EGI Check-in for the Federated Cloud

Delivering Services and Solutions - Workshop

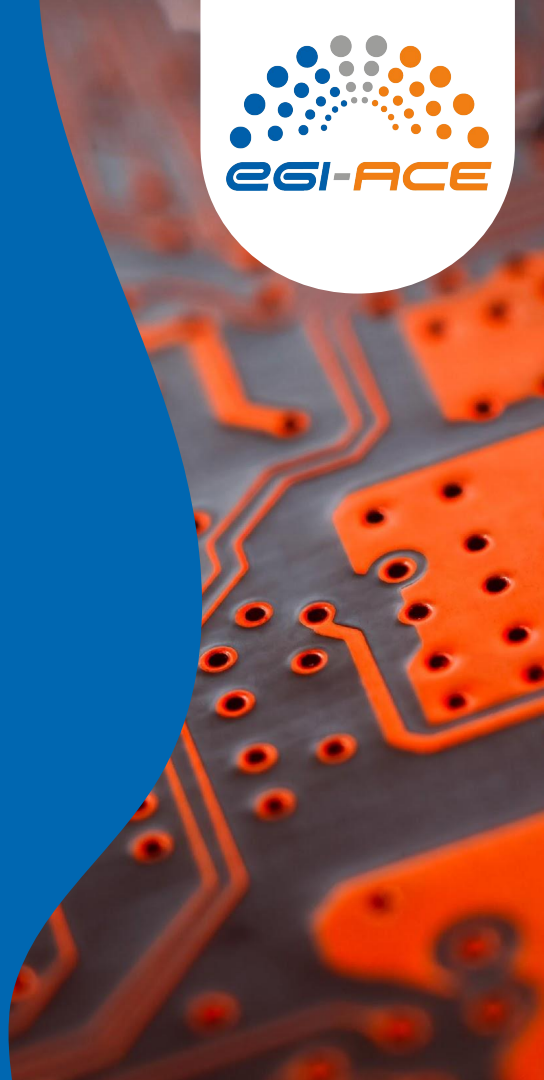
Andreas Kozadinos (GRNET)
Nicolas Liampotis (GRNET)
Valeria Ardizzone (EGI Foundation)

Dissemination level: Public

EGI-ACE receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101017567.

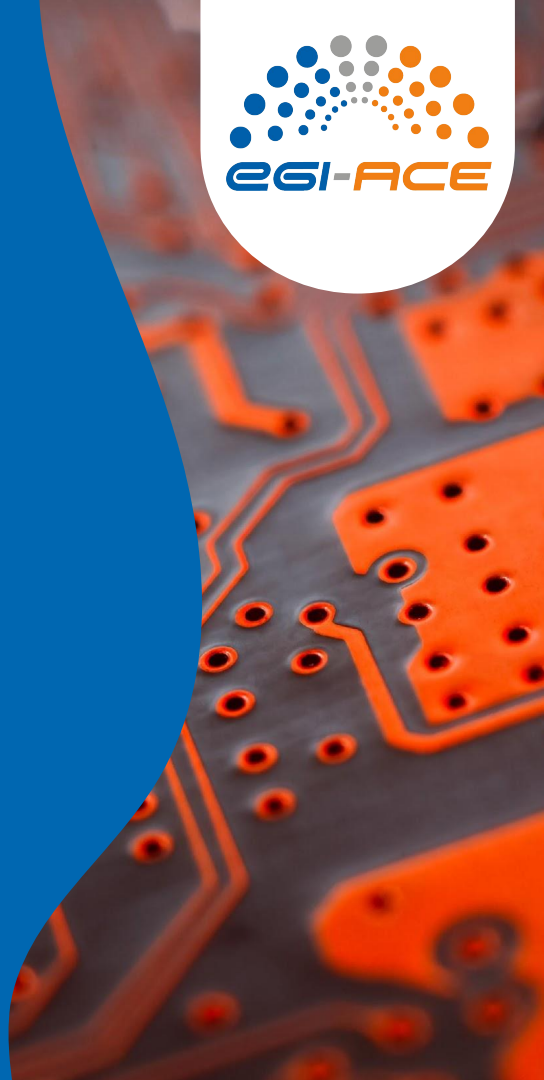
Outline

- *Check-in in a nutshell*
- *Federation Registry*
  - Service lifecycle
  - Service ownership
  - Integration environments
  - Service registration flow
  - Moving to production



Check-in

In a nutshell



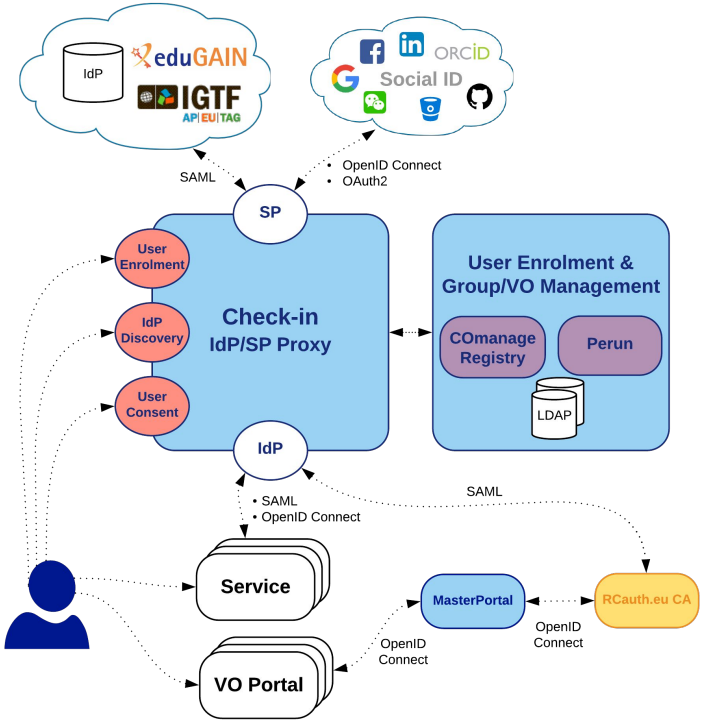
Check-in

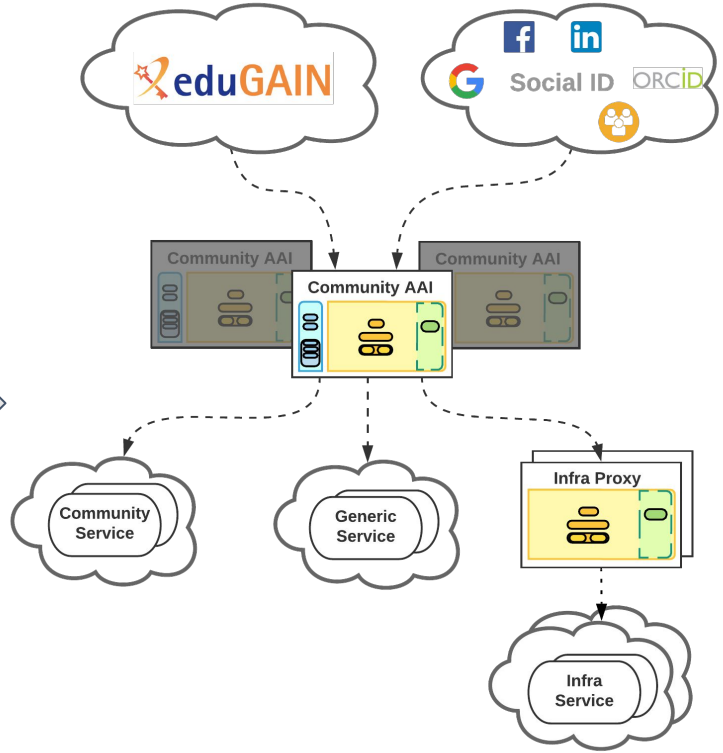
Brief introduction

- Identity and Access Management solution that makes it easy to secure access to services and resources
- Single sign-on to services through academic identity providers (eduGAIN), social media and other institutional or community-managed identity providers
- Federated access to multiple heterogeneous (web and non-web) service providers using different technologies (SAML, OpenID Connect/OAuth 2.0, X.509)
- Access to resources using different login credentials (academic/social) via identity linking
- Expressing the level of trust in the identity assertions
- Aggregation and harmonisation of authorisation information (Virtual Organisations/groups, roles, assurance) from multiple sources

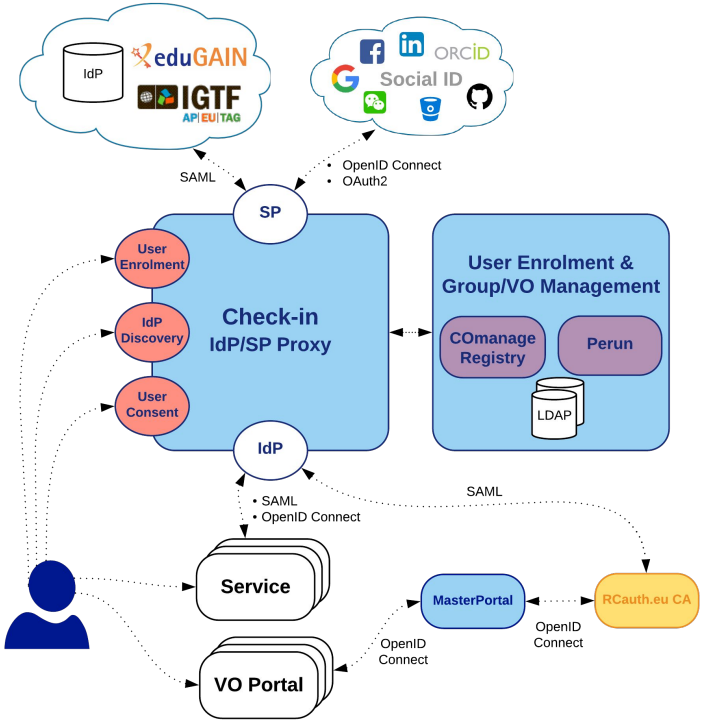
Check-in
Architecture

Implementation of the
AARC Blueprint Architecture





Check-in
Architecture



Implementation of the
AARC Blueprint Architecture

COMMUNITY AAI

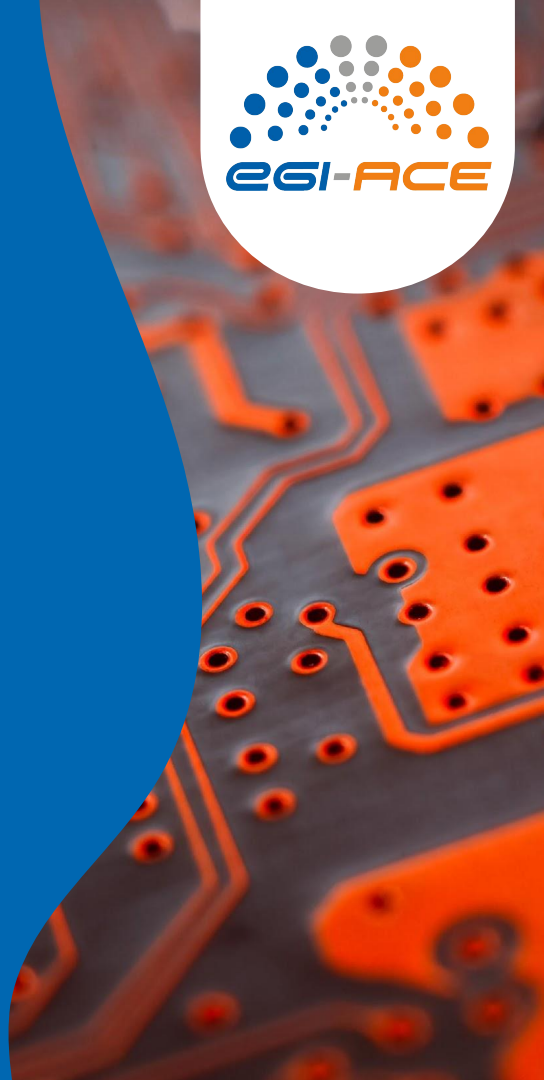
Enables the use and management of community identities, Virtual Organisations, groups and roles (COmanage Registry & Perun)

INFRASTRUCTURE PROXY

Enables communities (managed by Check-in or external Community AAIs) to access to resources offered by Service/Resource Providers

Federation Registry

Service Management Portal

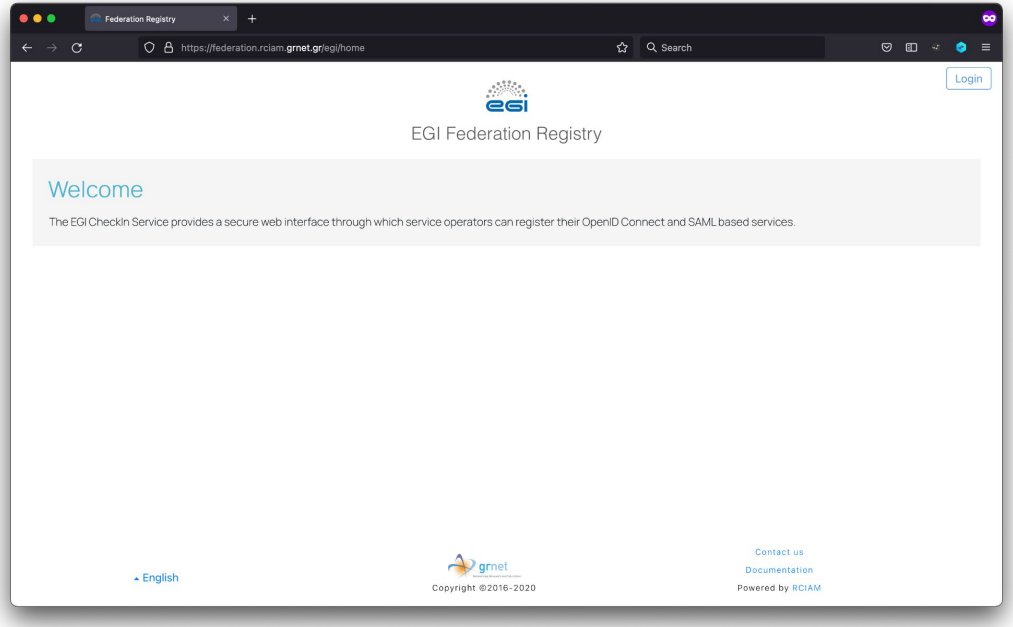


grnet
Networking Research and Education

Federation Registry

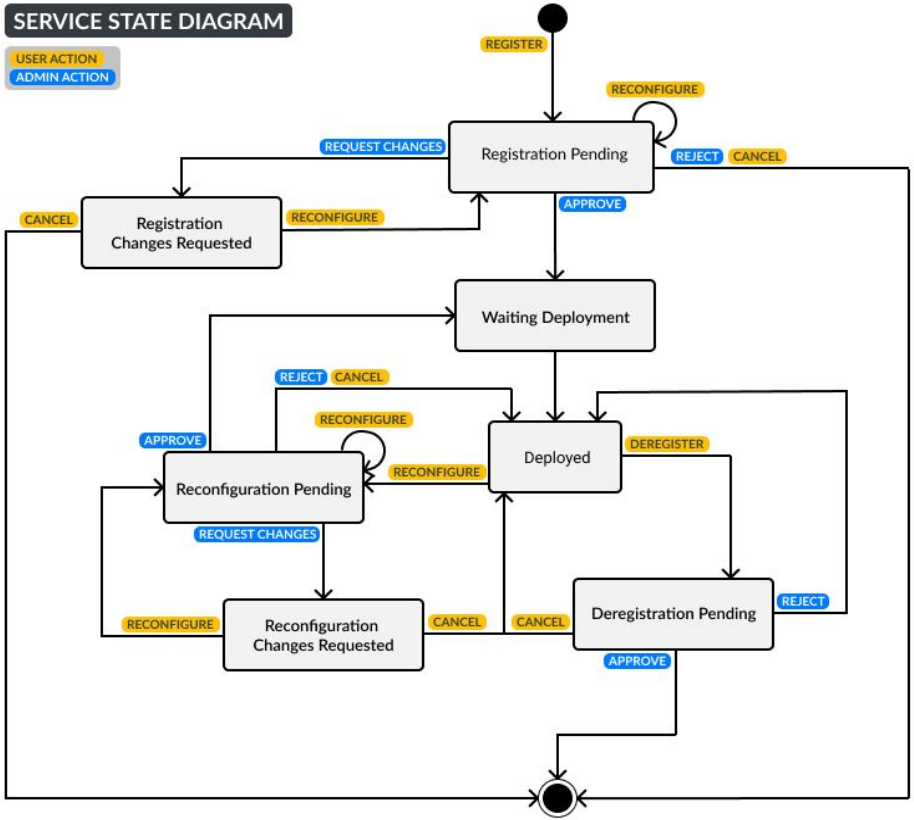
Introduction

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



Federation Registry

Service Lifecycle



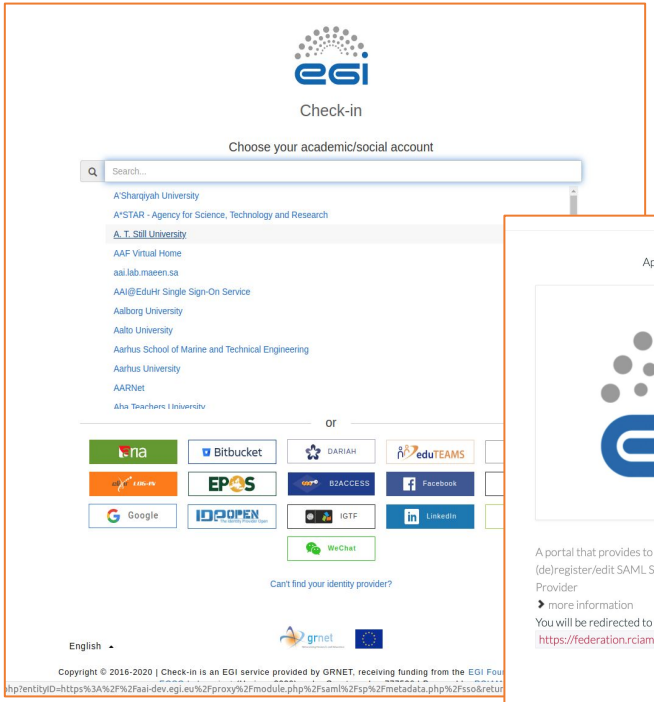
- A resource owner interacts with a service by creating **service requests**
- Resource owners can request to **register**, **reconfigure** or **deregister** a service
- Service requests can be **reviewed** by users who have reviewing rights
- A Reviewer can either **approve**, **reject**, or **request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

Federation Registry

Accessing the portal

Resource owners access the portal through Check-in:

1. Click the login button
2. Select your identity provider
3. Authenticate at your identity provider with your credentials
4. Sign up for Check-in identity (first time only)
5. Authorise Federation Registry to access your Check-in profile information:
   a. User identifier
   b. Name
   c. Username
   d. Email address



Federation Registry

In a nutshell

Resource owners use the EGI Federation Registry to manage their services. The platform provides a user friendly interface where resource owners can create, edit and delete services by creating requests. Resource owners can also co-manage their services with other members of their team.

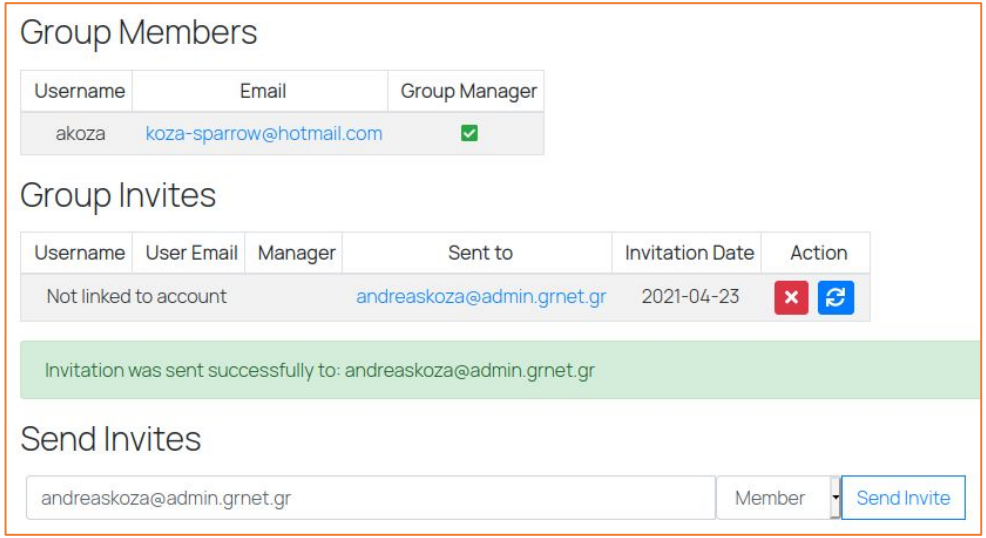
- View own services
- Create Requests to
  - Register a service
  - Reconfigure own services
  - Deregister own services
- Review their own Service Request
- Invite other users to collaboratively manage a service
- View History of Past Configurations
- Copy Service from one environment to another (e.g. from Demo to Production)

*A resource owner can create requests only for services they own

Federation Registry

Service Ownership

- A service is owned by a group of users called **owners group**
- Users in an owners group can take one of two roles:
  - **Member**
  - **Manager**
- Both **Members** & **Managers** can view and create reconfiguration requests for that service.
- **Managers** have control over group members, and can invite or remove users



Manage Owners

Federation Registry

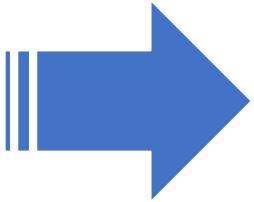
Integration Environments

DEMO

- Used for Production-ready Services
- Supports all academic & social login options
- Service registration / reconfiguration requires approval by Check-in admins:
  - Review of technical parameters

DEVELOPMENT

- Used for testing experimental features of Check-in
- Supports limited login options
- Service registration / reconfiguration can be self-approved by service owners



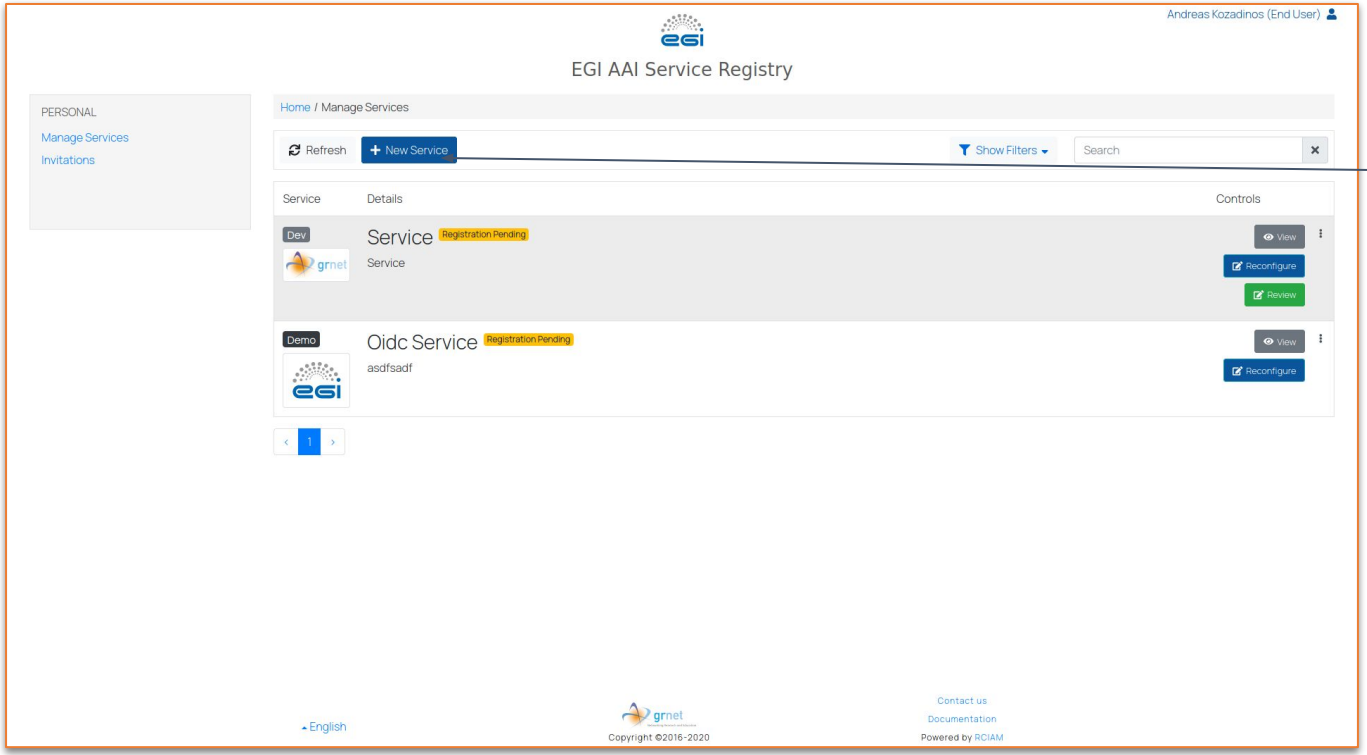
PRODUCTION

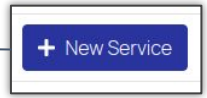
- Used for Services in Production
- Supports all academic & social login options
- Service registration / reconfiguration requires approval by Check-in admins:
  - Review of technical parameters
  - Review of policy aspects

See DOCUMENTATION

Federation Registry

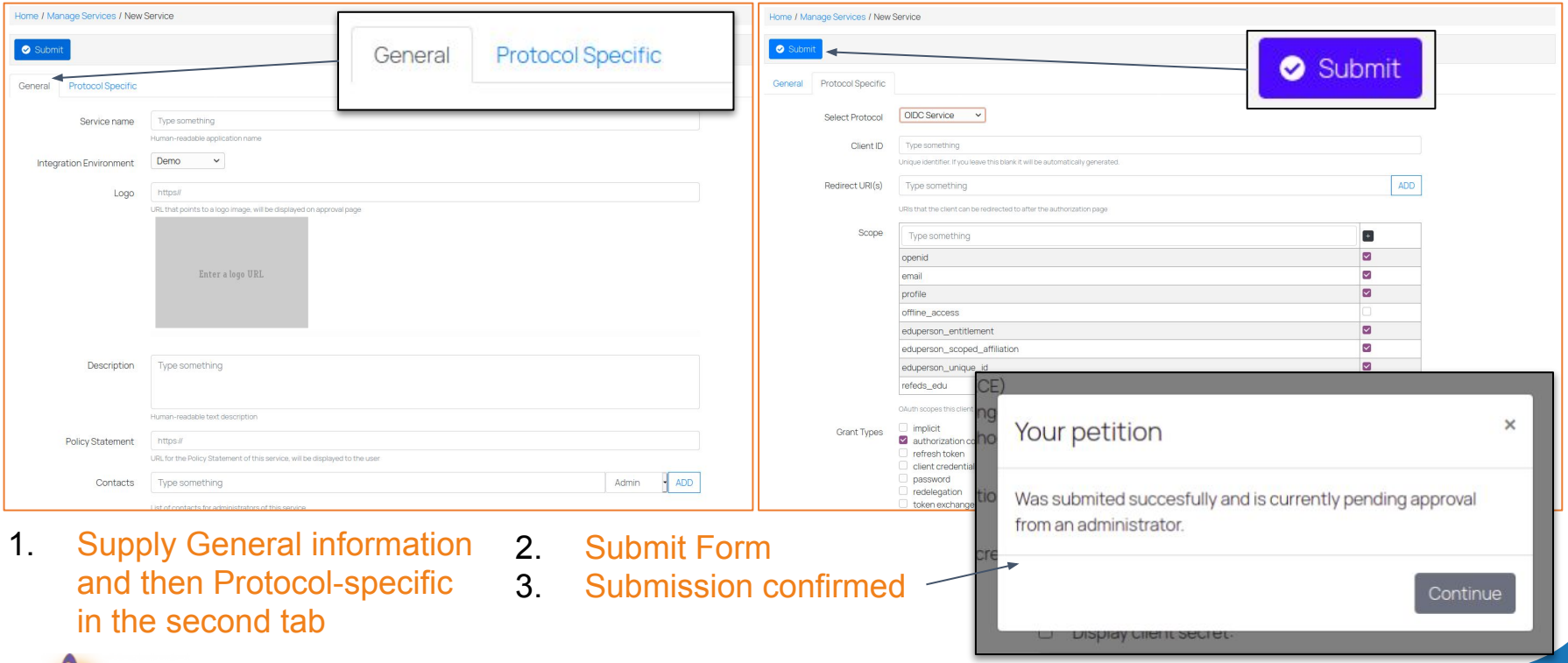
Register service: Create Registration Request





Federation Registry

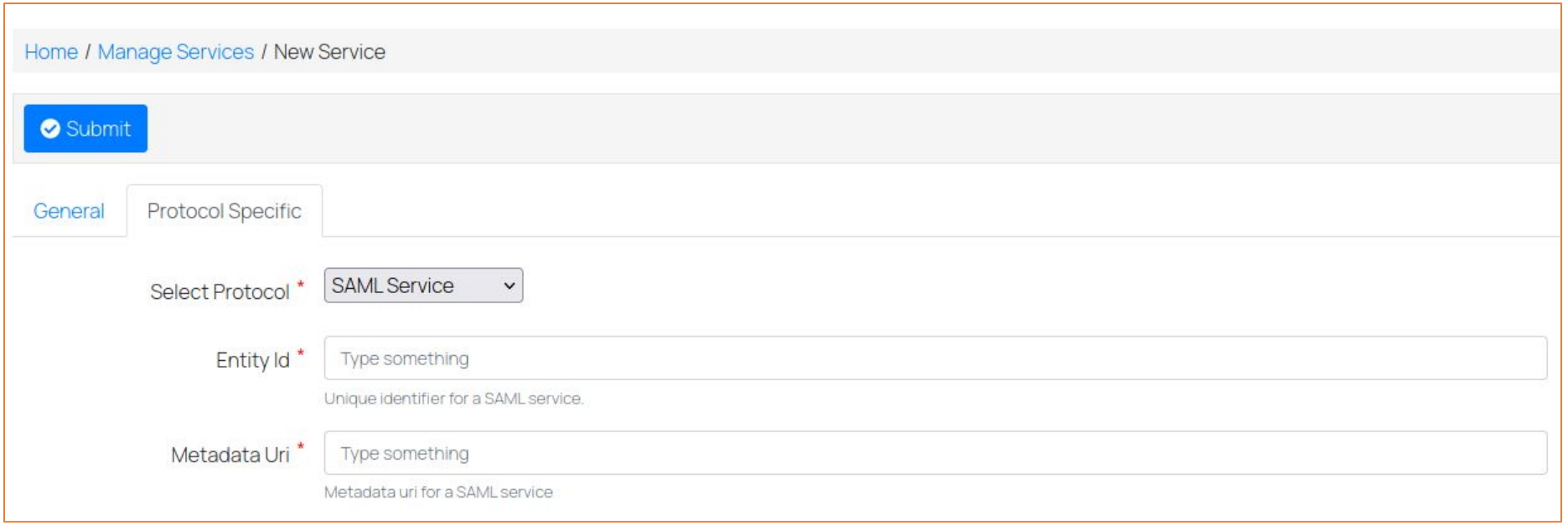
Register service: Create Service Request



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

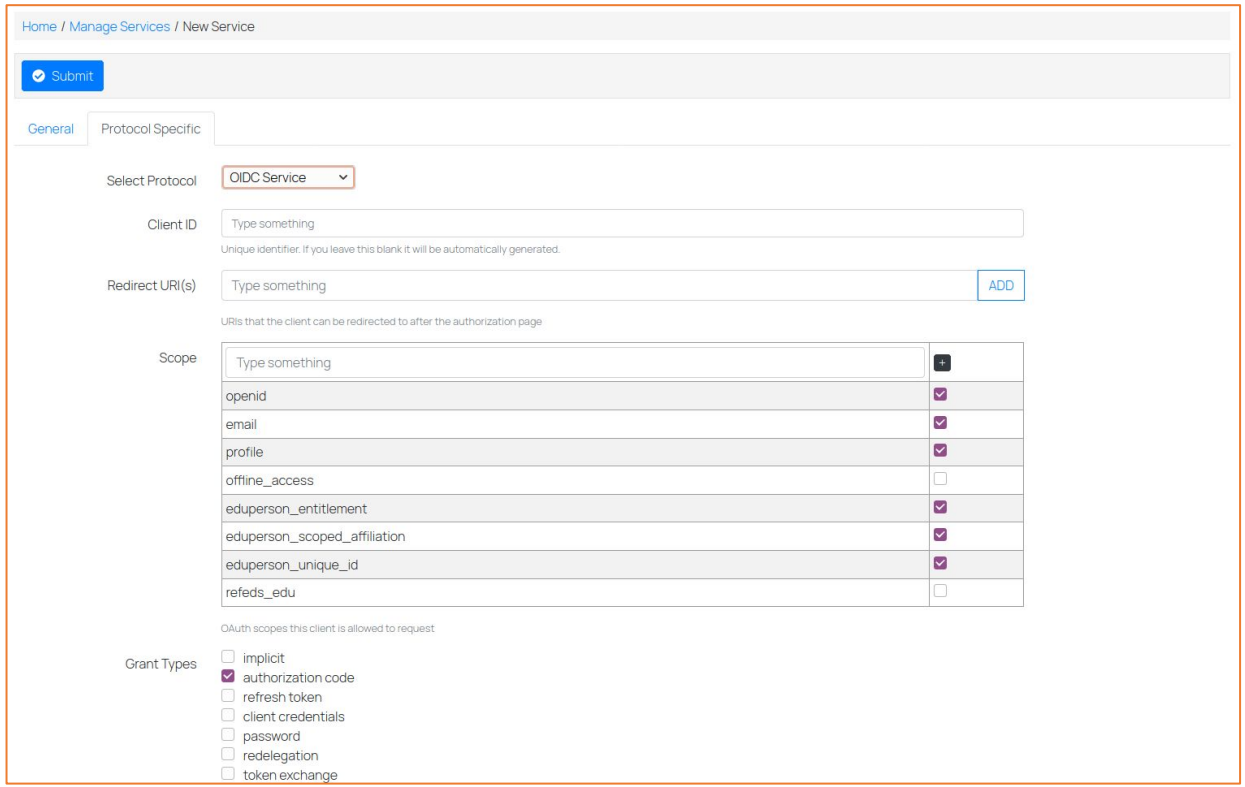
Federation Registry

Register service: Create Service Request (Saml)



Federation Registry

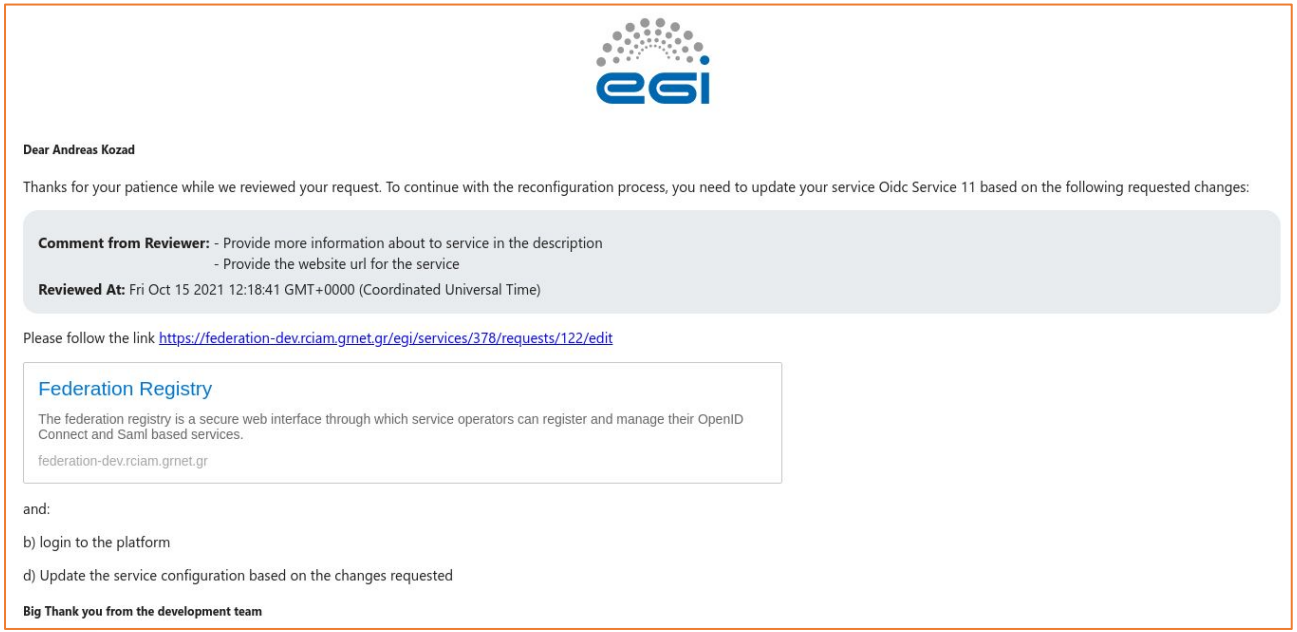
Register service: Create petition - Choosing scopes



Federation Registry

Review Request: Requested Changes

Resource owners are notified and prompted to reconfigure their petition when a reviewer has requested changes.



Dear Andreas Kozad

Thanks for your patience while we reviewed your request. To continue with the reconfiguration process, you need to update your service Oidc Service 11 based on the following requested changes:

Comment from Reviewer: - Provide more information about to service in the description
- Provide the website url for the service

Reviewed At: Fri Oct 15 2021 12:18:41 GMT+0000 (Coordinated Universal Time)

Please follow the link https://federation-dev.rciam.grnet.gr/egi/services/378/requests/122/edit

Federation Registry

The federation registry is a secure web interface through which service operators can register and manage their OpenID Connect and Saml based services.

federation-dev.rciam.grnet.gr

and:

b) login to the platform

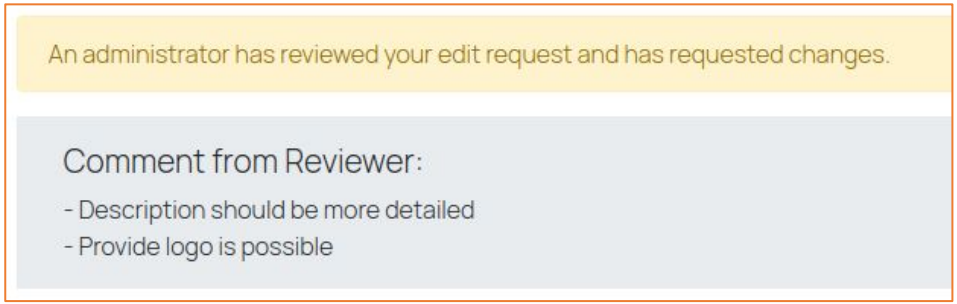
d) Update the service configuration based on the changes requested

Big Thank you from the development team

Federation Registry

Review Request: Requested Changes

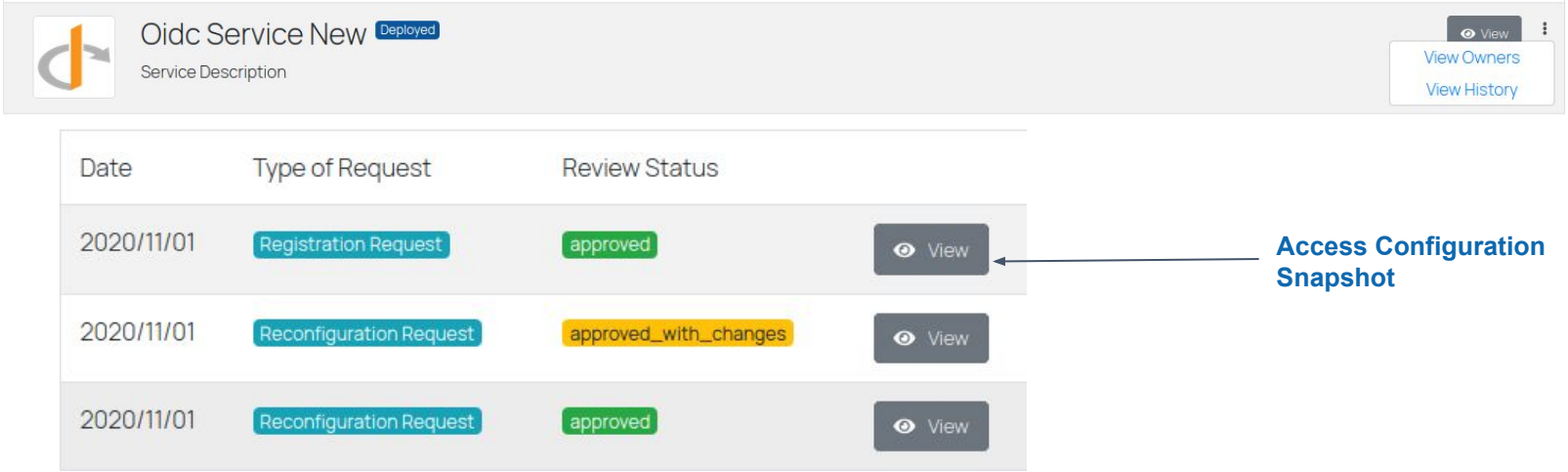
When reconfiguring their service request, resource owners can also view the comment the reviewer left



Federation Registry

Service History

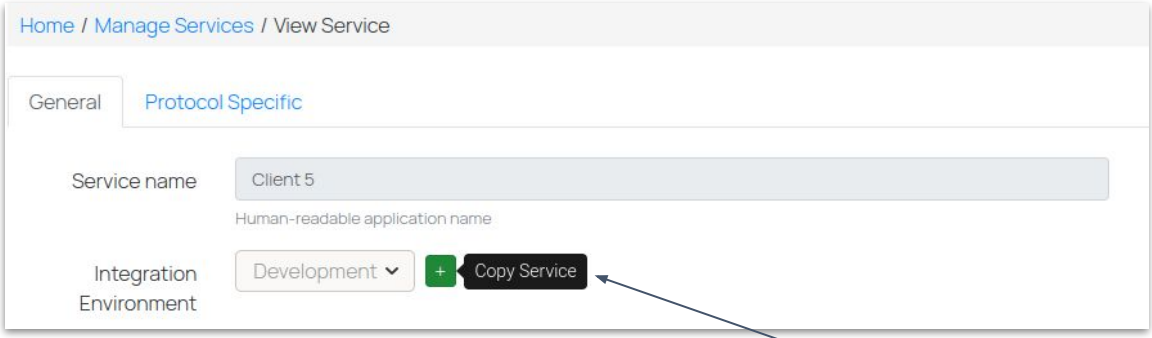
- Resource owners can also view the History of a service since it's registration
- Each time a petition is reviewed a new snapshot of the service configuration is added to History



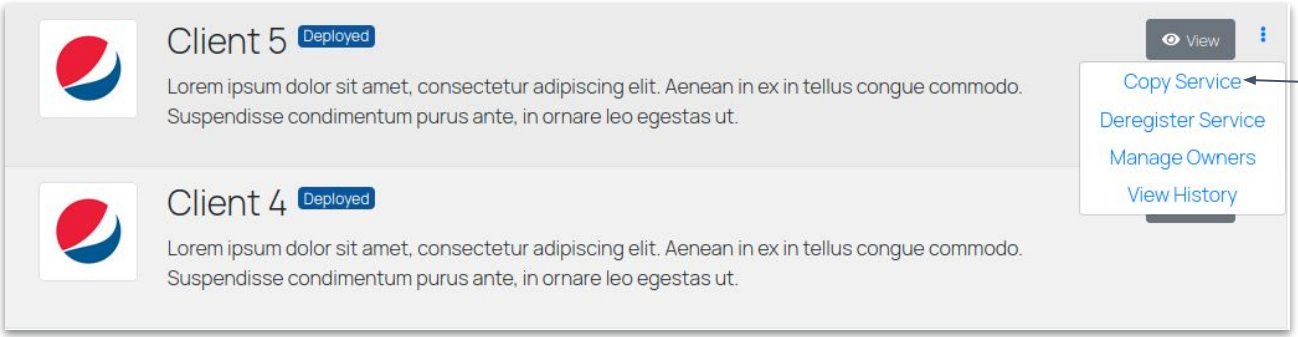
Federation Registry

Moving to production

Deployed services can be copied to different environments by using the copy option.



When viewing the service

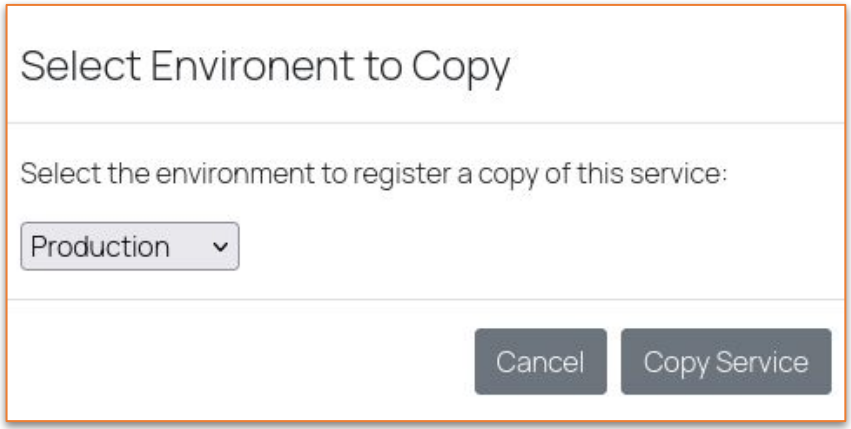


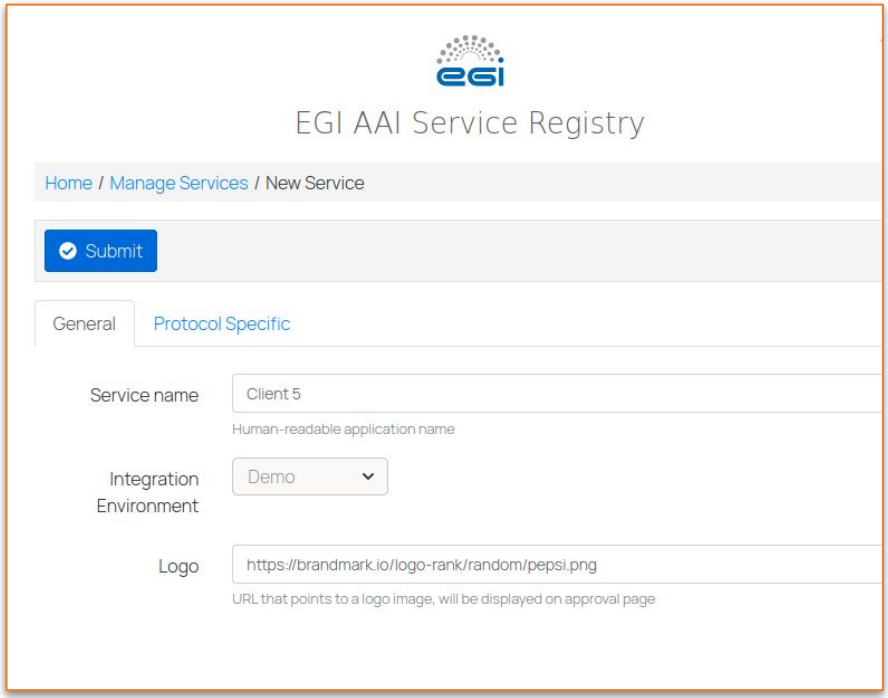
More Service Options Dropdown Menu

Federation Registry

Moving to production

- Users select target environment
- A copy of the selected service is loaded into a new service form
- Users may edit the configuration and then submit the petition request



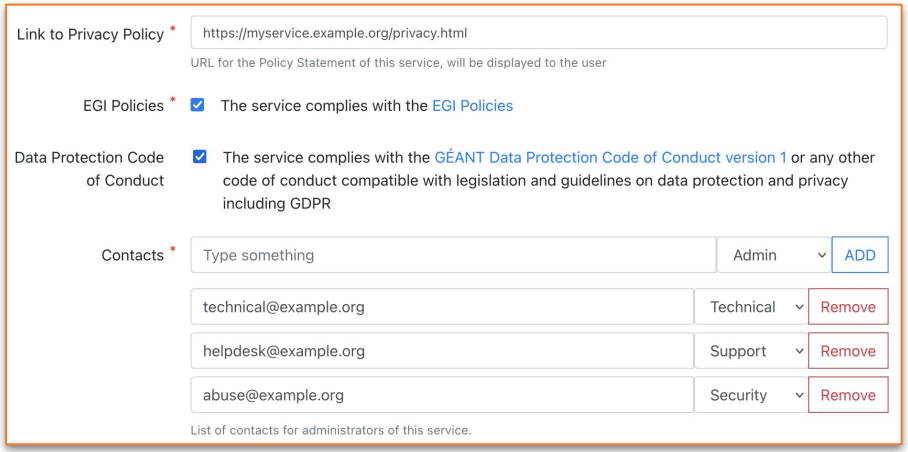


Federation Registry

Moving to production

Policy requirements:

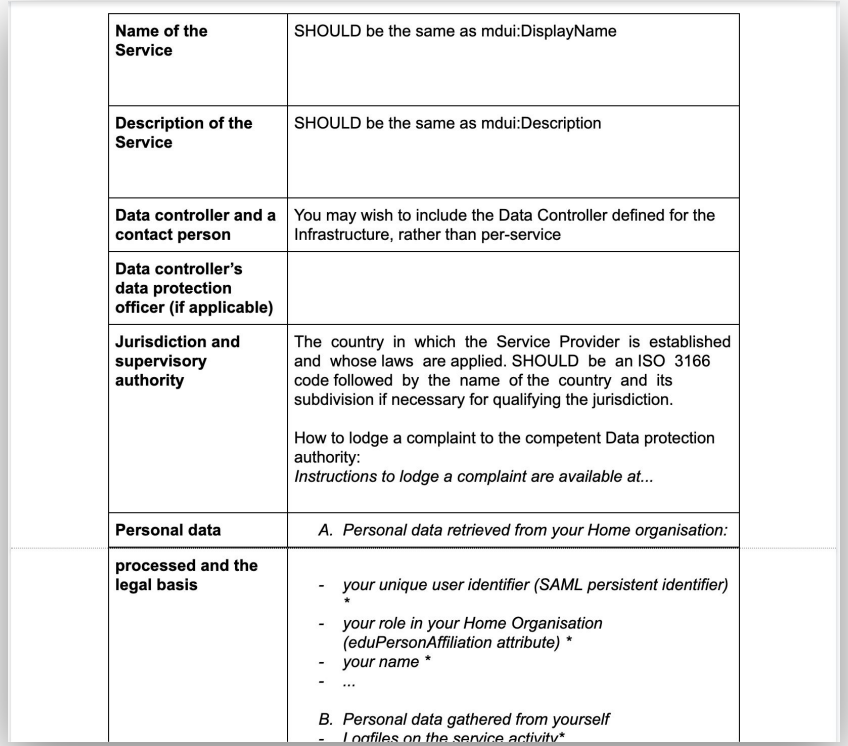
- Link to privacy policy
- Compliance with EGI security policies
- Compliance with data protection code of conduct (e.g. GÉANT Code of Conduct version 1 or any other code of conduct compliant with GDPR)
- Security contact (SIRTFI security incident response framework)



Federation Registry

Moving to production: Privacy Policy

- Questions to ask yourself when defining this policy:
  - Which information do you need to collect on the user?
  - Is the collected information shared with third parties?
  - How long will the data be kept?
- Need help?
  - See AARC template

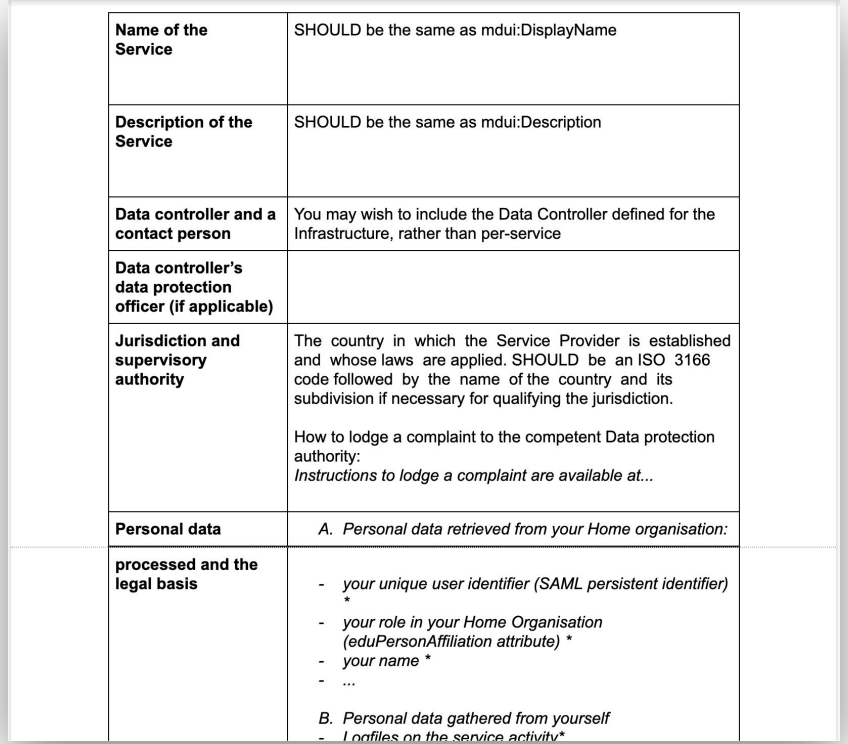


Name of the Service	SHOULD be the same as mdui:DisplayName
Description of the Service	SHOULD be the same as mdui:Description
Data controller and a contact person	You may wish to include the Data Controller defined for the Infrastructure, rather than per-service
Data controller's data protection officer (if applicable)	
Jurisdiction and supervisory authority	The country in which the Service Provider is established and whose laws are applied. SHOULD be an ISO 3166 code followed by the name of the country and its subdivision if necessary for qualifying the jurisdiction. How to lodge a complaint to the competent Data protection authority: *Instructions to lodge a complaint are available at...*
Personal data	*A. Personal data retrieved from your Home organisation:*
processed and the legal basis	- *your unique user identifier (SAML persistent identifier) ** - *your role in your Home Organisation (eduPersonAffiliation attribute) ** - *your name ** - *...* *B. Personal data gathered from yourself* - *Logfiles on the service activity**

Federation Registry

Moving to production: Privacy Policy

- Help users make informed decisions about the collection and use of their data
- Provided in a concise, transparent, intelligible, and easily accessible form
- Written in clear and plain language



Name of the Service	SHOULD be the same as mdui:DisplayName
Description of the Service	SHOULD be the same as mdui:Description
Data controller and a contact person	You may wish to include the Data Controller defined for the Infrastructure, rather than per-service
Data controller's data protection officer (if applicable)	
Jurisdiction and supervisory authority	The country in which the Service Provider is established and whose laws are applied. SHOULD be an ISO 3166 code followed by the name of the country and its subdivision if necessary for qualifying the jurisdiction. How to lodge a complaint to the competent Data protection authority: *Instructions to lodge a complaint are available at...*
Personal data	*A. Personal data retrieved from your Home organisation:*
processed and the legal basis	- *your unique user identifier (SAML persistent identifier) ** - *your role in your Home Organisation (eduPersonAffiliation attribute) ** - *your name ** - *...* *B. Personal data gathered from yourself* - *Logfiles on the service activity**

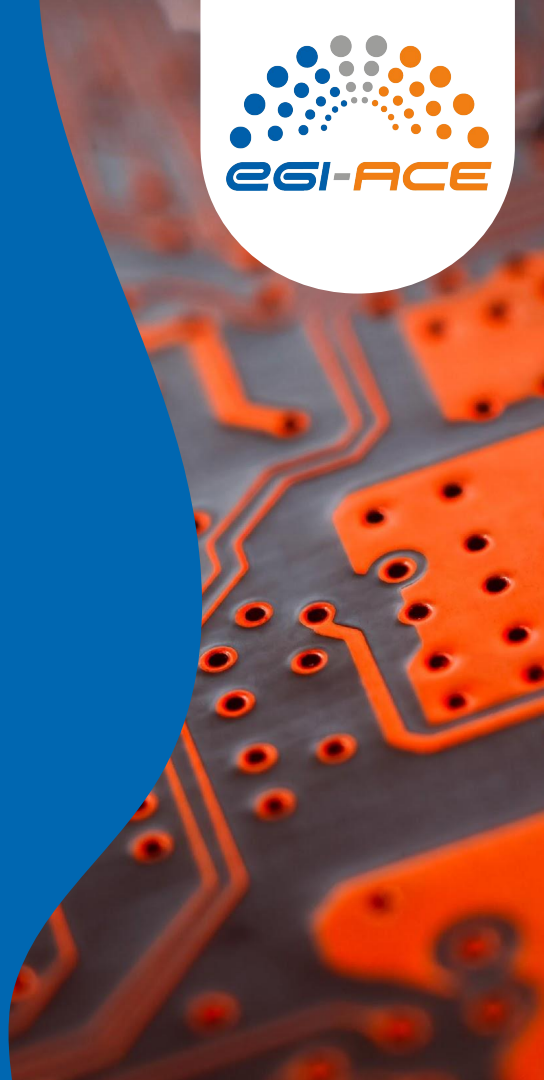
Federation Registry

Future Plans

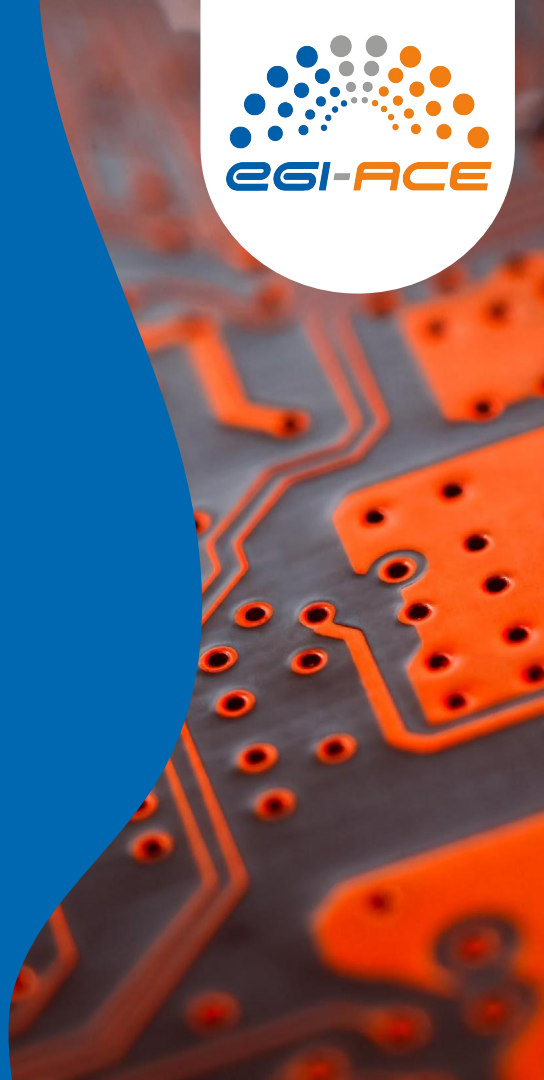
- Improve notifications
  - Include direct links to service requests
- Improve validation of different types of contact information (security, technical)
- Add Organisation information about the service provider
- Support additional deployment agents
  - Keycloak
- Support management of Identity Providers (including Community AAIs)

Useful links

- Live version of EGI Federation Registry can be accessed from https://aai.egi.eu/federation
- User manual and some helpful guidelines can be found at https://federation.rciam.grnet.gr/docs
- Webinars:
  - Providing controlled access to distributed resources and services with EGI Check-in: the provider perspective (slides & recording)
- Video Demonstration
- Other video resources for basic actions



Questions?



Thank you!

Contact: **egi-ace-po@mailman.egi.eu**
Website: **www.egi.eu/projects/egi-ace**

EGI Foundation

@EGI_eInfra

EGI-ACE receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101017567.