www.egi.eu
@EGI_eInfra

AAI services in EGI - Overview and use cases: Check-in - Latest updates and roadmap

Nicolas Liampotis (GRNET)
Valeria Ardizzone (EGI Foundation)

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

Check-in: What's new?

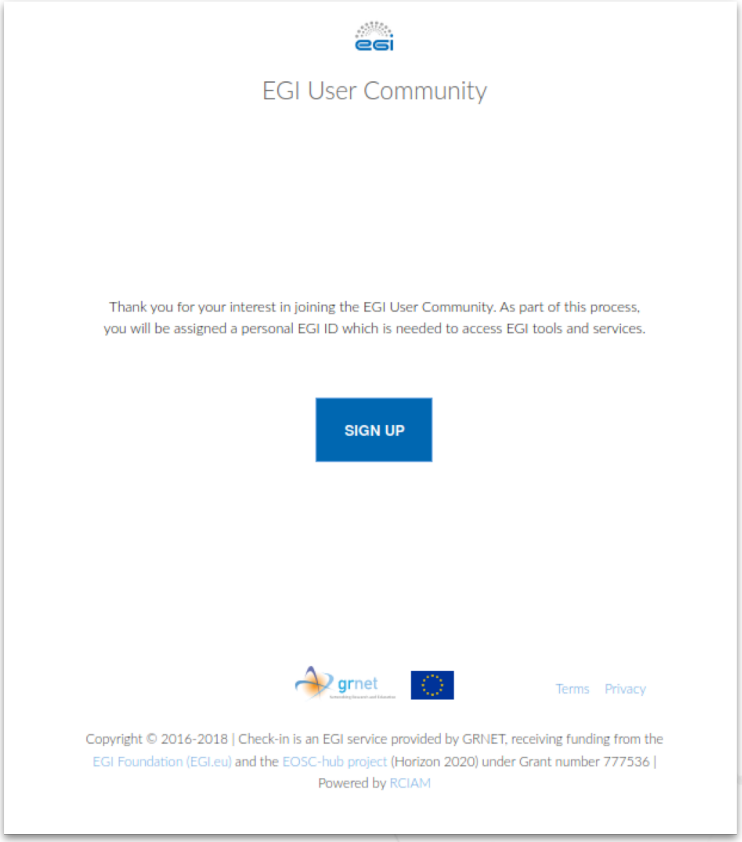
- Streamlined user onboarding: Improved UI for signing up using less steps
- Linking identities made easier and faster
- Improved RCauth certificate linking process
- Improved ORCID integration using ORCID API client credentials
- Added support for service 🤖 identities
- Added login, user & group statistics
- Updated VOMS (de)provisioning plugin with support for VOMS Admin SOAP and REST API v3.7.0
- Improved integration with GOCDB:
  - configuration of fallback server in case the main one fails
  - if no GOCDB server is available then inform the user and give the option to abort or continue without GOCDB role entitlements
- New operating environment to improve performance

Check-in User Registration

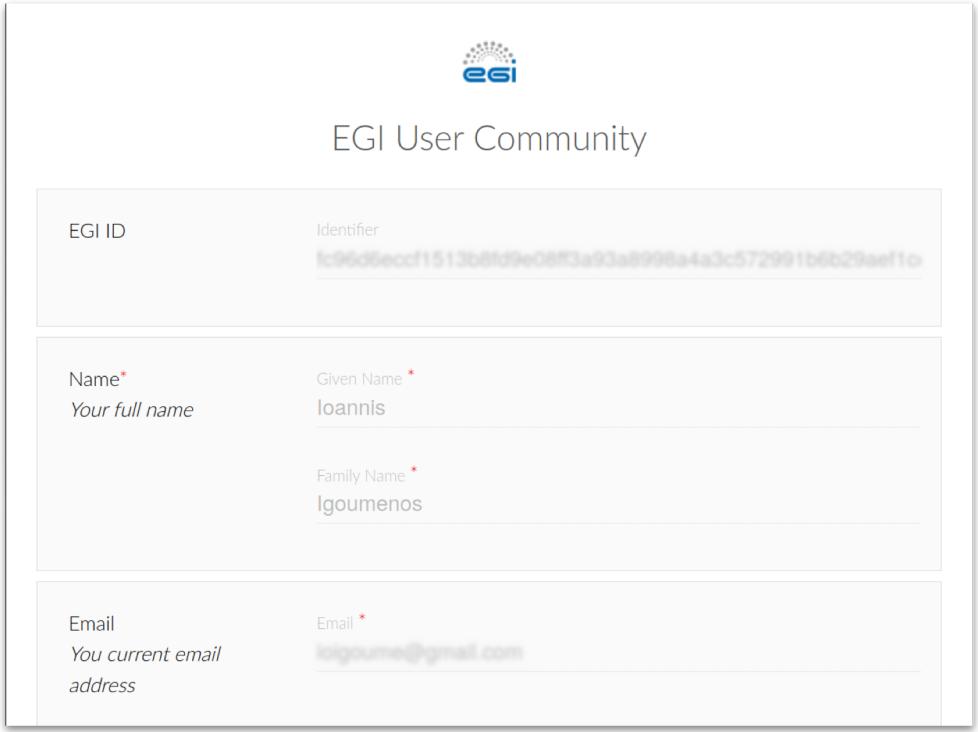
Step 1	Step 2	Step 3
Review user profile information ● name ● email ● affiliation and agree to Acceptable Use Policy (AUP)	Verify email address - *only if a verified email address is not released by the user's authenticating identity provider*	Access resources

Check-in User Registration

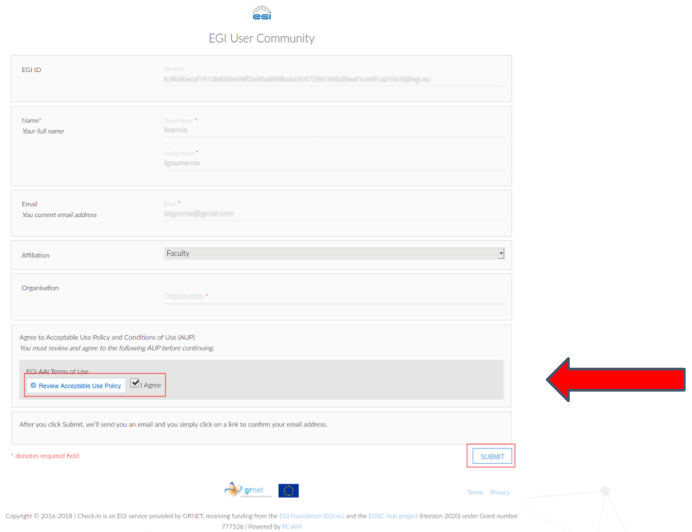
To access resources protected by EGI Check-in, you need to sign up for an account using an academic/social identity provider



Check-in User Registration



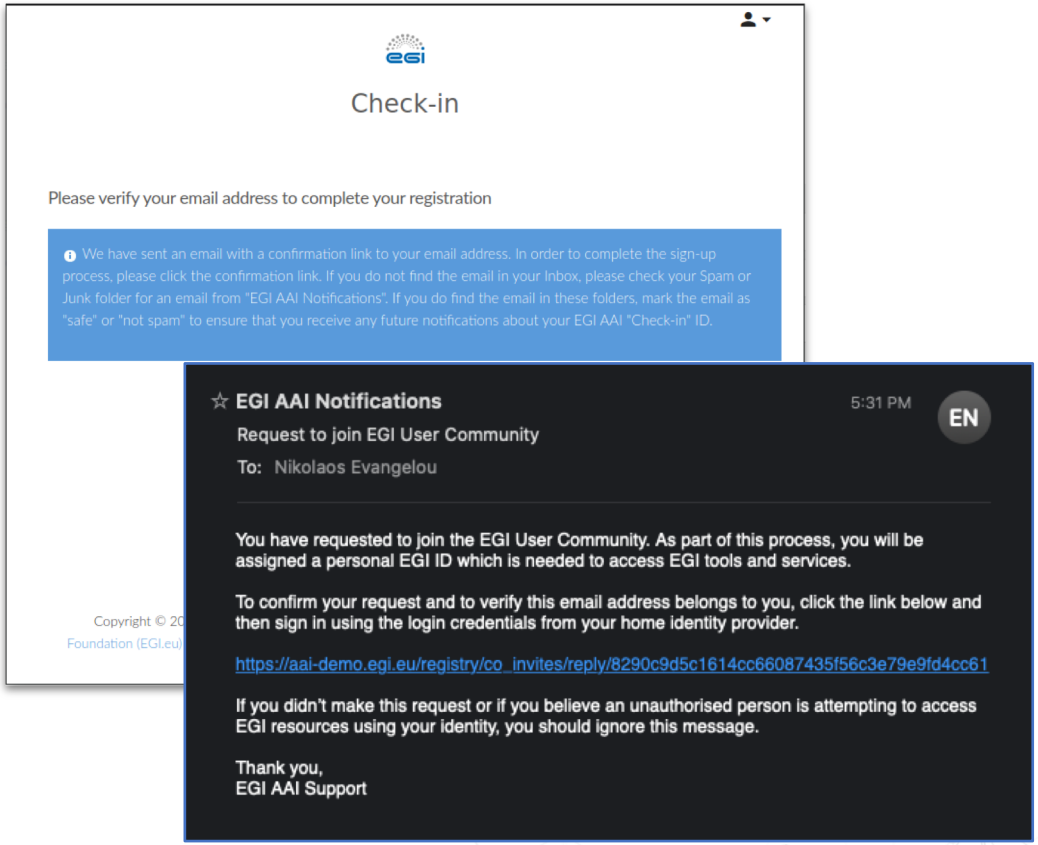
Review your information, agree to the AUP and click on “Submit”.



Check-in User Registration

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

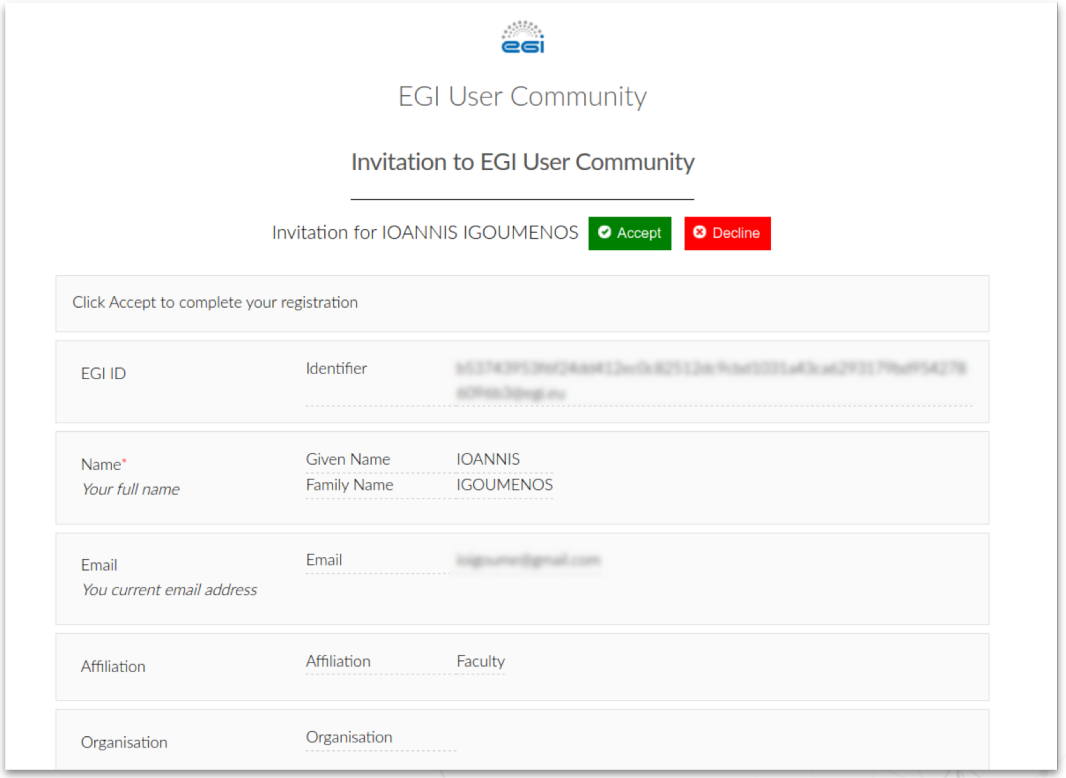
This step is SKIPPED in case of an email known to be verified by the Identity Provider



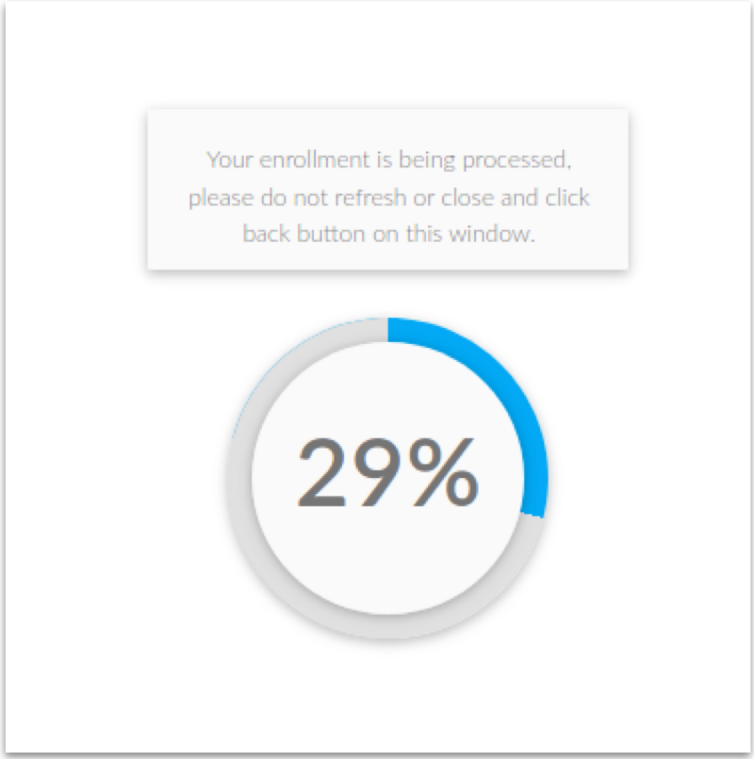
Check-in User Registration

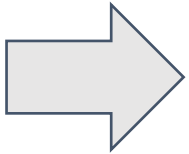
Click on “Accept” to finalize the registration.

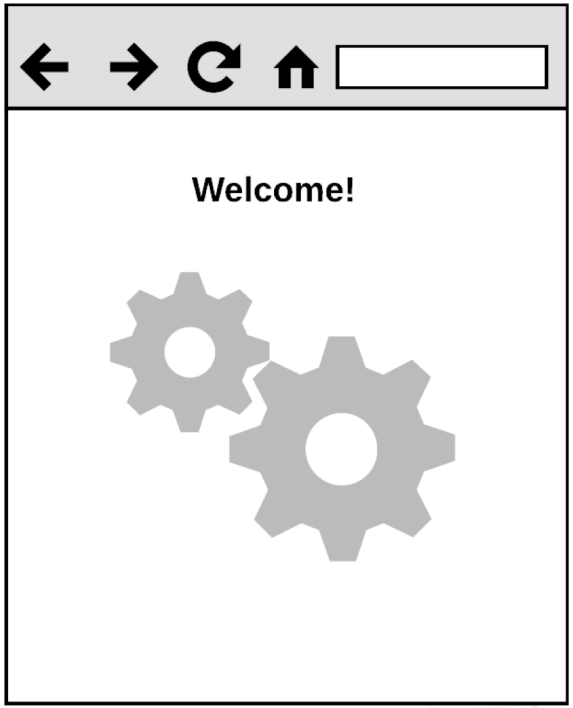
This step is SKIPPED in case of an email known to be verified by the Identity Provider



EGI Check-in User Registration



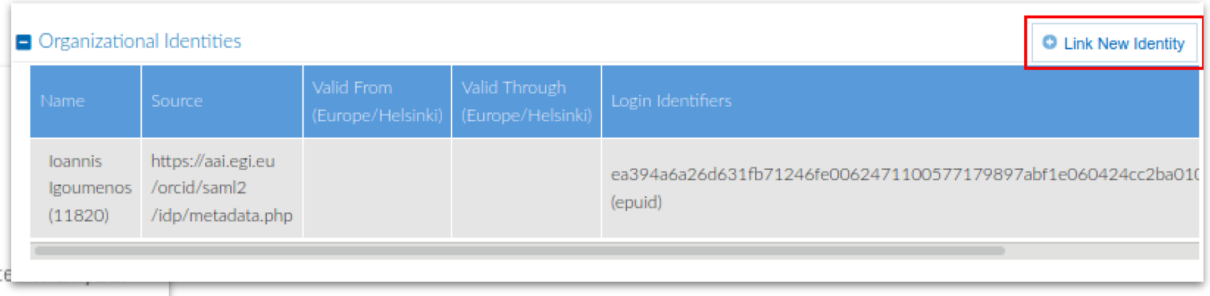


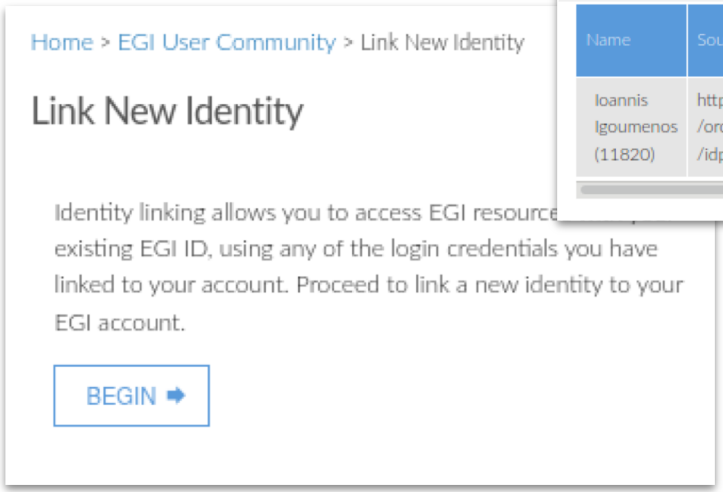


Identity Linking

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

1. Click **Link New Identity** from User's Profile View (https://aai.egi.eu/registry)



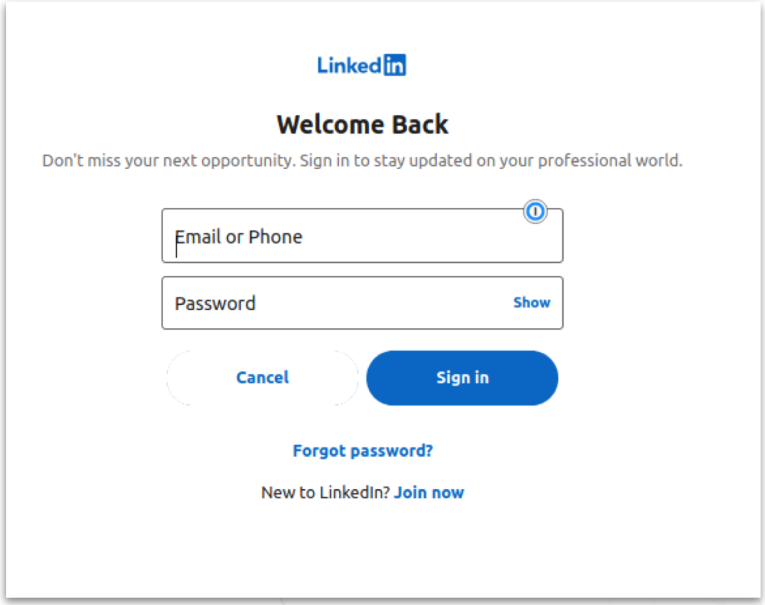


2. Click **Begin**

Identity Linking

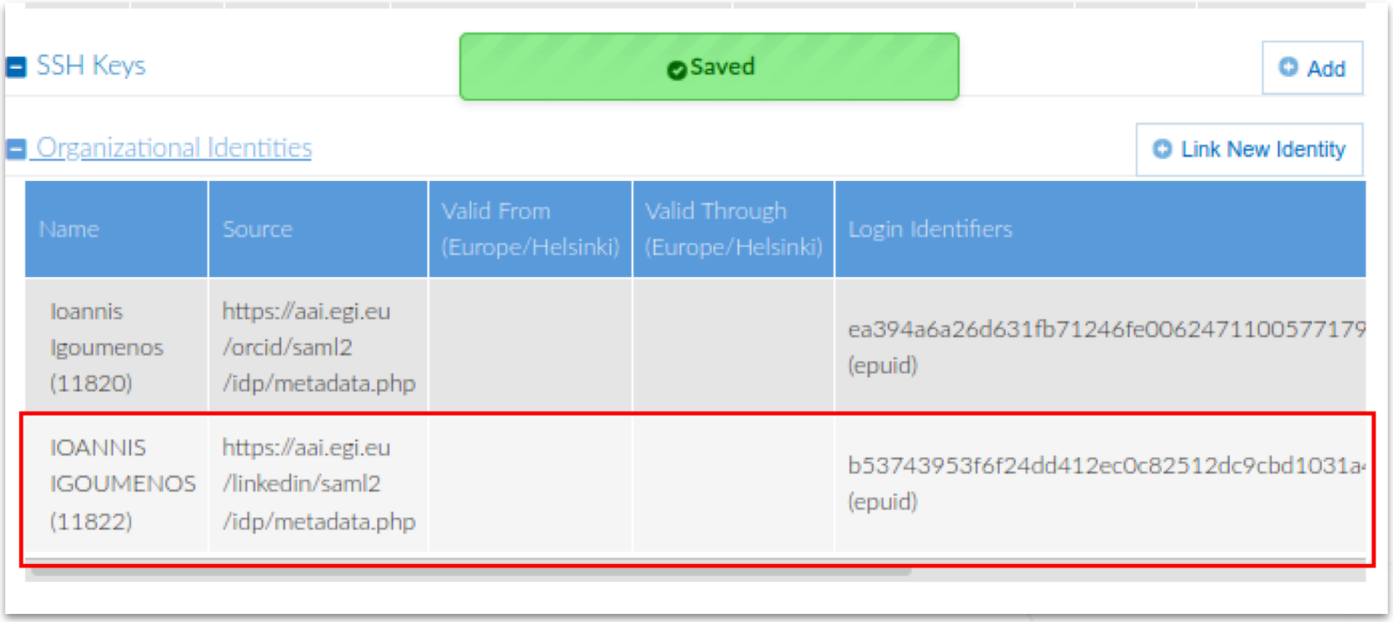
3. **Choose** new Identity Provider from the list

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



Identity Linking

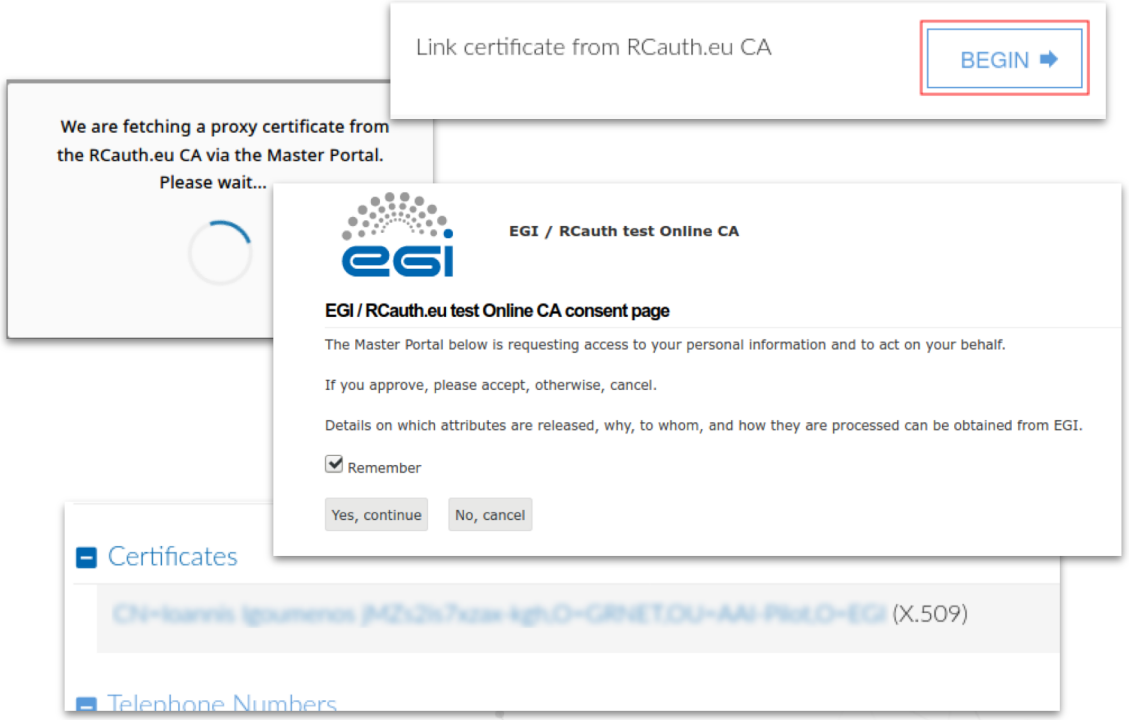
The new Identity is linked under your profile



RCauth certificate linking

Request and link an RCAuth Certificate under User's Profile takes up to **50% less** time

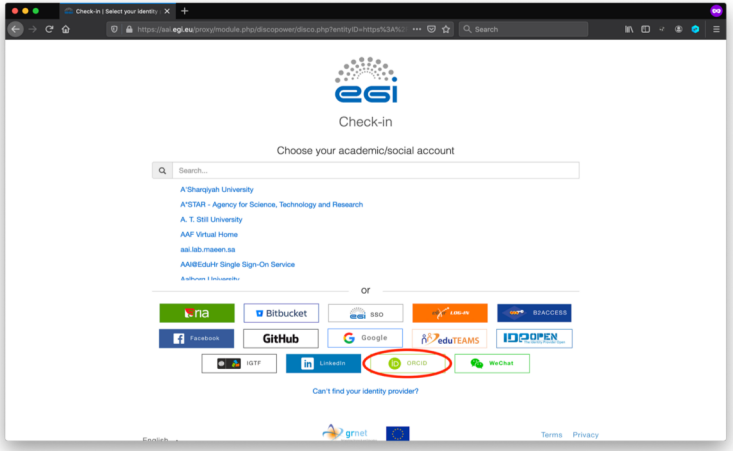
Click **Link certificate from RCauth.eu CA**

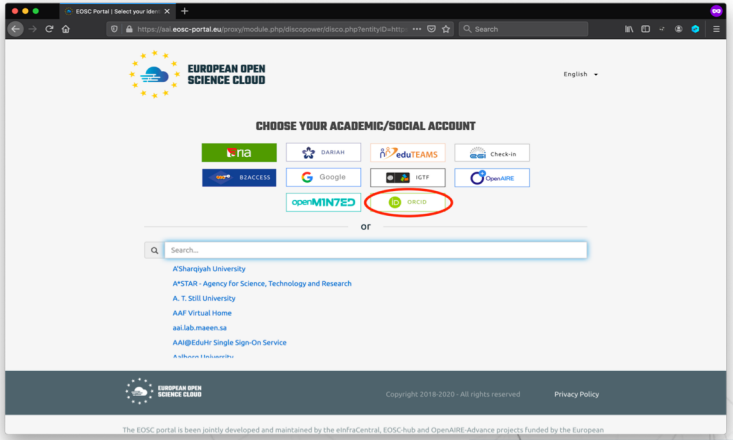


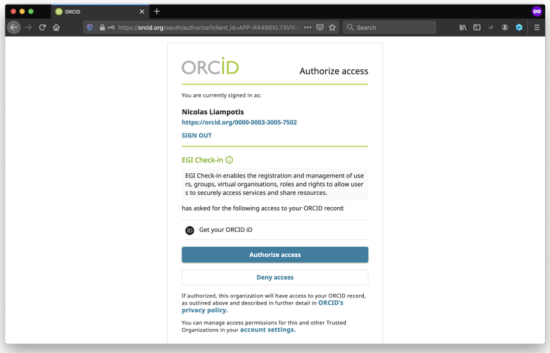
Improved ORCID integration

Member ORCID API

Member API credentials enable requesting permission from users to **read limited-access data** on their ORCID records (e.g. email) through 3-legged OAuth authorization



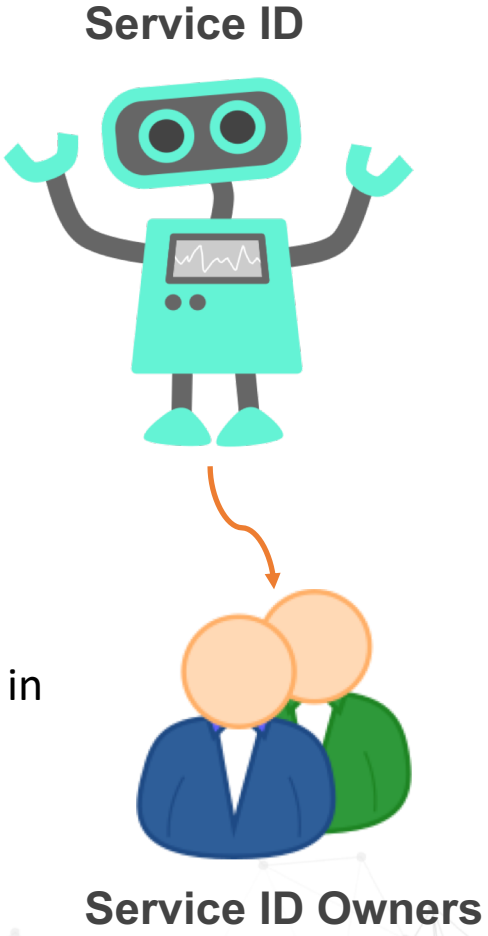




Service identities

What are they?

- A special kind of identity used by a service/application/resource, not a person
- Example: *“A portal needs to submit jobs/create VMs”*
- Associated with one or more persons → Service ID owners
- Comprises all the standard attributes of personal identities, incl. (group) email address, plus
  - `isServiceUser` attribute set to `1` (will be standardised in upcoming AARC-G056)
- Can be given permissions (VO/group membership & roles) to access the resources it needs
- Analogous to X.509 robot certificates



Service identities

Roles & responsibilities

Service ID Owner

- Manages Service ID credentials:
  - login & password
  - X509 certificate
- Registers Service ID in one or more VOs

Service ID Owner MUST be registered as a *regular member* of the **services.aai.egi.eu VO** (Perun)

Service ID Manager

- Creates Service ID (under the services.aai.egi.eu VO) upon request
- Assigns Service ID owners
- Removes Service ID

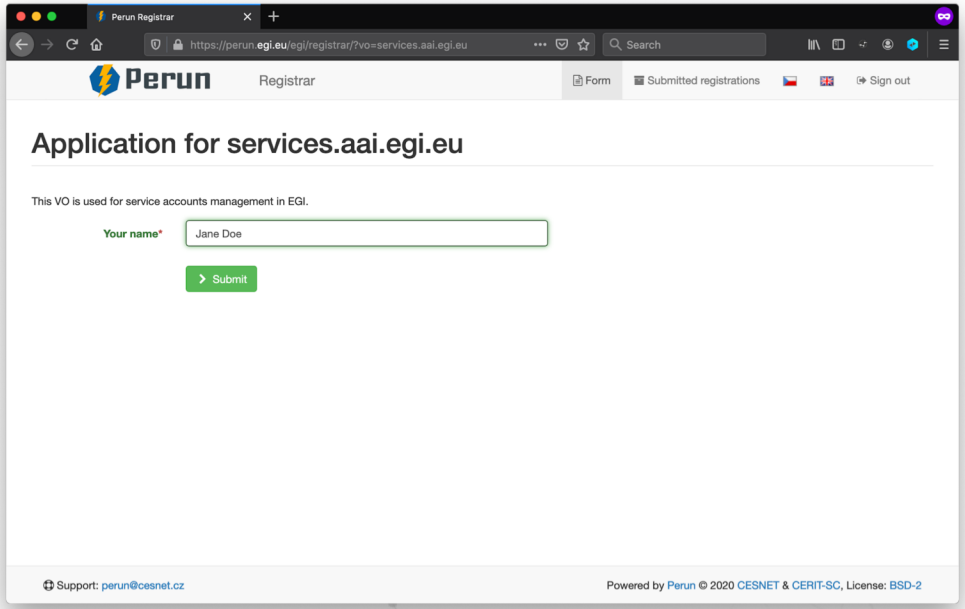
Service ID Manager MUST be registered as a *manager* of the **services.aai.egi.eu VO** (Perun)

Service identities

Registration procedure

https://perun.egi.eu/egi/registrar/?vo=services.aai.egi.eu

1 Service ID Owner registers in **services.aai.egi.eu VO**



Service identities

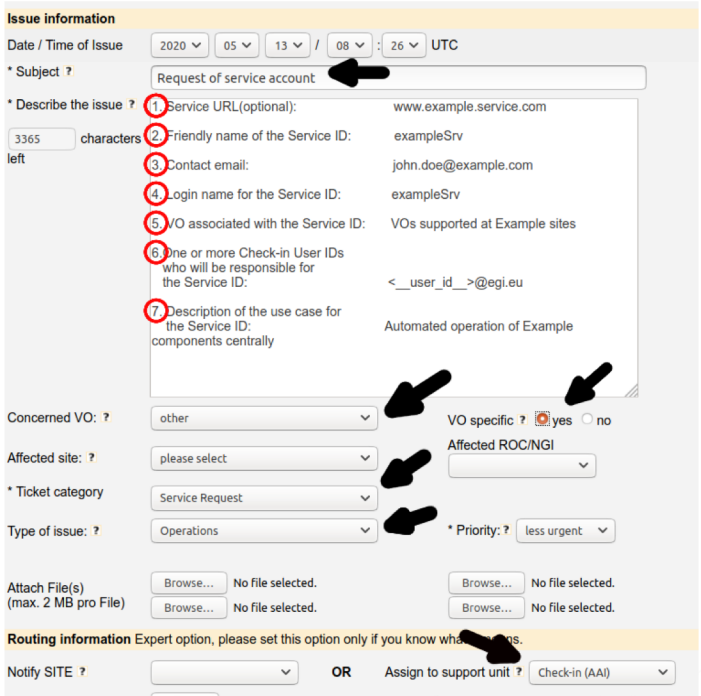
Registration procedure

https://ggus.eu/index.php?mode=ticket_submit

2

Service ID Owner submits GGUs ticket:

- Service URL (optional)
- Friendly name of the Service ID
- Contact email; it is recommended to supply a group email address if the Service ID is owned by multiple persons
- Login name for the Service ID
- One or more VOs associated with the Service ID
- One or more Check-in User IDs who will be responsible for the Service ID
- Use case description



Service identities

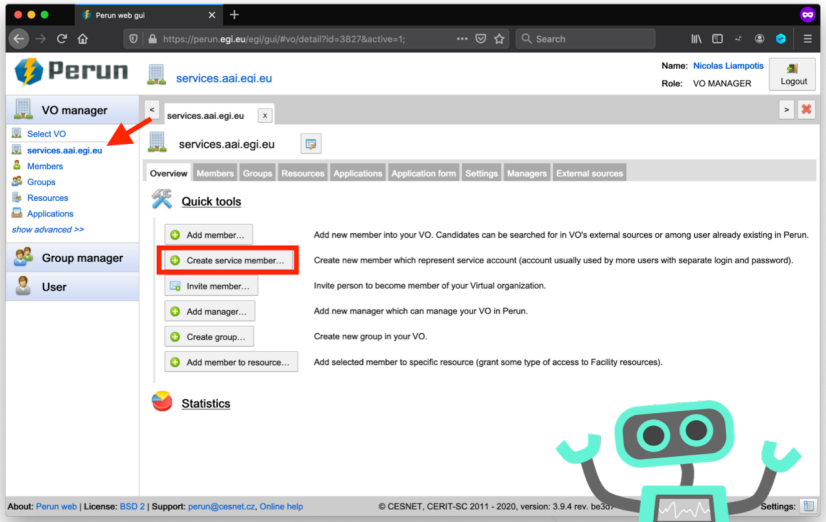
Registration procedure

https://perun.egi.eu/egi/gui

3

Service ID Manager:

- Creates the new Service ID under the **services.aai.egi.eu VO**
- Assigns Service ID Owners



Service identities

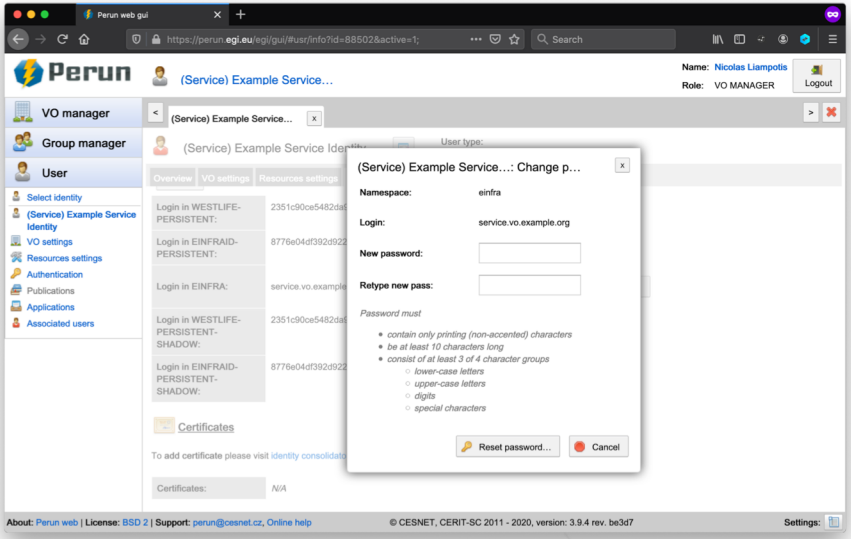
Registration procedure

https://perun.egi.eu/egi/gui

4

Service ID Owner creates Service ID credentials

- Username & password or
- X509 certificate



Service identities

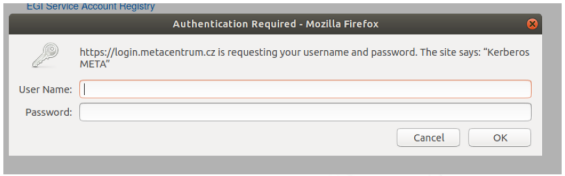
Registration procedure

https://aai.egi.eu/signup

5

Service ID Owner registers the Service ID in Check-in

- Selects **EGI Service Account Registry** IdP
- Authenticates using Service ID credentials

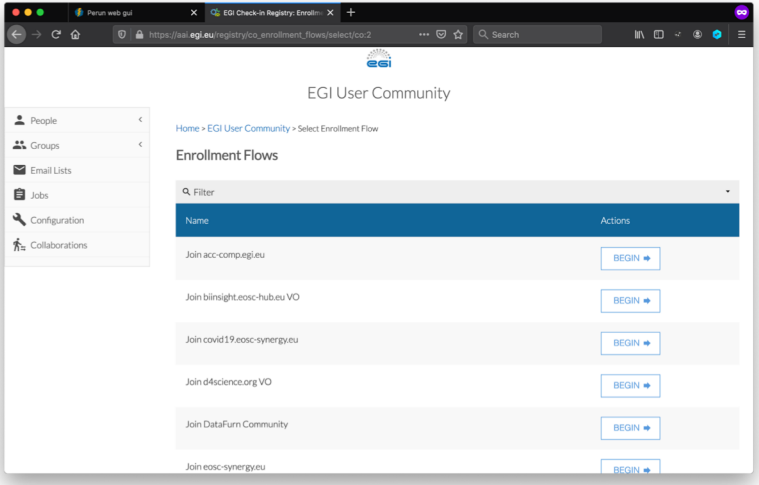


Service identities

Registration procedure

6

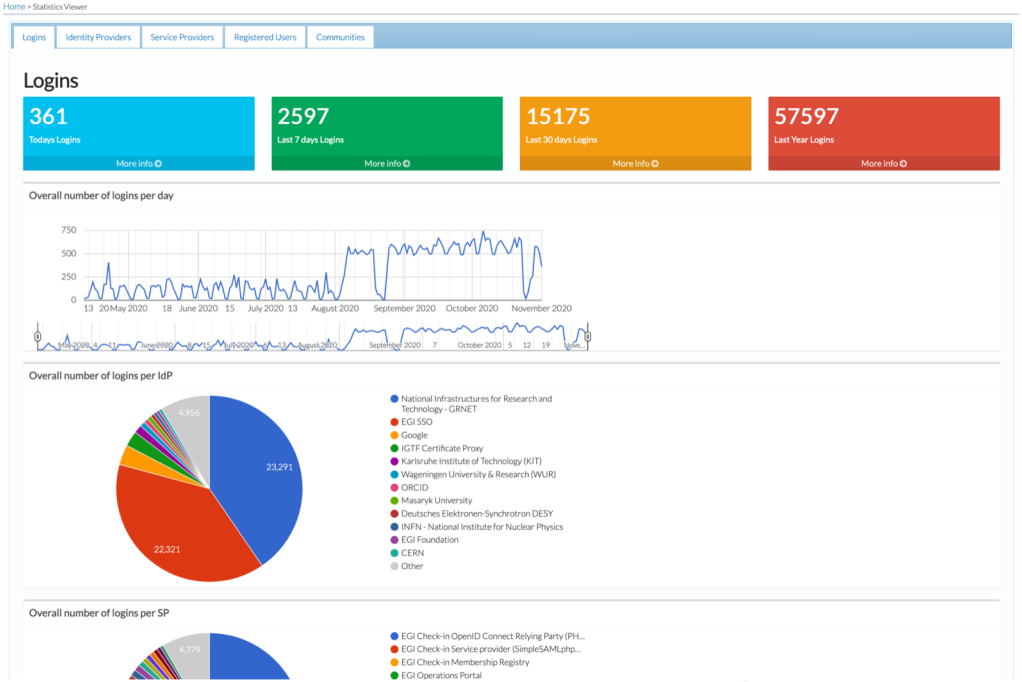
Service ID Owner registers the Service ID in one or more VOs



Check-in Statistics

Statistics Plugin is used for presenting statistics information regarding

- Logins
  - total
  - per Identity Provider
  - per Service Provider
- Registered users
- Communities/Virtual Organisations

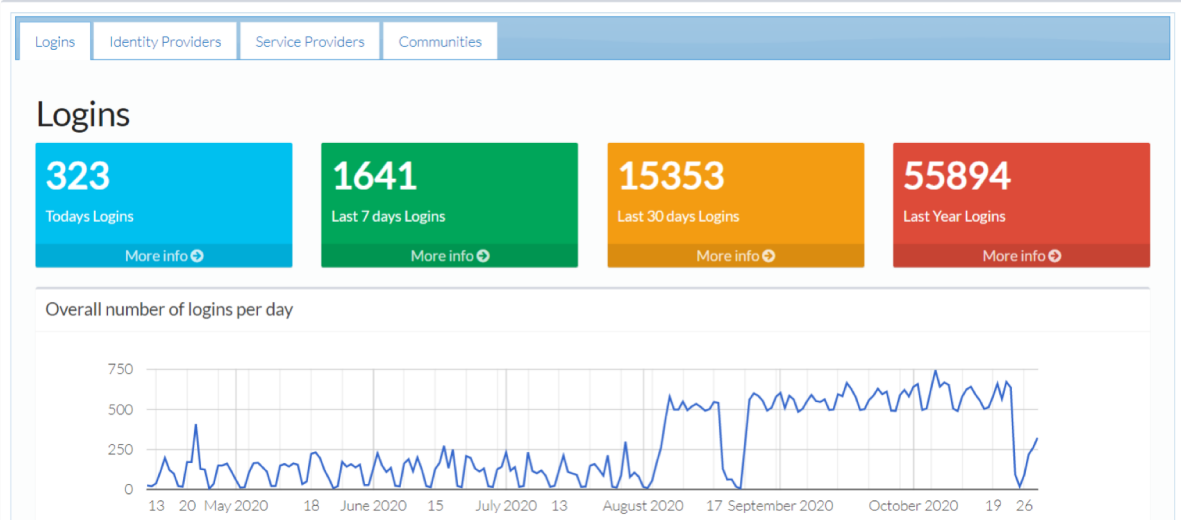


https://aai.egi.eu/registry

Check-in Statistics

Logins

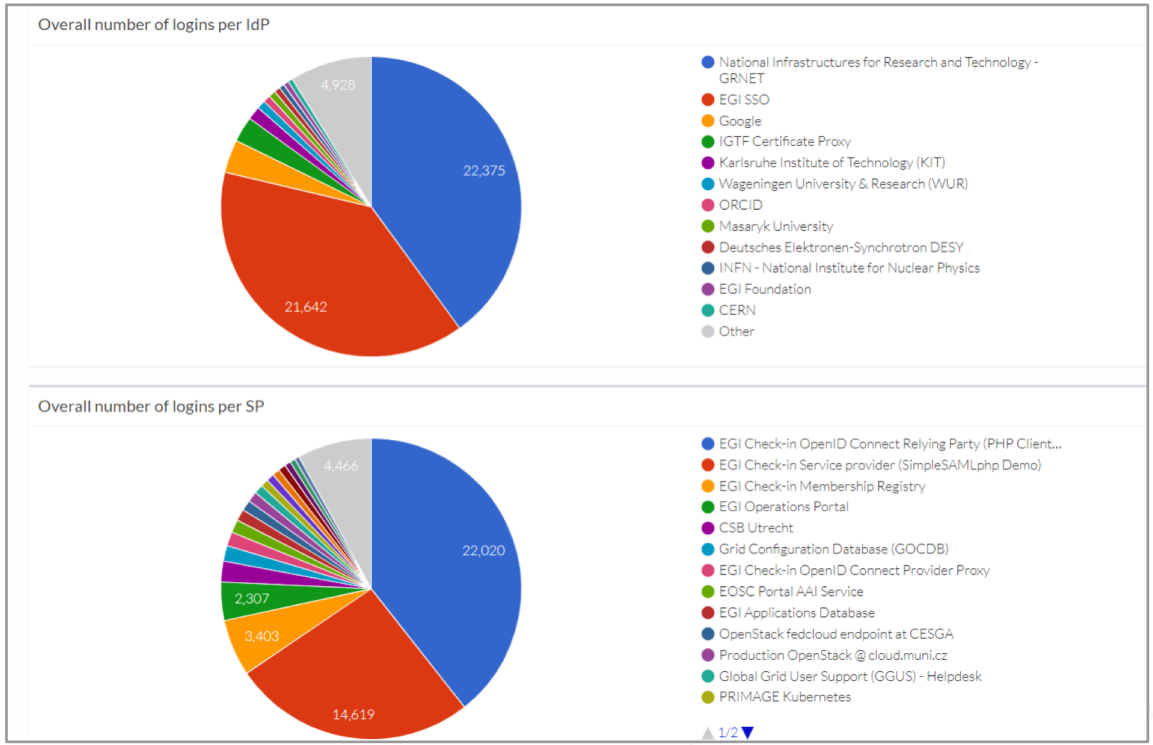
General login information



Check-in Statistics

Logins

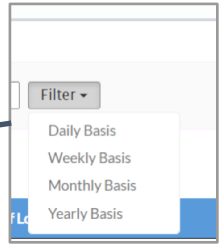
Per Identity Provider/Service Provider login information

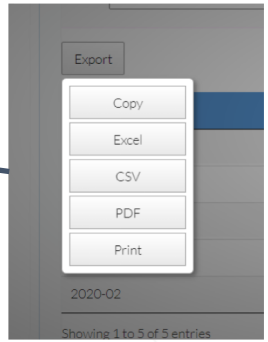


Check-in Statistics

Logins

Login information for specific date range

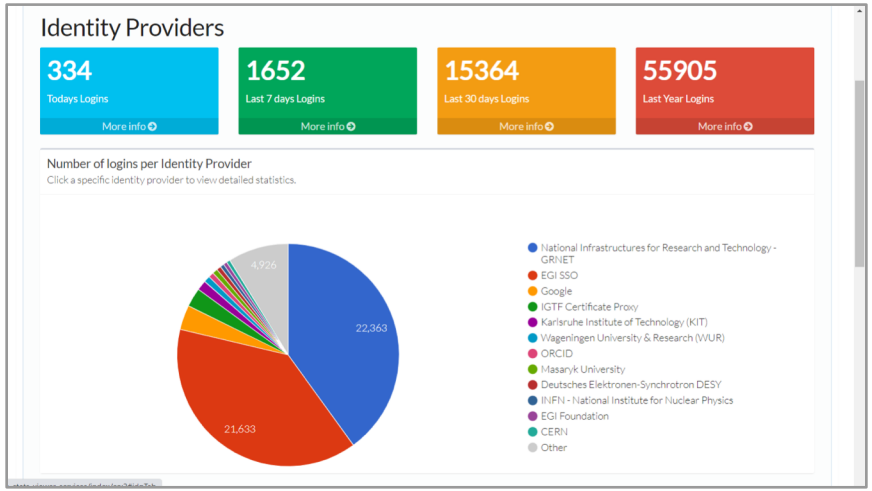


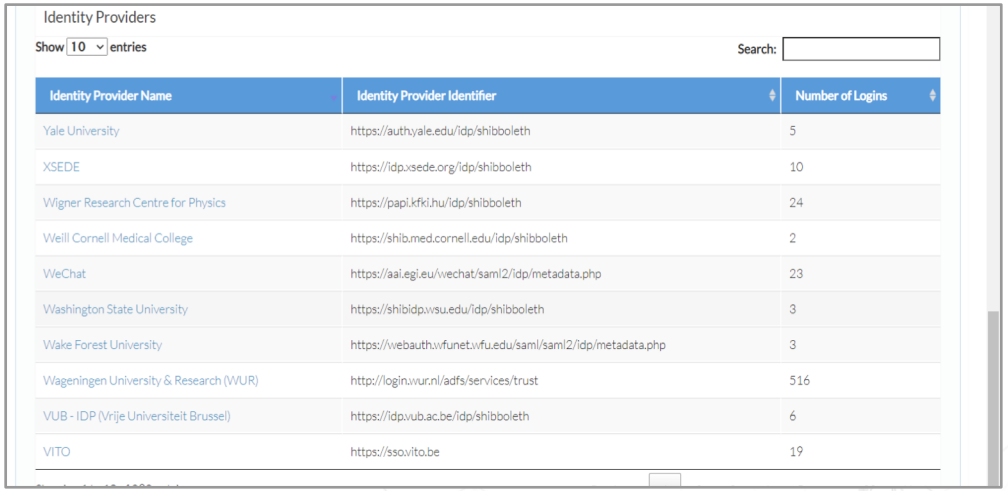


Check-in Statistics

Identity Providers

Detailed information about logins per **Identity Provider** in different views (tiles, pie charts and datatable)

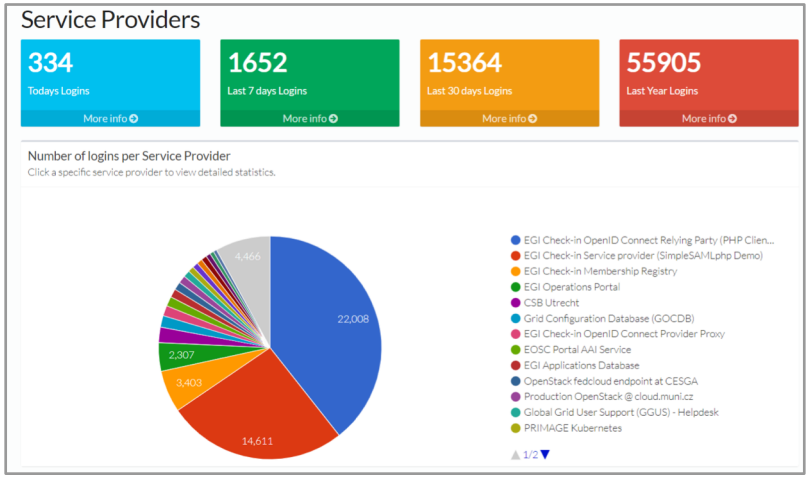


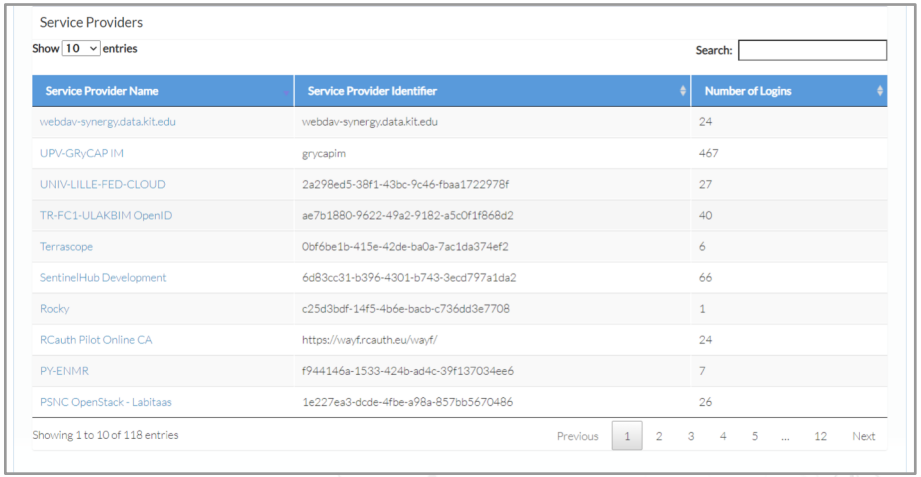


Check-in Statistics

Service Providers

Detailed information about logins per **Service Provide**r in different views (tiles, pie charts and datatable)

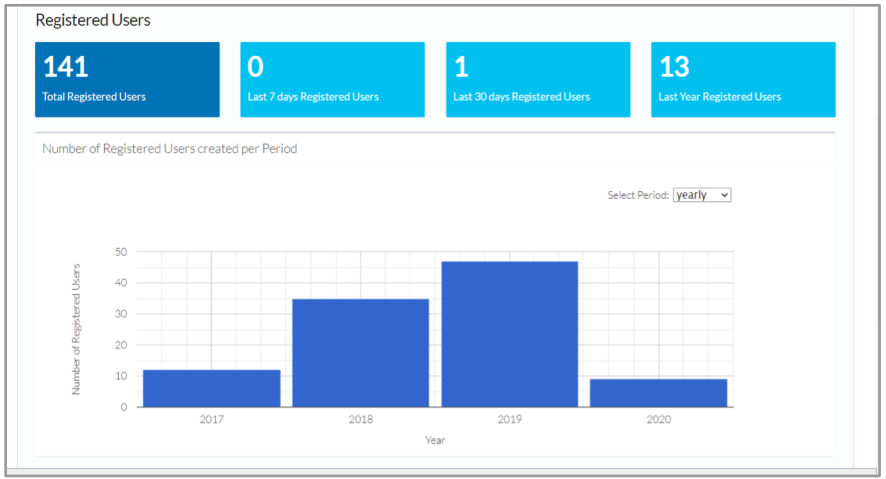


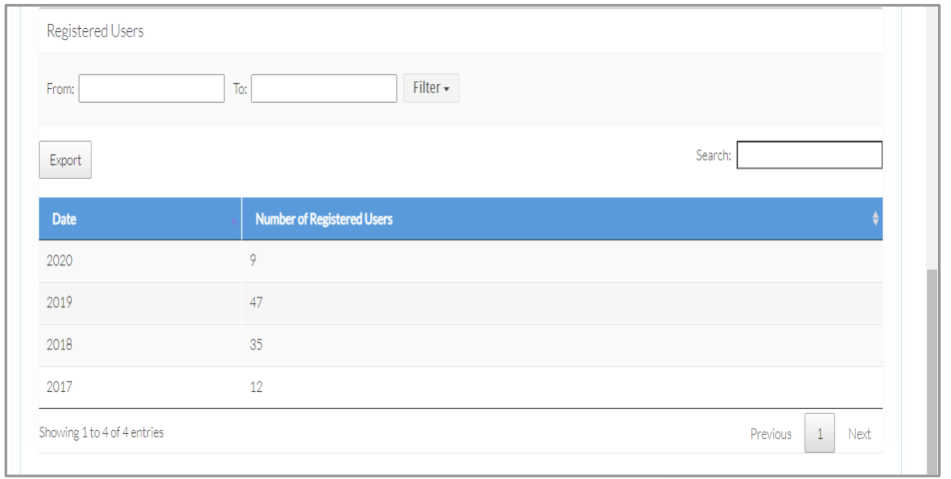


Check-in Statistics

Registered Users

Information about registered users

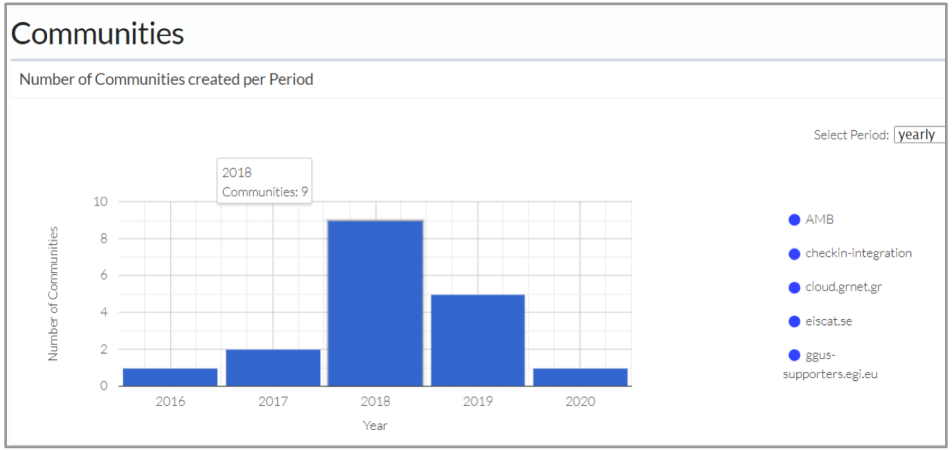


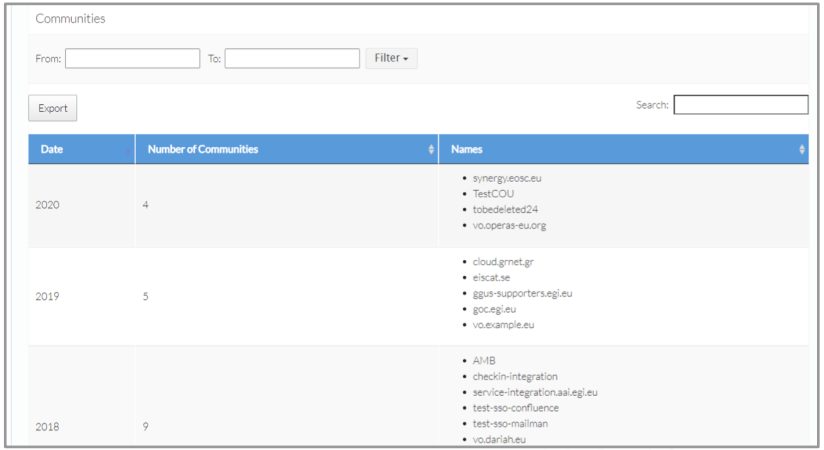


Check-in Statistics

Communities

Information about communities (Virtual Organisations) managed in Check-in COmanage Registry

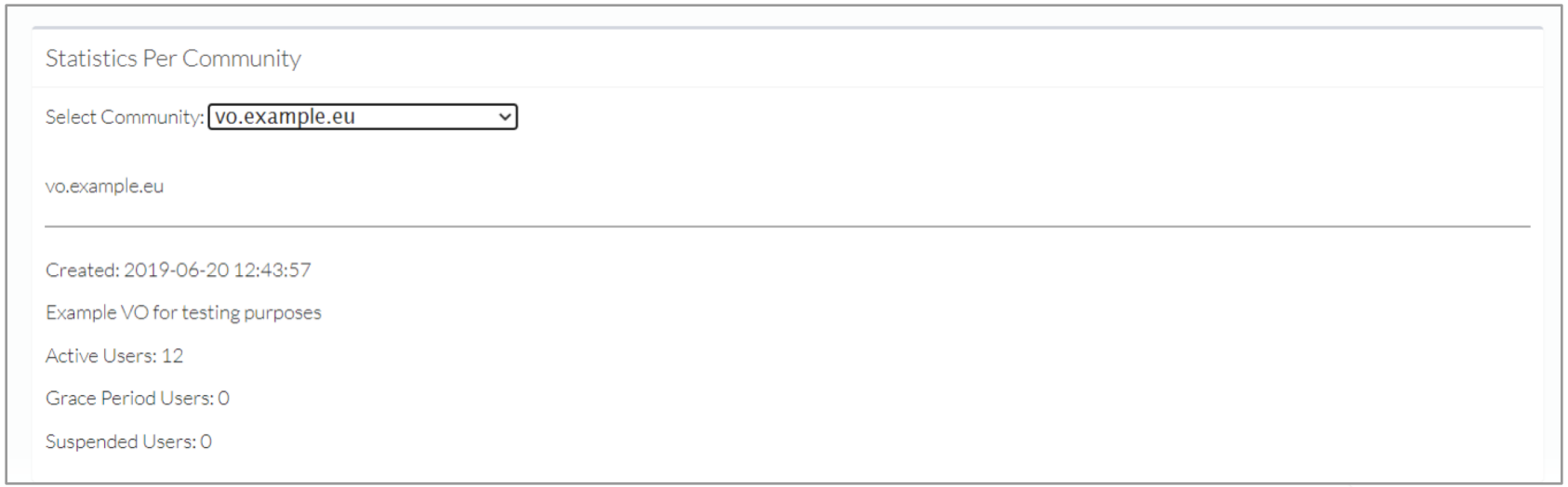




Check-in Statistics

Communities

Statistics per community

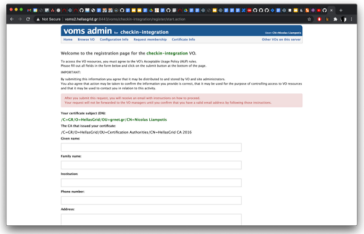


Check-in

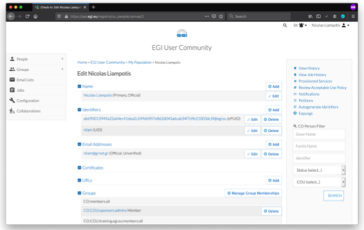
Coming soon

- Improved end-user experience
  - Identity lifecycle management
    - VO group management operations
    - Identity linking (new implicit mode)
  - IdP discovery (hinting)
- Easier integration for SAML & OIDC services and identity providers via the Federation Registry tool
- New technology options: Keycloak
- Improved statistics
  - Geo distribution of user logins
  - Per VO service statistics

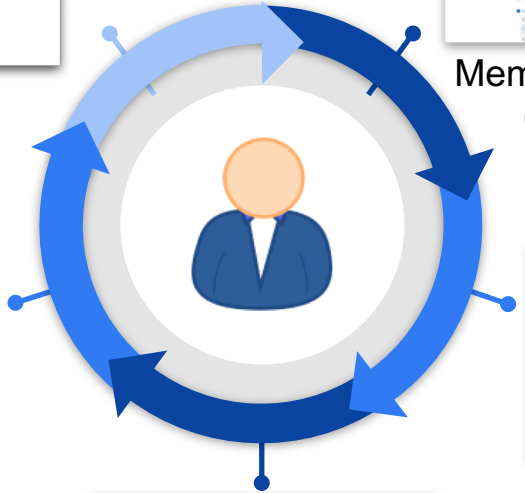
Check-in: Identity Lifecycle Management

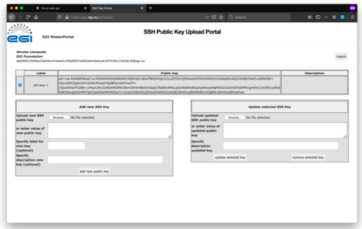


VOMS

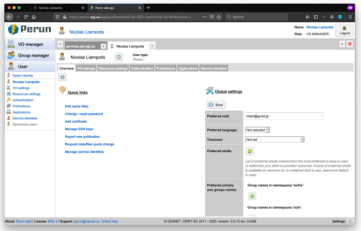


Membership Registry (COmanage)

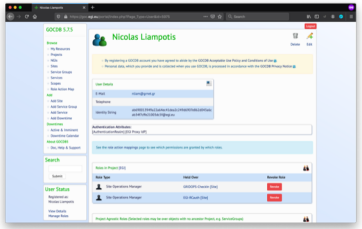




MasterPortal SSH Keys



Perun

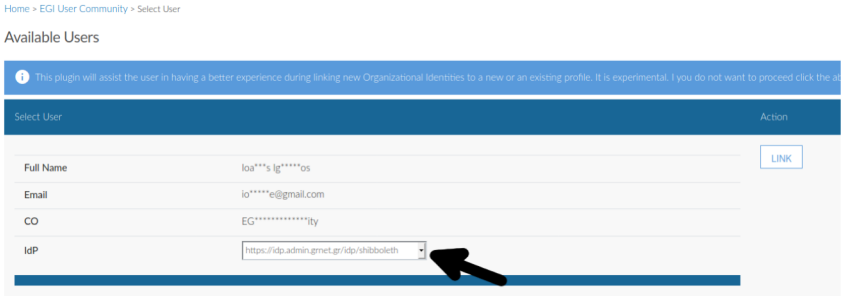


GOCDB Roles

Implicit identity linking

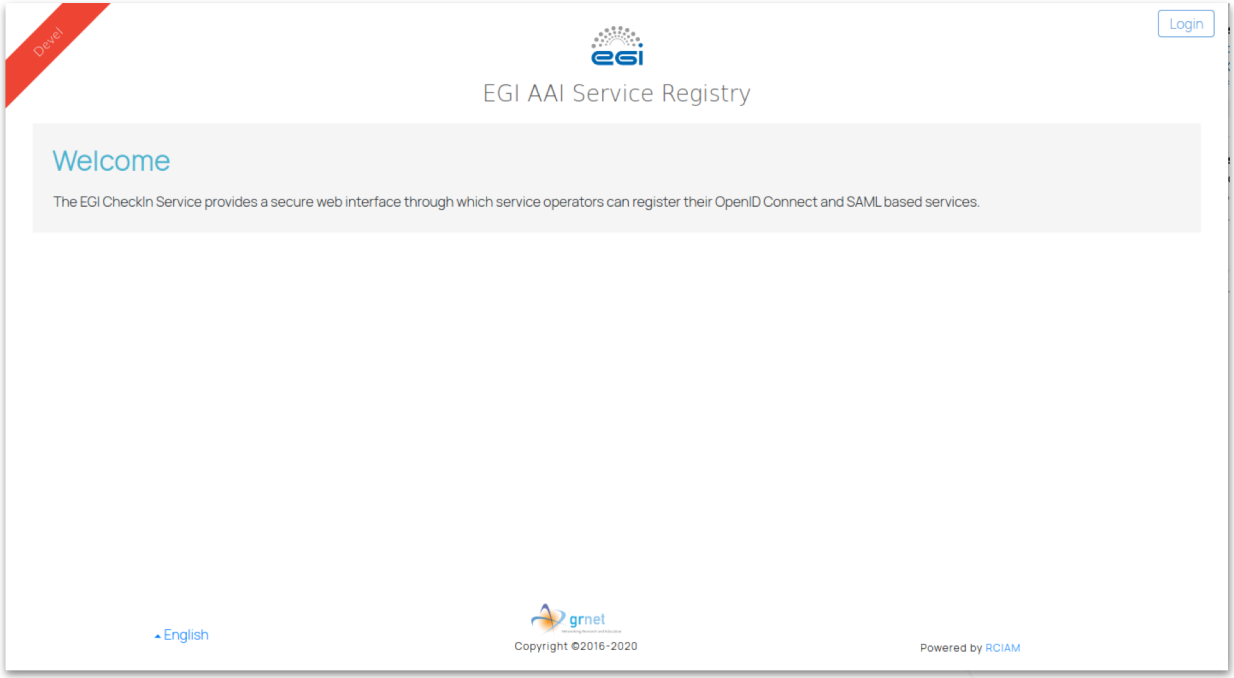
Triggered automatically when one attribute (e.g. email) -or a combination of attributes- of one identity correlate to one or more attributes of another identity that is already associated with a registered user

- Can prevent an individual from accidentally registering distinct identities



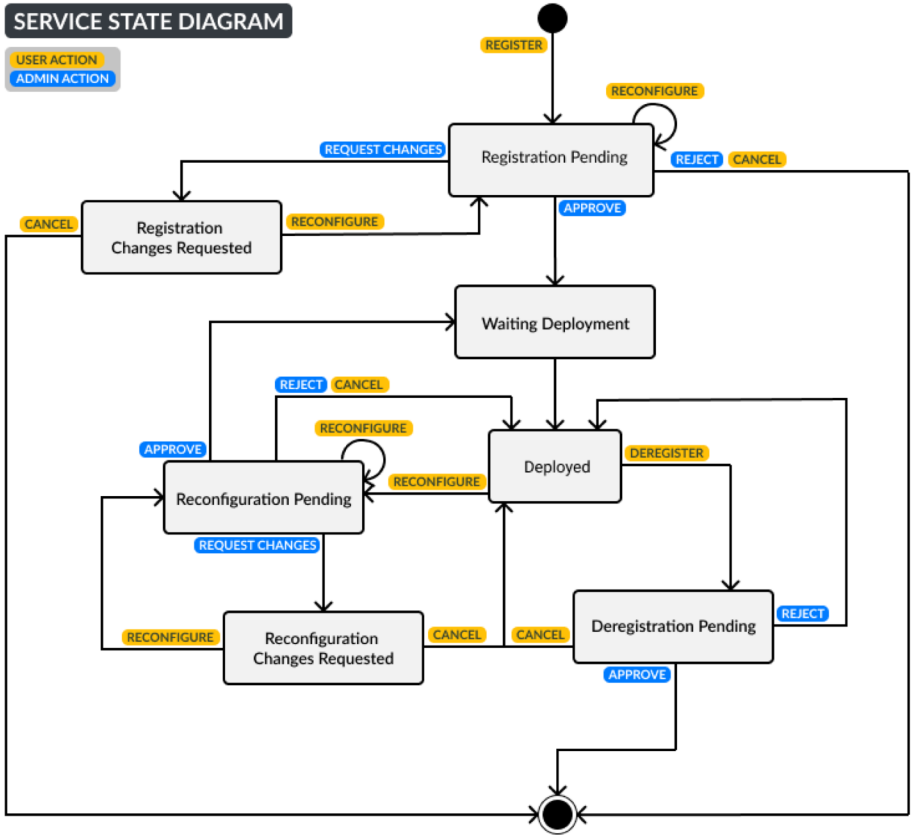
Federation Registry

- Enables the secure **registration**, **reconfiguration**, and **deregistration** of federated service and identity providers
- Provides **uniform interface** regardless of the underlying protocol (SAML vs OIDC)
- Supports **different AAI proxy technologies** (SimpleSAMLphp, MITREid Connect, SATOSA, Keycloak)



Federation Registry

Service Lifecycle

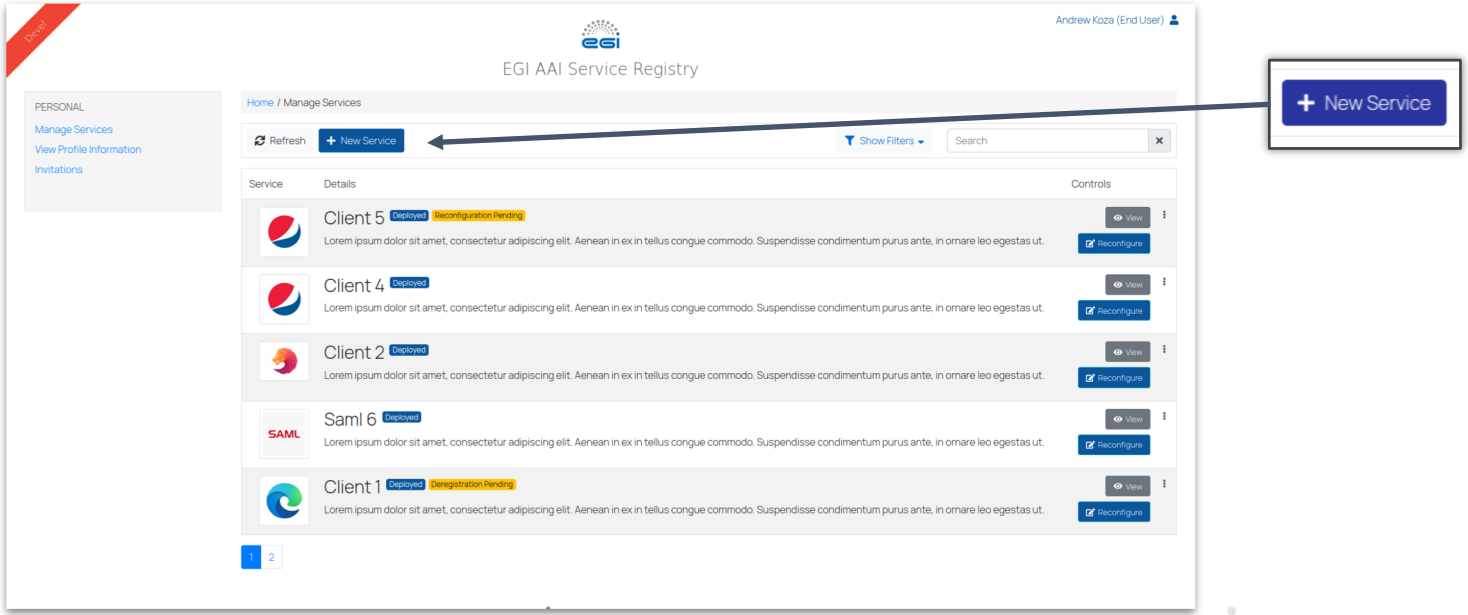


- A user interacts with a service by creating petitions
- A petition is a request to register reconfigure or deregister a service
- Petitions can be reviewed by users that have reviewing rights
- A Reviewer can either **approve**, **reject**, or **request changes**
- Once a petition has been approved the deployment procedure is initiated
- When the deployment finishes new petitions can be created once again for that service

Federation Registry

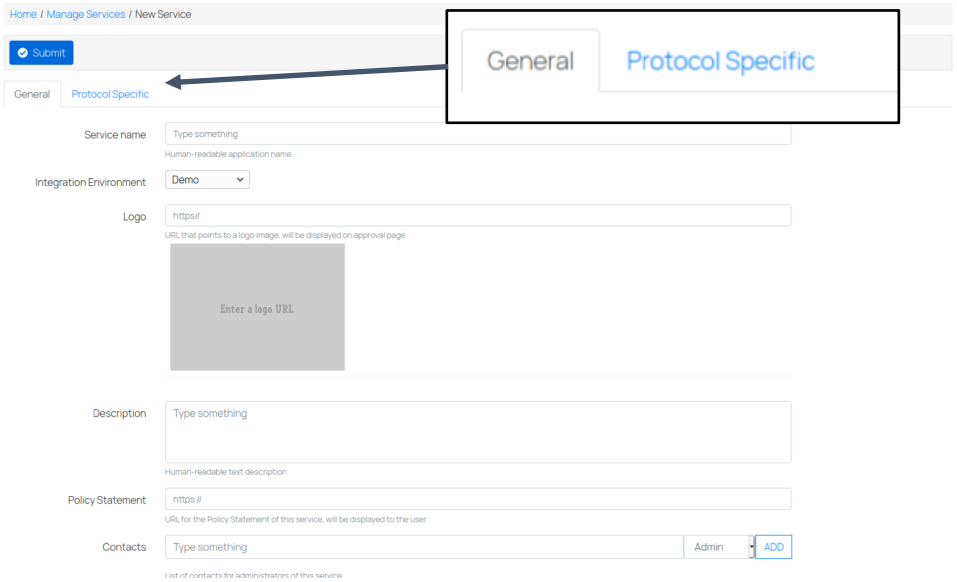
Register a service: Create petition

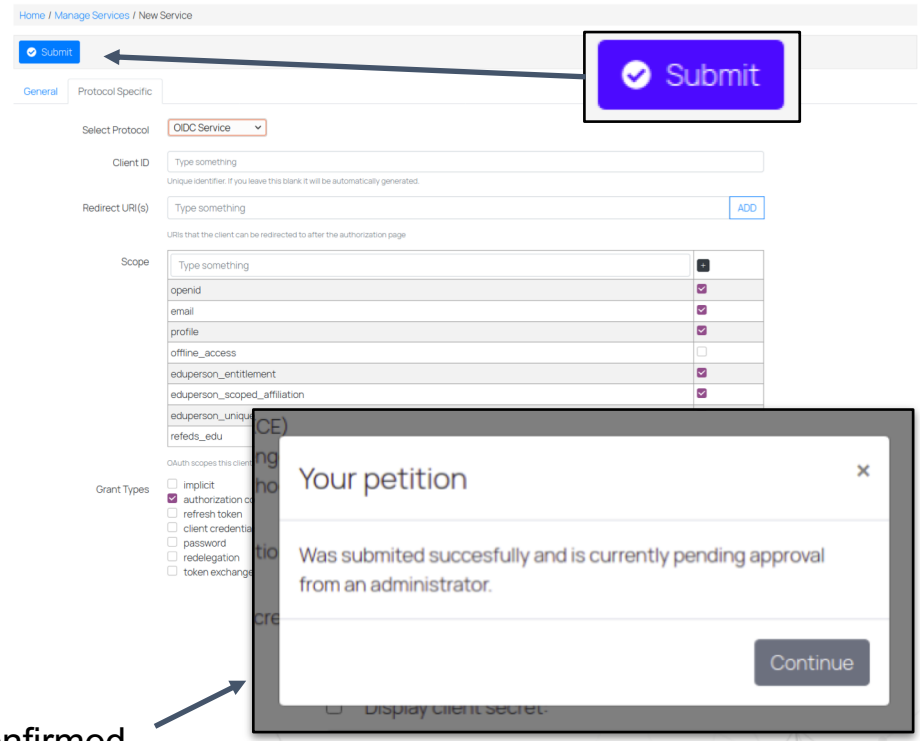
Service view



Federation Registry

Register service: Create petition



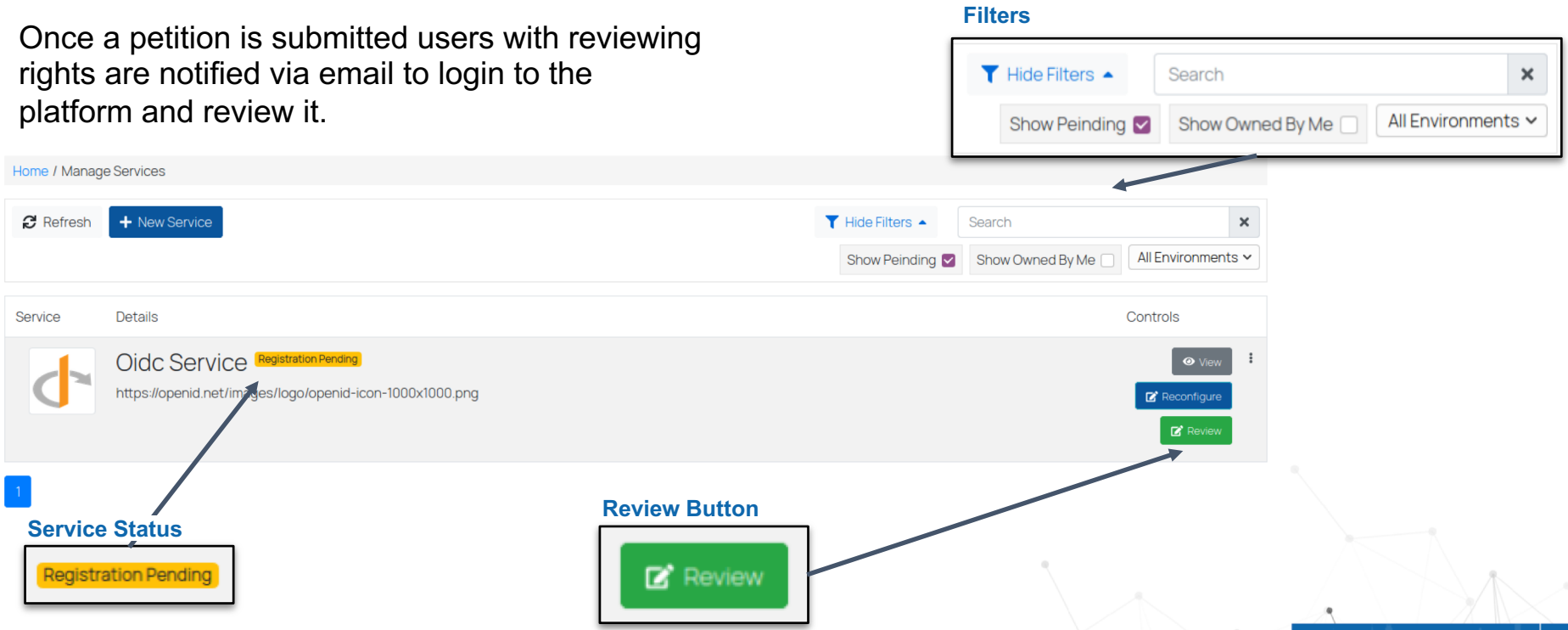


1. Fill General information and then Protocol specific in the second tab
2. Submit Form
3. Submission confirmed

Federation Registry

Register service: Review petition

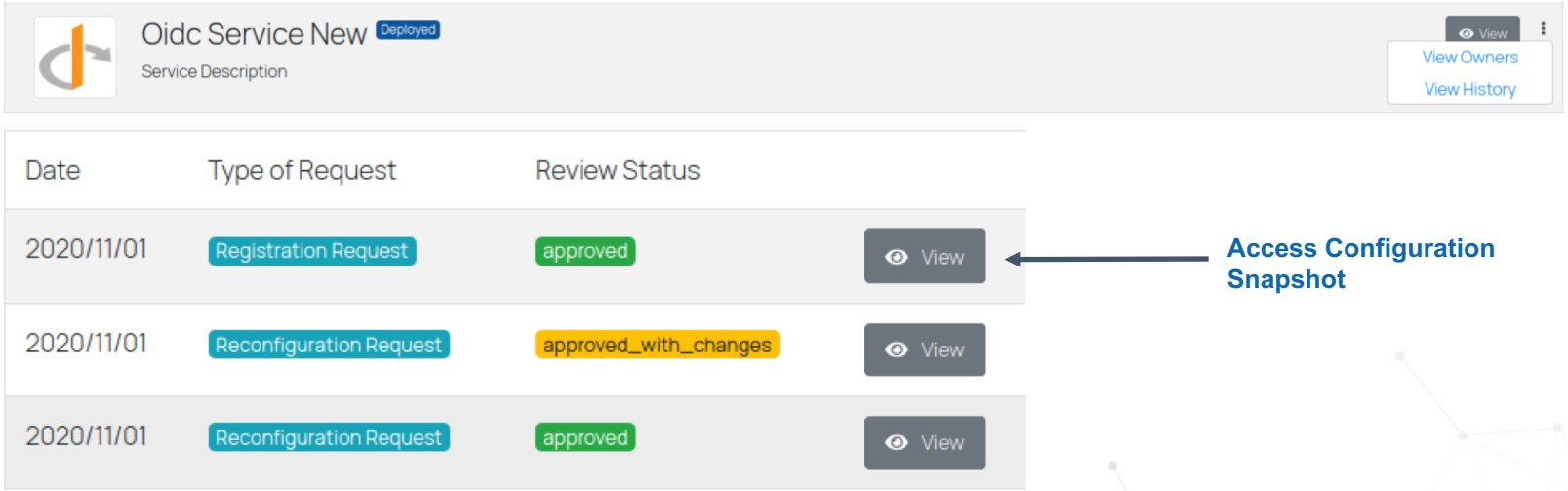
Once a petition is submitted users with reviewing rights are notified via email to login to the platform and review it.



Federation Registry

Service History

- Users can also view the History of a service since it's registration
- Each time a petition is reviewed a new snapshot of the service configuration is added to History



Federation Registry

Users

Users according the default configuration can take one of three roles “End User”, “Site-ops Manager” and “Admin”. These user roles grant users a set of actions. Role are flexible and can be modified accordingly.

End Users

- View own services
- Create Petitions to
  - Register a service
  - Reconfigure a service
  - Deregister a service

Site-ops Manager

- View own services
- Create Petitions to
  - Register a service
  - Reconfigure a service
  - Deregister a service
- Review petitions for services they own

Admin

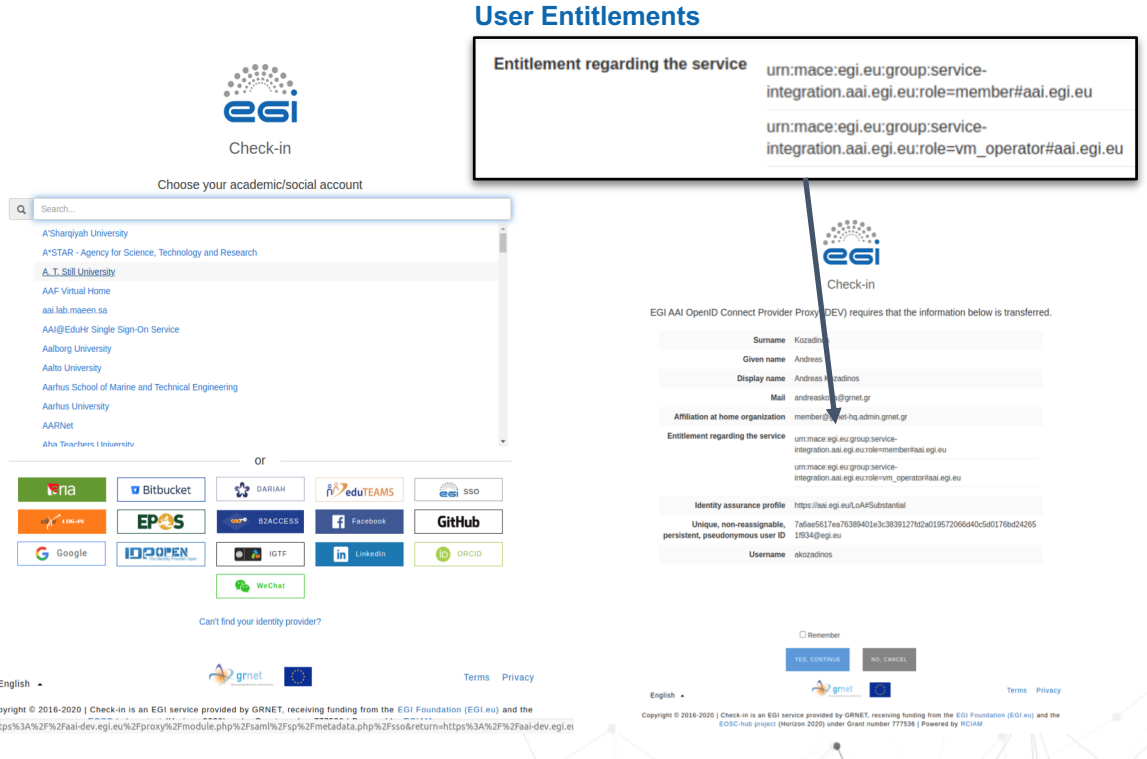
- View all services
- Create Petitions
  - Register a service
  - Reconfigure a service
  - Deregister a service
- Review petitions

*A user can create petitions only for services they own

Federation Registry

User Authorization

- Users are authenticated using an Oauth2.0 authentication proxy
- User roles are assigned based on entitlements included in user's claims
- Relation between entitlement and roles is configurable



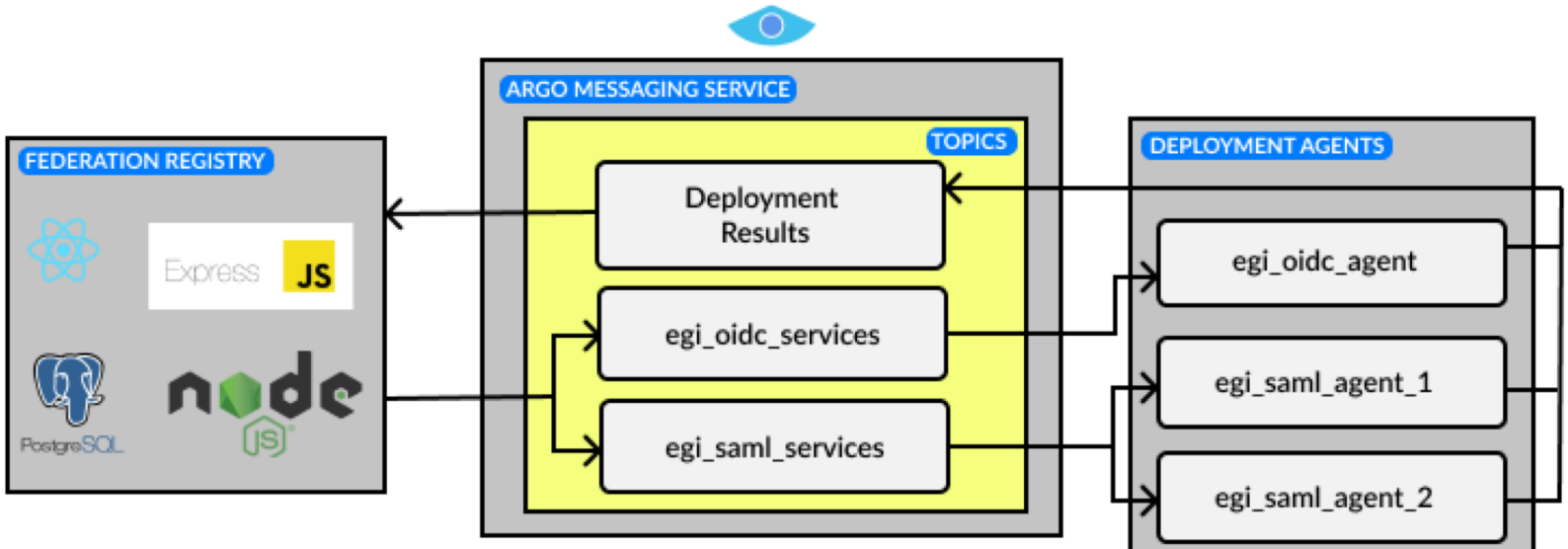
Federation Registry

Service Ownership

- A service is owned by a group of users called **owners group**
- Members of the group can view and create petitions for that service.
- Users in an owners group can take one of two roles (Member, Manager)
- Managers have control over group members, they can invite or remove members

Federation Registry

Deployment Process



1) Federation registry sends message to AMS describing new service configuration

2) Deployment Agents pulls message and updates configuration

3) Deployment Agents sends deployment result to AMS

4) AMS sends deployment result to Federation Registry

Federation Registry

Demos

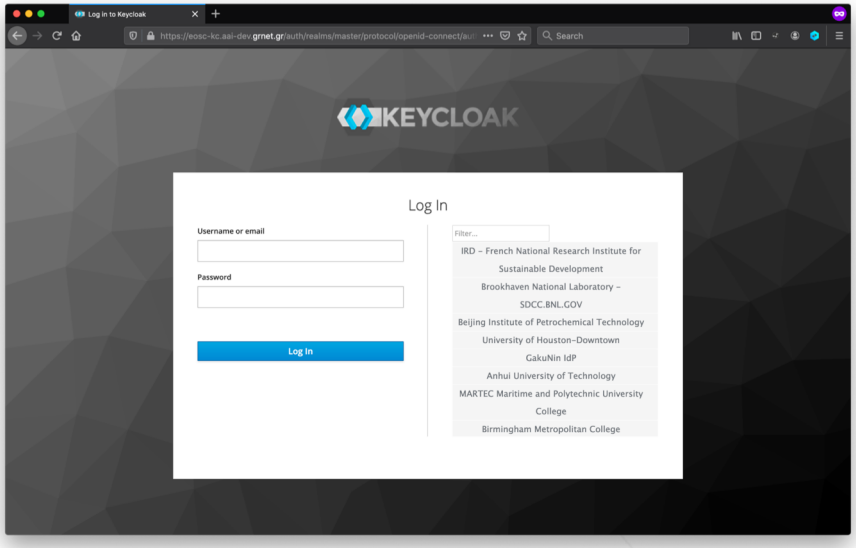
- Review & approve service registration petition
- Review & approve service reconfiguration petition
- Review service reconfiguration & request changes
- Invite user to service owner group

Check-in: New technology options

Keycloak

Extend SAML support to properly integrate with identity federations:

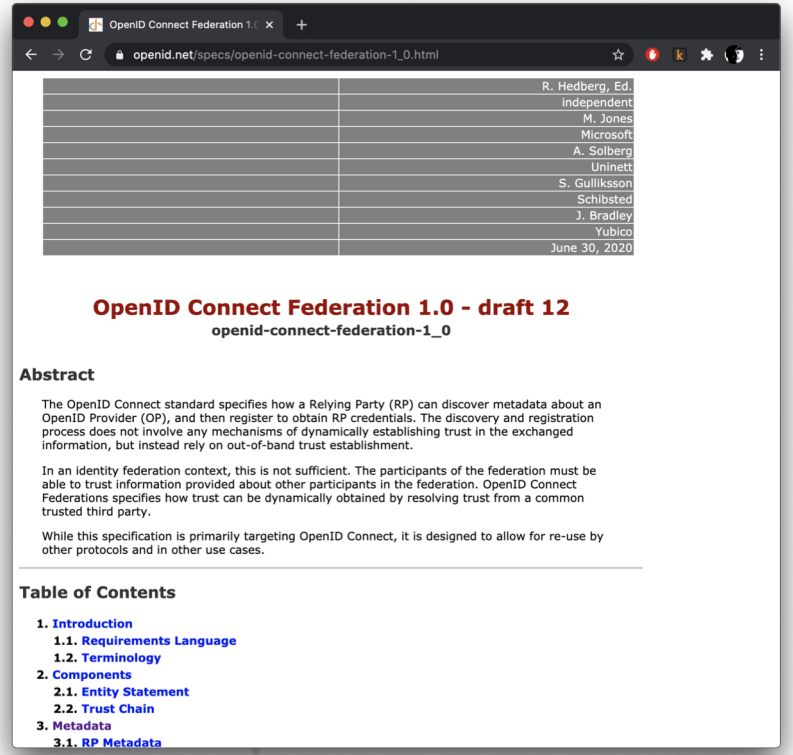
- Support federation metadata import, validation and timely refresh
- Enhance IdP discovery UI:
  - searching
  - multi-language support



Check-in: New technology options

Keycloak

- Extend Keycloak to support the OpenID connect federation standard
- Demonstrate interoperability with other components/libraries currently in development in the context of the OpenID foundation



Check-in Documentation

- Usage guide
- Integration guide for service providers
- Integration guide for identity providers
- Frequently Asked Questions

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