

AAI Roadmap

|  |  |
| --- | --- |
| Author:  | TCB-AAI |
| Version: | 0.8 |
| Document Link: | https://documents.egi.eu/document/3113 |

DOCUMENT LOG

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Date | Comment | Author |
| v.0.1 | 2/2/2017 | Initial version of the requirements as a google document. | Christos Kanellopoulos TCB-AAI |
| v.0.2 | 13/2/2017 | Updated version based on the input from the TCB meeting on 8/2/2017 | Christos Kanellopoulos TCB-AAI |
| v.0.3 | 22/2/2017 | Updated version based on the input from the TCB meeting on 17/2/2017 | Christos Kanellopoulos TCB-AAI |
| v.0.4 | 8/3/2017 | Updated version based on the input from the TCB meeting on 1/3/2017 | Christos Kanellopoulos TCB-AAI |
| v.0.5 | 2/5/2017 | Updated version considering the outcome of the discussions for EOSCHub | Christos Kanellopoulos TCB-AAI |
| v.0.6 | 9/5/2017 | Published on https://documents.egi.eu | Christos Kanellopoulos TCB-AAI |
| v.0.7 | 12/5/2017 | Minor text corrections | Christos Kanellopoulos TCB-AAI |
| v.0.8 | 15/6/2017 | Updated version based on the input from the TCB meeting on 12/5/2017 | Nicolas Liampotis TCB-AAI |

TERMINOLOGY

The EGI glossary of terms is available at: [https://wiki.egi.eu/wiki/Glossary](https://wiki.egi.eu/wiki/Glossary%20)

Contents

[1 Introduction 4](#_Toc487504981)

[2 Requirements 5](#_Toc487504982)

[3 Short-term roadmap (2017) 7](#_Toc487504983)

[3.1 Translation of VO information into VOMS proxies 7](#_Toc487504984)

[3.2 Provisioning of VOMS information through SAML and OIDC interfaces 7](#_Toc487504985)

[3.3 Provide user documentation - sample code for getting certificates through RCauth.eu 7](#_Toc487504986)

[3.4 User enrolment and account linking 7](#_Toc487504987)

[3.5 Self-service interface for managing OIDC tokens 8](#_Toc487504988)

[4 Medium-term roadmap (2017 - 2018) 9](#_Toc487504989)

[4.1 Web interface harmonisation and branding support for the EGI CheckIn Service 9](#_Toc487504990)

[5 Long-term roadmap (2018 - 2020) 10](#_Toc487504991)

[5.1 (New) RCAuth CA 10](#_Toc487504992)

[5.2 Master Portal Enhanced High Availability Support 10](#_Toc487504993)

[5.3 Evolution of the Discovery Service to support enhanced filtering capabilities 10](#_Toc487504994)

[5.4 Support for (de-)provisioning and continuous update of user account information 10](#_Toc487504995)

[5.5 Interoperability with EUDAT B2ACCESS 11](#_Toc487504996)

[5.6 Self-service web interface Web interface for registering OIDC & SAML based SPs 11](#_Toc487504997)

[5.7 Standalone VO/Group Management Service 11](#_Toc487504998)

[5.8 Support for centralised fine grained authorisation 12](#_Toc487504999)

# Introduction

The EGI AAI enables access to EGI services and resources using federated authentication mechanisms. It enables the Integration of external IdPs (from eduGAIN and individual organizations) with the EGI services through the CheckIn IdP/SP proxy component, so that users can access the EGI services (web and non-web based) using credentials from their home organizations or other external IdPs. The proxy supports credential translation from SAML2 to SAML2, OIDC and X.509v3 and from OIDC/OAUTH2 to SAML2, OIDC and X.509v3. through the integration of external token translation services.

The EGI AAI platform is comprised from the following components:

* the **SimpleSAMLphp based IdP/SP Proxy** component which includes:
	+ IdP connectors for SAML, OpenID Connect, OAuth2 and X.509,
	+ AAconnectors for SAML2.0 SAMLAttributeQuery, HTTP REST interfaces and LDAP interfaces
	+ SP connectors, supporting SAML2, OIDC and OAuth2.
* A **centralised IdP Discovery Service.** which supports SP specific IdP filtering.
* The **User Enrolment and VO Management Service**, which is based on COmanage and supports the management of the full life cycle of user accounts in the CheckIn Service.
* The **Master portal**, which is the access point to online X.509 credentials for all EGI services through the RCAuth CA.

The CheckIn Service enables the users to manage their accounts from a single interface, to link multiple accounts/identities together and to access the EGI services based on their roles and VO membership rights. For VOs, the CheckIn Service provides an intuitive interface to manage their users and their respective roles and group rights. For VOs, operating their own Group/VO Management system, the CheckIn service has a comprehensive list of connectors that allows to integrate their systems as externally managed Attribute Authorities. More information can be found on the EGI CheckIn Service web pages[[1]](#footnote-1).

# Requirements

The technical coordination board for the EGI AAI (TCB-AAI) is responsible for owning, defining and updating the EGI technical roadmap in the areas of Identity Provisioning, Authentication and Authorisation, in consultation with service providers, user communities and technology providers. The board was established in January 2017 and includes representatives from various EGI service areas, UCST, EGI operations and technology providers.

The table below provides a list of requirements that have been identified by the TCB. The requirements are prioritised based on the needs of the EGI AAI stakeholders. This is list of requirements is a “live” document and will be updated based on the received by the TCB.

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | Who | Priority | Target |
| Translation of VO information into VOMS proxies | All communities using services requiring VOMS proxies. | High | Q3 2017 |
| Provisioning of VOMS information through SAML and OIDC interfaces | All communities who use VOMS | High | Q3 2017 |
| Provide user documentation - sample code for getting certificates through RCauth.eu | Developers of science portals | High  | Q3 2017 |
| User enrolment and account linking | ALL | High | Q3 2017 |
| [Self-service interface for managing OIDC tokens](#_Self-service_interface_for) | All communities using services requiring OIDC/Integrators of new OIDC-enabled services | High | Q4 2017 |
| Web interface harmonisation and branding support for the EGI CheckIn Service | ALL | High | Q1 2018  |
| (New) RCAuth CA | All communities using services requiring (proxy) certificates | Medium | 2018 – 2020 |
| Master Portal Enhanced High Availability Support | All communities relying on RCAuth CA. | Medium | 2018 – 2020 |
| Evolution of the Discovery Service to support enhanced filtering capabilities | ELIXIR | Medium | 2018 – 2020 |
| Support for (de-)provisioning and continuous update of user account information | Fedcloud | Medium | 2018 – 2020 |
| Interoperability with EUDAT B2ACCESS | All communities accessing EUDAT and EGI resources | Medium | 2018 – 2020 |
| Self-service web interface Web interface for registering OIDC & SAML based SPs | Developers of OIDC/SAML based services | Low |  |
| Standalone VO/Group Management Service | Communities wanting to operate their own group and role management systems | Low |  |
| Support for centralised fine grained authorisation | Fedcloud | Low |  |

# Short-term roadmap (2017)

## Translation of VO information into VOMS proxies

**Priority: High**

**Status: In progress**

**Partners involved: GRNET, Nikhef**

The EGI AAI platform, through the integration with the RCAuth CA, enables users to access services, which require certificate based authentication. For those services that require VOMS proxy certificates, the AAI platform needs to be able translate SAML assertions or OIDC claims to VOMS proxy extensions. Having this capability, users without a personal certificate or users whose VO is not managed by VOMS, will be able to use certificate based services.

## Provisioning of VOMS information through SAML and OIDC interfaces

**Priority: High**

**Status: In progress**

**Partners involved: GRNET, CESNET**

Although we expect many new communities to use the group management system provided by the CheckIn service, still many communities will continue to be using VOMS as their preferred VO management systems. These users need to be able to access SAML/OIDC services, regardless of the group management system users. VO membership should be translated into an entitlement included in the attribute assertion.

## Provide user documentation - sample code for getting certificates through RCauth.eu

**Priority: High**

**Status: In progress**

**Partners involved: GRNET, Nikhef, LIP**

Although, the RCAuth CA is already integrated with the CheckIn service and the EGI AAI platform, there is lack of documentation guiding developers how they can integrate their science portal with the RCAuth CA and the Master portal. The AARC project has already produced sample code and examples. We need to evaluate them, refine them for the purposes of the EGI AAI platform and make them available to the developers.

## User enrolment and account linking

**Priority: High**

**Status: In progress**

**Partners involved: GRNET**

Users need to register for an EGI account to obtain a personal EGI ID, which can then be used to identify them consistently across all EGI tools and services. Specifically, each user must be associated with one persistent, non-reassignable, non-targeted, unique identifier within the EGI environment.

In addition to this identifier, there is a set of attributes required during registration to collect basic information about the user. Ideally, these attributes should be provided by the user’s Home Organisation. However, there are cases when not all the attribute values can be made available (e.g. due to insufficient attribute release policies) or asserted with high confidence (e.g. use of social identity providers and/or self-asserted values). The EGI user registration process needs to cater for such cases to support the release of all the required user profile information to connected Service Providers without administrative involvement (but subject to user consent).

Account linking allows a registered user to access EGI resources with their existing personal EGI ID, using any of the login credentials they have linked to their account. Any of the organisational or social login credentials can be used for this purpose. To link a new organisational or social identity to their EGI account, users need to be able navigate to their account management page and select to link a new identity under the Organisational Identities section.

## Self-service interface for managing OIDC tokens

**Priority: High**

**Status: Accepted**

**Partners involved: GRNET**

For users to be able to access non-browser accessible services, they need to retrieve OIDC access/refresh tokens from the EGI CheckIn Service. Today, there is no automated way to do this and the users are required to build their own OIDC client to be able to retrieve OIDC access/refresh tokens. The EGI AAI platform needs a central service that will allow users to generate and manage OIDC general or per service access/refresh tokens in a user friendly and secure way. This development, will lower the bar significantly for the adoption of non-browser based federated access.

This capability will be required if/when non-web based services start using OIDC access tokens instead of (proxy) certificates, which is the current case. **The priority of this requirement has been changed to high following the plans of TCB-Cloud to adopt OIDC as the means of accessing the Fedcloud APIs**.

# Medium-term roadmap (2017 - 2018)

## Web interface harmonisation and branding support for the EGI CheckIn Service

**Priority: High**

**Status: Accepted**

**Partners involved: GRNET**

The CheckIn Service should be provided "as a Service" to the research communities. The existing service needs to be enhanced, so that it can have community branding when it is used "as a Service". Furthermore, all the user facing web interfaces should have a common, customizable look and feel.

# Long-term roadmap (2018 - 2020)

## (New) RCAuth CA

**Priority: Medium**

**Status: Accepted**

**Partners involved: GRNET, JUELICH, Nikhef, STFC**

The RCAuth CA service generates X.509 certificates upon user request making available through the delegation service long-lived X.509 proxies. The RCAuth CA is already accredited as an IOTA CA in IGTF and the delegation portal is and will remain R&S and SIRTFI compliant. The EGI AAI platform relies on the RCAuth CA for enabling federated access to services which require certificate based authentication. The current RCAuth CA service is operated by Nikhef with limited capacity.

The operation of the RCAuth CA will be taken over jointly by EGI, EUDAT and GÉANT and will be operated in highly available environment that will meet the security and scalability requirements of the EGI AAI platform and the rest of the EI/RIs.

## Master Portal Enhanced High Availability Support

**Priority: Medium**

**Status: Accepted**

**Partners involved: Nikhef**

The Master Portal does not have built-in support for HA or load balancing configuration. The Master Portal service needs to be able to support HA configurations with automatic failover and load balancing across the HA instances.

## Evolution of the Discovery Service to support enhanced filtering capabilities

**Priority: Medium**

**Status: Accepted**

**Partners involved: GRNET**

The Discovery Service already supports basic filtering capabilities. The Discovery Service to be able to mask inconsistencies in the identity federations and protect the EGI services from being exposed to them.

## Support for (de-)provisioning and continuous update of user account information

**Priority: Medium**

**Status: Accepted**

**Partners involved: CESNET, GRNET**

Many services require accounts to be provisioned before the users access the service. Even for services, which can provision accounts at the time of the first user access, the account information needs to be kept up to date (e.g. VO/groups/roles) and the services needs to be notified to deprovision the accounts when they become inactive.

We need a solution based on standardized protocols, that will allow services that require it, to be notified for account provisioning, deprovisioning and updates. Investigate the use of the EGI Messaging Service as a reliable transport mechanism for the delivery of such notifications.

## Interoperability with EUDAT B2ACCESS

**Priority: Medium**

**Status: Accepted**

**Partners involved: GRNET, Nikhef, STFC, FZJ, KIT**

Many research communities are or will be using resources and service provided by EGI and EUDAT. The EGI CheckIn service is the AAI gateway for service operated on the EGI infrastructure, while B2AACCESS is a similar AAI gateway for all the EUDAT services.

Users should be able to share data, access services and roam across infrastructures in a seamless manner. A pilot activity has already started in the context of the EGI-Engage project with support from AARC.

## Self-service web interface Web interface for registering OIDC & SAML based SPs

**Priority: Low**

**Status: Discussion**

**Partner involved:**

The EGI CheckIn Service should provide a secure web interface through which service operators can register their OpenID Connect and SAML based services.

## Standalone VO/Group Management Service

**Priority: Low**

**Status: Discussion**

**Partners involved:**

The EGI CheckIn Service comes with a customized integration of the COmanage portal, which provides User Enrolment and VO Management capabilities. There are communities that prefer to operate their own group management system either for retaining certain level of autonomy or because they require dedicated services.

## Support for centralised fine grained authorisation

**Priority: Low**

**Status: Discussion**

**Partners involved:**

Access to most services is granted based on the roles a user holds or the groups {s}he is member of. Group and role based information and service access rights are made available to the EGI services in the form of eduPersonEntitlements. In the current scheme, authorisation policies are typically managed on the service side.

There are discussions within Fedcloud about the possible need of a centralised authorisation service based on XACML. Such a service would allow to support fine grained authorisation policies, which could be uniformly applied across the EGI services.

1. https://wiki.egi.eu/wiki/AAI [↑](#footnote-ref-1)