Service Level Agreement

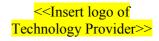between

EGI-InSPIRE

and

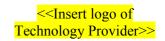## ~~Technology Provider Full Name~~The SAGA Project

**Service Level Agreement
between
EGI-InSPIRE and ~~Short Name~~The SAGA Project**

1 COPYRIGHT NOTICE

PARTIES

This Service Level Agreement describes, which services to which level the Technology Provider commits to deliver to EGI-InSPIRE as the consumer of the services. For the remainder of this document this Service Level Agreement will be referred to as "the Agreement".

1.1 EGI-InSPIRE

The EGI-InSPIRE project will support the transition from a project-based system to a sustainable pan-European e-Infrastructure, by supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI-InSPIRE will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit the user communities within the European Research Area.

> **Project EGI-InSPIRE**
> **c/o**
> **Stichting European Grid Infrastructure (EGI.eu)**
> **Science Park 105**
> **1098 XG Amsterdam**
> **The Netherlands**

For the remainder of this document EGI-InSPIRE will be referred to as "EGI".

1.2 Service provider

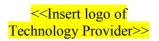~~<<Short text summarising the Technology Provider>>~~ The SAGA Project (hereafter referred to as "TSP") represents a community of developers and end users, which collectively work to (1) create and maintain the SAGA API specification documents, (2) implement the SAGA API and its middleware bindings, (3) create higher level of programming abstractions based on SAGA, and (3) deploy and support the SAGA implementations on a variety of DCIs. TSP is an active project since about 2003, and spans, as a rough estimate, about 20 academic groups from 10 countries, and a number of individual contributors. For more details on TSP, see http://www.saga-project.org/ .

> ~~<<Legal name of the Technology Provider~~
>
> ~~Address in provider's Locale format>>~~
>
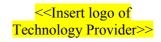> **The SAGA Project**
>
> **http://www.saga-project.org/**

info@saga-project.org

For the remainder of this document the service provider will be referred to as "the Provider".

2 GOVERNANCE

2.1 Terms

The Agreement shall be binding if and only if the representatives of both the Provider and EGI have signed the Agreement.

The Agreement shall have the following date of enforcement:

<<dd. MM. yyyy>> 00:00:00 GMT

~~The Agreement will terminate at the following date:~~

~~<<dd. MM. yyyy>> 00:00 GMT~~

The Agreement will not terminate at a pre-defined date. A termination date may be defined at a review of the Agreement<<Delete appropriate section >>

2.2 Reviews

The Agreement may be regularly reviewed. Any part of the Agreement may be subject to review and change given that it is recorded in review minutes and a new revision of the Agreement is produced.
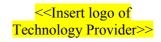
A review may take place any date and time agreed between the Provider and EGI. However, the Agreement shall be reviewed a minimum of once per year. In lieu of an review in any period, this Agreement shall remain in effect.

Any number of participants of either party may attend and are automatically accepted as soon as the review meeting is called to commence without objection. An agreed review date may only be cancelled with mutual agreement on a new date.

The review begins with appointing a minute taker, and ends with an agreement on the date of the next review meeting. The Provider and EGI may agree to not define a date of the next meeting.

Upon completion of the review a new version of the Agreement document is produced reflecting the changes agreed upon in the review meeting. Together with the recorded minutes this new version shall be circulated no later than 5 working days after the review meeting took place.

3 SCOPE OF THE AGREEMENT

The Provider agrees to deliver software components to EGI that, in total, implement the functionality of one or more capabilities defined in the UMD Roadmap [R 3]. The Provider is free in her choice as to which capability to implement and to provide to EGI. However, the Provider agrees to indiscriminately apply the service levels defined herein to all software components delivered to EGI. The detailed definition of which software components the Provider delivers to EGI is specified in section 8.

3.1 Management & Coordination

The Provider agrees to appoint fully authorised representatives and deputies to the relevant management boards of EGI-InSPIRE. The deputy temporarily takes over attendance, contribution and voting rights in the denominated boards at times of unavailability of the representative.

The following boards require regular attendance of Provider's representatives:
- Technology Coordination Board (TCB) [R 4]
- Deployed Middleware Support Unit (DMSU) [R 6]
- Risk Assessment Team (RAT) [R 5]

The respective board chair must be kept informed of any changes of roles of the Provider's representatives. ~~The current list of representatives is published in the Wiki domain of the respective board.~~

3.2 Software component delivery

3.2.1   Component roadmap and release plan

The Provider will publish a roadmap for each component it wishes to release to EGI. The roadmap may be consolidated into one document with the roadmaps for other components if the Provider releases more than one component to EGI. The roadmap must contain:
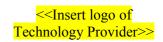- All planned major component releases
- All planned minor component releases
- Planned new features in the component
- Incompatibilities between releases

The Provider will update the roadmap(s) every half year (six calendar months) at least one calendar month before EGI publishes the UMD Roadmap on its scheduled dates [R 1].

The Provider will make available a release plan for each component registered in section 8. The Provider may consolidate release plans of more than one component into a consolidated series of one or more documents, for a better overview. The release plan must provide the planned release date for all maintained software components and must include the release dates for
- All major releases
- All minor releases

3.2.2 Release delivery and format

The Provider agrees to deliver releases on a regular basis and provides electronic access to the release contents as described in [R 8]~~, in one of the accepted formats defined by EGI (e.g. binary packages in DEB or RPM format, source releases in TGZ format).~~ The new release must be delivered by creating a tracker artefact in GGUS containing an ~~using EGI's software provisioning tools containing an~~ XML based technical description of the release [R 8Error: Reference source not foundError: Reference source not found].

Note AM: we need detailed documentation of the above release schedules, target release formats, and XML descriptions. So far, I only found parts of the information in the referenced docs, and am not sure if those references are up to date.

Note AM: ref not found

3.3 Quality Assurance

The Provider understands and accepts the Software Provisioning Process as described in EGI-InSPIRE Milestone MS503 [R 7Error: Reference source not found] and its designated successors.

Note AM: ref not found

3.3.1 Acceptance Criteria

The evolution of acceptance criteria is a normal process considering the settings within which EGI and the Provider operate.

Through active participation in the TCB the Provider advises EGI on the effort required to implement any changes to generic or specific acceptance criteria that may affect any of the maintained software components listed in section 8.

3.3.2 Test plans

The Provider agrees to formally provide or make available to EGI the complete test plans and results of continuous testing and integration of each maintainer software component.

The test plan for a given release of one particular component must include:

- All tests available, or at least an executive overview of all tests available
- The complete, detailed list of all tests executed for the given release of the component in question
- The complete, detailed result of each executed test
- Any required 3rd party software necessary to execute the test plans.
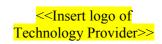
The test plan as described above must be made available to EGI prior to the planned release date for review:

- Major release: At least 20 working days
- Minor release: At least 15 working days
- Revision release: At least 10 working days

- Emergency release: N/A

Prior to entering EGI's Software Provisioning Process [Error: Reference source not found] and upon request of EGI's appropriate management unit, the Provider, in collaboration with EGI, agrees to the best of their ability to:

Note AM: ref not found

- Rerun the complete test plan for major releases
- Run a subset of the tests of the test plan (chosen by EGI) for minor releases

3.4 Issue management

The Provider has appointed personnel for technical issues concerning the maintained software components. Those technical contacts must be fully authorised to act as the Provider's representative in collaboration with EGI DMSU [R 6] regarding the triaging, assessment and resolution of any technical issues concerning the software components developed and maintained by the Provider.

3.4.1 Issue management infrastructure

The Provider makes accessible to EGI an issue tracking system providing contemporary issue management and reporting means. The Provider is free in choice of such issue management infrastructure in as much as the chosen product fully integrates with GGUS. EGI exclusively uses GGUS for its issue management hence the Provider is fully liable for any delay or subsequent issues caused by lack of integration of their chosen issue management product with GGUS.

Note AM: It is unclear from the text above if our TRAC installation meets the criteria.

3.4.2 Issue Resolution

The Provider constructively works in close collaboration with EGI DMSU on jointly investigating issues raised against software components maintained by the Provider. The investigation includes triaging the issue or incident, the problem and any known impacts. The details of the process of collaboration with the DMSU are outlined in [R 6Error: Reference source not found].

Note AM: ref not found.

In case the triage resolves to the production of a new release of the affected software component, DMSU and the service provider jointly agree on an Estimated Time of Availability (ETA) of the necessary new release of that software component.

Note AM: added comma above

The Provider agrees to prioritise the effort to resolve and fix reported issues according to their priority as set in GGUS, in the following order, while respecting the constraint of the agreed ETA:

1. Top priority
2. Very urgent

3. Urgent
4. Less Urgent

3.5 Vulnerability management

The Provider has appointed personnel for vulnerability issues concerning the maintained software components. Those security contacts must be fully authorised to act as the Provider's representative in collaboration with EGI SVG [R 9] and related boards regarding the triaging, assessment and resolution of any vulnerability issues concerning the software components developed and maintained by the Provider.

Note AM: SVG? Security Vulnerability Group?

Any appointed security contact for any delivered software component must respond to any request by the EGI SVG and associated groups (e.g. RAT). The response must be as soon as possible, or at least within 2 working days.

3.5.1 Vulnerability Resolution

The Provider agrees that any software vulnerability found in their delivered software while running on EGI production infrastructure must be handled using the SVG process [R 5Error: Reference source not found].

Note AM: ref not found

The Provider agrees that any software vulnerability in their delivered software found otherwise must be reported to the EGI SVG. If the vulnerability is reported before a fix is available, the vulnerability must be treated and resolved as if found on EGI production infrastructure, i.e. it must be handled using the SVG process. If the vulnerability is reported after a fix is available, the Provider coordinates with SVG to make available the new release including an appropriate advisory for SW release on EGI production infrastructure.

Note AM: "Must be reported" - how? Mailing list?

The Provider agrees to prioritise vulnerability resolution according to their risk assessment, in the following order:
1. Critical
2. High
3. Moderate
4. Low

For any vulnerability found in any software component delivered by the Provider, the Provider agrees to the best of their ability that no information about the vulnerability shall be disclosed to the public without consent of the SVG.

4 PERFORMANCE MEASUREMENT

The performance of the Provider shall be monitored against the metrics and objectives described in this section. The metrics and objectives are standing agenda items of each Agreement review conducted.

4.1 Definition of terms

TD – Target Date

The Target Date is the agreed date of availability to EGI of a release of a software component that fixes one or more reported vulnerabilities. Once agreed, the Target Date cannot be negotiated.

Note AM: does target date include the time for software rollout? How is the TD negotiated?

ETA – Estimated Time of Availability

The ETA is the agreed date of availability to EGI of a release of a software component that fixes one or more reported issues. The ETA may be revised between DMSU and the Provider.

Note AM: Is the ETA negotiated, or is it set by the provider?
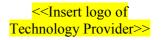
4.2 Metrics

Each metric is a positive integer number, including 0 (zero). "Secondary" metrics (i.e. metrics with an ID counter larger than 1) are constrained in that they cannot reach numbers greater than the pertinent "main" metrics (i.e. M.*.1).

Metric ID	Metric	Explanation
M.SVG.1	Number of confirmed new vulnerabilities per month	The total number of vulnerabilities discovered in all maintained software components, whether within EGI activities or outside, are collected and published. Aggregated during the reporting month.
M.SVG.2	Number of fixes delivered within TD	All fixes that are delivered within TD *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.SVG.3	Number of fixes delivered after TD	All fixes that are delivered *after* TD *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.SVG.4	Number of confirmed open vulnerabilities which have exceeded the TD	Number of confirmed vulnerabilities, which have not been fixed and have passed the TD at the time of calculating. Current value taken at the end of the reporting month on the last working at 18:00 CE(S)T.
M.SVG.5	Total number of open vulnerabilities	Current value taken at the end of the reporting month on the last working day at 18:00 CE(S)T.

M.SVG.6	Number of requests to Provider	The total number of vulnerability related requests to the appointed component contact are counted. Aggregated during the reporting month.
M.SVG.7	Number of contact responses below 2 day target	Each request made by the SVG or associated boards that were not reacted upon within 2 working days are counted. Aggregated during the reporting month.
M.DMSU.1	Number of issues assigned to the Provider	The total numbers of confirmed issues that require the Provider's effort to produce a new release are counted. Aggregated during the reporting month.
M.DMSU.2	Number of issues with revised ETA	The total number of issues for which the Provider changed the ETA are counted. Aggregated during the reporting month.
M.DMSU.3	Number of fixes delivered within ETA	All fixes that are delivered within ETA *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.DMSU.4	Number of fixes delivered within ETA + 1 week	All fixes that are delivered within ETA + 1 calendar week *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.DMSU.5	Number of fixes delivered within ETA + 1 month	All fixes that are delivered within ETA (+ 1 calendar month) *and* have passed the SW Rollout process are counted. Aggregated during the reporting month.
M.REPO.1	Number of releases delivered to EGI	The total number of releases made available to EGI through the SW Rollout process is counted. Aggregated during the reporting month.
M.REPO.2	Number of releases that passed the quality criteria verification.	All releases that passed the quality criteria verification process are counted. Release submissions that result in changes of quality criteria applicable to the pertinent component are not counted in this metric. Aggregated during the reporting month.
M.REPO.3	Number of releases that passed StageRollout verification	All releases that passed the StageRollout phase of the SW rollout process hence are accepted for production use, are counted. Aggregated during the reporting month.

Notes AM:
- 'vulnerability' == 'issue'? Or do the entries M.SVG.1-6 only refer to security issues?
- I assume that 'reacted on issue' does not mean 'issue is solved' (M.SVG.7)?
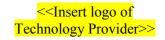
4.3 Objectives

Objectives are decimal numbers with a precision of 2 decimals rounded. In case of any main metric, at the point of collection, has the value 0 (zero) the related objective shall have the value "0.00%"

Objective ID	Objective	Calculation	Target
O.SVG.1	Proportion of issues fixed within TD	100 * M.SVG.2 / (M.SVG.2 + M.SVG.3 + M.SVG.4)	100.00%
O.SVG.2	Proportion of open issues beyond TD	M.SVG.4 / M.SVG.5 * 100	0.00%
O.SVG.3	Responsiveness of security contacts to vulnerability issues	(M.SVG.7 / M.SVG.6) * 100	100.00%
O.DMSU.1	Success rate of timely delivery within ETA	(M.DMSU.3 / M.DMSU.1) * 100	100.00%
O.DMSU.2	Success rate of timely delivery within ETA + 1 week	(M.DMSU.4 / M.DMSU.1) * 100	0.00%
O.DMSU.3	Success rate of timely delivery within ETA + 1 month	(M.DMSU.5 / M.DMSU.1) * 100	0.00%
O.REPO.1	Formal quality of component releases	(M.REPO.2 / M.REPO.1) * 100	100.00%
O.REPO.2	Functional quality of component releases	(M.REPO.3 / M.REPO.1) * 100	100.00%

Notes AM:

 - O.SVG.3: so, M.SVG.6 and M.SVG.7 *are* only about security?

5 PROBLEM MANAGEMENT & REMEDY

5.1.1 Agreement provisioning

Any failures during the provisioning of the Agreement itself must be reported to the EGI CTO (cto@egi.eu) and the Provider's contact person appointed for provisioning the Agreement.

Likewise, any perceived failure of the SLA document itself must be reported to the parties signing this Agreement.

5.1.2 Escalation

EGI and the Provider agree in a practical and benevolent approach in resolving any disputes or disagreements over any operational aspect of this agreement, or any process included herein or referenced externally.

Any reasonable and feasible attempt should be undertaken to resolve disagreements and disputes in the relevant activities on the operational day-to-day level (e.g. DMSU, RAT).
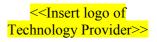
Issues that remain unresolved shall be brought to the attention of the TCB within reasonable time. The TCB then shall attempt to resolve the issue through common communication means as described in the TCB Terms of Reference [Error: Reference source not found]. Any issue discussed at the TCB will be handled openly and indiscriminately.

Note AM: ref not found

Further escalation if required, must be directed to the EGI Director and appointed overall managerial contact of the Provider.

If a resolution and consensus cannot be reached at this level, escalation may be directed to the EGI Executive Board. The EGI EB is the last instance that may reach a resolution to an escalated dispute. In case negotiations at this level fail to produce a resolution to the dispute, either party of this Agreement may initiate an extraordinarily, yet orderly, termination of the agreement and Memorandum of Understanding of the signed parties. The process of an orderly termination of the agreement is defined in section 7.

6 EGI DUTIES

To support the Provider in fulfilling ~~her~~ the duties described above~~duties~~, EGI agrees to the following.

EGI will communicate requirements and use cases collected from its end user and operations communities to the Provider through the Technology Coordination Board. These prioritised requirements may span new or existing features related to the maintained software components, and are communicated publicly and indiscriminately to any technology provider partaking in the TCB.

EGI will define and publish the environment (or environments) that the maintained software components are required to work in.

EGI will provide generic acceptance criteria related to all software components contributed to EGI.

EGI will provide specific acceptance criteria related to all software components maintained by the Provider.

EGI will inform the Provider of issues reported to EGI related to the maintained software components in use on EGI's production infrastructure.

EGI will include the Provider in the triaging of the issues mentioned above through the appointed DMSU.
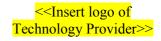
EGI will provide access to boards, process and knowledge of EGI's SVG to the Provider in order to develop and contribute corrections necessary to the maintained software components.

EGI will provide contact points for issue management, vulnerability management and general roadmap and requirements issues. The respective personnel will respond within 2 working days to issues raised by the Provider.

EGI will use the Provider's issue and vulnerability management system, where appropriate, to communicate about any issues vulnerabilities.

EGI will provide documentation about deployment and usage statistics of the delivered software components.

7 TERMINATION AND RELEASE FROM AGREEMENT

The Agreement may terminate at a date defined at the Agreement's inception (see section 2.1) or at a date agreed upon in a review. In some circumstances the Agreement may terminate because of breach of the Agreement.

Under all circumstances the termination of the Agreement must maintain productivity of EGI infrastructure at all times.

Note AM: what does that imply? If you consider SAGA a necessary requirement of EGI, are we then burning in hell forever? ;-) If you don't, does that paragraph make sense in this SLA?

Upon termination of the Agreement, the Provider is liberated from the obligation to provide any update on roadmaps, test plans or new releases to the agreed list of software components, except for already existing, confirmed issues and vulnerabilities reported against maintained software components.

Note AM: So, we will stay responsible for fixes for released versions forever? That makes some sense actually, just trying to confirm...

Upon termination of the Agreement EGI retains the right to operate the software components under the auspices of this Agreement at the current version running in the production infrastructure. To ensure continuous availability EGI may decide to roll back any delivered software component to a version EGI deems stable and suitable for production use on its infrastructure.

EGI and the Provider agree to phase out any software component specified in this Agreement according to EGI's procedures for Software Lifecycle Management in case an alternative complete implementation of the respective UMD capability is available to EGI.

Note AM: that is interesting: so the only way for you to get rid of our software is to find a new complete implementation? :-)

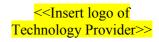## 7.1 Conditions of premature Agreement termination

EGI retains the right to terminate the Agreement whenever any of the following events occurs:

- The Provider persistently fails to meet the service levels defined in section 4.3. Persistent failure is defined as not meeting the defined objective targets for 3 consecutive months.
- The Provider persistently fails to contribute to the TCB, RAT or DMSU management bodies of EGI-InSPIRE. Failure to contribute includes representatives not joining F2F meetings or conference calls, and no contribution towards determining a Target Date for Vulnerability fixes or Estimated Times of Availability for bug fixes, respectively.

Note AM: under what circumstances are we allowed to terminate?   I assume if EGI violates (repeatedly) any item of paragraph 6?

8 SOFTWARE COMPONENTS

This section provides a detailed list of software components the Provider agrees to deliver to EGI under the terms and conditions defined in this Agreement. The list of components is provided in a series of tables aligned with the capabilities outlined with the UMD Roadmap [R 3].

The Provider is responsible for keeping the contact details up to date, and immediately communicates any changes to EGI.

The security contact is the main contact point for any vulnerabilities related to maintained software components. The appointed person serves as the first and main contact point; if requested, the Provider will communicate contact information of engineers directly involved in the development and maintenance of the pertinent software component with the best of their abilities.

Likewise, the technical contact is the main contact point for any issues related to maintained software components. The same responsibilities and roles as described for the security contact apply to the technical contact.

Managerial contacts are involved in any process related issues (i.e. non-day to day issues) related to the maintained software component, such as dispute resolution and escalation. Section 5 defines the process of dispute resolution and escalation.
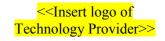
8.1 Functional Capabilities

The following table outlines all software component that implement functional capabilities described in the UMD Roadmap the Provider wishes to release to EGI under the auspices of this Agreement.

Instead of appointing individual contacts for issues concerning the delivered components the Provider wishes to appoint the following contacts for respective issues: <<Delete if not applicable>>

Management contact: Full Name   <<Delete if no overall management contact is appointed>>Shantenu Jha

                       E-Mail   sjha@cct.lsu.edu

                       Mobile   ???

Technical contact: Full Name   <<Delete if no overall management contact is appointed>>Ole Weidner

                       E-Mail   oweidner@cct.lsu.edu

                       Mobile   ???

Security contact: Full Name   <<Delete if no overall management contact is appointed>>Ole Weidner

                       E-Mail   oweidner@cct.lsu.edu

                       Mobile   ???

Notes AM:
 - emails may change to more persistent ones
 - tickets should be submitted to our bug tracking system, and not communicated via mail - correct? Who is taking care of that?

Name	First version delivered	UMD Capability	Technical Contact	Security Contact	Management Contact
Component name	1.0	One functional capability from UMD Roadmap	Full Name E-Mail Mobile	Full Name E-Mail Mobile	Full Name E-Mail Mobile
saga-core	1.6	Client API			
saga-adaptor-Globus	0.9.7	Client API			
saga-adaptor-SSH	0.9.0	Client API			
saga-adaptor-BES	0.9.0	Client API			
saga-adaptor-gLite	0.9.0	Client API			
saga-adaptor-sqladvert	0.5.0	Client API			
saga-bindings-python	0.9.5	Client API			

Note AM: this section seems not to specify *when* these first versions are being delivered?

8.2 Security Capabilities

Note AM: SAGA does not have any specific security components.

The following table outlines all software component that implement security capabilities described in the UMD Roadmap the Provider wishes to release to EGI under the auspices of this Agreement.

Instead of appointing individual contacts for issues concerning the delivered components the Provider wishes to appoint the following contacts for respective issues: <<Delete if not applicable>>

Management contact: Full Name <<Delete if no overall management contact is appointed>>
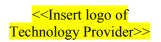   E-Mail
                        Mobile

Technical contact: Full Name <<Delete if no overall management contact is appointed>>
                        E-Mail
                        Mobile

Security contact: Full Name <<Delete if no overall management contact is appointed>>

E-Mail

Mobile

Name	First version delivered	UMD Capability	Technical Contact	Security Contact	Management Contact
Component name	1.0	One functional capability from UMD Roadmap	Full Name E-Mail Mobile	Full Name E-Mail Mobile	Full Name E-Mail Mobile

8.3 Operational Capabilities

Note AM: I don't think that SAGA, as a client API, falls into this category?

The following table outlines all software component that implement operational capabilities described in the UMD Roadmap the Provider wishes to release to EGI under the auspices of this Agreement.

Instead of appointing individual contacts for issues concerning the delivered components the Provider wishes to appoint the following contacts for respective issues: <<Delete if not applicable>>

Management contact: Full Name <<Delete if no overall management contact is appointed>>
                       E-Mail
                       Mobile

Technical contact: Full Name <<Delete if no overall management contact is appointed>>
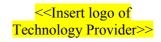   E-Mail
                       Mobile

Security contact: Full Name <<Delete if no overall management contact is appointed>>
                       E-Mail
                       Mobile

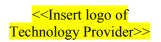| Name	First version delivered	UMD Capability	Technical Contact	Security Contact	Management Contact
Component name	1.0	One functional capability from UMD Roadmap	Full Name E-Mail Mobile	Full Name E-Mail Mobile	Full Name E-Mail Mobile

9 REFERENCES

The following table lists all references made throughout the Agreement. EGI agrees to make available to the Provider copies of any referenced document listed herein.

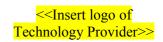| R 1	EGI-InSPIRE Description of Work, Part A, WT3, Work package 5 https://documents.egi.eu/document/10
R 2	EGI Technology Roadmap To be published
R 3	D1.1 UMD Roadmap: https://documents.egi.eu/document/100
R 4	Technology Coordination Board Terms of Reference https://documents.egi.eu/document/109
R 5	MS405: Incident Response Procedure & The software vulnerability issue handling process: https://documents.egi.eu/document/47
R 6	MS502: DMSU Operations Procedures https://documents.egi.eu/document/69
R 7	MS503: Software Provisioning Process https://documents.egi.eu/document/68
R 8	MS504: EGI Software Repository Architecture and Plans https://documents.egi.eu/document/89
R 9	Security Vulnerability Group Terms of Reference https://documents.egi.eu/document/108

n

Service Level Agreement between EGI-InSPIRE and Short Name

IN WITNESS WHEREOF, the Parties have caused their duly authorised representatives to sign two originals of this Service Level Agreement, in the English language.

The following agree to the terms and conditions of this SLA:

_____

Dr. Steven Newhouse
Director, EGI-InSPIRE

_____

Name of representative equivalent function, Short Name

_____

Date

_____

Date

10 APPENDIX A:

The SAGA project defines the following procedure for packaging and delivering software components to be delivered to EGI under the SLA defined in this document. This appendix is informative only, and not part of the SLA.

1. The source code for the provided software components is maintained in a publicly accessible code repository, under the administration and supervision of the Provider - additional external software components from other code repositories may only be included into the Providers set of deliverables if agreed by both the Provider and EGI.

2. The Provider will utilize EMI's ETICS infrastructure to
   - pull the code from the code repositories,
   - package the source distributions,
   - package the binary distributions, and
   - run integration tests to ensure the distributions fit into the EGI / UMD software stack.

3. The granularity of packages for each component it determined by the Provider, and may change between releases.

4. The Provider is able to deliver package types supported by ETICS, but no others.

5. If the software passes the EMI / ETICS integration tests, the Provider assumes the software is fit for release on the EGI infrastructure. Additional integration tests and software dependency resolutions need to be agreed upon mutually (this only affects deployment and integration tests - but does not affect software specific unit tests.).

6. EGI, and in particular UMD, will be able to pull the Provider's software deliverables from EMI's package repository (maintained via ETICS). That process will count as deliverance of the Provider's software components to EGI.

7. The Provider's performance will depend on the cooperation of the EMI project, which operates ETICS. Disruption of that cooperation, and technical problems with ETICS, may delay the deliverance of the software components. If either the Provider or EGI are unsatisfied by the packaging and delivery procedure defined above, an alternative procedure will be jointly defined.