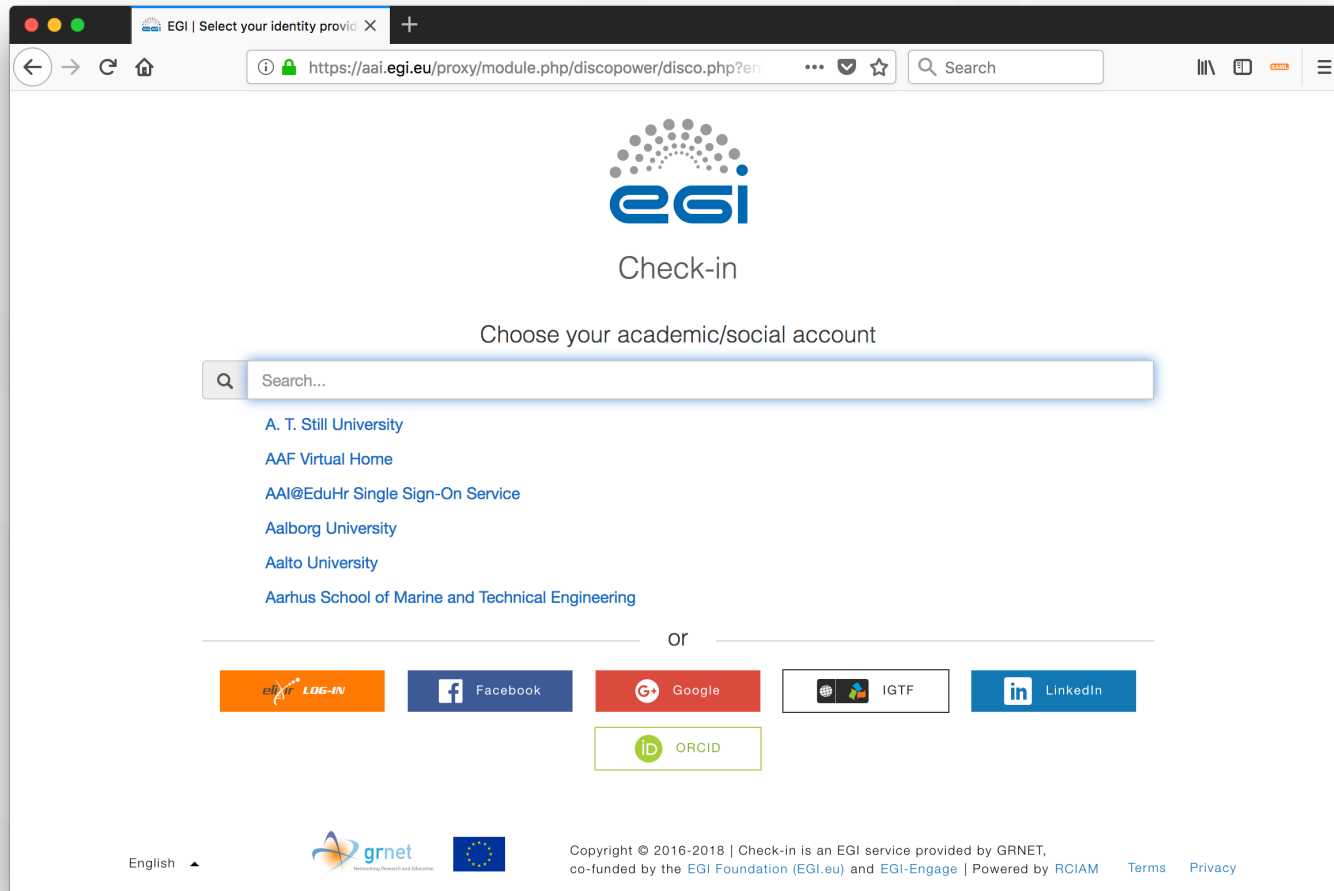


The screenshot shows the 'Sign Up' page in the EGI Account Registry. The form includes fields for EGI ID, Name (Given Name: Jane, Family Name: Doe), and an Enrollment Flow sidebar with steps: Start, Collect Petitioner Attributes, Request Email Address Confirmation, Wait For Confirmation, Confirm Email Address, Record Identifier, Process Confirmation, Finalize, and Provision.



The screenshot shows the 'Manage Jane Doe Group Memberships' page. The table lists various group memberships with columns for Name, Description, Open, Status, and Actions.

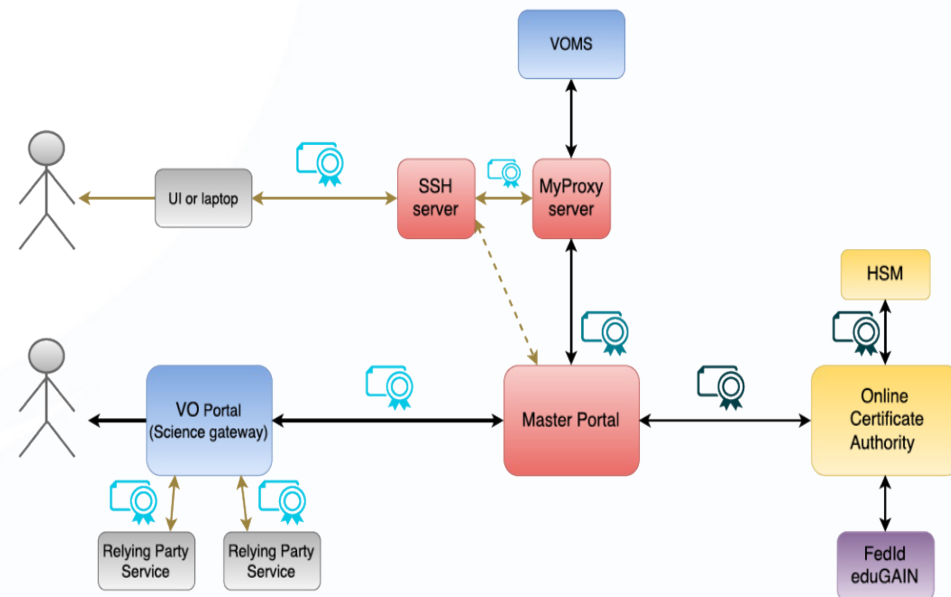
Name	Description	Open	Status	Actions
CO:admins	My Community Administrators	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:AMB:admins	AMB Administrators	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:AMB:members:active	AMB Active Members	Closed	Active	<input checked="" type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:AMB:members:all	AMB Members	Closed	Active	<input checked="" type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:sponsors:admins	sponsors Administrators	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:sponsors:members:active	sponsors Active Members	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:sponsors:members:all	sponsors Members	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:test-sso-confluence:admins	test-sso-confluence Administrators	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:test-sso-confluence:members:active	test-sso-confluence Active Members	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:test-sso-confluence:members:all	test-sso-confluence Members	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:test-sso-mailman:admins	test-sso-mailman Administrators	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner



The screenshot shows a web browser window with the URL `https://aai.egi.eu/proxy/module.php/discopower/disco.php?en`. The page features the EGI logo and the text "Check-in" and "Choose your academic/social account". A search bar contains the text "Search...". Below the search bar, a list of institutions is displayed: A. T. Still University, AAF Virtual Home, AAI@EduHr Single Sign-On Service, Aalborg University, Aalto University, and Aarhus School of Marine and Technical Engineering. Below this list, the word "or" is centered. A row of social login buttons includes EGI LOG-IN, Facebook, Google, IGTF, and LinkedIn. Below these buttons is an ORCID button. At the bottom of the page, there is a footer with the text "English", logos for GRNET and the European Union, and copyright information: "Copyright © 2016-2018 | Check-in is an EGI service provided by GRNET, co-funded by the EGI Foundation (EGI.eu) and EGI-Engage | Powered by RCIAM Terms Privacy".

- Check-in has been integrated with the production RAuth.eu Online CA
 - Users can retrieve X.509 proxies by authenticating through Check-in

- Check-in Master Portal retrieves end-entity certificate from RAuth.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



- 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

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

- Complete attribute and policy harmonisation activities:
 - Affiliation within Home Organisation/Research Infrastructure
 - REFEDS/AARC Assurance Framework
 - SAML-to-OIDC mapping
 - AUP alignment
- Complete integration activities with other EOSC-hub AAI solutions
- Add support for more (de)provisioning options (e.g. SCIM)
- Add support for active role selection

**Thank you for
your attention!**

nliam@grnet.gr



EOOSC-hub

 eosc-hub.eu  [@EOOSC_eu](https://twitter.com/EOOSC_eu)

Multi-tenant service

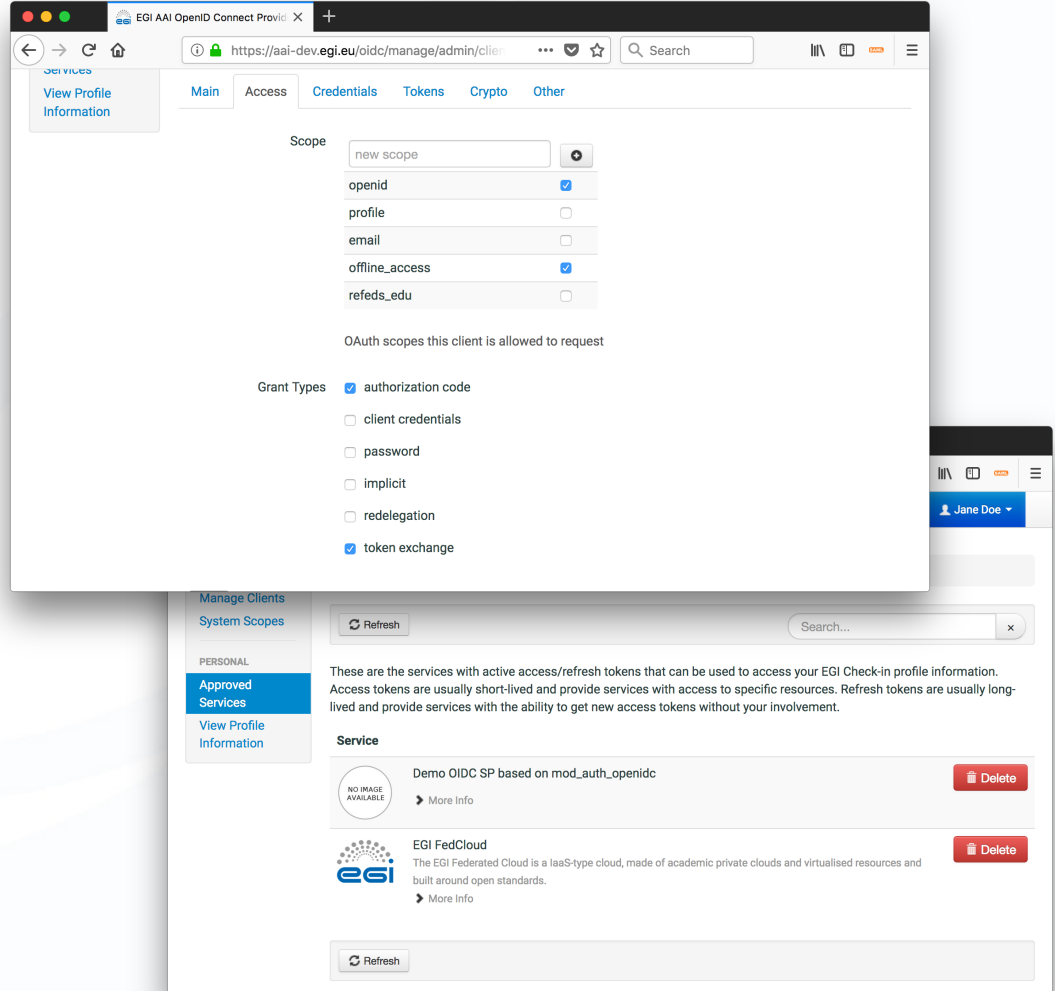
- All the standard Check-in authentication options
- Community management using COmanage or Perun
- Basic customisation of user-facing interfaces (e.g. community-specific themes for enrolment flows, group management)
- Basic customisation of AAI proxy behavior

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

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:
 - Revoke access for individual tokens or service as a whole
 - Retrieve access/refresh tokens to be used for federated access to CLI tools/APIs
- Multipath delegation via OAuth 2.0 Token Exchange (*)
 - Support for attenuation of rights/scopes



The screenshot displays the EGI AAI OpenID Connect Provider administration interface. The top window shows the 'Access' tab for a client, with a 'Scope' section containing checkboxes for 'openid', 'profile', 'email', 'offline_access', and 'refeds_edu'. Below this is the 'OAuth scopes this client is allowed to request' section with 'Grant Types' including 'authorization code', 'client credentials', 'password', 'implicit', 'redelegation', and 'token exchange'. The bottom window shows the 'Manage Clients' section with a search bar and a list of services with active access/refresh tokens, including 'Demo OIDC SP based on mod_auth_openidc' and 'EGI FedCloud'.