Webinar: Providing controlled access to distributed resources and services with EGI Check-in

The service provider perspective

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

Dissemination level: Public
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 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 (institutional/social) via identity linking
- Expressing the level of trust in the identity assertions
- Aggregation and harmonisation of authorisation information (VOs/groups, roles, assurance) from multiple sources
Check-in
Basic federated access flow

eduGAIN
Social

EGI Checkin
Virtual Organization

Service
Service
Check-in
Basic federated access flow

1. Click sign in
Check-in
Basic federated access flow

2. Select preferred authenticating Identity Provider
Check-in

Basic federated access flow

3. Authenticate using existing account credentials

Username: jdoe
Password: ******

Sign in
Check-in
Basic federated access flow

4. Redirect back to the service with Check-in profile information
Check-in

Instances

Development
● Log in using social accounts only
● Features in development state
● Integration tests

DEMO
● Log in using eduGAIN and social accounts
● Stable features
● Integration tests

Production
● Log in using eduGAIN and social accounts
● Stable features
Check-in
Supported Authentication & Authorization Protocols

EGI Check-in can secure access to services using different protocols:

- SAML (Security Assertion Markup Language)
- OAuth 2.0 / OpenID Connect (OIDC)
- X.509 Certificates (for more info see X.509 section in appendix)
Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
What is OpenID Connect

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol, which allows clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user.
Check-in

Controlling access to resources

1. User attribute-based authorisation
   - VO/Group membership and role information
   - GOCDB roles
   - Assurance information
   - Affiliation with home organisation

2. Capability-based authorisation
   - Resources a user is allowed to access
   - Optional list of specific actions the user is entitled to perform
Check-in

Controlling access to resources based on groups

- 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**

\[
\text{<NAMESPACE>:group:<VO>[ :<GROUP>*][:role=<ROLE>]#<GROUP-AUTHORITY>}
\]
Check-in
Controlling access to resources based on groups

• Example group membership values:

\[
\text{urn:mace:egi.eu:group:vo.example.eu:role=member#aai.egi.eu}
\]

NAMESPACE  VO  ROLE  GROUP AUTHORITY

\[
\text{urn:mace:egi.eu:group:vo.example.eu:role=vm_operator#aai.egi.eu}
\]

NAMESPACE  VO  ROLE  GROUP AUTHORITY

EGI Webinars
Check-in

Controlling access to resources based on capabilities

• Capabilities can be used to convey authorisation information to services *in a compact form*

• One or more values encapsulated in:
  ▪ eduPersonEntitlement attribute (SAML)
  ▪ eduperson_entitlement claim (OIDC)

• URN syntax → **AARC-G027**

```
<NAMESPACE>:res:<RESOURCE>[:<CHILD-RESOURCE>][::<CHILD-RESOURCE>][::act::<ACTION>][,:<ACTION>][,:<ACTION>][..]#<AUTHORITY>
```
Check-in

Controlling access to resources based on capabilities

- Example capability value:

  urn:mace:egi.eu:res:gocdb#aai.egi.eu

  - **NAMESPACE**: urn:mace:egi.eu
  - **RESOURCE**: res:gocdb
  - **AUTHORITY**: #aai.egi.eu
Check-in

How Service Registration works for each protocol

1. SAML
   ● Both parties need to exchange metadata in order to know and trust each other.

2. OIDC
   ● The Relying Party (RP) needs to register to the OpenID Provider (OP) to receive a Client ID - Client Secret pair, that the RP can use to authenticate to the OIDC endpoints.
Check-in

Current Service Registration Flow - OIDC

EGI AAI OpenID Connect Provider

Administrative
- System Scopes
- Manage Clients
- Manage Services
- View Profile
- Information

Home / Manage Clients / Edit Client

Edit Client
- Save
- Cancel

Main
- Access
- Credentials
- Tokens
- Crypto

Registered at: 2021-04-21T11:43:02+0000

Client name: myOidcService

Human-readable application name

Client ID: 12703c9c9242-49c3-3c51-239000000321f

Unique identifier. If you leave this blank it will be automatically generated.

Redirect URI(s)
- https://
- There are no items in this list.

Issue Information

Date / Time of Issue: 2021-05-05 05:05 / 13:00 UTC

Subject: Move myOidcService to EGI Check-in Production

Describe the issue:
Dear Check-in Support team,

I would like to move the service "myOidcService" (client_id: XXX) to EGI Check-in Production instance.

BR,

Concerned VO?: none

Affected site?: please select

Type of issue?: Service Request

* Priority?: less urgent

Routing Information

Expert option, please set this option only if you know what it means.

Notify SITE?:
- Submit

Assign to support unit?: Check-in (AAI)

* Required fields
Federation Registry

Service Management Portal
Federation Registry

Introduction

● 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

User Authorization

- Users are authenticated through Check-in (production)
- User roles are assigned based on entitlements included in user’s claims
- Relation between entitlement and roles is configurable
Users can take one of two basic roles “End User” and “Administrators”. These roles grant users a set of actions. Actions allow Roles to be flexible and customizable.

**End Users → Service owners**
- View own services
- Create Petitions to
  - Register a service
  - Reconfigure own services
  - Deregister own services

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

*A user can create petitions only for services they own*
Federation Registry
Integration Environments

Federation registry allows users to register and manage services in multiple environments. When integrating a new service users should select the appropriate environment according to the state of the service.

Development
- Used for Testing Services
- Users can review their own petitions
- No Privacy Policy Required

Demo
- Production Ready Services
- Petitions are reviewed only by Technical Administrators or Site-ops Managers
- No Policy Required

Production
- Services for Actual Use
- Policy required
- Petitions go through a 2 step review system
  - Technical Review
    - By Technical Admins
  - Policy Review
    - By Policy Admins

Under Implementation
Federation Registry
Help your users feel safe & secure: 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

<table>
<thead>
<tr>
<th>Name of the Service</th>
<th>SHOULD be the same as mdul:DisplayName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of the Service</td>
<td>SHOULD be the same as mdul:Description</td>
</tr>
<tr>
<td>Data controller and a contact person</td>
<td>You may wish to include the Data Controller defined for the Infrastructure, rather than per-service</td>
</tr>
<tr>
<td>Data controller’s data protection officer (if applicable)</td>
<td></td>
</tr>
<tr>
<td>Jurisdiction and supervisory authority</td>
<td>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...</td>
</tr>
<tr>
<td>Personal data</td>
<td>A. Personal data retrieved from your Home organisation:</td>
</tr>
<tr>
<td>processed and the legal basis</td>
<td>- your unique user identifier (SAML persistent identifier) *</td>
</tr>
<tr>
<td></td>
<td>- your role in your Home Organisation (eduPersonAffiliation attribute) *</td>
</tr>
<tr>
<td></td>
<td>- your name *</td>
</tr>
<tr>
<td></td>
<td>- ...</td>
</tr>
<tr>
<td></td>
<td>B. Personal data gathered from yourself</td>
</tr>
<tr>
<td></td>
<td>- identifies the service activity *</td>
</tr>
</tbody>
</table>
Federation Registry
Register 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: Create petition - Choosing scopes

![Image of web interface for choosing scopes in Federation Registry]

### General
- **Select Protocol**: Choose an option from the dropdown.
- **Client ID**: Unique identifier; if you leave this blank, it will be automatically generated.
- **Redirect URI(s)**: Type something, add more with the ADD button.

### Protocol Specific
- **Scope**: Select one or more options.
  - openid
  - email
  - profile
  - offline_access
  - eduperson_entitlement
  - eduperson_scoped_affiliation
  - eduperson_unique_id
  - reNets_edu

### Grant Types
- **implicit**
- **authorization code**
- **refresh token**
- **client credentials**
- **password**
- **renew**
- **token exchange**
Federation Registry

Review Petition: Locate Service to Review

Once a petition is submitted users with reviewing rights are notified via email to login to the platform and review it.
Federation Registry
Review Petition: Review Request

When reviewing a service request reviewers view the service configuration and then submit their review.

- **Approve Request**
  Valid petition request ready to deploy

- **Reject Request**
  Invalid petition request

- **Request Changes**
  Reviewer suggests specific changes
Users are notified and prompted to reconfigure their petition when a reviewer has requested changes.

When reconfiguring their petition request users can also view the comment the reviewer left.

An administrator has reviewed your edit request and has requested changes.

Comment from Reviewer:
- Description should be more detailed
- Provide logo is possible
Federation Registry

Copying Service to other environment

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

Copying Service to other environment

- 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

Select Environment to Copy

Select the environment to register a copy of this service:

- Demo

EGI AAI Service Registry

Service name: Client 5
Integration Environment: Demo
Logo: https://brandmark.io/logo-rank/random/logo.png
URL that points to a logo image will be displayed on approval page.
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

<table>
<thead>
<tr>
<th>Date</th>
<th>Type of Request</th>
<th>Review Status</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020/11/01</td>
<td>Registration Request</td>
<td>approved</td>
<td>View</td>
</tr>
<tr>
<td>2020/11/01</td>
<td>Reconfiguration Request</td>
<td>approved_with_changes</td>
<td>View</td>
</tr>
<tr>
<td>2020/11/01</td>
<td>Reconfiguration Request</td>
<td>approved</td>
<td>View</td>
</tr>
</tbody>
</table>

Access Configuration Snapshot
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)
- All Members of the group can view and create petitions for that service.
- Managers have control over group members, and can invite or remove users
Federation Registry

Finally

Future plans include:

- Privacy/Policy Review on production environment
- Extend Service schema to also include information about the Organization it belongs to
- Identity Provider Management

Useful Links:

- You can find a live version of federation registry at https://aai-demo.egi.eu/federation
- A user manual and some helpful guidelines for testing can be found here
- Video Demonstration link
- Other video resources for basic user actions link
Demo

1. Register OpenID Connect Service
2. Change integration environment
3. Register SAML Service
4. View history of Service petitions
5. Invite users to manage the Service configuration
End User Creates Registration Petition
Questions?
Interactive Session/Homework
Create a OIDC Service in EGI Check-in Devel

1. Go to https://aai.egi.eu/federation and log in
   a. Authenticate using your institutional/social account
   b. If it’s your first time, you will need to sign up
2. Then go to “Manage Services” and click on “New Service”
3. Complete the fields in “General” tab
   a. Select “Devel” as “Integration Environment”
4. In the “Protocol Specific” select “OIDC Service”
5. Add as redirect URI the following link
   a. https://openidconnect.net/callback
6. Click on “Submit” and self-approve the petition
Interactive Session
Create a OIDC Service in EGI Check-in Devel

1. Go to https://openidconnect.net and click on “Configuration” and select the following:
   a. Server Template: Custom
   b. Discovery Document URL: https://aai-dev.egi.eu/oidc/.well-known/openid-configuration
      And click “Use Discovery Document”
   c. OIDC Client ID: yourClientId
   d. OIDC Client Secret: yourClientSecret
   e. Scope: openid profile email
      And click “Save”

2. Under “Redirect to OpenID Connect Server” click on “Start” button

3. Under “Exchange Code from Token” click on “Exchange” button
Thank you!

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

EGI Foundation

@EGI_elInfra

EGI-ACE receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 101017567.
Appendix
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
X.509 Certificate
What is X.509

X.509 is a standard format for public key certificates, digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or organizations.

<table>
<thead>
<tr>
<th>Subject Name</th>
<th>org</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>GR</td>
</tr>
<tr>
<td>Organization</td>
<td>Greek Research and Technology Network</td>
</tr>
<tr>
<td>Common Name</td>
<td>Nikolaos Evangelou <a href="mailto:nikosev@grnet-hq.admin.grnet.gr">nikosev@grnet-hq.admin.grnet.gr</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issuer Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>NL</td>
</tr>
<tr>
<td>State/Province</td>
<td>Noord-Holland</td>
</tr>
<tr>
<td>Locality</td>
<td>Amsterdam</td>
</tr>
<tr>
<td>Organization</td>
<td>TERENA</td>
</tr>
<tr>
<td>Common Name</td>
<td>TERENA eScience Personal CA 3</td>
</tr>
</tbody>
</table>
X.509 for non-web use cases & delegated access

RCauth.eu Online CA issued certificates

Check-in has been integrated with the production RCAuth.eu Online CA for allowing users to retrieve X.509 proxy certificates using their federated credentials

- **Master Portal** retrieves end-entity certificate from RCauth.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
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, similarly to the eID Assurance Framework (eIDAF). 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
## Attribute-based Authorisation

**Assurance information**

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

New profiles!

- AARC Assam
- IGTF Dogwood
- RAF Cappuccino
- IGTF Birch
- RAF Espresso