EGI Foundation

Services for AAI

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Service Supplier	**CESNET, GRNET, NIKHEF**
Start Date	1st January 2021
End Date	30th June 2023
Status	FINAL
Agreement Date	14th June 2021
OLA Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
			Małgorzata Krakowian
			Peter Solagna
1.1	05/10/2017	added a reference to the availability and continuity plans	Alessandro Paolini
2.0	17/11/2017, 27/06/2018	New OLA covering 2018, 2019, 2020 years	Alessandro Paolini, Nicolas Liampotis
2.1	13/11/2019	yearly review; introduced the Service Provider and the Component Provider roles; updated Violations, Escalation, and Complaints sections; added the distinction between Component Providers involvement; added the description of TTS component	Alessandro Paolini, Nicolas Liampotis
3.0	16/12/2020, 23/04/2021, 14/06/2021	Covering EGI ACE from Jan 2021 to June 2023; renamed EGI Corporate Level as EGI Default OLA; updated section 1; updated the support unit name; updated section 7 on security requirements; changed frequency of the reports; A/R targets for MasterPortal are now 95%; added Software and ITSM compliance in section 8; added in section 9 the requirement about periodic supplier process audits conducted by EGI Foundation	Alessandro Paolini, Nicolas Liampotis
3.1	04/07/2022	yearly review; added the Federation Registry in section 1; introduced the term Service Supplier; updated section 7 and section 8; updated some links.	Alessandro Paolini, Nicolas Liampotis

TERMINOLOGY

The EGI glossary of terms is available at: http://go.egi.eu/glossary

For the purpose of this Agreement, the following terms and definitions apply. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", “MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Contents

Contents

The present Operational Level Agreement ("the Agreement') is made between EGI Foundation **(the Service Provider)** and CESNET, GRNET, NIKHEF **(the Service Suppliers)** to define the provision and support of the provided services as described hereafter. Representatives and contact information are defined in Section 6.

This Agreement is valid from **1st January 2021** to **30th June 2023**.

The Agreement was discussed and approved by the Service Provider and the Component Providers **14th June 2021**.

The Service Suppliers are bound by the terms and conditions of the EGI Default Operational Level Agreement[1] supplemented by the terms and conditions of this specific Agreement:

1 The Services

The Services are defined by the following properties:

Technical	The **Check-in** service is the AAI Platform for the EGI infrastructure: • It enables the Integration of external IdPs (from eduGAIN and individual organisations) 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 organisations 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 User Enrolment and VO/Group Management Service allows to create Virtual Organisations (VOs), manage these VOs, invite users to collaborate, manage registration flows, organise users in groups and assign them roles and resource entitlements as needed within the VOs. • 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. • The Check-in User Enrolment and VO/Group Management Service supports two of the most popular membership and group management systems, namely COmanage Registry and Perun. • For VOs, operating their own VO/Group Management system, the Check-in service has a comprehensive list of connectors that allows

[1] https://documents.egi.eu/document/2752

	it to integrate their systems as externally managed Attribute Authorities. ● 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. It also enables transparent caching between Science Gateways and the RCauth online CA, handling the complexity of obtaining certificates for the Science Gateways and end-users. In addition, the MasterPortal allows end users to upload SSH public keys and retrieve proxy certificates using those keys. ● The **Federation Registry** component provides a secure web interface through which service operators can manage the connection of their OpenID Connect and SAML based services to Check-in. The web interface of the Federation Registry covers the whole service lifecycle, including the initial registration, reconfiguration, and deregistration. The service configurations are deployed by sending configuration messages to the Federation Registry Deployment Agents running on the IdP/SP Proxy component. These configuration messages are exchanged asynchronously through the ARGO Messaging service following the Google pub/sub protocol. The activity also includes the support of the **VOMS Catch-All** and **DTEAM VO membership management** services as legacy services for the authentication and authorisation of users in EGI. **PERUN** is a group management system, developed, maintained and operated by CESNET, in use by some scientific communities. CESNET will host scientific communities on a shared instance or provide a dedicated instance for those that require it, providing support for (de-)provisioning and continuous update of user account information.
Coordination	This activity is responsible for the coordination of the system operations in collaboration with those partners that are in charge of operating other systems that depend on the EGI AAI infrastructure, including: ● operation teams of the federated IdPs/SPs ● EGI Operations for the policy and operational requirements ● members of the AARC Engagement Group for Infrastructures (AEGIS) and other Research/e-Infrastructures for any alignment activities required

	System operations and upgrade activities will be coordinated among partners to ensure continuity of the service.
Operation	● Daily running of the system: ○ Check-in IdP/SP Proxy, COmanage Registry, the MasterPortal (Token Translation functionality), the Federation Registry and the VOMS-based Catch-all VO membership management are operated by GRNET ○ development and support for MasterPortal component (TTS functionality) is provided by NIKHEF ○ PERUN is operated by CESNET ● Provisioning of a high availability configuration for all the components: ○ The core components of the Check-in service, namely the IdP/SP Proxy, the IdP Discovery, the COmanage Registry-based User Enrolment, and the Federation Registry 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. ○ The VOMS Catch-All and DTEAM VO services as legacy services do not offer High Availability Configuration but regular backup and automation scripts allow the quick recovery of the service if needed. ○ The PERUN service hosted in the CESNET cloud infrastructure is periodically backed-up, as well as the database; the LDAP service is hosted in two instances geographically separated, and the data are replicated in real time between them; PERUN and its components are monitored by Nagios, with SMS notification in case of failures. ● Creating an Availability and Continuity Plan for the AAI[2] services and implementing countermeasures to mitigate the risks defined in the related risk assessment ● Support request for changes through the GGUS support unit ● Support to:

[2] https://wiki.egi.eu/wiki/Services_Availability_Continuity_Plans

	○ Identity providers who are integrated in Check-in, only for issues concerning the Check-in service ○ Attribute providers who are integrated in Check-in, only for issues concerning the Check-in service ○ End users who use Check-in to authenticate in EGI and to access to services and resources that are offered through the EOSC portal ○ Service providers about the interaction of the services with Check-in proxy
Maintenance	The activity involves maintaining online documentation with guides and support material for end users, VO managers, service operators and IdP administrators. The activity will also be responsible for gathering new requirements for the improvement of the services. As part of this activity, the required probes for testing the functionality of the service will be maintained.

2 Service hours and exceptions

As defined by the EGI Default Operational Level Agreement.

3 Support

As defined by the EGI Default Operational Level Agreement.

Support is provided via EGI Service Desk[3] Support Units:

- Check-in: Check-in (AAI)
- EGI Catch-all: Catch-all services
- Perun: Attribute Management (Perun)

Support is available between:

- Monday and Friday
- 9:00 and 17:00 CET/CEST time

This excludes public holidays at the same time in all organizations providing the service.

[3] http://helpdesk.egi.eu/

3.1 Incident handling

As defined by the EGI Default Operational Level Agreement.

3.2 Service requests

As defined by the EGI Default Operational Level Agreement.

4 Service level targets

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.
- Minimum (as a percentage per month) for IdP/SP Proxy, IdP Discovery Service and PERUN (shared instance) User Enrolment: 99%
- Minimum (as a percentage per month) for VO Management Service, VOMS: 95%
- Minimum (as a percentage per month) for Master Portal: 95%

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.
- Minimum (as a percentage per month) for IdP/SP Proxy, IdP Discovery Service, PERUN (shared instance) User Enrolment and VO Management Service, VOMS: 99%
- Minimum (as a percentage per month) for Master Portal: 95%

Quality of Support level

- Medium (Section 3)

5 Limitations and constraints

As defined by the EGI Default Operational Level Agreement.

6 Communication, reporting and escalation

6.1 General communication

The following contacts will be generally used for communications related to the Services in the scope of this Agreement.

Service Provider contact	Alessandro Paolini

	operations@egi.eu
Service Suppliers contact	CESNET: ● Slavek Licehammer: slavek@ics.muni.cz GRNET: ● Nicolas Liampotis: nliam@grnet.gr NIKHEF: ● David Groep: davidg@nikhef.nl
Service Support contact	See Section 3

6.2 Regular reporting

As part of the fulfilment of this Agreement and provisioning of the Services, the following reports will be provided:

Report title	Contents	Frequency	Produced by	Delivery
Service Performance Report	The document provides the overall assessment of service performance (per month) and OLA target performance achieved during the reference reporting period	10 months (first report covering the period Jan – Oct 2021)	Service Suppliers	Survey form prepared by EGI Foundation

6.3 Violations

The Service Suppliers commits to inform the Service Provider, if this Agreement is violated or violation is anticipated. The following rules are agreed for communication in the event of violation:

- In case of any violations of the Services targets, the Service Suppliers will provide justifications and a plan for Services enhancement to the Service Provider. The Service Suppliers will produce a status report and a Service enhancement plan for the improvement of the Services within one month from the date of the first notification.
- The Service Provider will notify the supporting Resource Centres in case of suspected violation via the EGI Service Desk. The case will be analysed to identify the cause and verify the violation.

6.4 Escalation and complaints

For escalation and complaints, the Service Suppliers contact point shall be used, and the following rules apply.

- In case of repeated violation of the Services targets for two consecutive months or four months over a period of 12 months, a review of the Agreement and of the Services enhancement plan will take place involving the parties of the Agreement.
- Complaints or concerns about the Services provided should be directed to the Service Suppliers contact who will promptly address these concerns. Should the Service Provider still feel dissatisfied, about either the result of the response or the behaviour of the Service Suppliers, EGI Foundation Director director@egi.eu should be informed.

7 Information security and data protection

As defined in the EGI Default Operational Level Agreement.

The following rules for Information Security and data protection should be enforced when they are applicable:

- The Service Suppliers agrees to make every effort to maximise security level of users' data and minimise possible harm in the event of an incident. Security Incidents affecting the services described in Section 1 must be immediately reported to the EGI Foundation using ism@mailman.egi.eu and will have to be reported to EGI CSIRT using abuse@egi.eu within 4 hours after their discovery and handled according to the SEC01[4] procedure.
- EGI Foundation holds the role of the Data Controller while the Service Suppliers hold the role of Data Processor. Data Processing Agreements must be signed between EGI Foundation (the Data Controller) and Component Provider (the Data Processor).
- The Service Suppliers must comply with the EGI Policy on the Processing of Personal Data[5] and provide a Privacy Notice. This privacy Notice must be agreed with EGI Foundation and must be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)[6].
- The Service Suppliers must enforce the EGI WISE Acceptable Usage Policies[7].
- The Service Suppliers shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[8] in its most current version[9], which will be made available to the Service Suppliers by EGI Foundation upon request.

[4] https://go.egi.e/usec01

[5] https://documents.egi.eu/public/ShowDocument?docid=2732

[6] https://aarc-project.eu/policies/policy-development-kit/

[7] https://documents.egi.eu/public/ShowDocument?docid=3600

[8] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

[9] https://refeds.org/category/code-of-conduct/v2

- The Service Suppliers must meet all requirements of any relevant EGI policies or procedures[10] and also must be compliant with the relevant national legislation. Regarding EGI requirements, please refer to the following reference documentation:
    - EGI-doc-3015: e-Infrastructure Security Policy
    - EGI-doc-3601: Service Operations Security Policy
    - EGI-doc-2732: Policy on the Processing of Personal Data
    - EGI-doc-3600: Acceptable Use Policy and Conditions of Use
    - EGI-doc-2934: Security Traceability and Logging Policy
    - EGI-doc-2935: Security Incident Response Policy
    - EGI-doc-710: Security Incident Handling Procedure

8 Responsibilities

8.1 Of the Service Suppliers

Additional responsibilities of the Service Suppliers are as follows:

- Adhering to all applicable operational and security policies and procedures[11] and to other policy documents referenced therein.
- Using the communication channels defined in this Agreement.
- Attending OMB[12] and other operations meeting when needed
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.
- The Service endpoints with associated roles is registered in GOC DB[13] as site entity under the EGI.eu Operations Centre hosting EGI central operations tools[14].
- Changes in the system must be rolled in production in a controlled way in order to avoid service disruption.
- Putting in place an effective way to manage and control configuration items and changes such that they can meet the CHM requirements coming from EGI as a customer including making risk assessments and considering high risk changes

8.1.1 Software compliance

Unless explicitly agreed, software being used and developed to provide the service should:

- Be licensed under an open source and permissive licence (e.g. MIT, BSD, Apache 2.0,...).

[10] https://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home

[11] https://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home

[12] https://confluence.egi.eu/display/EGIBG/Operations+Management+Board

[13] http://goc.egi.eu/

[14] https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

- Unless otherwise agreed, be licensed to provide unlimited access and exploitation rights to the EGI Federation.
- Have source code publicly available via a public source code repository (if needed a mirror can be put in place under the EGI organisation in GitHub[15].) All releases should be appropriately tagged.
- Adopt best practices:
    - Defining and enforcing code style guidelines.
    - Using Semantic Versioning.
    - Using a Configuration Management frameworks such as Ansible.
    - Taking security aspects into consideration at every point in time.
    - Having automated testing in place.
    - Using code reviewing.
    - Treating documentation as code.
    - Documentation should be available for Developers, administrators and end users.

8.1.2 IT Service Management compliance

- Key staff who deliver services should have foundation or basic level ITSM training and certification
    - ITSM training and certification could include standards and best practices such as FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key service management processes for their services.
- Service Suppliers should have clear interfaces with the EGI Service Management System processes and provide the required information.
- Service Suppliers should commit to improving their management system used to support the services they provide.

8.2 Of the Service Provider

The responsibilities of the Service Provider are:

- Delivering and planning the Services according to a ISO compliant manner.
- Raising any issues deemed necessary to the attention of the Service Suppliers.
- Collecting requirements from the Resource infrastructure Providers.
- Supporting coordination and integration with other EGI services.
- Providing monitoring to measure fulfilment of agreed service level targets.
- Providing clear interfaces to the EGI SMS processes.

[15] https://github.com/EGI-Federation

9 Review, extensions, and termination

There will be reviews of the service performance against service level targets and of this Agreement at planned intervals with the Service Provider according to the following rules:

- Technical content of this Agreement and targets will be reviewed on a yearly basis
- EGI Foundation shall be entitled to conduct audits or mandate external auditors to conduct audits of suppliers and federation members at a reasonable frequency. These will aim to evaluate the effective provision of the agreed service or service components and the execution of activities related to providing and managing the service prior to the commencement of this Agreement and then on a regular basis. EGI Foundation will announce audits at least one month in advance. The Service Suppliers / federation member shall support EGI Foundation and all auditors acting on behalf of EGI Foundation to the best of their ability in carrying out the audits. The Service Suppliers / federation member is obliged to provide the auditors, upon request, with the information and evidence necessary. Efforts connected to supporting these audits by the Service Suppliers / federation member will not be reimbursed.