www.egi.eu
@EGI_eInfra

Authentication and Authorisation Infrastructure Training: Identity management with Check-in VO management with COmanage

Nicolas Liampotis (GRNET)
Nick Evangelou (GRNET)

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

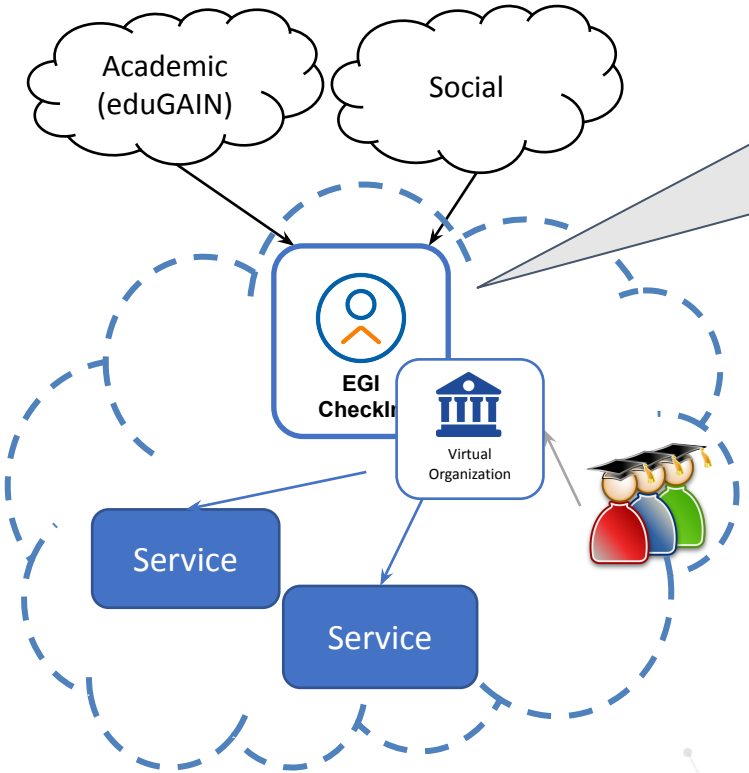
Outline

- Introduction
- User Identity Management with EGI Check-in
  - Sign-up
  - Profile view
  - Identity linking
- Virtual Organization (VO) Management with COmanage Registry
  - VO enrollment flows
  - VO group membership & role management
  - VO statistics
  - VO membership API
  - LDAP Access to VO membership information

Authentication & Authorisation

The big picture

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance



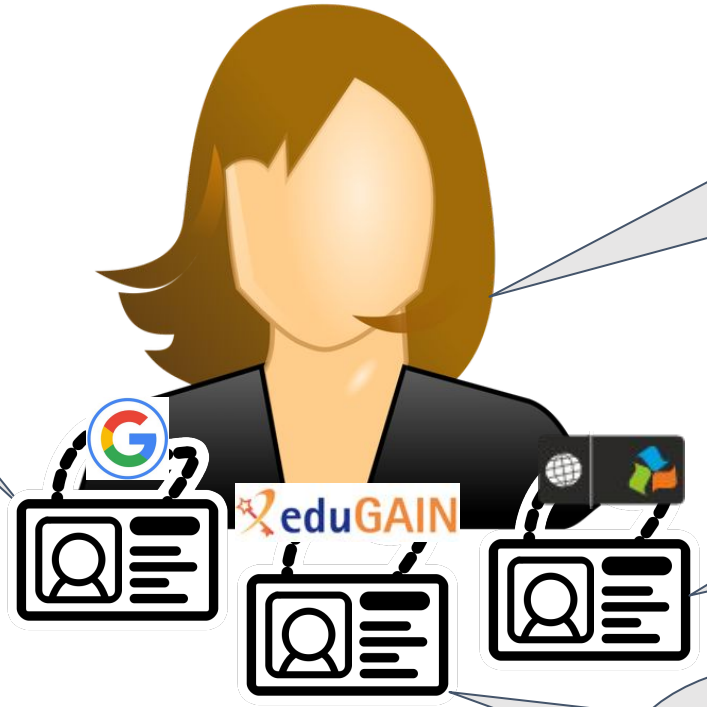
- Unique Check-in identifier → linked to one or more HO identities
- Assurance
- VO/group membership & roles
- Capabilities
- Site/service roles (GOCDB)

HO	Home Organisation
VO	Virtual Organisation

Authentication & Authorisation

Identity attributes

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance



- Unique Check-in identifier → linked to one or more HO identities
- Assurance
- VO/group membership & roles
- Capabilities
- Site/service roles (GOCDB)

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance

HO	Home Organisation
VO	Virtual Organisation

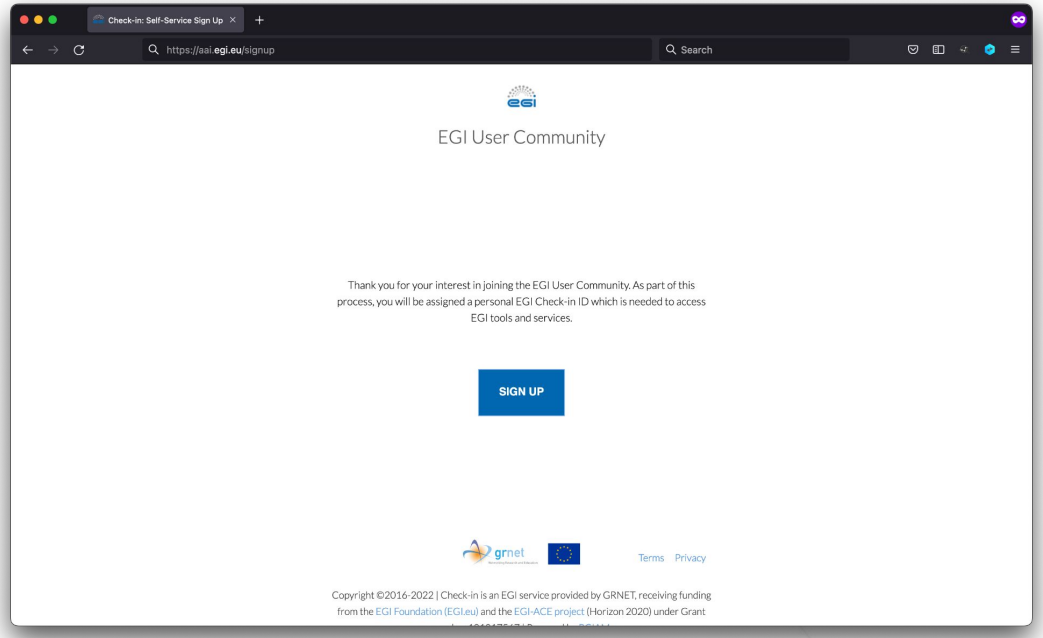
User Identity Management with EGI Check-in

User Sign-up

Accessing resources protected by EGI Check-in requires signing up using your existing academic/social account

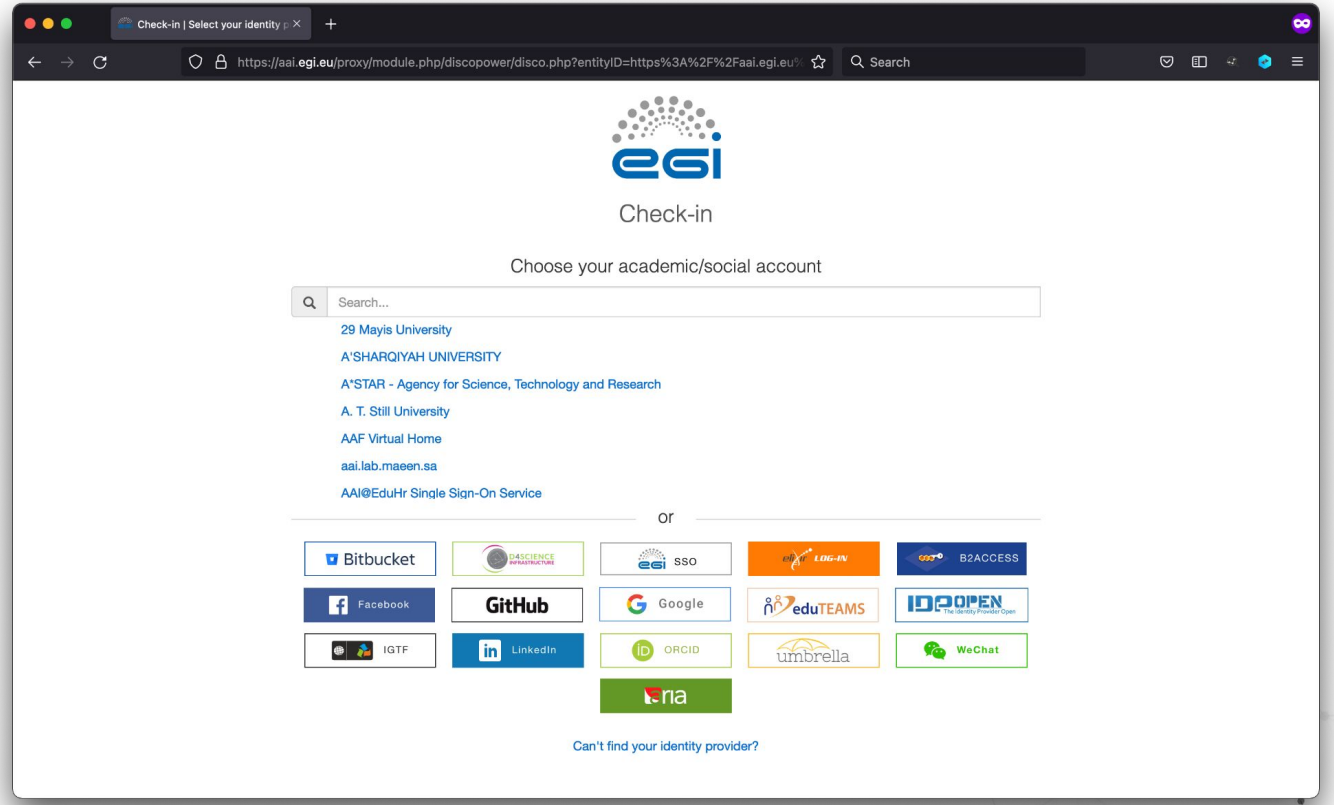
➔ *Try me!*

https://aai-demo.egi.eu/signup



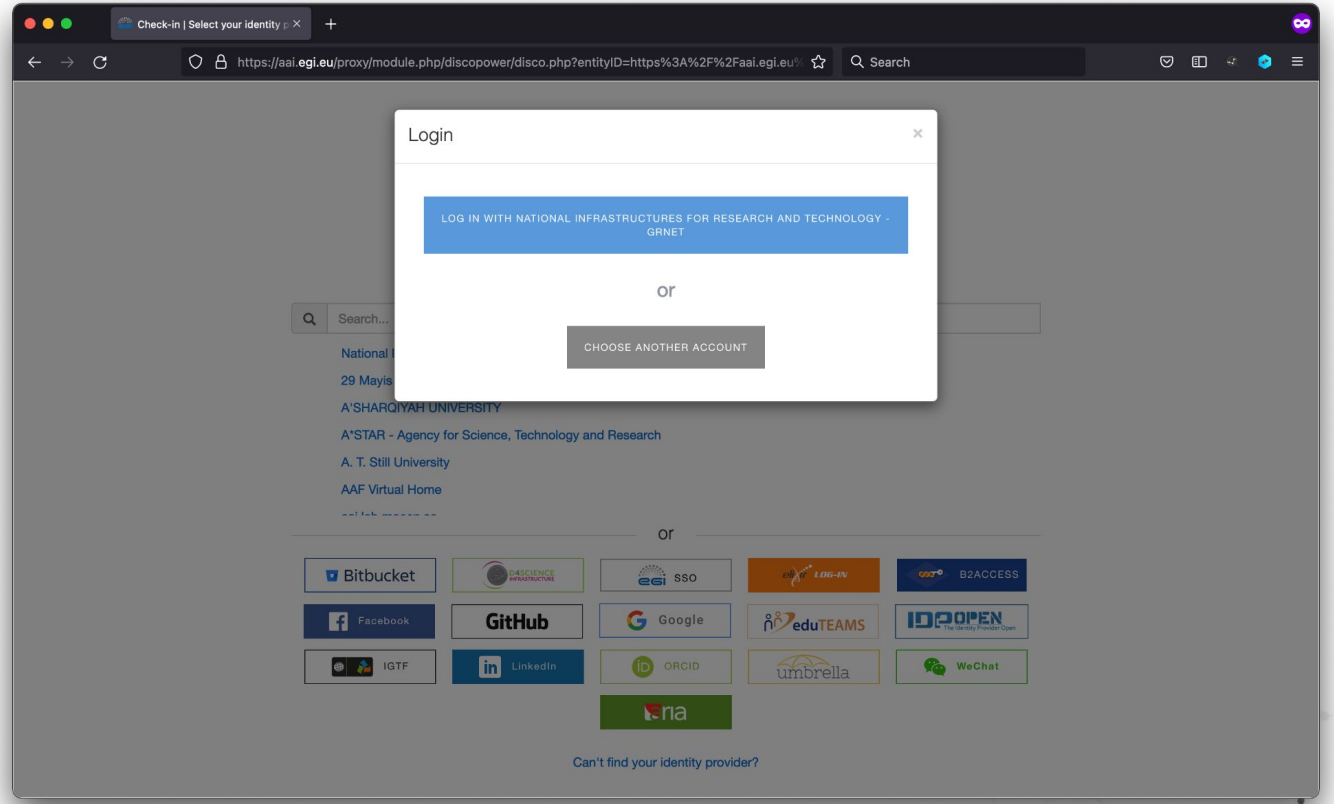
User Sign-up | Login

Identity Provider Discovery



User Login

Identity Provider Discovery

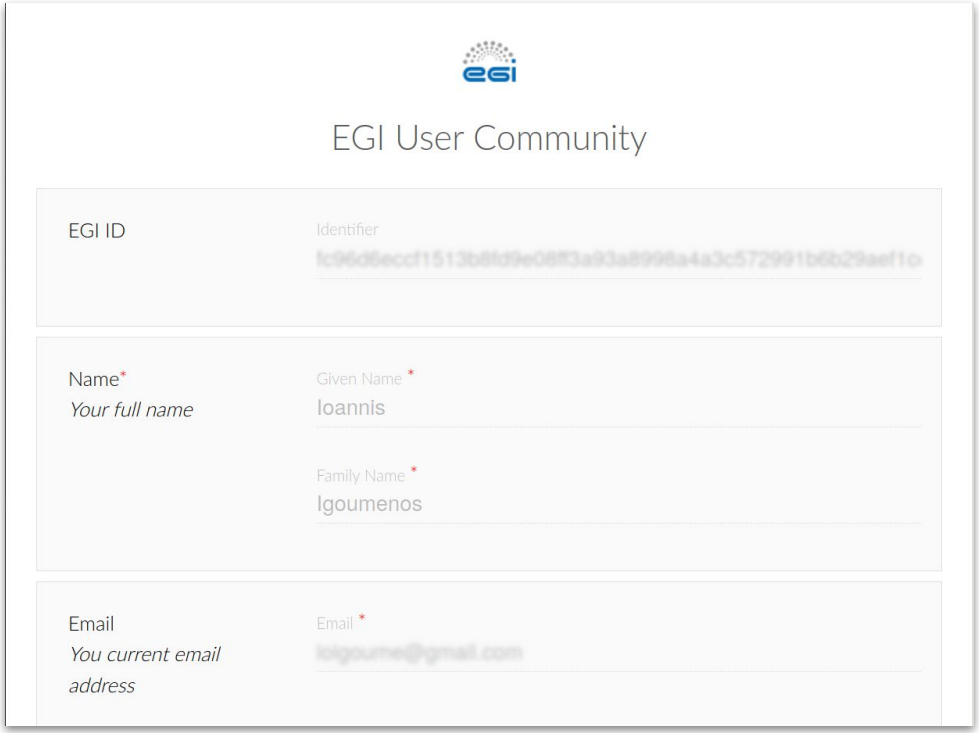


User Sign-up

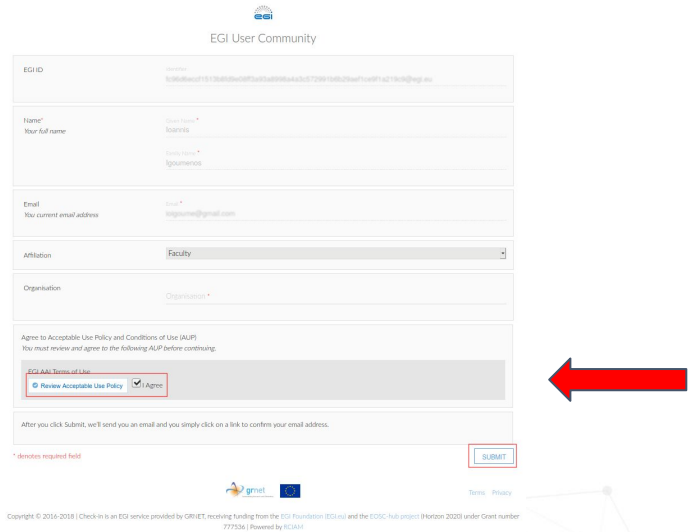
Step 1	Step 2	Access
Review user profile information ● name ● email ● affiliation and agree to Acceptable Use Policy (AUP)	Verify email address - *only if a verified email address is not released by the user's authenticating identity provider*	Gain *authorised* access to resources

User Sign-up

Step 1 - Review



- ✓ Review profile information
- ✓ Agree to AUP

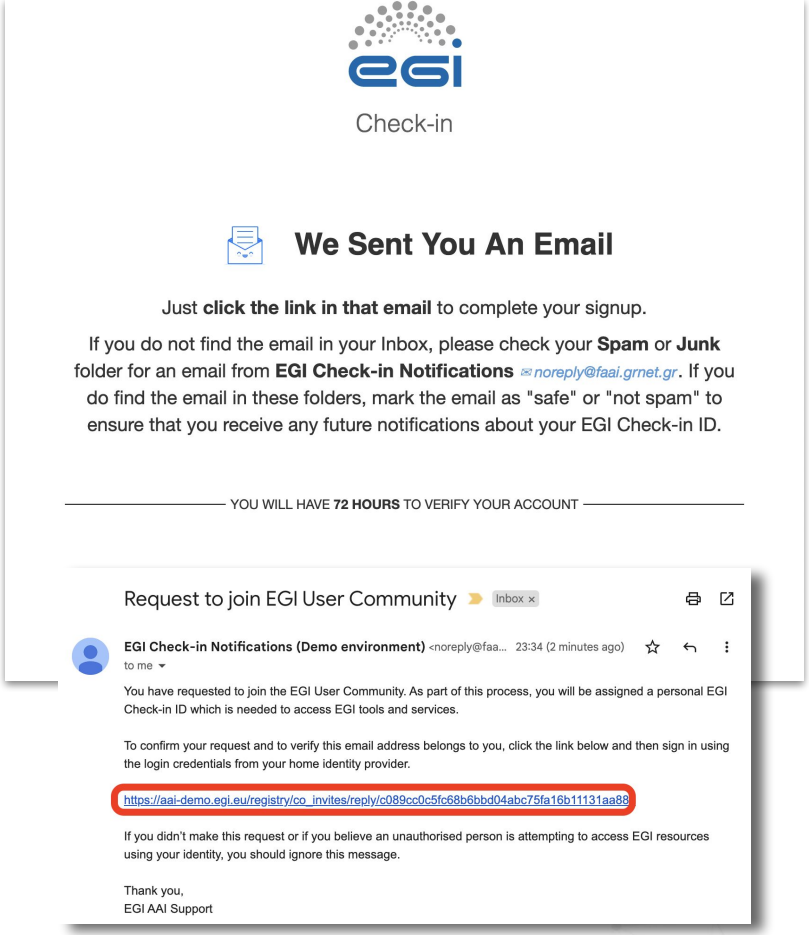


User Sign-up

Step 2

Next, you will need to confirm your email address. Check your inbox and open the link on your browser.

This step is SKIPPED in case of an email known to be verified by the Identity Provider

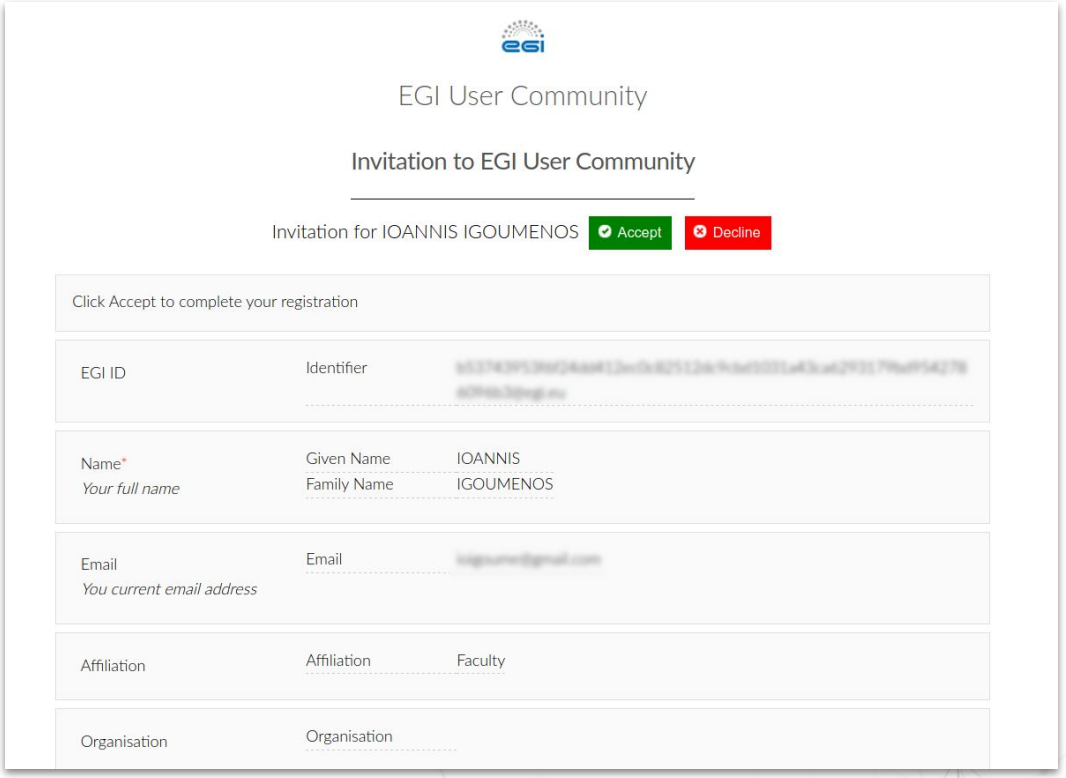


User Sign-up

Step 2 - Verify email

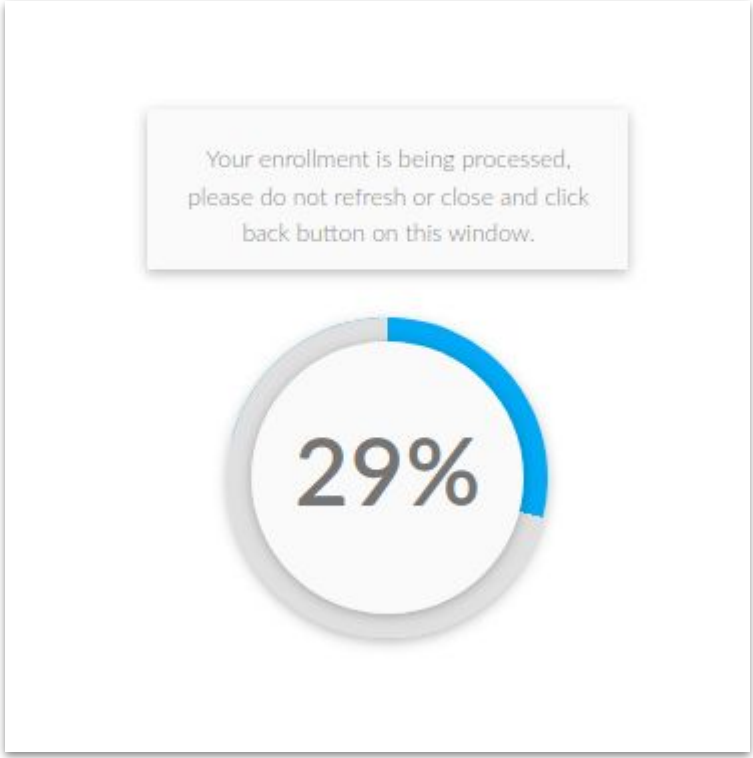
Click on “Accept” to finalise the registration.

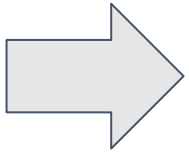
This step is SKIPPED in case of an email known to be verified by the Identity Provider

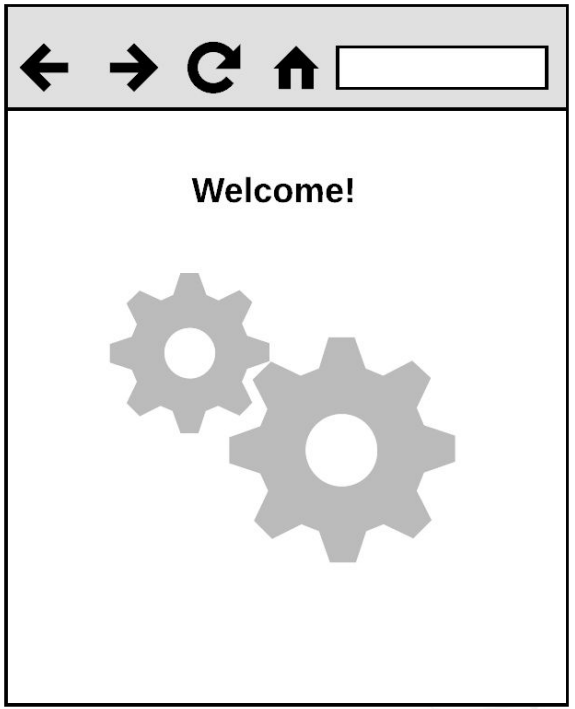


User Sign-up

Access resources

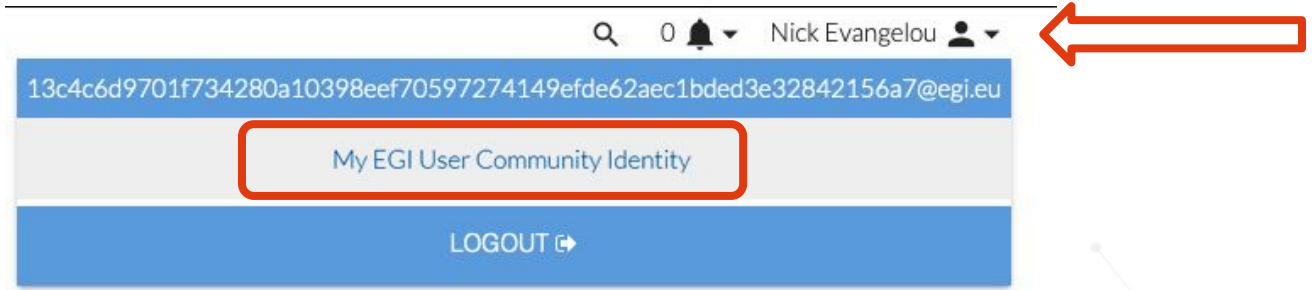






Check-in Profile View

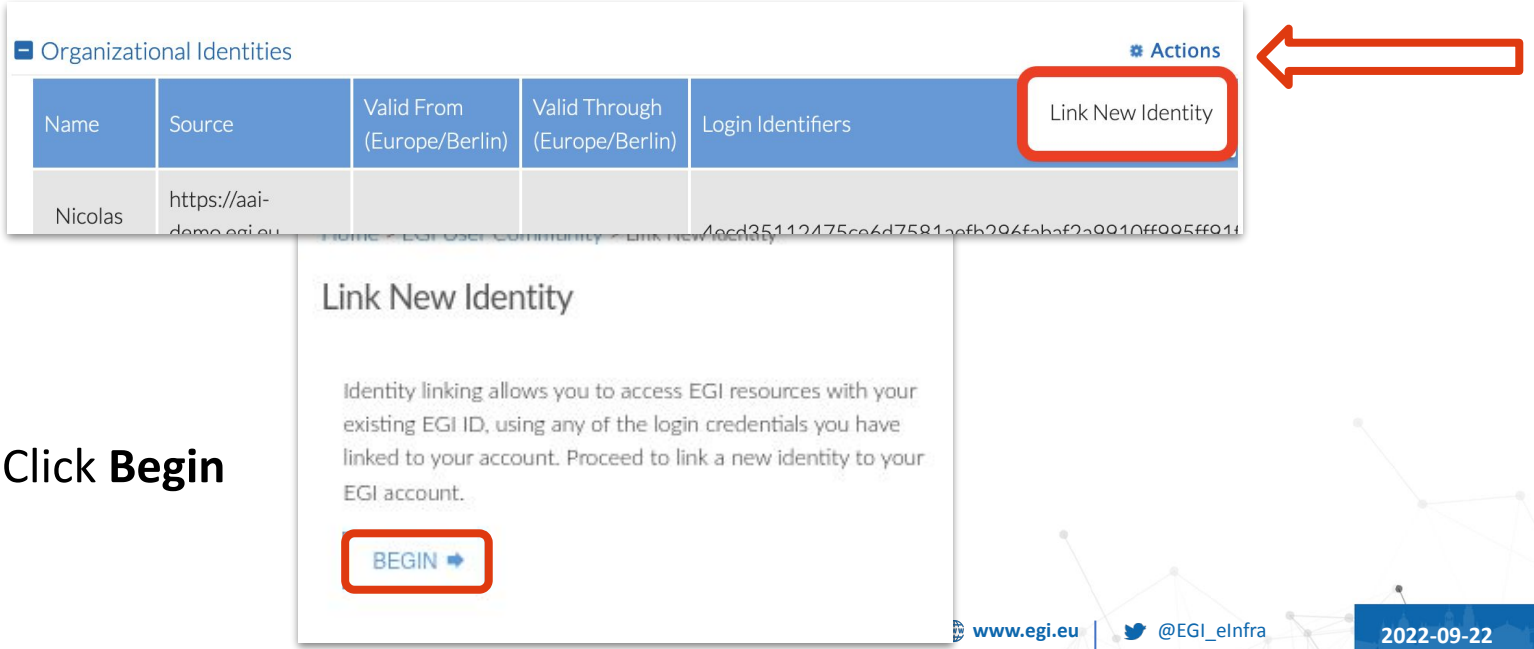
1. Go to https://aai.egi.eu/registry (or https://aai-demo.egi.eu/registry for the DEMO environment)
2. Select **Login** and authenticate using any of the login credentials already linked to your Check-in profile
3. From the top bar menu, select **<Your name>** and click **My EGI User Community Identity**



Identity Linking

Identity linking allows accessing resources with the same Check-in ID using different login credentials

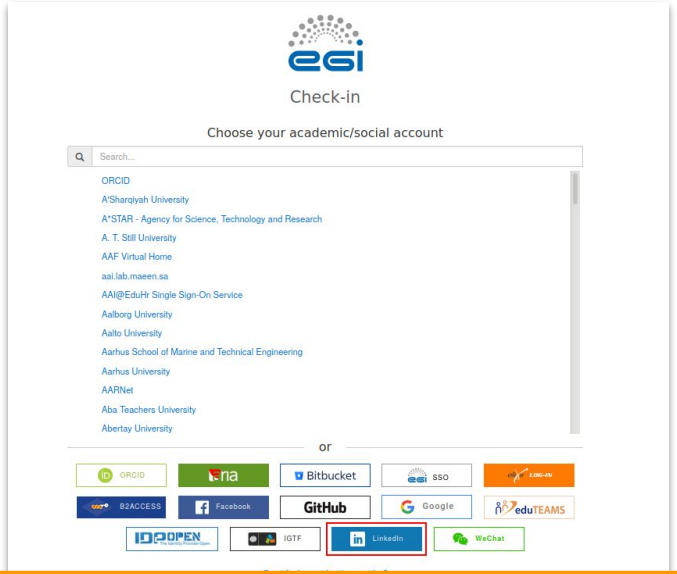
1. Select **Actions** → **Link New Identity** from your Check-in Profile page



2. Click **Begin**

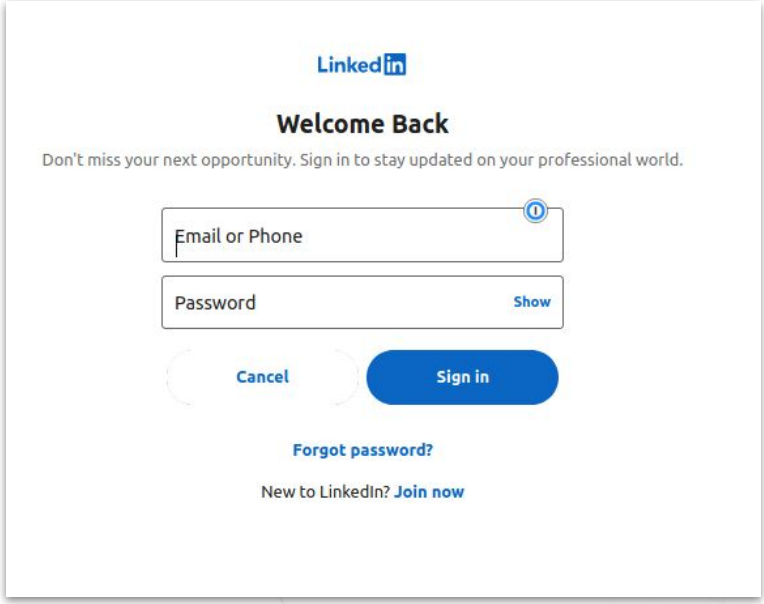
Identity Linking

3. **Choose** new Identity Provider from the list



IMPORTANT: Select "CHOOSE ANOTHER ACCOUNT"

4. **Authenticate** with the new Identity Provider

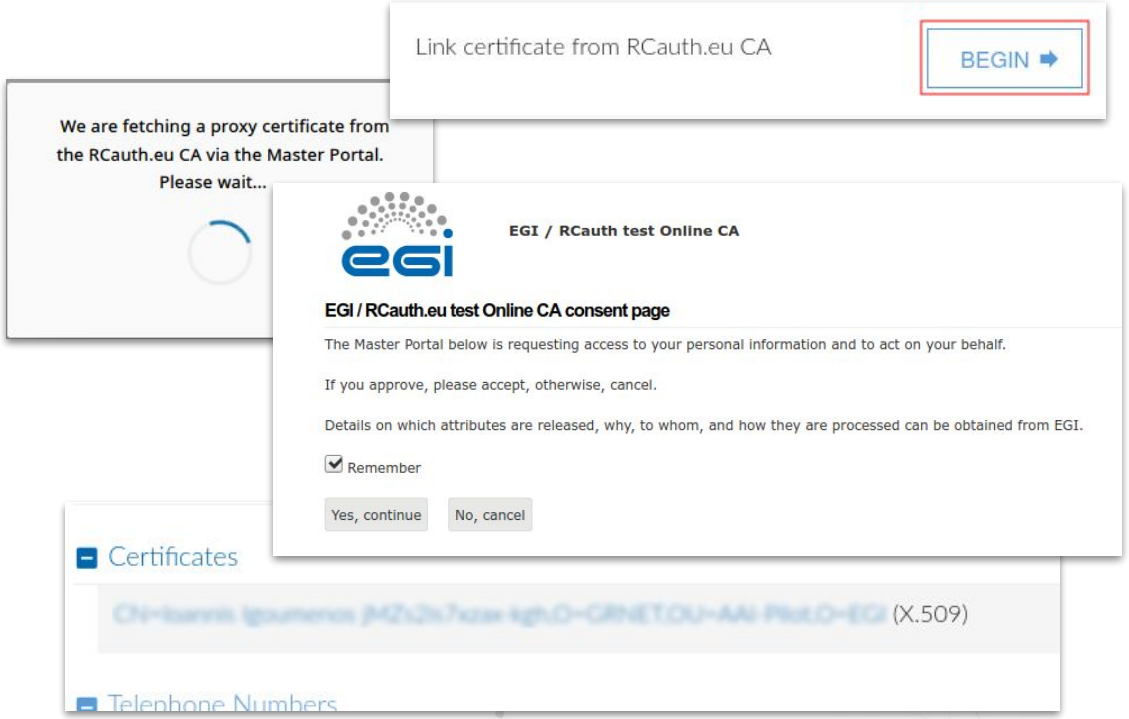


Identity Linking

The new Identity is linked under your profile

RCauth certificate linking

Select **Actions → Link certificate from RCauth.eu CA**



VO Management with COmanage Registry

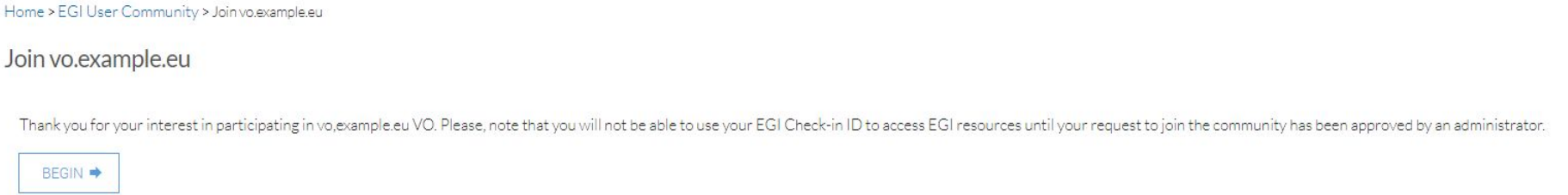
Requesting VO Membership

- User can request membership to a VO through an **enrollment flow**
- Each enrollment flow has a unique **URL** where the user can go to enroll to the desired VO
  - VO managers can share this URL to users, or
  - Users can click **Enroll** from the **People** menu and select the suitable enrollment flow

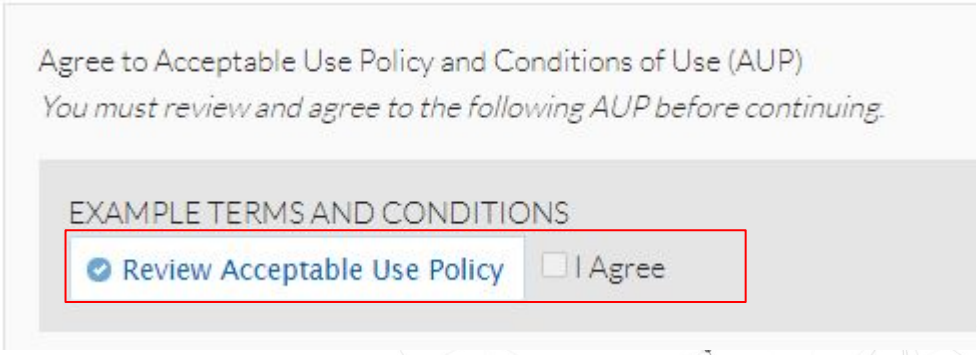
`https://aai.egi.eu/registry/co_petitions/start/coef:<##>`

Requesting VO Membership

Click **Begin** to start the enrollment flow:



At the next page, click **Review Acceptable Use Policy** and check the **I Agree** box. Then, you can click "**SUBMIT**" to continue the enrollment flow.



Requesting VO Membership

When the petition is submitted, a message will be shown at the top of the screen:

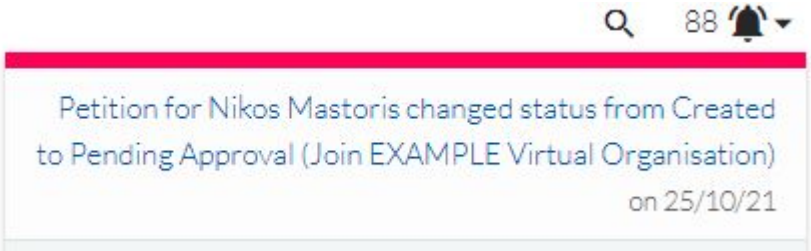
Then a VO manager can approve or deny your request

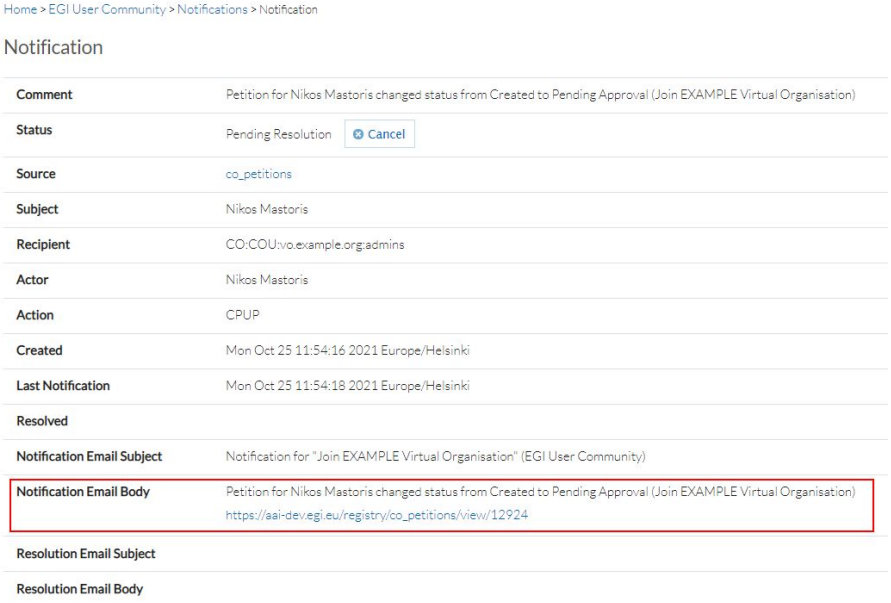
Managing VO Memberships

VO membership request notification

Once a user submits a VO membership petition:

- all VO managers are notified with an email containing a link to the petition.
- they will receive a notification on their COmanage profile. At the top right corner clicking the bell icon someone can see all the notifications.

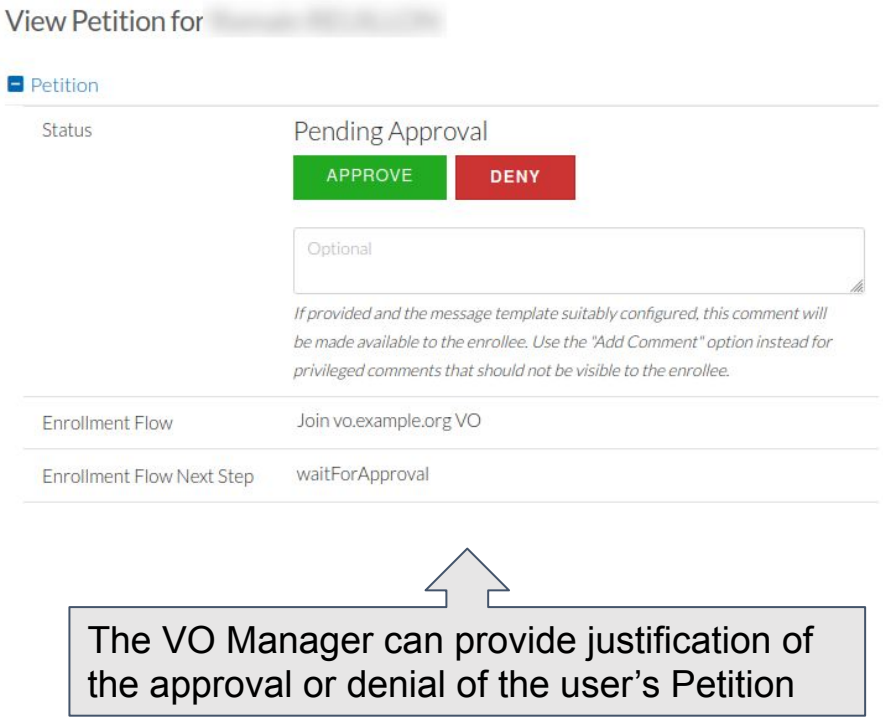




Clicking the petition URL either from the email you received or at the notification message, you can review the request.

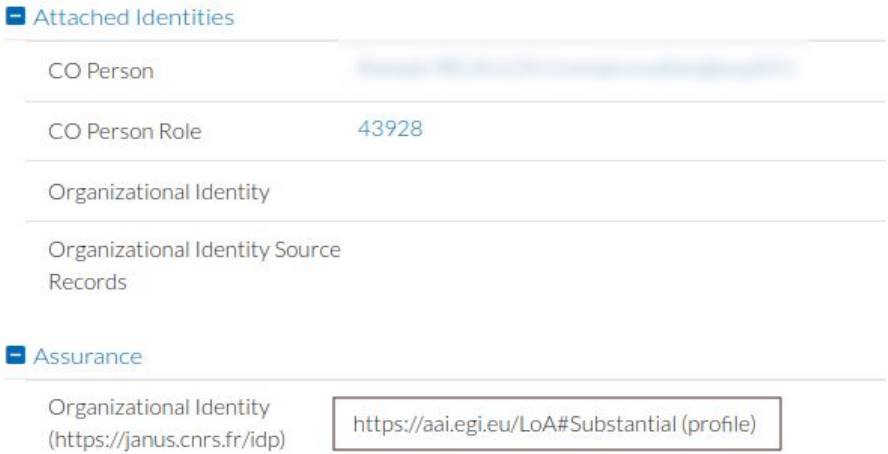
Managing VO Memberships

VO membership request review



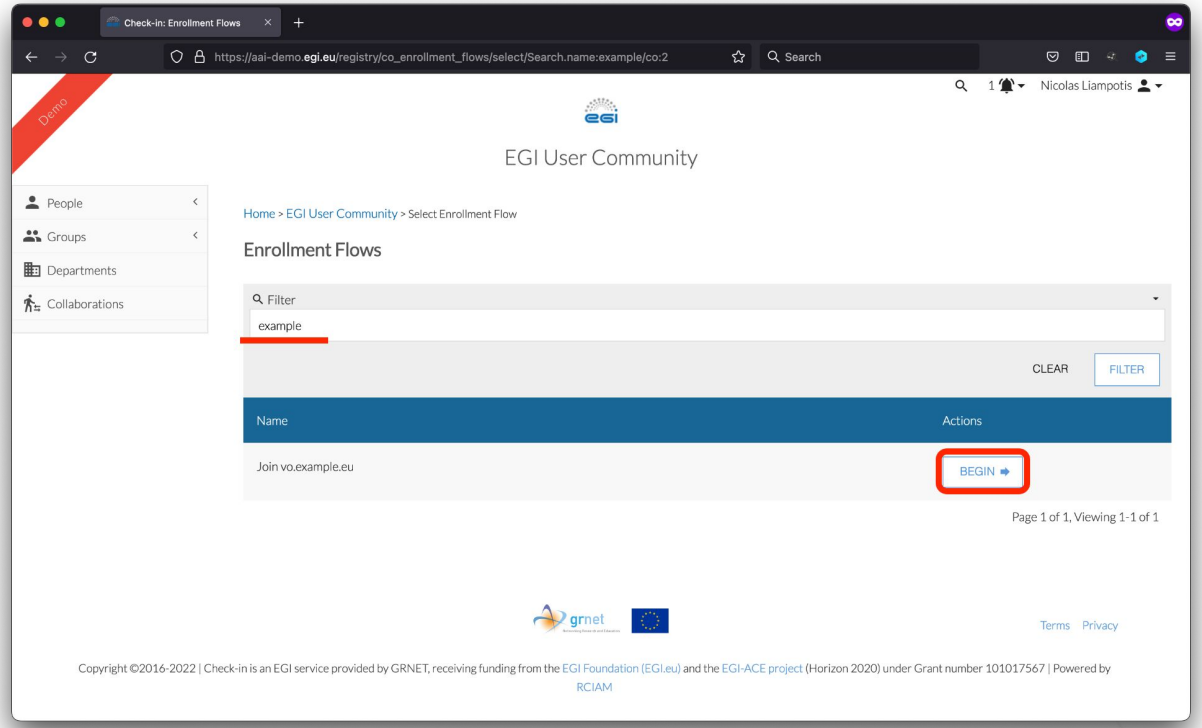
The VO Manager can provide justification of the approval or denial of the user's Petition

The Petition review page release information about the User's level of assurance.



Requesting VO Membership

➔ *Try me!*



https://aai-demo.egi.eu/registry/co_petitions/start/coef:45

Using VO Membership for Authorization

VO/Group membership and role information

- Allows services to control access to resources based on information about the VO/groups a user is a member of

- One or more values encapsulated in:
  - `eduPersonEntitlement` attribute (SAML)
  - `eduperson_entitlement` claim (OIDC)

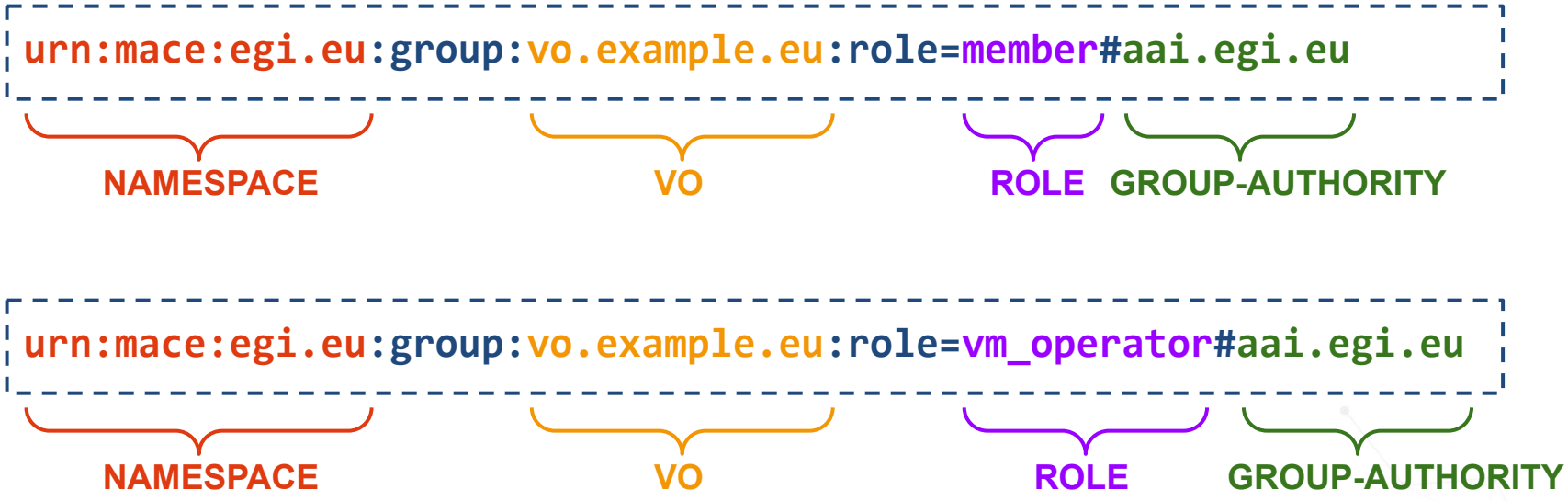
- Each value formatted as a URN → AARC-G002

```
<NAMESPACE>:group:<VO>[:<GROUP>*][:role=<ROLE>]#<GROUP-AUTHORITY>
```

Using VO Membership for Authorization

VO/Group membership and role information (Contd.)

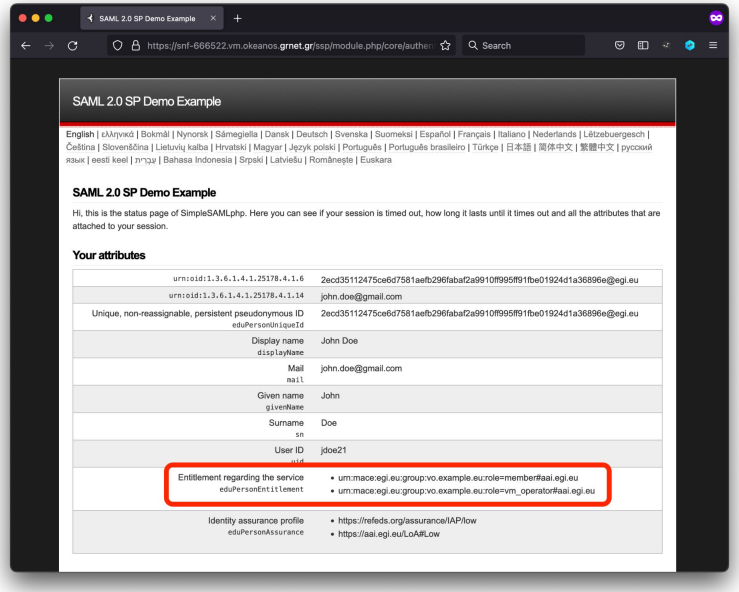
- Example values:



Using VO Membership for Authorization

VO/Group membership and role information (Contd.)

➔ *Try me!*



https://snf-666522.vm.okeanos.grnet.gr/ssp/module.php/core/authenticate.php?as=egi-demo-sp

VO Group Management

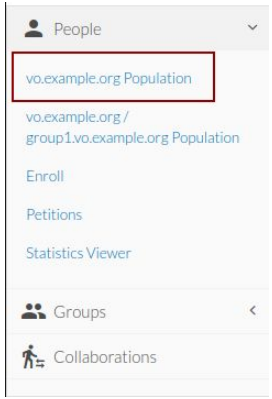
- VO groups in COmanage can only be created by Check-in platform administrators
- Contact checkin-support@mailman.egi.eu indicating the following information for every (sub)group:
  - VO name
  - Group name
  - Group description
  - Optional, Group manager(s)
  - Optional, Parent VO group name (in the case of a hierarchical group, e.g. <VO> → <PARENT_GROUP> → <GROUP>)
- *Known limitation: Group names must be unique so the names may need to be adjusted to guarantee their uniqueness*

https://docs.egi.eu/users/aai/check-in/vos/#managing-vo-groups

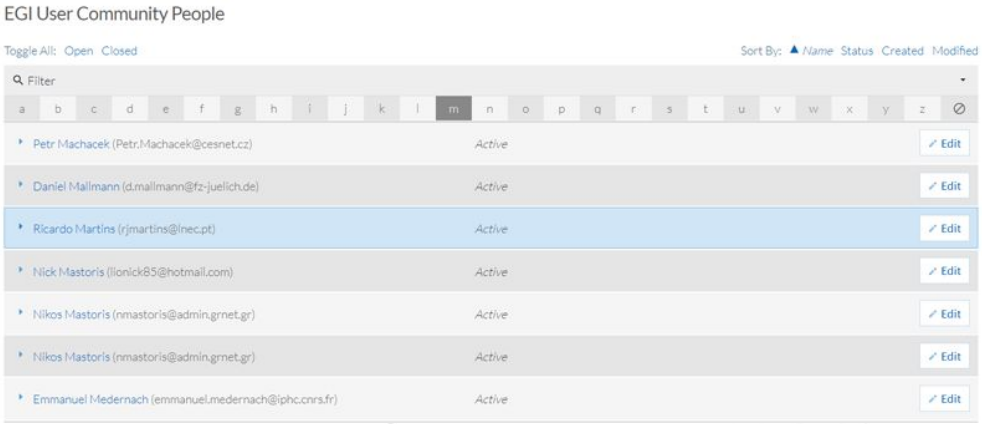
Management of VO group members

Adding member to VO group (1/2)

1) Expand the People drop down menu and click **<VO-NAME> Population** (for example, vo.example.org Population)



2) Find the user you want to add to the VO Group and click **Edit**.

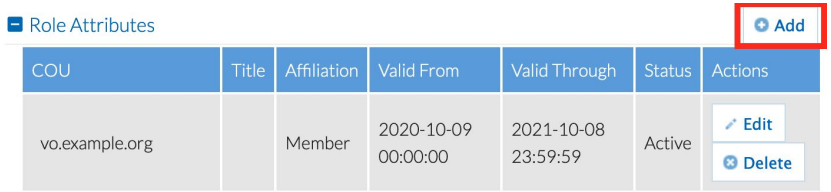


https://docs.egi.eu/users/aai/check-in/vos/#adding-members-to-vo-groups

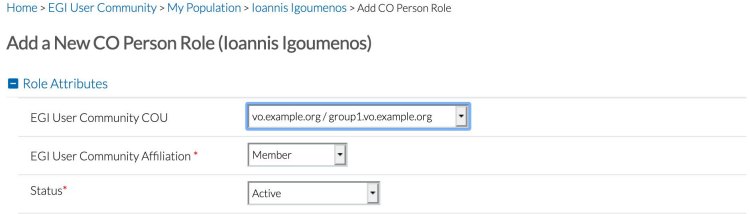
Management of VO group members

Adding member to VO group (2/2)

3) Click Add at the Role Attributes section of the user profile



4) Fill in the fields in the form and click **Add**. The user now is a member of the new VO group.

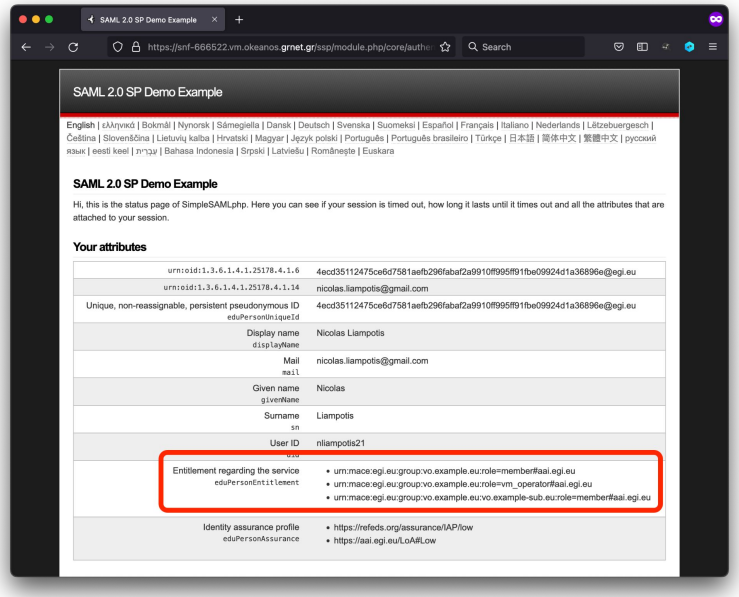


https://docs.egi.eu/users/aai/check-in/vos/#adding-members-to-vo-groups

Using VO Membership for Authorization

VO/Group membership and role information

➔ *Try me!*

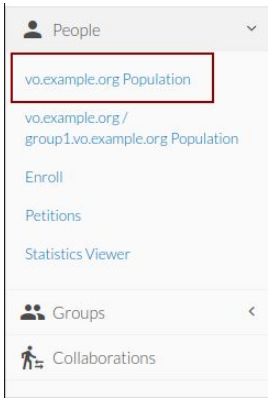


https://snf-666522.vm.okeanos.grnet.gr/ssp/module.php/core/authenticate.php?as=egi-demo-sp

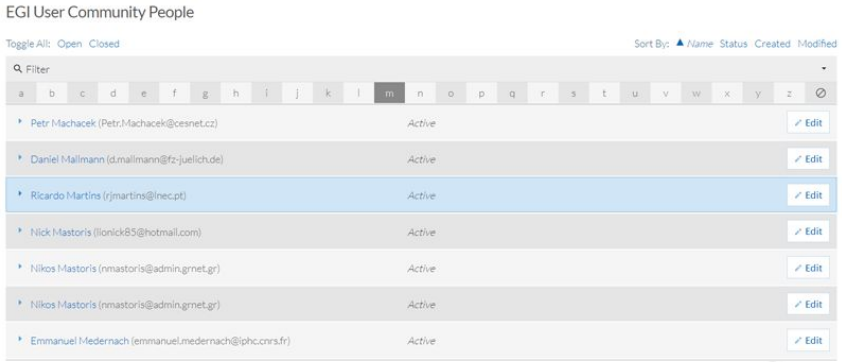
Management of VO group members

Removing member from VO group (1/2)

1) Expand the People drop down menu and click <VO-NAME> Population (for example, vo.example.org Population)



2) Find the user you want to add to the VO Group and click **Edit**.

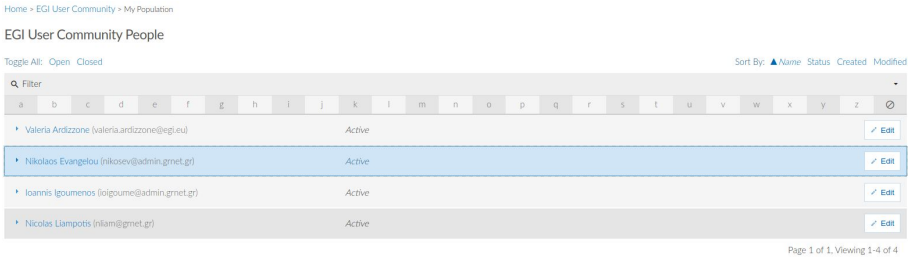


https://docs.egi.eu/users/aai/check-in/vos/#removing-members

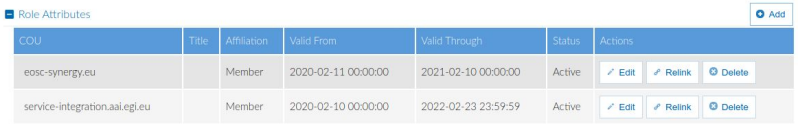
Management of VO group members

Removing member from VO group (2/2)

3) From the VO members list, click **Edit** on the person that is going to be removed.



4) Under Role Attributes click **Delete** on the right of the COU entry of interest (for example, eosc-synergy.eu). On success the selected row will be removed.



https://docs.egi.eu/users/aai/check-in/vos/#removing-members

Role Management

Assigning role to VO member

1. Navigate to Co Person Role view

2. Choose Role from drop down list, if available, or add custom text if no list is present.

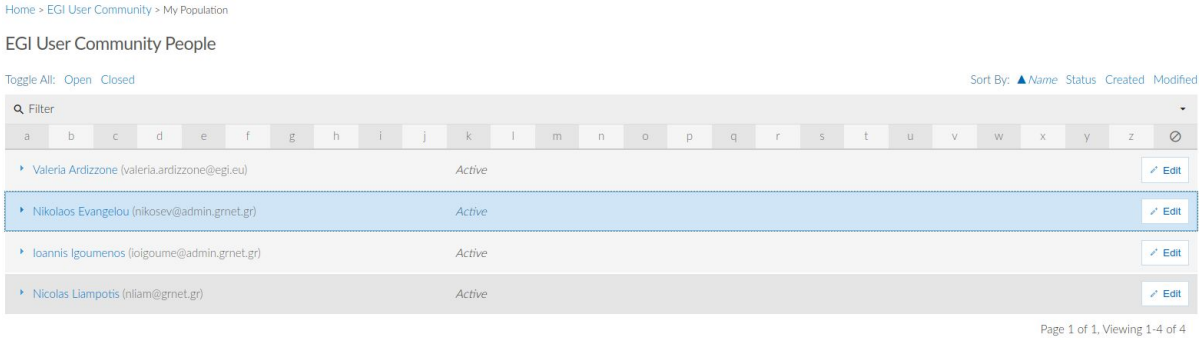
A custom role can be assigned to a VO member during the Enrollment flow process if the user case requires it

Role Management

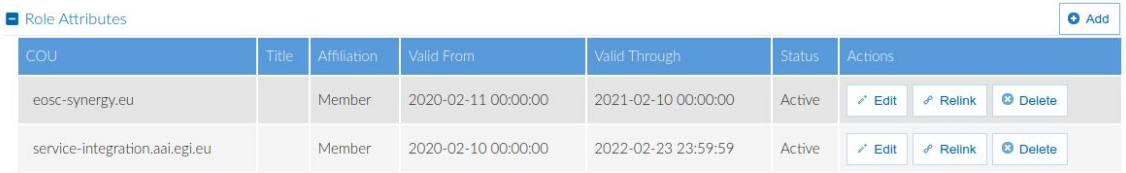
Removing role from VO member

From the VO members list (see Viewing VO members above):

1. Click Edit on the person that is going to be removed.

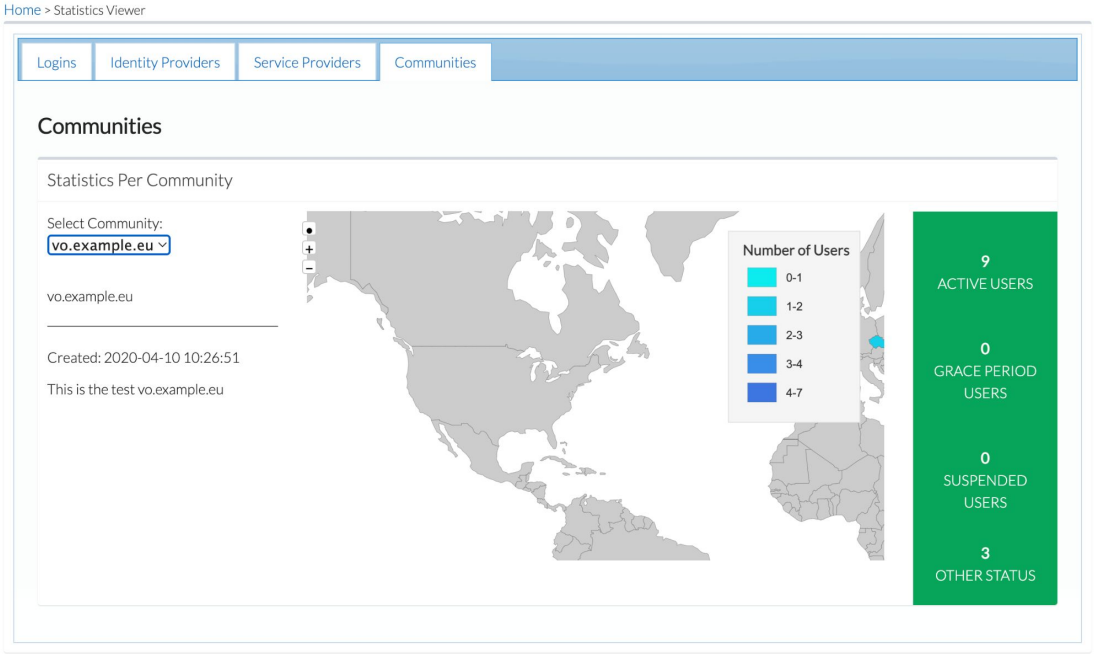


2. Under **Role Attributes** click **Delete** on the right of the COU entry of interest (for example, vo.example.com). On success the selected row will be removed. In this example we removed the **vo.geoss.eu** that we previously added.



VO Statistics

Accessible via **People → Statistics Viewer**



VO Membership API

COmanage provides a REST API that allows VO managers to:

- Manage membership information only for the VOs they are authoritative for
- Retrieve VO group information only for the VOs they are authoritative for

Features:

- Members of the VO are identified via their EGI Check-in Community User Identifier (CUID)
- Membership can be limited to a specified period
- All REFEDS membership affiliations are supported
- Role titles are supported
- Different membership status values are supported, namely Active, Expired, Deleted, Suspended
- Check-in automatically changes the membership status from Active to Expired beyond the validity period

https://docs.egi.eu/users/aai/check-in/vos/#vo-api

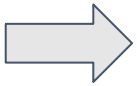
VO Membership API

Example: Adding VO member

Requires specifying the following mandatory params:

- User's EGI Check-in identifier,
- Name of the VO (e.g. vo.example.eu),
- status (Active),
- valid from/through dates.

```
$ curl -vX POST $VO_API_BASE_URL.json \
       --user "example-client":"veryverysecret" \
       --data @add.json \
       --header "Content-Type: application/json"
```




```
{
  "RequestType": "CoPersonRoles",
  "Version": "1.0",
  "CoPersonRoles": [
    {
      "Version": "1.0",
      "Person": {
        "Type": "CO",
        "Identifier": {
          "Type": "epuid",
          "Id": "01234567890123456789@egi.eu"
        }
      },
      "Cou": {
        "CoId": "2",
        "Name": "vo.example.org"
      },
      "Affiliation": "member",
      "Title": "Engineer",
      "Status": "Active",
      "ValidFrom": "2022-02-16 11:19:38",
      "ValidThrough": "2022-05-16 11:19:38"
    }
  ]
}
```


https://docs.egi.eu/users/aai/check-in/vos/#vo-api

LDAP access to VO Membership information

Attribute	Description	Example
`objectClass`		`inetOrgPerson`, `eduPerson`, `voPerson`, `eduMember`, `ldapPublicKey`
`voPersonId`	Community User Identifier (`voPersonID`)	`befd2b9ed8878c542555829cb21da3e25ad91a0f9cg54gsdcs35htf@egi.eu`
`uid`	user ID	`john.doe`
`cn`	Full name	`John Doe`
`displayName`	Full name	`John Doe`
`givenName`	First name	`John`
`sn`	Last name	`Doe`
`mail`	Email address	`john.doe@mail.com`
`edupersonUniqueID`	Community User Identifier (see also `voPersonId`)	`befd2b9ed8878c542555829cb21da3e25ad91a0f9cg54gsdcs35htf@egi.eu`
`eduPersonPrincipalName`	A scoped identifier for a person. The value is the same as the	`befd2b9ed8878c542555829cb21da3e25ad91a0f9cg54gsdcs35htf@egi.eu`
`eduPersonEntitlement`	URN that indicates a set of rights to specific resources	urn:mace:egi.eu:group:vo.example.org:role=member#aai.egi.eu
`sshPublicKey`	SSH public key	
`isMemberOf`	Group memberships	`CO:COU:vo.example.org:members`
`voPersonCertificateDN`	The Subject Distinguished Name of an X.509 certificate held by the person	`voPersonCertificateDN;scope-cert1: CN=John Doe A251,O=Example,C=US,DC=cilogon,DC=org`
`voPersonCertificateIssuerDN`	The Subject Distinguished Name of the X.509 certificate issuer	`voPersonCertificateIssuerDN;scope-cert1: CN=CILogon Basic CA 1, O=CILogon, C=US, DC=cilogon, DC=org`

https://docs.egi.eu/users/aai/check-in/vos/#ldap

Check-in Documentation

- Usage guide
- Integration guide for service providers
- Integration guide for identity providers

EGI: Advanced Computing for Research

www.egi.eu
@EGI_eInfra

Thank you
for your attention.

Questions?

This work by the EGI Foundation
is licensed under a Creative Commons Attribution 4.0 International License.

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

Assurance: What is it?

REFEDS Assurance Components & Profiles

Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

AARC Assam
IGTF Dogwood
RAF Cappuccino
IGTF Birch
RAF Espresso

New profiles!

Assurance: What is it?

EGI Check-in Profiles

Based on the authentication method selected by the user, EGI Check-in Proxy assigns a Level of Assurance (LoA).

EGI Check-in currently distinguishes between three LoA levels. Each level is represented by a URI as follows:

- **Low**: Authentication through a social identity provider or other low identity assurance provider: `https://aai.egi.eu/LoA#Low`
- **Substantial**: Password/X.509 authentication at the user's home IdP: `https://aai.egi.eu/LoA#Substantial`
- **High**: Substantial + multi-factor authn (not supported yet): `https://aai.egi.eu/LoA#High`