

**EGI-Engage**

Identity Management for Distributed User Communities

D3.9

|  |  |
| --- | --- |
| **Date** | 23 December 2016 |
| **Activity** | WP3 |
| **Lead Partner** | GRNET |
| **Document Status** | FINAL |
| **Document Link** | <https://documents.egi.eu/document/3017> |

Abstract

This document presents the architecture, the integration workflows, as well as an assessment for the EGI CheckIn service which offers a set of advanced authentication and authorisation capabilities to allow secure and user-friendly access to EGI services. CheckIn has proven to be a reliable and interoperable multi-protocol identity management and access service through the successful integration with several EGI operational tools and services, meeting the needs of the Research Communities and other stakeholders. Considering the modular structure of the CheckIn service, features can be easily added to support new requirements and use cases.

**COPYRIGHT NOTICE**



This work by Parties of the EGI-Engage Consortium is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). The EGI-Engage project is co-funded by the European Union Horizon 2020 programme under grant number 654142.

**DELIVERY SLIP**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***Name*** | ***Partner/Activity*** | ***Date*** |
| **From:** | C. Kanellopoulos  N. Liampotis  P. Solagna  M. Salle | GRNET/WP3  GRNET/WP3  EGI Foundation/WP3  Nikhef/WP3 | 03/03/2017 |
| **Moderated by:** | Małgorzata Krakowian | EGI Foundation/WP1 |  |
| **Reviewed by** | A.M.J.J. Bonvin  Enol Fernandez  Chris Morris | BCBR-UU/PMB  EGI Foundation/WP4  STFC | 6/03/2017  7/03/2017  3/03/2017 |
| **Approved by:** | AMB and PMB |  |  |

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author/Partner*** |
| **v.1** | 03/03/2017 | Initial version submitted for external review | C. Kanellopoulos/GRNET  N. Liampotis/GRNET  P. Solagna/EGI Foundation  M. Salle/Nikhef |
| **V2** | 08/03/2017 | Update after the external review | N. Liampotis/GRNET |
| **FINAL** |  | Final version |  |

**TERMINOLOGY**

A complete project glossary and acronyms are provided at the following pages:

* <https://wiki.egi.eu/wiki/Glossary>
* <https://wiki.egi.eu/wiki/Acronyms>
* <https://wiki.edugain.org/Terminology>
* <https://www.oasis-open.org/committees/download.php/21111/saml-glossary-2.0-os.html>

**AAI:** Acronym for Authentication and Authorisation Infrastructure.

**Assertion:** A digital statement issued by an IdP, derived from the digital identity of an end user. An assertion is typically digitally signed and optionally encrypted.

**Attribute:** A distinct characteristic of a subject.

**Attribute Authority (AA):** An entity that produces attribute assertions.

**Authentication:** The process of confirming an end user’s identifier with a specified, or understood, level of confidence.

**Authorisation:** The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.

**Digital Identity:** A set of information that is attributable to an end user. It is issued and managed by an IdP Operator on the basis of the identification of the end user.

**End User:** A natural person who makes use of resources for application purposes (as opposed to system management purposes).

**Identity Provider (IdP):** The entity that issues assertions on behalf of end users who use them to access the resources of SPs.

**Principal:** An entity whose identity can be authenticated.

**Proxy:** An entity authorised to act for another.

**Relying Party (RP):** An entity that decides to take an action based on information from another entity.

**Service Provider (SP):** The entity that evaluates the assertion from an IdP and uses the information from the assertion for controlling access to protected resources.

**Subject:** A principal in the context of a security domain.

**Virtual Organisation (VO):** A group of people (e.g. scientists, researchers) with common interests and requirements, who need to work collaboratively and/or share resources (e.g. data, software, expertise, CPU, storage space) regardless of geographical location. They join a VO in order to access resources to meet these needs, after agreeing to a set of rules and Policies that govern their access and security rights (to users, resources and data).

**Contents**

[1 Introduction 7](#_Toc476743713)

[2 Architecture 8](#_Toc476743714)

[2.1 High-level functional architecture 9](#_Toc476743715)

[2.2 Deployment architecture 10](#_Toc476743716)

[2.3 Token translation 10](#_Toc476743717)

[2.4 Integration with operational tools 11](#_Toc476743718)

[2.4.1 GOCDB 11](#_Toc476743725)

[2.4.2 AppDB 11](#_Toc476743726)

[3 Support for distributed user communities 12](#_Toc476743727)

[3.1 Requirements for integrating identity providers 12](#_Toc476743728)

[3.1.1 Attribute release requirements 12](#_Toc476743731)

[3.1.2 Operational and security requirements 13](#_Toc476743732)

[3.2 User enrolment and identity linking 14](#_Toc476743733)

[3.2.1 User registration 14](#_Toc476743736)

[3.2.2 Identity linking 15](#_Toc476743737)

[3.3 Guest users 15](#_Toc476743738)

[3.4 Attribute authorities and attribute aggregation 15](#_Toc476743739)

[3.5 User community integration success story: ELIXIR 16](#_Toc476743742)

[4 Support for the integration of service providers 17](#_Toc476743743)

[4.1 Requirements for integrating service providers 17](#_Toc476743744)

[4.1.1 Services federated in EGI 17](#_Toc476743747)

[4.1.2 Services not federated in EGI 17](#_Toc476743748)

[4.2 Integration workflow for service providers 18](#_Toc476743749)

[4.3 EGI ID 18](#_Toc476743750)

[4.4 Authorisation 19](#_Toc476743751)

[4.4.1 Entitlements 20](#_Toc476743752)

[4.4.2 Level of Assurance 21](#_Toc476743757)

[5 Requirements and acceptance criteria for the production service 21](#_Toc476743758)

[6 Conclusions and future plans 24](#_Toc476743759)

[7 Plan for Exploitation and Dissemination 24](#_Toc476743760)

**Executive summary**

The CheckIn service is the AAI Platform for the EGI infrastructure. The CheckIn service enables the Integration of external Identity Providers (from eduGAIN and individual organisations) with the EGI services through the CheckIn Identity/Service Provider Proxy component, so that users are able to access the EGI services (web and non-web based) using existing credentials from their home organisations. To this end, CheckIn has been published in eduGAIN as a Service Provider. Through eduGAIN, EGI operational tools and services that are connected to CheckIn can become available to more than 2000 Universities and Institutes from the 41 eduGAIN Federations with little or no administrative involvement. Compliance with the REFEDS Research and Scholarship (R&S[[1]](#footnote-1)) entity category and the Sirtfi[[2]](#footnote-2) framework ensure sufficient attribute release, as well as operational security, incident response, and traceability. Complementary to this, users without an account on a federated Identity Provider are still able to use social media or other external authentication providers for accessing EGI Services that do not require substantial level of assurance.

The adoption of standards and open technologies by CheckIn, including SAML 2.0[[3]](#footnote-3), OpenID Connect[[4]](#footnote-4) and X.509v3[[5]](#footnote-5), has facilitated interoperability and integration with the existing AAIs of other eInfrastructures and research communities, such as ELIXIR[[6]](#footnote-6) and LToS[[7]](#footnote-7). The CheckIn Service enables 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 integrating their systems as externally managed Attribute Authorities.

In summary, user communities have several options to integrate with CheckIn in order to access the EGI resources:

* Users authenticate using their institutional identity provider, which is part of an identity federation and eduGAIN
* Users authenticate using a community-specific identity provider, for example ELIXIR.
* Authorisation information about the users (VO/group memberships and roles) is managed by the community’s group management service, which is connected to CheckIn as an external attribute authority
* Communities that do not operate their own group management service can leverage the group management capabilities of the CheckIn platform.

EGI CheckIn is a contribution towards the development of Single Sign On to e-infrastructures for European researchers. It lowers the barriers to use of EGI resources today, and has been designed with an eye to integration with other planned and probable developments. CheckIn can be found at <https://aai.egi.eu/>

Stakeholders are: researchers (users), research communities, and service providers.

# Introduction

Task JRA1.1 activity started in May 2015 by collecting requirements from EGI users and other stakeholders, in order to understand their short and medium-term requirements, and establishing relationships with AARC[[8]](#footnote-8), GN4[[9]](#footnote-9), EUDAT2020[[10]](#footnote-10) and PRACE[[11]](#footnote-11), in order to work together towards an interoperable AAI. Liaison with the AARC project in particular, has been established to adopt AAI policies, solutions and best practices defined at European level.

This process led to the specification of a set of core requirements that drove the design of the CheckIn service, which is the AAI platform for EGI. Specifically, the following requirements were identified:

* Obtain access to EGI services with credentials released by a user’s home organisation enabling the support for National Federations via eduGAIN.
* Support “homeless” users, who cannot rely on a reliable institutional IdP.
* Release by Identity Providers (IdPs) of an identifier that uniquely identifies the user in the scope of that organization.
* Ability to extract attributes from different sources including community attribute providers.
* Ability to associate a Level of Assurance (LoA) to each identity in the EGI infrastructure.
* Availability of a persistent non-reassignable unique identifier for users in order to support the linking of multiple identities.
* Provisioning of credential translator mechanisms/token translator services (TTSs) is needed to hide the complexity of the new EGI AAI to connected Service Providers (SPs).

By the end of the first year of JRA1.1, a first prototype of the CheckIn service was made available, providing support for SAML 2.0 IdPs and SPs. With the basic AAI functionality in place, EGI started the on-boarding activity for scientific communities (e.g. ELIXIR), and core operational tools, such as the GOCDB and the AppDB. By the end of Q2 2016, the CheckIn service joined eduGAIN as a Service Provider under the REFEDS Research and Scholarship (R&S) entity category in order to ensure sufficient attribute release, as well as the uniqueness and non-reassignability of user identifiers retrieved from upstream authentication providers. Complementary to this, CheckIn added support for OpenID Connect/OAuth2 IdPs, allowing users without an institutional account to use their Google, Facebook, LinkedIn and ORCID accounts to access EGI Services that do not require substantial level of assurance. By the end of Q3 2016, CheckIn introduced support for OpenID Connect relying parties, thereby allowing integration with a wider range of services built on top of modern web standards (OAuth 2.0, REST and JSON) and, at the same time, enabling federated access for non-browser based resources, such as CLI tools and APIs in a standardised way. Recently, in February 2017, CheckIn asserted compliance with the Sirtfi framework, which together with R&S, allowed connecting to the new IOTA RCauth.eu online CA in order to support federated access to services using X.509 proxy certificates in a secure and user-friendly way.

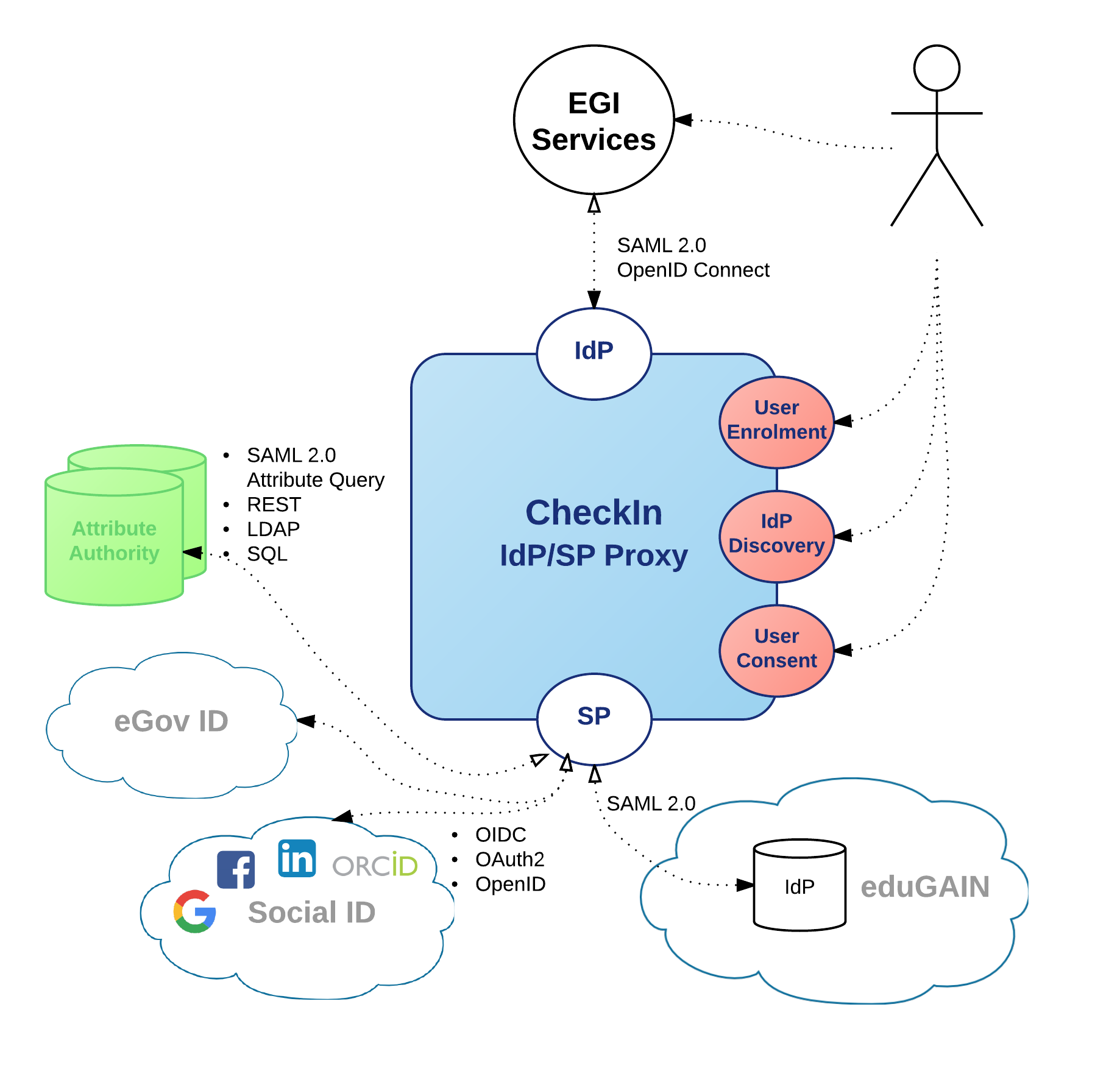
The remainder of this document is structured as follows. Section 2 presents the architecture of the CheckIn service, providing details on the token translation capabilities and the integration with EGI core operational tools. Section 3 contains information about integrating identity providers with the CheckIn service to allow users in a community to access EGI operational tools and services. It also covers topics such as the process for user enrolment and identity linking, the different options for guest users, as well as the aggregation of attributes from multiple sources (attribute authorities) using different technologies. Section 4 describes the integration workflow for service providers, discussing various aspects, such as the uniform identification of authenticated users through the generated EGI ID, and the authorisation capabilities based on the attributes made available by CheckIn, which include VO/group memberships and roles, as well as the achieved Level of Assurance. Section 5 provides an assessment of the CheckIn service based on the identified functional requirements and acceptance criteria. In Section 6, conclusions are drawn and future plans for the evolution of the CheckIn service are briefly discussed. Finally, Section 7 presents the dissemination and exploitation plan.

# Architecture

The design and implementation of the CheckIn service architecture have been driven by a set of core functional requirements defined at the beginning of the project (please refer to milestone document M3.4[[12]](#footnote-12) for a detailed description of these requirements). This section presents the functional and the deployment view of the produced architecture and, in addition, provides details on the token translation capabilities and the integration with EGI core operational tools.

## High-level functional architecture

Figure 1 illustrates a high-level view of the CheckIn architectural elements that deliver the system’s functionality. The view depicts the system’s functional structure, including the key functional components, their responsibilities, the interfaces they expose, and the interactions between them.



The core of EGI AAI CheckIn Service is the **IdP/SP Proxy** component, which acts as a bridge between the EGI services and external authentication sources and identity providers. This decoupling of the internal services and the external authentication sources/identity providers, reduces the complexity of the service implementation as it removes dependencies on the heterogeneity of multiple IdPs, Federations, Attribute Authorities and different authentication and authorization technologies. This complexity is handled centrally by the proxy.

The introduction of a IdP/SP Proxy entity brings additional benefits. Specifically, as illustrated in Figure 1, services only need to establish trust with one entity, the IdP/SP proxy. Typically, services will have one static configuration for the IdP/SP proxy. Having one configured IdP also removes the requirement from the service providers to operate their own IdP Discovery Service (a common requirement for services supporting federated access). Furthermore, all internal services will get consistent and harmonised user identifiers and attributes, regardless of the home organisation or the research community the authenticating user belongs to. Finally, this separation simplifies change management processes, as the internal services are independent from the IdPs run by the home organisations. Similarly, IdPs establish trust with one entity, the operator of the IdP/SP proxy, and they are not impacted by the operational changes introduced by each individual service.

The **User Enrolment and VO Management** service supports the management of the full life cycle of user accounts in the CheckIn Service. This includes the initial user registration, the acceptance of the terms of use of EGI, account linking, group and VO management, delegation of administration of VOs/Groups to authorized users and the configuration of custom enrolment flows for VOs/Groups via an intuitive web interface.

## Deployment architecture

The core components of the EGI CheckIn service, namely the IdP/SP Proxy, the IdP Discovery, and the User Enrolment and VO Management service, are operated in High Availability mode. To achieve this, there are two instances of each of these components in active - active configuration. The active - active configuration allows for both high availability and load balancing across the instances. It should be noted that this architecture can scale horizontally by provisioning more nodes, if required to increase service capacity. Furthermore, the backend database store for all of these components is operated in clustered mode, supporting streaming replication and Point-in-Time Recovery (PITR) for a period of six months (minimum).

## Token translation

For various use-cases, a user might need to use different types of credentials, for example an X.509 (proxy) certificate for accessing storage element. In order to provide such functionality, the EGI CheckIn service has been connected to the new IOTA RCauth.eu online CA[[13]](#footnote-13).

When a certain web-flow requires a X.509 credential, the user will be redirected via a new component, a so-called MasterPortal[[14]](#footnote-14), to the Online CA. There the user will login again transparently (due to SSO) to the CheckIn service and will have to give consent for the management of user credentials. It will then be redirected to the originating service. In the process, a new credential is cached in the MasterPortal which subsequently will be retrieved by whichever service initiated this flow, typically a Science Gateway.

When needed a VOMS proxy can be requested initially. When the user is already enrolled in the VOMS server, this can be done completely transparently; otherwise a form of provisioning is needed. This latter issue is currently under active investigation in connection with the AARC project.

## Integration with operational tools

Integration activities for enabling federated access to EGI central operational tools started from the pilot phase of the EGI CheckIn service. The choice of the services added to the integration plan is driven by priorities and needs of the Research Communities that are being on-boarded. We have started with the research communities from the ELIXIR and the EPOS Competence Centres and we will continue with the research communities from the other Competence Centres.



### GOCDB

The Grid Configuration Database (GOCDB[[15]](#footnote-15)) has been integrated as a SP with EGI CheckIn to allow users without a client X.509 certificate to access the GOCDB web portal. Being the central configuration management database, GOCDB requires a high level of assurance. Therefore, users are required to authenticate via the CheckIn IdP Proxy using an authentication scheme that provides an adequate level of assurance. The LoA category that is assigned to the user's authenticated session is communicated to the GOCDB during user login. As such, if the user authenticates using a scheme that provides a low level of assurance (e.g. social media), then access to GOCDB is denied. Conversely, if the user authenticates using a scheme that provides a high LoA (e.g. trusted institutional home organisations), access is granted.

1. When a user is granted access, they can use the existing GOCDB role mechanisms to request roles and permissions. The workflow can be described as follows: User logs in to the GOCDB web portal[[16]](#footnote-16) with their EGI ID
2. User requests a role. The request is passed to the existing users who already own the necessary roles to approve or reject the role request. User is granted with the approved role at next login, and can perform authorised operations.

Furthermore, GOCDB has been integrated as an Attribute Authority to allow CheckIn to retrieve information describing the user’s role(s) when operating EGI Resource Centres (also named “sites”). This information is encapsulated in URN-formatted eduPersonEntitlement values, which are incorporated into the original SAML attribute assertion sent by the user’s IdP before being passed on to the relying party.

### AppDB

The EGI Application Database (AppDB[[17]](#footnote-17)) has been integrated as a SP with CheckIn to enable authorised access to the Software and Cloud marketplace. Authorization of user actions is based on the VO membership and role information of authenticating users. This information is encapsulated in URN-formatted eduPersonEntitlement values, which are incorporated into the SAML attribute assertion returned by the EGI CheckIn IdP Proxy. Specifically, a user can have different roles when accessing the EGI AppDB marketplace:

* Visitor: Can browse publicly visible Virtual Machine Images (VMIs), can download them for local use. Visitors do not have to login through CheckIn.
* VMI developer: Any user with a valid account can register new VMIs and VMI versions in the marketplace and (optionally) can submit these to the community coordinator for inclusion in the community image list.
* Coordinator of a scientific community: Can add VMIs to the community image list to trigger the replication of these VMIs to the cloud sites that support the community. The community image list includes VMs that are of high relevance to the scientific community. Community coordinators have to login to AppDB and must have attributes that express affiliation to a community and coordinator role within that community.

The automatic AppDB role assignment for users authenticating through CheckIn based on the received VO membership and role information is already being used in production to support the ELIXIR Competence Centre (since June 2016) and the LToS research community (since January 2017).

# Support for distributed user communities

This section contains information about integrating an identity provider with the CheckIn service in order to allow users in a community to access EGI operational tools and services.

## Requirements for integrating identity providers

An institution or a community may connect their IdP with CheckIn to allow their users to access EGI services, or any other services that have enabled CheckIn as an authentication provider. The requirements for integrating an IdP with EGI CheckIn are presented hereafter.



### Attribute release requirements

As a bare minimum, the IdP of a user’s Home Organization is expected to release an identifier that uniquely identifies the user within the scope of that organization. This is required by the CheckIn service in order to generate the EGI ID, which is a persistent, non-reassignable, non-targeted, opaque, and globally unique identifier that is used to identify the user both within and outside the EGI e-infrastructure. The generated EGI ID must be accompanied with a minimum set of attributes which the CheckIn SP Proxy will attempt to retrieve from the user’s IdP. If this is not possible, the missing user attributes will be acquired and verified through the user registration process with the EGI Account Registry. Table 1 describes the data requested from the user’s Home Organisation, which are communicated to the CheckIn SP as either SAML attributes or OIDC claims, depending on the protocol supported by the authenticating IdP.

|  |  |  |
| --- | --- | --- |
| **Description** | **SAML attribute** | **OIDC claim** |
| At least one of the following unique user identifiers (see also Section 4.3):   1. pseudonymous, non-reassignable identifier; 2. name-based identifier; 3. pseudonymous identifier | 1. eduPersonUniqueId 2. eduPersonPrincipalName 3. eduPersonTargetedID or SAML persistent identifier | 1. sub (public) 2. sub (public) 3. sub (pairwise) |
| Preferred name for display purposes, for example to be used in a greeting or a descriptive listing | displayName | name |
| First name | givenName | given\_name |
| Surname | sn | family\_name |
| Email address | mail | email |
| Role at Home Organisation | eduPersonScopedAffiliation | N/A |

Note that the above set of requested attributes complies with the REFEDS R&S[[18]](#footnote-18) attribute bundle.

### Operational and security requirements

The IdP needs to comply with additional requirements to achieve a higher level of assurance (see section 4.4.3) and allow its users to gain access to a wider set of EGI services.

A first group of additional requirements are defined by the Sirtfi framework[[19]](#footnote-19). Adherence to these requirements can be asserted either by publishing Sirtfi compliance in the eduGAIN metadata or by declaring it in a form submitted to CheckIn. These requirements are in the areas of operational security, incident response, traceability and IdPs and users responsibility.

The last area where an IdP can add additional compliances is the users’ identity vetting. To be classified with a LoA comparable to the IGTF BIRCH[[20]](#footnote-20), comparable to the traditional X.509 personal certificates, an IdP must provide a certain level of identity vetting, e.g. user ID verification.

IdPs not federated in eduGAIN, or not publishing R&S compliance, will be asked to sign a form to express their level of compliance with the requirements above. eduGAIN IdPs can still complement the published information by submitting a form and gain a higher level of assurance.

## User enrolment and identity linking

This section describes the process for registering an account with CheckIn to allow users to access a variety of EGI tools and services. Users need to register for an EGI account in order to obtain a personal EGI ID, which can then be used to identify them consistently across all EGI tools and services. Specifically, the idea is to associate each user 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 in order 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 of 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 in order to support the release of all the required user profile information to connected Service Providers without administrative involvement (but subject to user consent).



### User registration

As described in Section 3.1.1, the EGI CheckIn SP Proxy requests a set of attributes from the IdP of the home organisation in accordance with the REFEDS R&S attribute bundle definition, therefore R&S IdPs should be able to automatically release the requested information to the EGI CheckIn SP Proxy without administrative involvement, subject to user consent. On the other hand, if any of the information above cannot be released by the user’s Home Organisation, the user will be prompted to provide the values of the missing attributes. In a nutshell, depending on the attributes released by the Home IdP, users will need to go through one of the following account registration processes:

1. **Self-service Sign Up:** Allows a user to register without approval by an administrator if all the information above is asserted by the Home Organisation
2. **Approval-based Sign Up:** User is prompted to self-assert any of missing attribute values. The request to join the EGI User Community must then be approved by an EGI User Sponsor. Users may optionally select a particular individual to review their request through the Sponsor dropdown list.

A step-by-step guide through the proposed user registration flows can be found here:

<https://wiki.egi.eu/wiki/AAI_usage_guide#Signing_Up_for_an_EGI_Account>

### Identity linking

Identity 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 navigate to their account management page and select to link a new identity under the Organisational Identities section. The proposed user workflow is detailed in the wiki:

<https://wiki.egi.eu/wiki/AAI_usage_guide#Linking_Additional_Organisational.2FSocial_Identities_to_your_EGI_Account>

## Guest users

CheckIn enables users to access EGI Services/Tools using credentials provided by the IdP of their Home Organisation, typically through eduGAIN. However, users that do not have an account on one of the federated IdPs, are still able to access the EGI services using social identity providers or other selected external identity providers. To achieve this, the EGI AAI has builtin support for SAML, OpenID Connect and OAuth2 providers and already enables user logins through Facebook, Google, LinkedIn, and ORCID. Support for user authentication through GitHub and Microsoft Live Connect is also underway. Each external IdP has a LoA assigned to it that is conveyed to the SP through the eduPersonAssurance attribute and the Authentication Context Class of the SAML authentication response or via the acr claim in the case of OpenID Connect. EGI AAI currently distinguishes between three LoA levels, namely, Low, Substantial and High. All social identity providers are assigned the Low LoA. It should be noted that some EGI SPs have been configured to provide limited access (or not to accept at all) credentials with the Low LoA.

## Attribute authorities and attribute aggregation

The CheckIn service enables users to manage their accounts through the EGI Account Registry[[21]](#footnote-21) which allows them to access EGI resources with their unique personal EGI ID, using any of the login credentials they have linked to their account. The EGI Account Registry is based on COmanage[[22]](#footnote-22), which maintains information about the user’s identity, such as their name, email, and affiliation, as well as group membership(s) and role(s) within EGI. For VOs, operating their own Group/VO Management system, the CheckIn service has a comprehensive list of connectors that allows integrating these systems as externally managed Attribute Authorities. Having the attribute aggregation performed centrally by CheckIn allows the implementation of central strategies for attribute mapping and harmonisation so that EGI services receive a uniform set of attributes following well-defined structure and semantics. At the same time, EGI services don’t need to implement complex technical solutions for supporting multiples AAs.

EGI CheckIn supports attribute aggregation using a variety of technologies:

* AQ Attribute Aggregator SimpleSAMLphp module - Enables SimpleSAMLphp to issue SAML 2.0 attribute queries to Attribute Authorities that support SAML 2.0 SOAP binding
* LDAP/SQL Attribute Aggregator SimpleSAMLphp module - Allows SimpleSAMLphp to issue LDAP/SQL queries for retrieving attributes from LDAP/SQL directories/databases
* REST Attribute Aggregator SimpleSAMLphp module - Allows SimpleSAMLphp to query user information from RESTful Web services, such as the GOCDB Programmatic interface[[23]](#footnote-23), the COmanage REST API[[24]](#footnote-24), and the Unity IDM RESTful Administration API[[25]](#footnote-25).
* OpenConext attribute aggregation Java application *(Work in progress)* - Handles attribute aggregation and provides REST API for accessing attribute information

At the moment, the major use case to connect an attribute authority to CheckIn is to provide attributes for specifying users’ group membership. In the context of the EGI services, users are always members of one or more Virtual Organizations (VO), and more fine-grained authorisation information can be modeled via the use of VO groups and VO roles (see also Section 4.4).

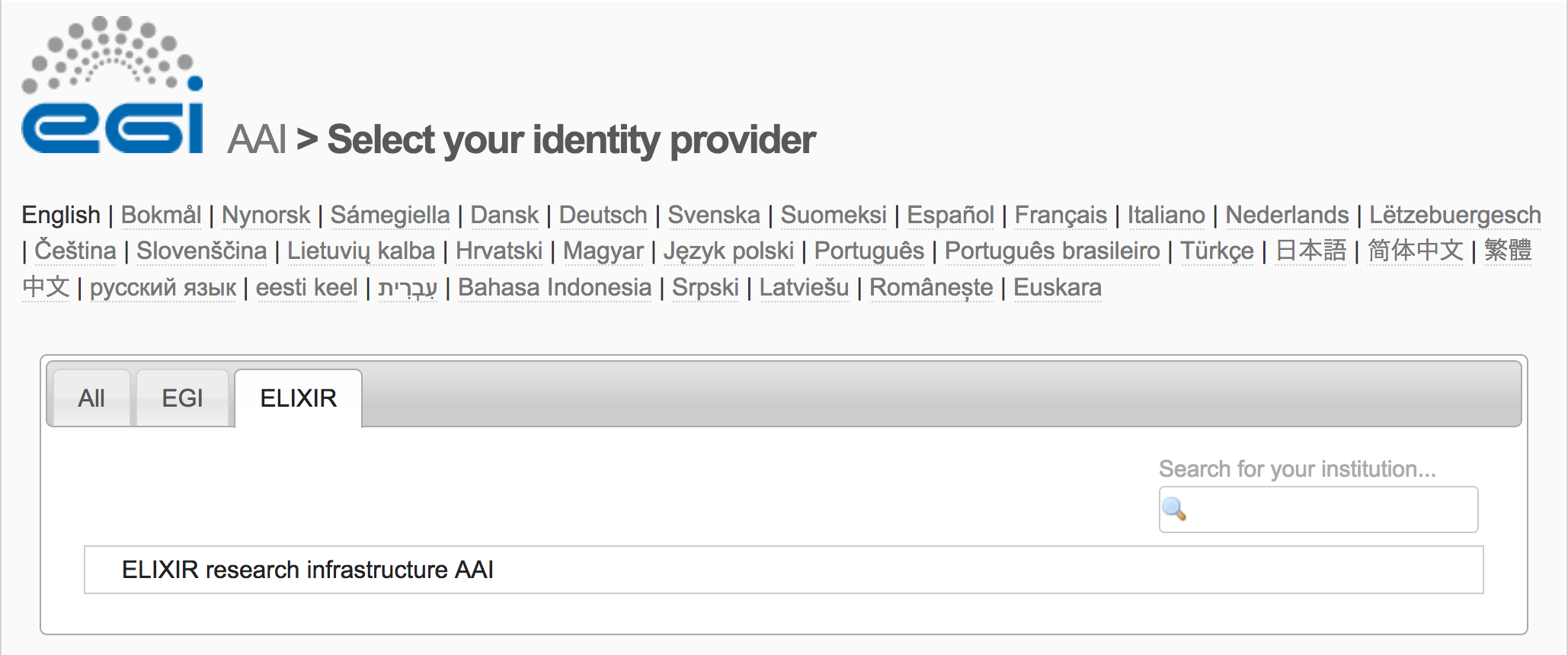


## User community integration success story: ELIXIR

CheckIn has been integrated with the ELIXIR AAI IdP Proxy to enable members of the ELIXIR Community to interact with EGI resources using their ELIXIR user identities. The GOCDB service registry and the AppDB Virtual Machine Image catalogue were selected as priority services to conduct the integration:

* GOCDB: ELIXIR service providers can register and manage the registration of basic infrastructure resources (cloud and storage).
* AppDB: ELIXIR application developers can register Virtual Machine Images and Virtual Appliances for publishing these on the ELIXIR cloud sites and for sharing these with the broader life science community.

The ELIXIR AAI appears as an IdP in CheckIn, ELIXIR users can choose this option and being redirected to the ELIXIR AAI to log in as per ELIXIR specific services. Most of the time users have a valid authentication session in their browser and do not need to enter again their username/password in the ELIXIR AAI. The login option is shown in the following figure.



# Support for the integration of service providers

Service providers can integrate their service instances, for example community-specific services, with CheckIn, to enable their users to authenticate with eduGAIN IdPs or any other IdP already integrated with CheckIn. CheckIn provides IdP discovery mechanisms, aggregation of attributes from multiple sources (IdP, attribute authorities or group management services) with zero overhead for the developers of the service: services need to configure CheckIn as an IdP and automatically access all these features.

## Requirements for integrating service providers

EGI Operations must approve every request for integration of new services with the CheckIn service. The approval (or non-approval) is based on a set of prerequisites, the relevance of the service for the EGI community and the available resources to support the integration. The prerequisites are described in the following sections.



### Services federated in EGI

All services that are operated by Resource Providers participating in the EGI federation and that abide to the RC OLA, and consequently to the relevant security policies of EGI, are eligible for the EGI CheckIn service. By complying with the relevant EGI policies, a service claims that it will not use attributes released by CheckIn for purposes that fall outside of the service definition as presented at the time of registration to EGI users

### Services not federated in EGI

A service not part of the EGI federation can be integrated as a SP with Checkin if the organisation providing the service commits to all the EGI policies that are relevant to a service provider. By accepting the policies, a service provider assures that they will operate the service in good faith, without deliberately exposing the user to security risks, without claiming intellectual property on the data owned by the user, and protecting sensitive data generated by the interaction of the user with the service.

The policies that a service provider must accept are available in the EGI Policies and procedures page[[26]](#footnote-26) and specifically are:

* Grid Security Policy[[27]](#footnote-27)
* Service Operations Security Policy[[28]](#footnote-28)
* Traceability and Logging Policy[[29]](#footnote-29)
* Security Incident Response Policy[[30]](#footnote-30) limited to incidents that can expose or compromise in any way the information released by CheckIn to the service

## Integration workflow for service providers

The integration of Service Providers with EGI CheckIn is a two-step process:

1. The Service Provider is registered with the development instance of EGI CheckIn. The development instance allows for testing authentication and authorisation without affecting the production CheckIn service. Note that the development instance is not connected to the production service and no information is shared between the two systems. However, the development instance has identical functionality, with the exception that the list of supported Identity Providers is limited. Therefore, it is recommended to use the EGI SSO or any of the social identity providers to test the login workflow when using the development instance.
2. The Service Provider is registered with the production instance of EGI CheckIn to allow members of the EGI User Community to access the service. This requires that the service meets all the eligibility criteria (please refer to Section 4.1) and that integration has been thoroughly tested during Step 1.

## EGI ID

EGI users should be identified by one persistent, non-reassignable, non-targeted, and globally unique identifier, even if such an identifier is not provided by the IdP of the user’s home organisation. The most appropriate identifier in the eduPerson schema is the eduPersonUniqueId[[31]](#footnote-31) (urn:oid:1.3.6.1.4.1.5923.1.1.1.13) attribute, as it meets all of the identified requirements, and can be easily derived algorithmically based on the information available from the home organisations. Furthermore, the fact that this attribute can be scoped is a very important characteristic for creating globally unique identifiers that can be used across infrastructures.

Based on the eduPersonUniqueId specification, the EGI ID is of the form uniqueID@scope, where:

* the "uniqueID" portion is unique within the EGI environment and contains only alphanumeric characters (a-z, A-Z, 0-9).
* the length of the “uniqueID” portion is less than or equal to 64 characters.
* the "scope" portion is the administrative domain of the identity system where the identifier was created and assigned, i.e. egi.eu.

Specifically, the EGI ID is generated based on the first non-empty value from the following list of attributes originating from the user’s Home IdP (ordered by precedence):

1. eduPersonUniqueId
2. eduPersonPrincipalName
3. eduPersonTargetedID / SAML2 Persistent NameID

As such, the Home IdP of the user MUST release at least one of the above user identifiers.

The selected attribute value is concatenated with the entityID of the Home IdP and a secret salt. The resulting string is hashed (using the sha256 algorithm) as follows:

EGI ID = sha256 (home\_UID + ‘!’ + home\_IdP + ‘!’ + secret\_salt)

Finally, the "egi.eu" scope portion is added in order to generate a globally unique ePUID, e.g.: ef72285491ffe53c39b75bdcef46689f5d26ddfa00312365cc4fb5ce97e9ca87@egi.eu

## Authorisation

As already described, the CheckIn service is able to aggregate user attributes from different attribute authorities in order to create a “composite” user identity that also combines the attributes retrieved from the user’s home organisation. This “composite” user identity is then made available to EGI services enabling them to make the appropriate authorisation decisions. Specifically, the attributes that can be used by SPs to control access to resources convey two types of information about the authenticated user, namely Entitlements and Level of Assurance (LoA). These types of information are detailed in the subsections that follow.

### Entitlements

User entitlements indicate a set of rights to specific resources. In the case of SAML 2.0, entitlements are expressed as eduPersonEntitlement[[32]](#footnote-32) (ePE) attribute values, whereas in OIDC via the edu\_person\_entitlements[[33]](#footnote-33) claim. While ePE values can be either URLs or URNs, EGI CheckIn has adopted URNs which are currently more commonly used by existing IdPs/AAs/Federations and can easily support scoping following a hierarchical structure. For this purpose, the Middleware Architecture Committee for Education (MACE) has delegated the operation of “urn:mace:egi.eu” namespace to EGI. Using the namespace identifier registry delegation model, URN values can thus be managed in a distributed fashion by different EGI issuing authorities, communities/VOs, group management systems.

Entitlements can either refer explicitly to the protected resources in question, or implicitly by conveying the user’s VO/group membership and role information (group- and/or role-based access control).



#### Resource-specific entitlements

A resource-specific entitlement represents the right of a user to access a particular resource. For example, the “urn:mace:egi.eu:aai.egi.eu:rcauth” value is currently being used to indicate that the holder of this entitlement is eligible for accessing the RCauth.eu Online CA service. The EGI AAI URN registry[[34]](#footnote-34) lists all supported entitlement values.

Note that the resource-specific entitlements are meant to be used to grant access to specific EGI central services rather than distributed services, such as HTC or cloud resources, for which authorisation is based on group membership.

#### Entitlements expressing VO/group membership and role information

To express VO/group membership and role information for use within the EGI environment, each entitlement value represents a particular position of the user within a VO. A user may be member or hold more specific roles within the groups associated to a VO. Groups are organised in a tree structure, meaning that a group may have subgroups, which in turn may have subgroups, etc. This hierarchical structure implies that if someone is member of a subgroup, then they are also member of the parent group.

Specifically, the eduPersonEntitlement values expressing VO/group membership and role information adopt the following formatting specification:

urn:mace:egi.eu:<authority-fqdn>:[<group>[:<subgroup>:…]]:<role>@<vo-fqdn>

where:

* <authority-fqdn> is the FQDN of the authoritative source for the entitlement value
* <vo-fqdn> is the FQDN of the Virtual Organisation
* <group> is the name of a group in the identified VO; specifying a group is optional
* zero or more <subgroup> components represent the hierarchy of subgroups in the <group>; specifying sub-groups is optional
* the <role> component is scoped to the rightmost (sub)group; if no group information is specified, the role applies to the VO

### Level of Assurance

Based on the authentication method selected by the user, EGI CheckIn assigns a Level of Assurance (LoA), which is conveyed to the SP through either the eduPersonAssurance attribute and the Authentication Context Class (AuthnContextClassRef) of the SAML authentication response, or using the acr claim in the case of OIDC services. The EGI AAI originally distinguished between three LoA levels, namely Low, Substantial and High. These levels have been refined as follows:

* **LoA Null:** Authentication through an IdP with no identity vetting and no guarantees on the uniqueness of the provided user identifier (e.g. Social media).
* **LoA A:** Authentication through an IdP that participates in one of the eduGAIN Federations
* **LoA B:** As Per “A”, plus compliance with REFEDS R&S and Sirtfi.
* **LoA C:** As per “B”, plus documented identity vetting procedure
* **LoA D:** As per “C”, plus multi-factor authentication

Note that a low LoA, i.e. “Null” or “A”, usually provides limited or no access to EGI resources.

# Requirements and acceptance criteria for the production service

The design and implementation of the CheckIn service has been driven by a set of core functional requirements defined at the beginning of the project.

The requirements of the user communities have been collected both from the existing EGI communities, including the Competence Centres supported by WP6, and the existing documentation produced by previous initiatives, such as FIM4R[[35]](#footnote-35).

The requirements from the service providers federated in EGI have been identified considering the existing policies, procedures and the technologies available for user authentication and authorization.

In the process of defining the CheckIn service according to the ITSM best practices, an additional set of requirements has been added, as acceptance criteria to be verified before rolling the service in production.

Both initial requirements and acceptance criteria are summarized in the following table.

|  |  |  |
| --- | --- | --- |
| Requirement description | Type of requirement | Status of implementation |
| Obtain access EGI services with credential released by their home organisation enabling the support for National Federation via eduGAIN | Functional | CheckIn is federated as a service provider in eduGAIN, publishing both RnS and Sirtfi metadata. This allows CheckIn to be as much inclusive as possible. Other IDPs not in eduGAIN can be configured individually, as it has been done for the ELIXIR AAI. |
| Support ‘homeless users’, who cannot rely on a reliable institutional IdP | Functional | CheckIn integration with social media identity provider has been avaialble from the first deployment of CheckIn. Users can register and create an EGI UID with, for example, google or facebook credentials. |
| Ability to extract attributes from different sources including community attribute providers | Functional | CheckIn can get attributes |
| Ability to associate a Level of Assurance (LoA) to each identity in the EGI infrastructure | Functional | CheckIn at the moment is technically able to associate different level of assurance based on the information available on the IDP. But the classification of the LoAs is not yet been formally published for being implemented by the service providers in EGI, because this will happen after that a common LoA semantic is agreed by the AARC project |
| Availability of a persistent non-reassignable unique identifier for users in order to manage the accounting linking | Functional | CheckIn associate an EGI UID to the registered users. The account linking has not been released yet in production |
| Provisioning of credential translator mechanisms/token translator services (TTSs) is needed to hide the complexity of the new EGI AAI to the service providers | Functional | CheckIn is currently able to translate between SAML and OIDC credentials. Through the recent integration with RC Auth, users can access X.509 credentials with their username/password credential. |
| Integrate with IdPs supporting SAML standard, OIDC/OAuth standard  Integrate with SPs supporting SAML and OIDC  Provide support for command-line access using OIDC/OAuth | Acceptance criteria | CheckIn implements all these protocol in the current version |
| Gather attributes from existing EGI ops tools, as required | Acceptance criteria | CheckIn can consume user attributes from GOCDB, which is the source of information for admin roles in the resource centres and operations centres operations. |
| Implement EGI-specific policies where required | Acceptance criteria | CheckIn has implemented some ad hoc policies to implement specific requests, such as dedicated entitlements for users accessing CheckIn through the ELIXIR AAI. |
| High availability configuration | Acceptance criteria | CheckIn is deployed in an high availability configuration |
| Fulfil also: REFEDS Code of Conduct  Sirtfi | Acceptance criteria | CheckIn is publishing Sirtfi compliance, plus RnS.  Code of conduct compliancy has been delayed to wait for the new version under publication. |

All the green rows in the table above are the requirement fully fulfilled by CheckIn in its current implementation. The white rows are functional requirements or acceptance criteria that are only partially satisfied by CheckIn. There are not requirements that are at least non-partially satisfied.

The acceptance criteria not fully satisfied have been delayed to wait for the AARC outputs, for a better alignment with the recommendations and to ensure better compatibility of CheckIn with the respective tools of the relevant e-Infrastructures or research infrastructures.

# Conclusions and future plans

CheckIn has proven to be a reliable multi-protocol authentication and authorisation service through the successful integration with several EGI operational tools and community services. Specifically, EGI tools, such as the GOCDB and AppDB have already been integrated and we have started integration activities for FedCloud. In parallel, integration with research communities from the ELIXIR Competence Centre and the LToS platform has been completed and we will continue with the AAIs of other eInfrastructures and the rest of the Competence Centres.

CheckIn is a production-ready service, deployed in a reliable configuration and compliant with the policies endorsed by the most relevant identity federations and Infrastructures in Europe. CheckIn can cater for multiple use cases, including the existing ones and also those that will be supported in the future by EGI. Considering the modular structure of the CheckIn service, features can be easily added to support new requirements. It should be noted that the service has the potential to be offered both as an access gateway to the EGI-specific services, as well as a service integrated with community-specific services to simplify the AAI integration work.

Future plans include the integration of CheckIn with the rest of the EGI tools and services. The choice of the services added to the integration plan, is driven by priorities and needs of the Research Communities that are being on-boarded. As such, the integration plan has been organised as follows:

* Operations portal, accounting and other operational tools
* Command line tools and APIs, particularly for FedCloud
* VOMS to automatically generate group information in the X.509 domain

# Plan for Exploitation and Dissemination

|  |  |
| --- | --- |
| *Name of the result* | *CheckIn* |
| *DEFINITION* | |
| *Category of result* | * *Policy & Procedure developments: Technical procedures directed at users, service and infrastructure providers (for example to govern access and allocation to resources), policy reports and recommendations, and strategic analysis* * *Software & service innovation: Software developments: (e.g.: workflows, Virtual Machines, applications), new software services deployed for the direct benefit of researchers (e.g.: web portals, gateways), e-Infrastructure Commons such as accounting, AAI, and the Federated Cloud platform and the Open Data platform, demonstrators and prototypes.* |
| *Description of the result* | *The results described in this deliverable are the following:*   * *Production version of the CheckIn service* * *Secondary: Procedures and policies to support the checkin service* |
| *EXPLOITATION* | |
| *Target group(s)* | * *Research communities* * *Research infrastructures* * *Service providers* |
| *Needs* | *AAI platform that allows the integration of service providers with identity federations. Enable uniform authentication and authorization workflows to reduce the overhead on the service providers and users.* |
| *How the target groups will use the result?* | The service is going to be used integrated with existing and new services provided by RIs or used by users.  EGI will provide the service to such entities and support the integration with CheckIn. CheckIn will configure Sps and IdPs to support the use case of the customers.  For the moment the support for third-parties deployment is not foreseen. |
| *Benefits* | *Integration with identity federation, access to distributed service with uniform authentication.* |
| *How will you protect the results?* | CheckIn is a service offered deploying a number of components mostly available as open source software. At the moment there are no IPR or other protections in place. |
| *Actions for exploitation* | *To be fully usable by the target groups CheckIn needs a marketing/dissemination package to be used to communicate to potential customers the features of the product.* |
| *URL to project result* | [*https://wiki.egi.eu/wiki/AAI*](https://wiki.egi.eu/wiki/AAI)  *CheckIn is not a web site, but a service that works behind the scenes.* |
| *Success criteria* | *4 communities accessing EGI services through CheckIn*  *8 services integrated with CheckIn (by the end of EGI-Engage)* |
| *DISSEMINATION* | |
| *Key messages* | *Easy to use - Ready to use - low overhead - AAI solution* |
| *Channels* | *R.I. events. FIM4R and other specific AAI events. EGI website as part of the EGI service catalog* |
| *Actions for dissemination* | *Presentation at FIM4R (Done February 21st)* |
| *Cost* | *N.A.* |
| *Evaluation* | *# of contacts from potential customers* |

1. <https://refeds.org/category/research-and-scholarship> [↑](#footnote-ref-1)
2. <https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf> [↑](#footnote-ref-2)
3. <https://wiki.oasis-open.org/security/FrontPage#SAML_V2.0_Standard> [↑](#footnote-ref-3)
4. <http://openid.net/developers/specs/> [↑](#footnote-ref-4)
5. <https://tools.ietf.org/html/rfc5280> [↑](#footnote-ref-5)
6. <https://www.elixir-europe.org/> [↑](#footnote-ref-6)
7. <https://wiki.egi.eu/wiki/Long-tail_of_science> [↑](#footnote-ref-7)
8. <https://aarc-project.eu/> [↑](#footnote-ref-8)
9. <https://www.geant.org/Projects/GEANT_Project_GN4> [↑](#footnote-ref-9)
10. <https://eudat.eu/> [↑](#footnote-ref-10)
11. <http://www.prace-ri.eu/> [↑](#footnote-ref-11)
12. EGI-Engage M3.4 Pilot services and best practices to enable federated AAI solutions: <https://documents.egi.eu/public/ShowDocument?docid=2825> [↑](#footnote-ref-12)
13. <https://rcauth.eu/> [↑](#footnote-ref-13)
14. <https://wiki.nikhef.nl/grid/AARC_Pilot_-_Architecture> [↑](#footnote-ref-14)
15. <https://wiki.egi.eu/wiki/GOCDB> [↑](#footnote-ref-15)
16. <http://goc.egi.eu> [↑](#footnote-ref-16)
17. <https://wiki.egi.eu/wiki/AppDB> [↑](#footnote-ref-17)
18. <https://refeds.org/category/research-and-scholarship> [↑](#footnote-ref-18)
19. <https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf> [↑](#footnote-ref-19)
20. <https://www.igtf.net/ap/authn-assurance/igtf-authn-assurance-1.0.pdf> [↑](#footnote-ref-20)
21. <https://aai.egi.eu/registry/> [↑](#footnote-ref-21)
22. <http://www.internet2.edu/products-services/trust-identity/comanage/> [↑](#footnote-ref-22)
23. <https://wiki.egi.eu/wiki/GOCDB/PI/Technical_Documentation> [↑](#footnote-ref-23)
24. <https://spaces.internet2.edu/display/COmanage/REST+API> [↑](#footnote-ref-24)
25. <http://www.unity-idm.eu/documentation/unity-1.9.4/manual.html#endp-rest-admin> [↑](#footnote-ref-25)
26. <https://wiki.egi.eu/wiki/Policies_and_Procedures> [↑](#footnote-ref-26)
27. <https://documents.egi.eu/document/86> [↑](#footnote-ref-27)
28. <https://documents.egi.eu/document/1475> [↑](#footnote-ref-28)
29. <https://documents.egi.eu/document/2934> [↑](#footnote-ref-29)
30. <https://documents.egi.eu/document/2935> [↑](#footnote-ref-30)
31. <http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html#eduPersonUniqueId> [↑](#footnote-ref-31)
32. <http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html#eduPersonEntitlement> [↑](#footnote-ref-32)
33. There is currently no standard OpenID Connect claim to express entitlements. However, the REFEDS OpenID Connect for Research and Education Working Group (OIDCre) is already investigating the standardisation of new claims for expressing the attributes defined in the eduPerson schema, including the eduPersonEntitlement. [↑](#footnote-ref-33)
34. <https://wiki.egi.eu/wiki/URN_Registry> [↑](#footnote-ref-34)
35. <https://cdsweb.cern.ch/record/1442597> [↑](#footnote-ref-35)