



Authentication and Authorisation for Research and Collaboration

WLCG AAI Pilot Update

EGI Check-in

Nicolas Liampotis

GRNET



Pre-GDB - Authz Working Group, CERN

2018-07-17

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

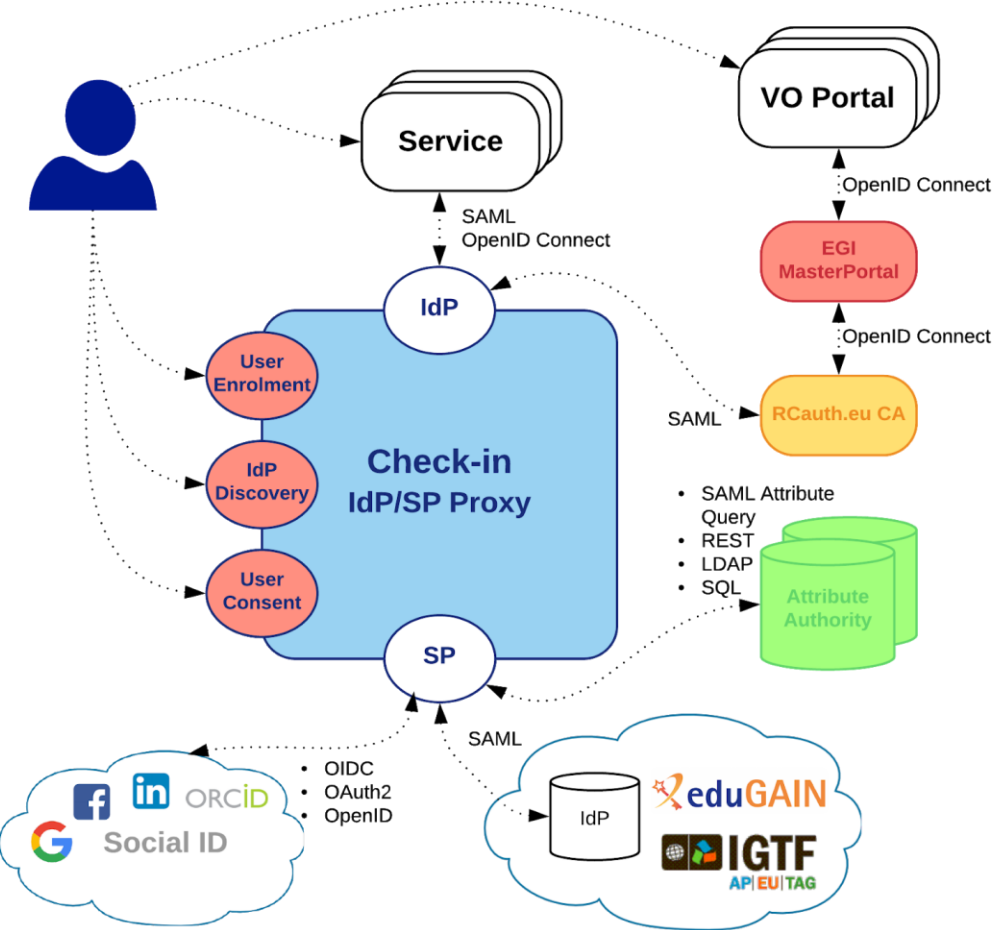
Only one account needed for federated access to multiple heterogeneous (web and non-web) service providers using different technologies (SAML, OpenID Connect, OAuth 2.0, X509)

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

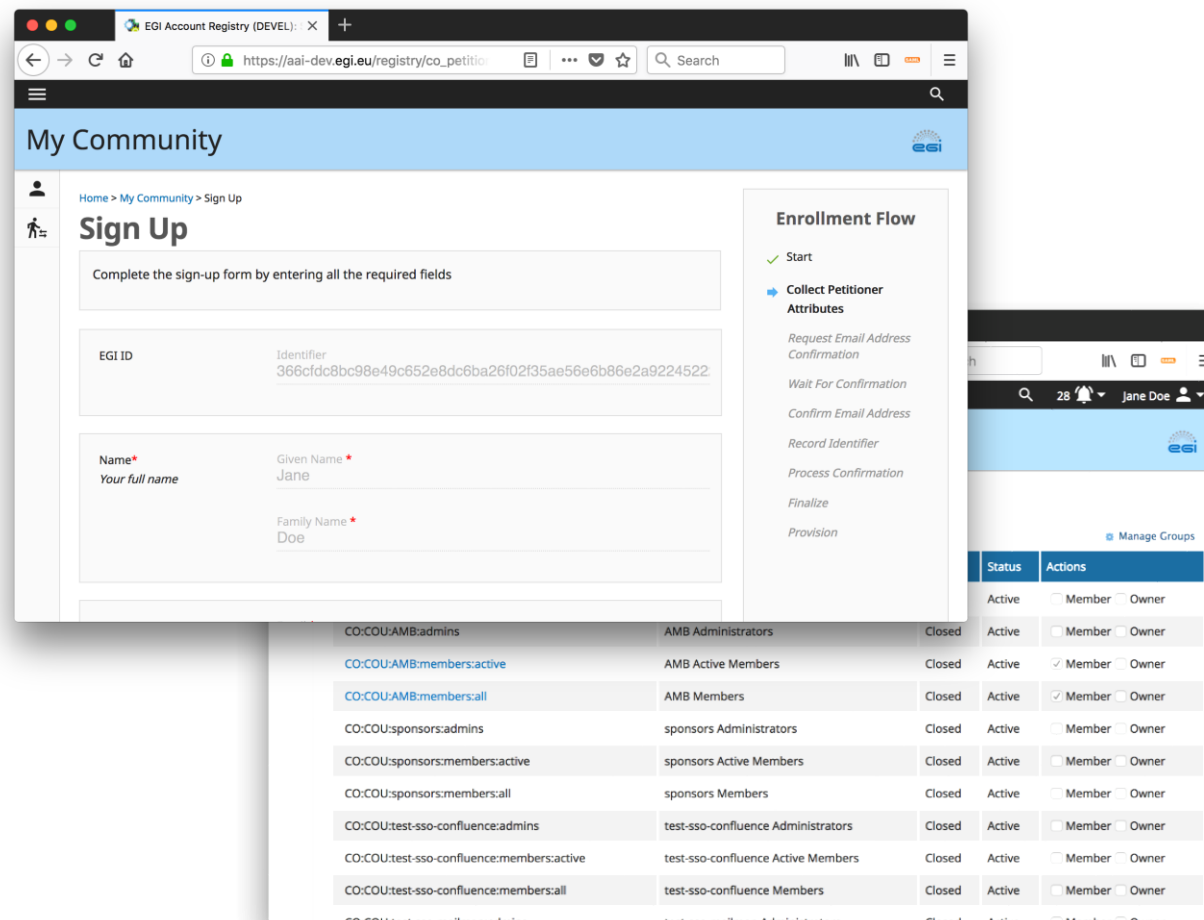
High-level architecture



- 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 with Comanage Registry

- Ability to create enrolment flows specific to a community's requirements
- Support for organising users in hierarchical COUs/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 (spoiler alert: and VOMS!)



The screenshot displays the EGI Account Registry (DEVEL) web interface. The main content area shows a 'Sign Up' form with the following fields:

- EGI ID:** Identifier: 366cfdc8bc98e49c652e8dc6ba26f02f35ae56e6b86e2a9224522
- Name:** Given Name: Jane, Family Name: DOE

The 'Enrollment Flow' sidebar on the right lists the following steps:

- Start
- Collect Petitioner Attributes (active)
- Request Email Address Confirmation
- Wait For Confirmation
- Confirm Email Address
- Record Identifier
- Process Confirmation
- Finalize
- Provision

Below the form, there is a 'Manage Groups' section with a table showing various groups and their status.

Status	Actions
Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input checked="" type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input checked="" type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner
Closed	Active <input type="checkbox"/> Member <input type="checkbox"/> Owner

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
 - 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

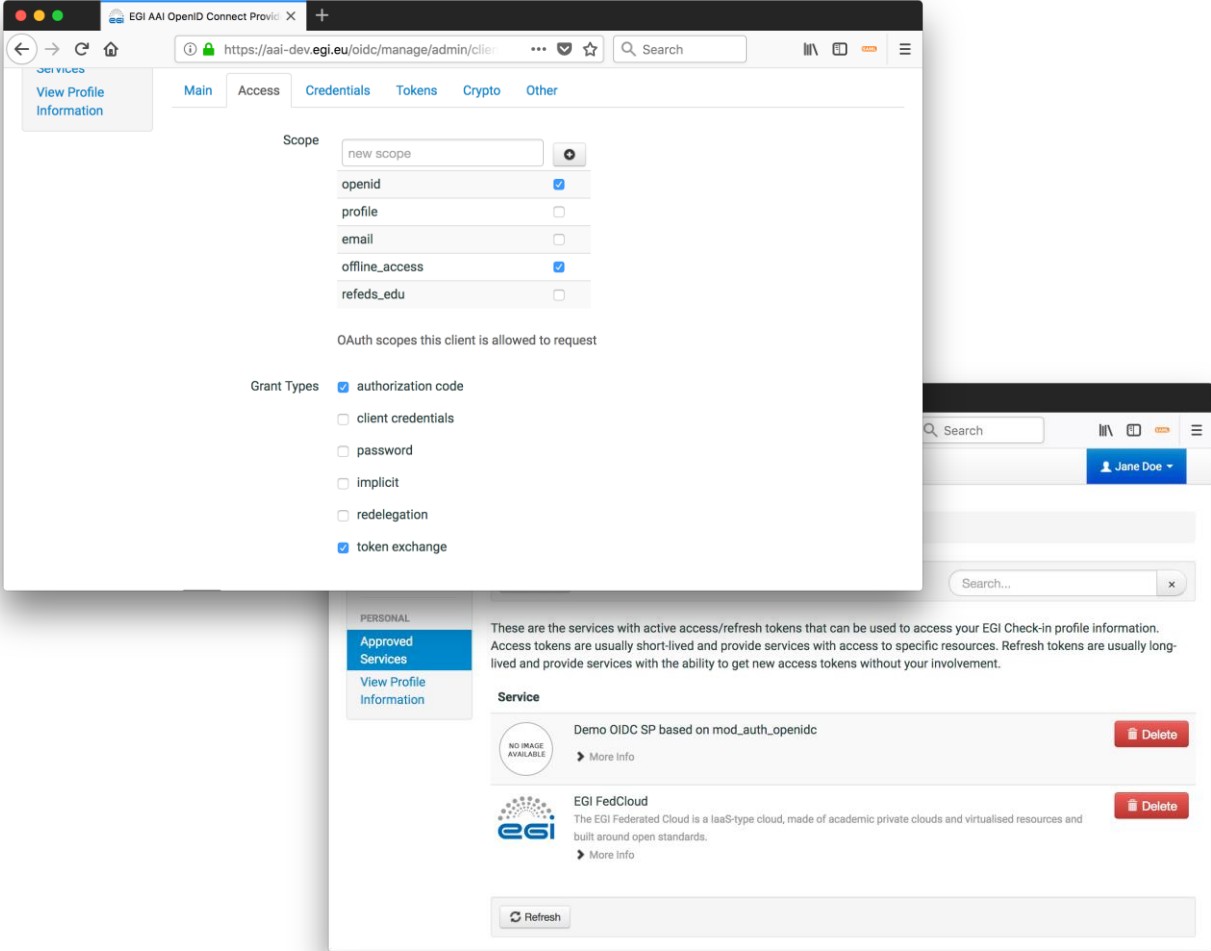
Use of URN-formatted entitlement values based on AARC guidelines:

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

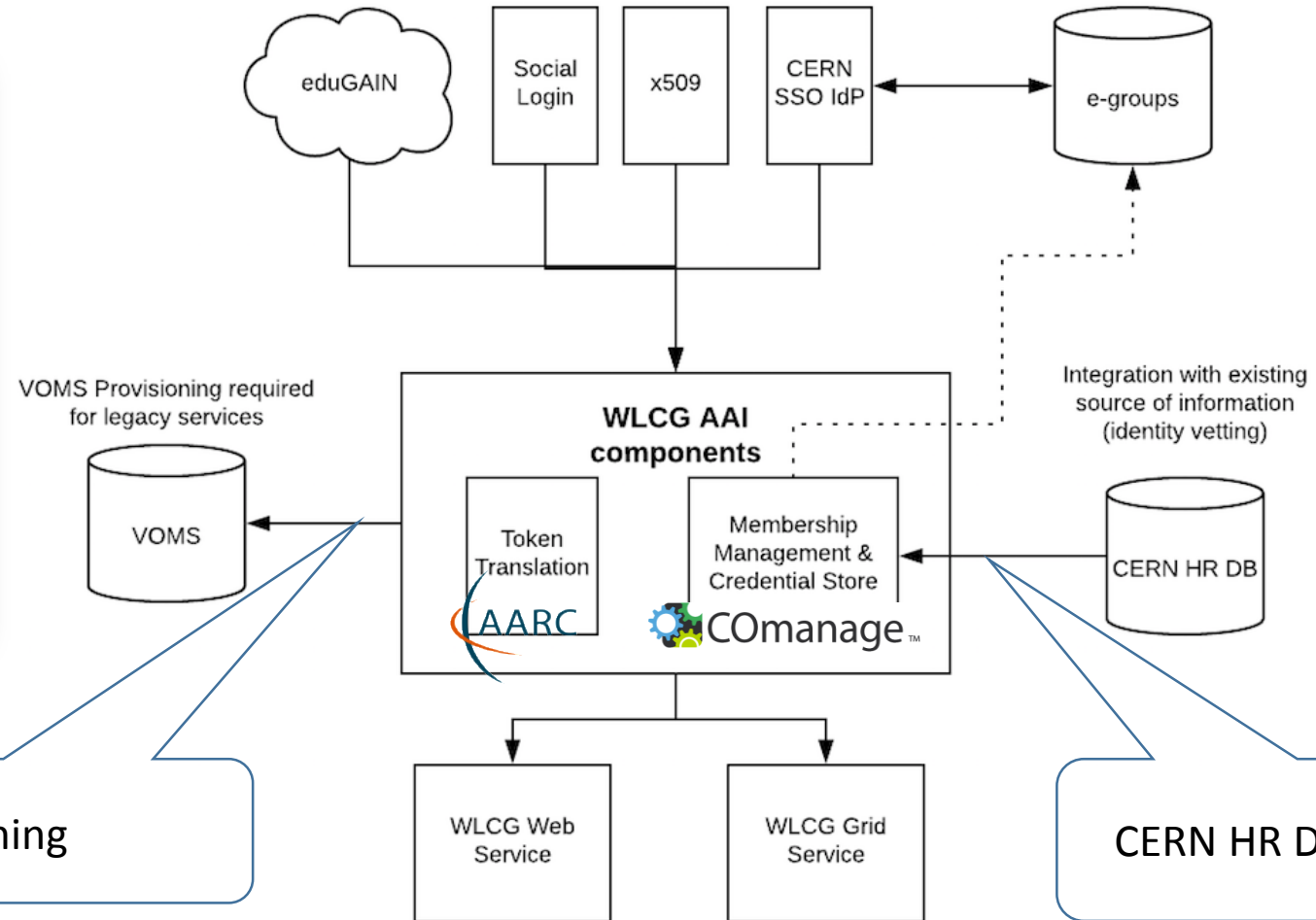
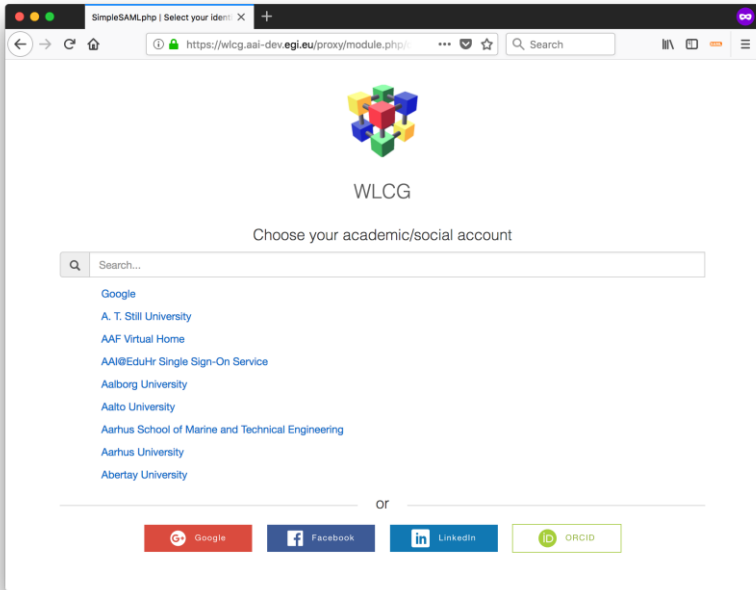
- **<group>** is the name of a VO, research collaboration or a top level arbitrary group; unique within a given <namespace>
- optional list of **<subgroup>** components represents the hierarchy of subgroups in the <group>
- optional **<role>** component indicates particular position of the user; scoped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

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



WLCG AAI Pilot Status

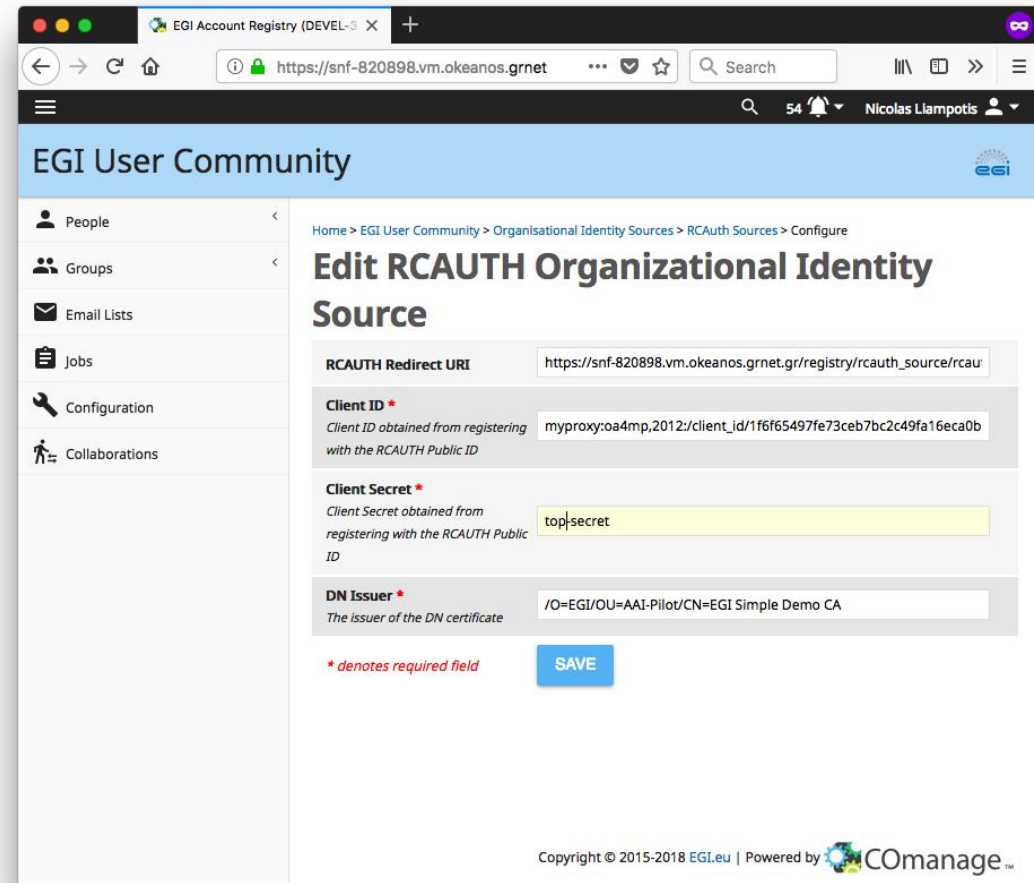


Filling in the missing pieces

VOMS Provisioning: RCauth plugin

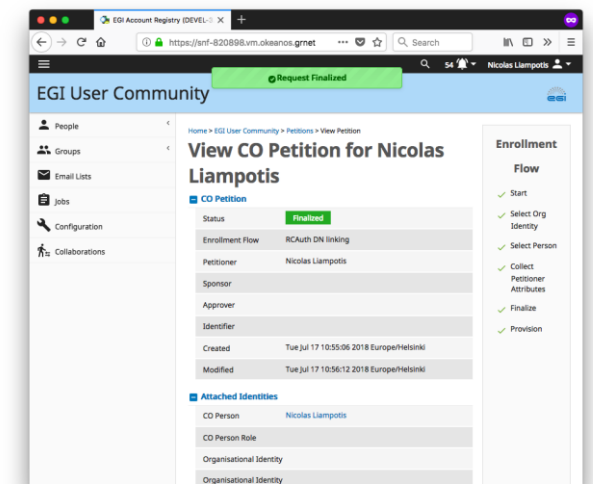
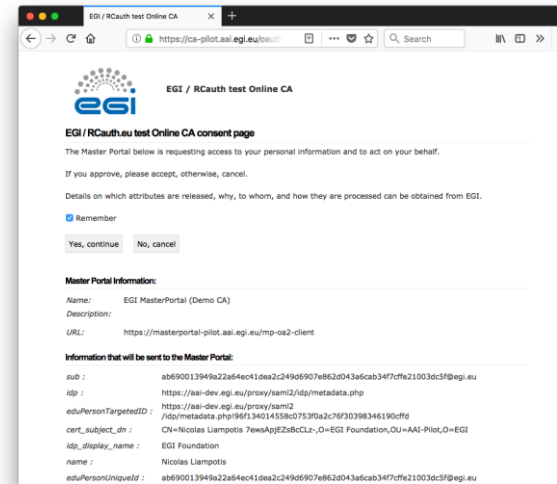
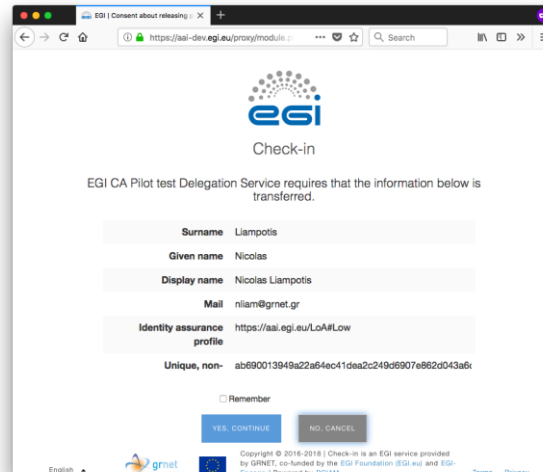
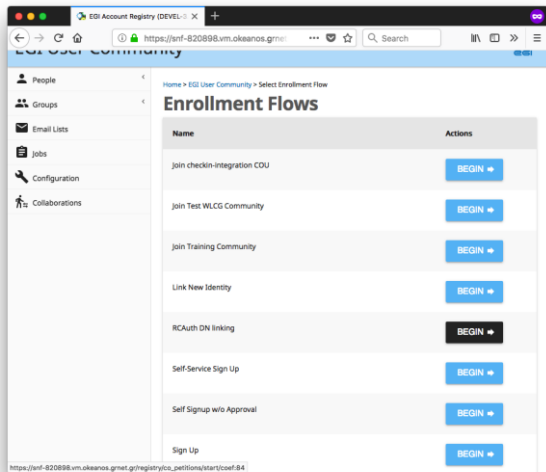
Challenge: Associate subject DN of certificate issued by RCauth to user profile

- Solution: RCauth DN linking plugin for Comanage
 - Implemented as CManage Organisational Identity Source
 - Integrated as an OIDC client to the MasterPortal



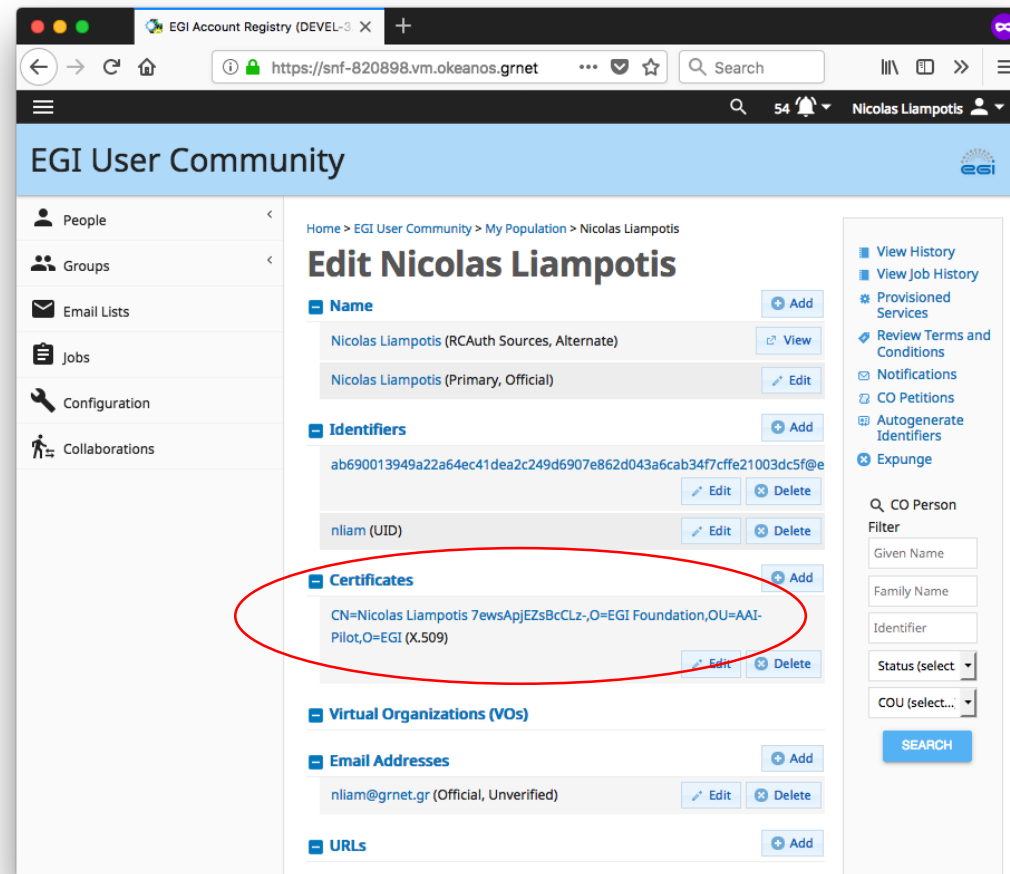
Filling in the missing pieces

VOMS Provisioning: RCauth plugin



Filling in the missing pieces

VOMS Provisioning: RCauth plugin



The screenshot shows the EGI User Community interface for editing the profile of Nicolas Liampotis. The browser address bar indicates the URL is <https://snf-B20898.vm.okeanos.grnet>. The page title is "EGI User Community".

The main content area is titled "Edit Nicolas Liampotis" and includes the following sections:

- Name:** Nicolas Liampotis (RCAuth Sources, Alternate) [View], Nicolas Liampotis (Primary, Official) [Edit]
- Identifiers:** ab690013949a22a64ec41dea2c249d6907e862d043a6cab34f7cffe21003dc5f@e [Edit] [Delete], nliam (UID) [Edit] [Delete]
- Certificates:** CN=Nicolas Liampotis 7ewsApjEZsBcCLz-,O=EGI Foundation,OU=AAI-Pilot,O=EGI (X.509) [Edit] [Delete] (This section is circled in red)
- Virtual Organizations (VOs):**
- Email Addresses:** nliam@grnet.gr (Official, Unverified) [Edit] [Delete]
- URLs:**

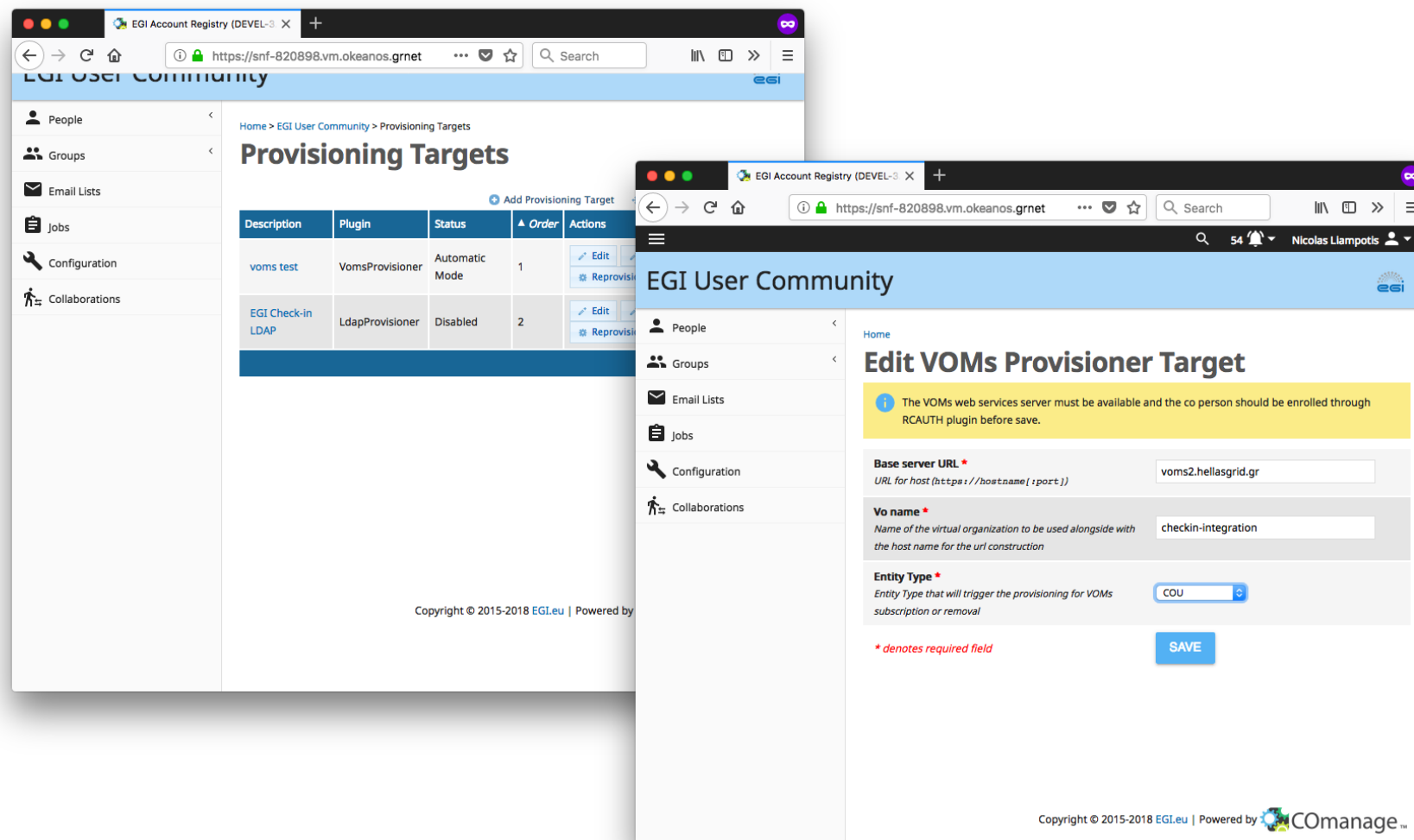
On the right side, there is a sidebar with navigation options: View History, View Job History, Provisioned Services, Review Terms and Conditions, Notifications, CO Petitions, Autogenerate Identifiers, and Expunge. Below this is a "CO Person Filter" section with input fields for Given Name, Family Name, and Identifier, and dropdown menus for Status and COU, followed by a SEARCH button.

Filling in the missing pieces

VOMS Provisioning: VOMS plugin

Challenge

- Query VOMS users
- Add/remove users to/from VOMS
- Solution: VOMS provisioning plugin for CManage
 - Implemented as CManage Provisioning plugin
 - Requires VOMS-admin access to VOMS servers



The image displays two screenshots of the EGI Account Registry (DEVELOP) web interface. The left screenshot shows the 'Provisioning Targets' page, which contains a table with the following data:

Description	Plugin	Status	Order	Actions
voms test	VomsProvisioner	Automatic Mode	1	Edit, Revisions
EGI Check-in LDAP	LdapProvisioner	Disabled	2	Edit, Revisions

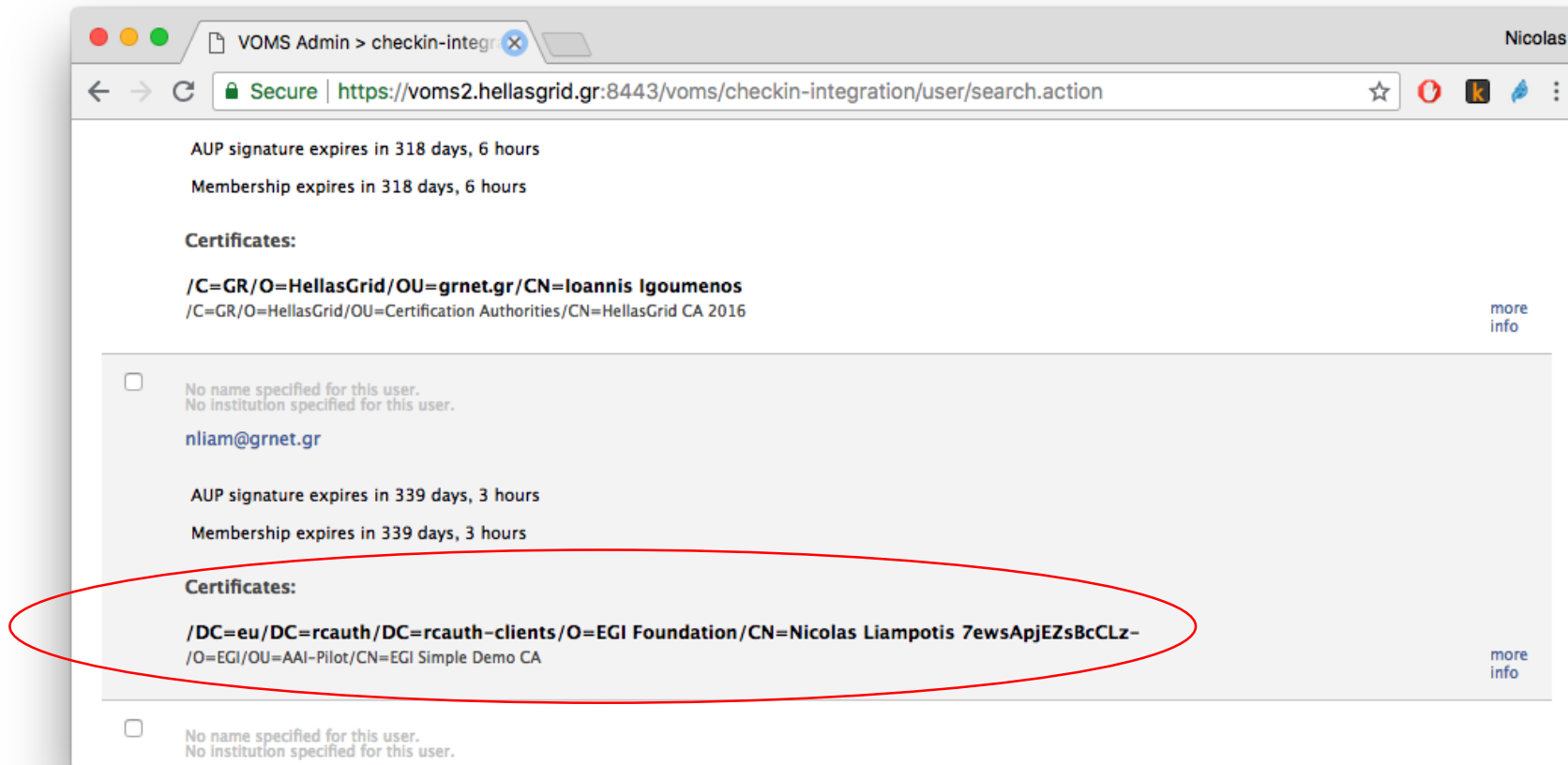
The right screenshot shows the 'Edit VOMS Provisioner Target' form. It includes a warning message: 'The VOMS web services server must be available and the co person should be enrolled through RCAUTH plugin before save.' The form fields are:

- Base server URL ***: voms2.hellasgrid.gr
- Vo name ***: checkin-integration
- Entity Type ***: COU

A 'SAVE' button is located at the bottom right of the form. The footer of both screenshots reads 'Copyright © 2015-2018 EGI.eu | Powered by CManage™'.

Filling in the missing pieces

VOMS Provisioning: VOMS plugin



VOMS Admin > checkin-integr

Secure | <https://voms2.hellasgrid.gr:8443/voms/checkin-integration/user/search.action>

AUP signature expires in 318 days, 6 hours
Membership expires in 318 days, 6 hours

Certificates:

/C=GR/O=HellasGrid/OU=grnet.gr/CN=Ioannis Igoumenos
/C=GR/O=HellasGrid/OU=Certification Authorities/CN=HellasGrid CA 2016 [more info](#)

No name specified for this user.
No institution specified for this user.
nlam@gnet.gr

AUP signature expires in 339 days, 3 hours
Membership expires in 339 days, 3 hours

Certificates:

/DC=eu/DC=rcauth/DC=rcauth-clients/O=EGI Foundation/CN=Nicolas Liampotis 7ewsApjEZsBcCLz-/O=EGI/OU=AAI-Pilot/CN=EGI Simple Demo CA [more info](#)

No name specified for this user.
No institution specified for this user.

Next steps

- Complete deployment of pilot infrastructure
 - Add support for “idphint” to improve user experience
- Refine RCauth linking/VOMS (de)provisioning workflows
 - Push plugins upstream
- Define VO enrolment flows
- Integrate with CERN HR DB (deferred for Sept?)
- Add support for active role selection

Thank you Any Questions?

nliam@grnet.gr



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).