EGI Foundation

Data Management Service - Rucio

Operational level Agreement

Service Provider	EGI Foundation
Service Supplier	**UKRI**
First day of service delivery	1st January 2021
Last day of service delivery	30th June 2023
Status	Final
Agreement finalisation date	25th February 2021
Agreement Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
0.1	10/12/2020	first draft of the document	Andrea Manzi, Alessandro Paolini
1.0	25/02/2021	document finalised	Alessandro Paolini, Alastair Dewurst
1.1	01/07/2022	yearly review; introduced the term Service Supplier; updated section 7 and section 8; corrected some typos; updated the contacts section;	Alessandro Paolini, Timothy Noble

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 Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **UKRI (the Service Supplier)** 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 EGI Foundation and the Service Supplier **25th February 2021**.

The Service Supplier(s) is (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	Rucio is a software framework that provides services and associated libraries for allowing scientific collaborations to manage large volumes of data spread across facilities at multiple institutions and organisations. Rucio offers advanced features, is highly scalable, and modular. It is a data management solution that could cover the needs of different communities in the scientific domain (e.g., HEP, astronomy, biology). Rucio has been designed for extreme scalability and has many components making it a daunting prospect for small VOs to use. Even if a VO only has data at a single site, it can still be useful as it provides an abstraction layer between the user and the storage, as well as a file catalogue and monitoring. The Multi-VO Rucio development that STFC is leading is designed to allow smaller VO (aka the long tail of science) to take advantage of Rucio's many features. Rucio can be accessed through CLI, REST API or UI
Coordination	The service team is responsible for the coordination of the system operation and upgrade activities with those partners that are in charge of operating other systems that depend on it.

Operation	• Daily running and maintenance of the system, including managing updates and support.
	• Provisioning of a high availability configuration
	  ○ Rucio Servers behind an HA Proxy Service,
	  ○ Multiple Rucio Auth and Daemon nodes

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

	○ A test infrastructure to verify interoperability and the impact of software upgrades on depending systems ● The service database is hosted by the Scientific Computing Department's Database Services group on production infrastructure. This includes nightly DB back-ups to the STFC tape storage facility and UPS support. ● The service database will be managed by professional database admins on resilient production infrastructure, which will be backed up regularly. ● The Multi-VO Rucio instance should be TRL9 ● The Multi-VO Rucio instance should be integrated with EGI Check-in ● Support for new VOs must be explicitly requested as they need to be configured ● Integration of more storage endpoints ○ development of tools to quickly configure a wide range of new storage endpoints. ● User specific monitoring and accounting: ○ build additional monitoring and accounting dashboards for early adopters; ○ planning the further work necessary for a "complete" monitoring service; ○ provide accounting information that isn't available via existing services. ● Creating an Availability and Continuity Plan[2] and implementing countermeasures to mitigate the risks defined in the related risk assessment
Maintenance	● Bug fixing, proactive maintenance, improvement of the system ● Coordination of software maintenance activities with other technology providers that provide software for the EGI Core Infrastructure or remote systems deployed by integrated and peer infrastructures that interoperate with the central EGI components of the system ● Maintenance of probes to test the functionality of the service ● Requirements gathering for new features and service enhancements ● Maintaining documentation

[2] https://confluence.egi.eu/x/dwHhBw

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 Unit: Rucio

Support is provided via EGI Service Desk. Access requires a valid X.509 or the login via a EGI SSO account[4].

Support is available between:

- Monday and Friday
- 9:00 and 17:00 UTC time

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

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): 98%

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.

[3] http://helpdesk.egi.eu/
[4] https://www.egi.eu/sso/

- Minimum (as a percentage per month): 98%

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 service in the scope of this Agreement.

Service Provider contact	Alessandro Paolini operations@egi.eu EGI Foundation Operations officer
Component Provider contact	Timothy Noble Timothy.noble@stfc.ac.uk
Service Support contact	See Section 3

6.2 Regular reporting

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

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

All reports shall follow predefined templates[5].

[5] https://documents.egi.eu/document/2881

6.3 Violations

The Service Supplier 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 Supplier will provide justifications and a plan for Services enhancement to the Service Provider. The Service Supplier 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 Supplier 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 Supplier 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 Supplier, EGI Foundation Director director@egi.eu should be informed.

7 Information Security and data protection

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

- The Service Supplier 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[6] procedure.
- EGI Foundation holds the role of the Data Controller while the Service Supplier holds the role of Data Processor. Data Processing Agreements must be signed between EGI Foundation (the Data Controller) and Service Supplier (the Data Processor).

[6] https://go.egi.eu/sec01

- The Service Supplier must comply with the EGI Policy on the Processing of Personal Data[7] 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)[8].
- The Service Supplier must enforce the EGI WISE Acceptable Usage Policies[9].
- The Service Supplier shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[10] in its most current version, which will be made available to the Component Provider by EGI Foundation upon request.
- The Service Supplier must meet all requirements of any relevant EGI policies or procedures[11] 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 Supplier

Additional responsibilities of the Service Supplier are as follows:

- Adhering to all applicable operational and security policies and procedures[12] and to other policy documents referenced therein.
- Using communication channels defined in the agreement.
- Attending OMB[13] and other operations meetings when needed.
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.
- The service endpoints with associated roles are registered in GOC DB[14] as site entity under EGI.eu Operations Centre hosting EGI central operations tools[15].

[7] https://documents.egi.eu/public/ShowDocument?docid=2732
[8] https://aarc-project.eu/policies/policy-development-kit/
[9] https://documents.egi.eu/public/ShowDocument?docid=3600
[10] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
[11] https://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home
[12] https://www.egi.eu/about/policy/policies_procedures.html
[13] https://confluence.egi.eu/display/EGIBG/Operations+Management+Board
[14] http://goc.egi.eu/
[15] https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

- 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 (like MIT, BSD, Apache 2.0,...).
- 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[16].) All releases should be appropriately tagged.
- Adopt best practises:
    - 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 reviews.
    - 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 FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key processes for their services.
- Service Supplier should have clear interfaces with the EGI SMS processes and provide the required information.
- Service Supplier 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:

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

- Delivering and planning the Services according to an ISO 20000 compliant manner.
- Raise any issues deemed necessary to the attention of the Service Supplier.
- Collecting requirements from the Resource infrastructure Providers.
- Supporting coordination with other EGI services.
- Providing monitoring to measure fulfilment of agreed service level targets.
- Providing clear interfaces to the EGI SMS processes.

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 the 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 at evaluating the effective provision of the agreed service or service component and 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 provider / 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 provider / federation member is obliged to provide the auditors, upon request, with the information and evidence necessary. Efforts connected to supporting these audits by the provider / federation member will not be reimbursed.