EGI Foundation

UMD and CMD software provisioning infrastructure

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Service Suppliers	**IBERGRID (CSIC, LIP)**
Start Date	1st January 2021
End Date	30th June 2023
Status	FINAL
Agreement Date	21st January 2021

OLA Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
2.0	9/11/2017	New OLA covering 2018, 2019, 2020	Alessandro Paolini
2.1	27/06/2018	Changed the reporting period to 9 months	Alessandro Paolini
2.2	16/09/2019	Yearly review; introduced the roles Service Provider and Component Provider; updated contacts; updated sections on Violations, Escalations, and Complaints	Alessandro Paolini
3.0	07/01/2021, 23/02/2021	Covering EGI ACE from Jan 2021 to June 2023; renamed EGI Corporate Level as EGI Default OLA; updated section 7 on security requirements; changed frequency of the reports; added Software and ITSM compliance in section 8; added in section 9 the requirement about periodic supplier process audits conducted by EGI Foundation; switched provider to IBERGRID, A/R percentage updated to 90% according to bid; added note on holidays in the Support section	Alessandro Paolini, Vincenzo Spinoso, Isabel Campos, Joao Pina
3.1	10/02/2022	Yearly review; introduced the term Service Supplier; updated section 7 and section 8	Alessandro Paolini

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 **IBERGRID (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**21st January 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	The software provisioning infrastructure is composed by the following components: ● Integration with RT, a new product release (the tuple Product, Platform, Architecture) is associated with a RT ticket, which tracks the status of the product in the software provisioning process. ● Submission of new products with XML. ● Repository Back-end: responsible unit for handling the movement of packages between repositories, validating the individual product releases submissions, building accumulative as well as per-product YUM/APT repositories (multiple per OS/Arch case) and the other automations needed to perform the UMD and CMD operations. It also provides a RESTful API for external integrations (e.g. with the UMD and CMD portal/frontend). ● Composer: a web-based interface for bundling versioned software products that have successfully passed the UMD and CMD verification process, into a robust UMD and CMD release ready to be deployed either to the production or the candidate repositories. ● Repositories: the following repositories must be maintained for every operating system and major release supported: ○ Untested: contains the packages to be installed during the verification ○ Testing: contains the packages to be installed during staged rollout ○ Base: contains the packages released in the first major release ○ Update: contains the packages released in the update releases

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

	○ Release Candidate: it is generated before a UMD and CMD release, to simulate the production repositories after the UMD and CMD release under preparation. This is used to test the installability of the newly released components, as well as the products already in production. ● The processes to move products between repositories and to create releases must be as automated as possible. ● The task must provide statistics about the repository usage in terms of downloads, aggregated by packages and time. ● Front-end, the information about UMD and CMD releases (release notes, list of components, configuration) must be available in a web frontend. **Note**: the architecture of the internal components is not mandatory, but the services provided must be equivalent. The software provisioning infrastructure must support multiple distributions, multiple operating system (EL based, and Debian based) and major releases (at least two major releases). The infrastructure should also support a "Preview" repository where products are quickly released without verification. It is not an official UMD repository, but it represents a place where products can be made available to service providers more quickly and directly, bypassing the quality assurance steps.
Coordination	The task must coordinate with the UMD and CMD quality assurance task as well as EGI Operations when necessary, and with the AppDB provider to support the community repositories.
Operation	● The task must operate all the technical services described before: ○ Repositories (production, testing, untested and RC, community repositories) ○ Repositories back-end (including UMD composer) ○ Web pages (repository front-end, Release XML editor) ● The task will articulate with UMD Software provisioning team the technical requirements. ● The task must support the creation of the distributions and for each distribution the creation of the releases, creating the release candidates and the actual releases.
Maintenance	● Adapt repositories according to SWPP requirements, such as supporting new OS distributions or adding new types of artefacts. ● Regular (yearly) requirements gathering for future improvements of the service. ● Maintain up-to-date documentation of the service

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[2] Support Unit: Software Repository

Support is available between:

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

This excludes public holidays and site closures for the Component Providers.

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):
  - UMD repositories, web front-end, the community repository: 90% (as a percentage per month)
  - the other components (Repository backend and Composer): 75% (as a percentage per month)

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): 90%

Quality of Support level

- Medium (Section 3)

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

5 Limitations and constraints

As defined by the EGI Default Operational Level Agreement.

The provisioning of the service under the agreed service level targets is subject to the following limitations and constraints:

- Support is provided in the following language: English
- Downtimes caused due to upgrades for fixing critical security issues are not considered Agreement violations.
- Force Majeure. A party shall not be liable for any failure or delay in the performance of this Agreement for the period that such failure or delay is due to causes beyond its reasonable control. Means any
    - fire, flood, earthquake, or natural phenomena,
    - war, embargo, riot, civil disorder, rebellion, revolution

  which is beyond the Provider's control, or any other causes beyond the Provider's control

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
Service Supplier contact	Jorge Gomes: jorge@lip.pt Mário David: david@lip.pt Joao Pina: jpina@lip.pt Isabel Campos: isabel@campos-it.es Pablo Orviz: orviz@cern.ch
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 the overall	10 months (first report covering the	Service Supplier	Survey form prepared by EGI Foundation

	assessment of service performance (per month) and OLA target performance achieved during reporting period	period Jan – Oct 2021)		

All reports shall follow predefined templates[3].

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

As defined by the EGI Default Operational Level Agreement.

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

- The Component Provider 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

[3] https://documents.egi.eu/document/2748

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 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).
- The Service Supplier 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 Supplier must enforce the EGI WISE Acceptable Usage Policies[7].
- The Service Supplier shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[8] 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[9] 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:

- Using communication channels defined in the agreement.
- Attending OMB[10] and other operations meetings when needed.
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.

[4] https://go.egi.eu/sec01https://wiki.egi.eu/wiki/SEC01
[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://www.egi.eu/about/policy/policies_procedures.html
[10] https://wiki.egi.eu/wiki/OMB

- Service with associated roles is registered in GOC DB[11] as site entity under EGI.eu Operations Centre hosting EGI central operations tools[12].
- 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[13].) All releases should be appropriately tagged.
- Adopt best practises:
    - Defining and enforcing code style guidelines.
    - Using Semantic Versioning.
    - Using a Configuration Management framework 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 standards and best practises such as FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key processes for their services.
- Component Providers should have clear interfaces with the EGI SMS processes and provide the required information.

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

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

[13] https://github.com/EGI-Foundation

- Component Providers should commit to the continuous improvement of 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 component according to an ISO 20000 compliant manner.
- Raising 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.

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 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 supplier 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 supplier 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.