Test report and feedback from the customers

Author: Diego Scardaci

Version: 1.0

Document Link: https://documents.egi.eu/document/3580

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v.0.1	2019-10-31	Initial version	Nicolas Liampotis; Ioannis Igoumenos, Nick Evangelou (GRNET) Diego Scardaci and Valeria Ardizzone (EGI F.)
v.1	2020-03-09	First version	Nicolas Liampotis; Ioannis Igoumenos, Nick Evangelou (GRNET) Diego Scardaci and Valeria Ardizzone (EGI F.)
…			
…			
v.n			

TERMINOLOGY

The EGI glossary of terms is available at: https://wiki.egi.eu/wiki/Glossary

Contents

1 Introduction

The Check-in service is the AAI Platform for the EGI infrastructure. The Check-in service enables the Integration of external IdPs (from eduGAIN and individual organizations) with the EGI services through the Check-in IdP/SP proxy component, so that users are able to 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. The Check-in 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 Check-in 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 Check-in service has a comprehensive list of connectors that allows to integrate their systems as externally managed Attribute Authorities. This is not meant to be an exhaustive list of the functionality of the Check-in Service. More information can be found on the EGI Check-in Service wiki page (https://wiki.egi.eu/wiki/AAI).

2 Testing

Check-in Service framework gets periodically tested and evaluated in order to be robust and available to its users 24/7. It depends on the specific stage of the development, deployment or operational cycle we need to evaluate the approach of testing we will follow. For example, we perform different testing during the development of new features, than during the deployment phase. Also the deployment phase needs to fulfil different criteria for each environment. Currently we sustain three different environments, the development, the demo and the production.

In addition, there are health checks/tests that provide a snapshot of the availability and status of the service and its different components.

The table below summarises the different categories of the performed tests and their results.

Testing	
Testing Category	**Tested Activity and Results**
Functional and technical	Check-in is able to: - Integrate with IdPs supporting the SAML2 standard - Integrate with IdPs supporting the OpenID Connect/OAuth2 standard - Integrate with SPs supporting SAML2 and OpenID Connect/OAuth2 - Provide support for command-line access using OpenID Connect/OAuth2 - Gather attributes from existing EGI ops tools such as the GOCDB (site roles) and the Ops Portal (membership in VOMS-managed VOs) - Has been registered with eduGAIN as an SP - Consume group information from multiple attributes authorities and aggregate
Availability, continuity and performance-related	Monthly Availability - Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month. - For IdP/SP Proxy (including IdP Discovery Service): Over 99% (minimum requirement: 99%) - User Enrolment and Group/Virtual Organisation (VO) Management: 99% (minimum requirement: 99%) - For TTS (Master Portal): Over 99% (minimum requirement: 90%) Monthly Reliability - Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month, excluding scheduled maintenance periods. - For IdP/SP Proxy (including IdP Discovery Service): Over 99% (minimum requirement: 99%) - User Enrolment and Group/Virtual Organisation (VO) Management: 99% (minimum requirement: 99%) - For TTS (Master Portal): Over 99% (minimum requirement: 90%)

	See also ARGO dashboard
Security and data protection-related	Service is compliant with the privacy European regulations. It also fulfils: - REFEDS Code of Conduct - SIRTIFI - It is ready to comply with additional requirements provided by actions such as the AARC/AARC2 projects A thorough process of system security testing from a user's as well as inside and outside (black-box) point of view together with testing of the underlying operating system, other software package dependencies and its configurations. The main results are summarized in Annex I which follows the WISE based Risk Assessment template. At the end of each periodic assessment we document the results and undertake any necessary actions.
Usability-related	The service provides information to the user about: - Who is asking for authentication - Who is providing attributes (e.g. which IdP) - Consent/user notice The service is easy to use and transparent for the users in most of the usage scenarios. It works in a 'set and forget' fashion for SPs and IdPs, and users of course. Documentation evaluation: Usually the first sanity check aiming to help to identify early potential risks (ie. the required documentation is missing), spaces for improvements and possibilities for optimising the system (ie. desirable documentation is missing).
Code quality-related	Code review completed by the code inspection (expert analysis) to examine the source code and identify: potential bugs, bad code architecture, duplicated code and similar coding irregularities. Functional and user interface testing is being held before every change. Higher risk changes are reviewed by the EGI Change Advisory Board before being released in production.

3 Service Components

Check-in comprises two main components, namely the Identity Provider (IdP)/Service Provider (SP) Proxy (IdP/SP Proxy) and the User Enrolment and Group/Virtual Organisation (VO) Management. Figure 1 shows the Check-in high-level architecture diagram and interconnections to other AAI services, IdPs and tools.

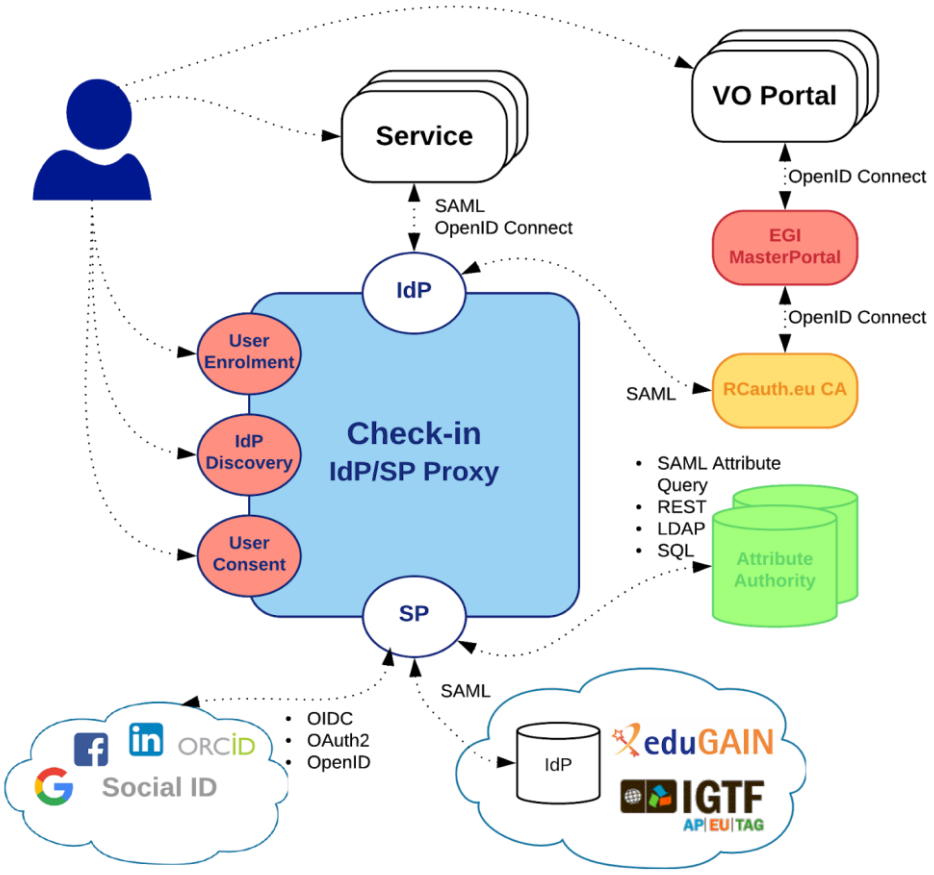

Figure 1. EGI Check-in High-level service architecture

Service components					
#	Type	Description	Related technology	Organisation and contact	TRL [1]

1	*Enabling*	**IdP/SP proxy:** providing connection with the IdPs and authentication information to EGI service providers	SimpleSAMLphp,MitreId Connect	UNINETT - support, MITRE Corporation and MIT Internet Trust Consortium (ITC) - support	9
2	*Enabling*	**User enrolment and VO/Group Management:** Supports the management of the full life cycle of user accounts in Check-in. This includes the initial user registration, the acceptance of the terms of use of the infrastructure, account linking, group and VO management, delegation of administration of VOs/Groups to authorised users and the configuration of custom enrolment flows for VOs/Groups via an intuitive web interface. For VOs, operating their own Group/VO Management system, the Check-in service has a comprehensive list of connectors that allows to integrate their systems as externally managed Attribute Authorities.	COmanage(see also InCommon)	website-email	9
3	*Enabling*	• **simplesamlphp-module-userid :** A SimpleSAMLphp module for generating long-lived, non-reassignable, non-targeted, opaque and globally unique user identifiers based on the attributes received from the identity provider • **simplesamlphp-module-attributelimit :** A	RCIAM	GRNET - EGI AAI CheckIn Support <egi-aai-checkin@lists.grnet.gr>	9

		SimpleSAMLphp module for limiting which attributes are passed on • **simplesamlphp-module-fullnameparser :** A SimpleSAMLphp module for generating given name and surname attributes based on the full name information received from the identity provider • **simplesamlphp-module-authoauth2 :** OAuth2/OIDC Authentication module for SimpleSAMLphp • **simplesamlphp-module-attrauthgocdb :** A SimpleSAMLphp module for retrieving attributes from the Grid Configuration Database (GOCDB) and adding them to the list of attributes received from the identity provider • **simplesamlphp-module-authorcid :** A SimpleSAMLphp module for authenticating users' ORCID iDs and retrieving publicly-visible information from the ORCID registry • **simplesamlphp-module-**			

		authnauthority : A SimpleSAMLphp module for generating an attribute with the value(s) of the <AuthenticatingAuthority> element contained in a SAML authentication response • **simplesamlphp-module-attrauthcomanage:** A SimpleSAMLphp module for retrieving attributes from COmanage Registry and adding them to the list of attributes received from the identity provider • **simplesamlphp-module-assurance:** A SimpleSAMLphp module for determining and indicating the Level of Assurance (LoA) of an authentication event			

4	*Enhancing*	**Token Translation Service:** The MasterPortal provides a Token Translation capability from (primarily) SAML to X.509 leveraging the RCauth online CA, and enabling pure web-based portals to access X.509 resources on behalf of their users. Transparent caching service between Science Gateways and the RCauth online CA, handling the complexity of obtaining certificates for the Science Gateways and end-users. Additionally provides capability to upload SSH public keys and retrieving proxy certificates using those.	Master Portal	NIKHEF - EGI AAI CheckIn Support <egi-aai-checkin@lists.grnet.gr>	9

3.1 Monitoring

Monitoring is a crucial part of EGI Check-in infrastructure, as a result we use ARGO framework for this purpose. ARGO is a lightweight monitoring service for Availability and Reliability provided by EGI foundation. Below we provide a list of the services and the corresponding metrics currently tracked by the framework.

Table 1. Monitored Services and Metrics

Service Types	Metrics
egi.aai.oidc	eu.egi.CertValidity
	org.nagios.OIDC-AuthZ
	org.nagios.OIDC-Provider-Config
	org.nagios.IdP-DiscoveryService

egi.aai.saml	org.nagios.SAML-IdP
	org.nagios.SAML-SP
egi.aai.tts	org.nagios.TTS-MasterPortal-Config
	org.nagios.TTS-MasterPortal-Register

4 Approval of the acceptance criteria

The EOSC Synergy project[1] has adopted Check-in as its main AAI service. The following table lists the feedback received by EOSC Synergy on the Check-in acceptance criteria.

Table 2. Feedback from EOSC Synergy project on the Check-in acceptance criteria

Category	Acceptance criteria	Critical (Yes/No)
Functional and technical acceptance criteria	• Is Check-in federated in eduGAIN? • Is Check-in compliant with R&S and Sirtifi?	• Yes • Yes
Availability, continuity and performance-related acceptance criteria	• Is the deployment of the service reasonably supporting high availability requirements?	• Yes
Security and data protection-related acceptance criteria	• Is the data protection policy technically fulfilled?	• Yes
Usability-related acceptance criteria	• Is the authentication through Check-in transparent and smooth without errors/latency? • Is Check-in displaying clear and understandable messages in case of error?	• Yes • Yes
Organisational acceptance criteria	• Is GGUS SU active? • Is documentation sufficient for the SPs and IdPs to integrate with Check-in?	• Yes • Yes

[1] https://www.eosc-synergy.eu/