

**EGI-Engage**

Platforms for the long tail of science

D5.2

|  |  |
| --- | --- |
| **Date** | 09 February 2016 |
| **Activity** | SA1 |
| **Lead Partner** | EGI.eu |
| **Document Status** | DRAFT |
| **Document Link** | https://documents.egi.eu/document/2671 |

Abstract

**COPYRIGHT NOTICE**



This work by Parties of the EGI-Engage Consortium is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). The EGI-Engage project is co-funded by the European Union Horizon 2020 programme under grant number 654142.

**DELIVERY SLIP**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***Name*** | ***Partner/Activity*** | ***Date*** |
| **From:** |  |  |  |
| **Moderated by:** |  |  |  |
| **Reviewed by** |  |  |  |
| **Approved by:** |  |  |  |

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author/Partner*** |
| **v.1** |  |  |  |
| **...** |  |  |  |
| **...** |  |  |  |
| **v.n** |  |  |  |

**TERMINOLOGY**

A complete project glossary is provided at the following page: <http://www.egi.eu/about/glossary/>

**Contents**

1 Introduction 5

2 Architecture of the Long Tail of science Platform 6

3 Operational processes and business model 7

3.1 User validation 7

3.2 Business model 7

3.3 Integration of new services in the platform 7

4 Services integrated or evaluated for integration 8

4.1 Catania science gateway 8

4.2 8

4.3 Security risks assessment 8

5 Assessment of the requirements of the long tail of science users 9

5.1 Services for data management 9

5.2 Computing services 9

5.3 Discipline specific services 9

5.4 Roadmap for the integration 9

6 Figures and captions 10

Appendix I. Appendix example 11

**Executive summary**

# Introduction

EGI identifies as Long Tail of Science (LTOS) users as the individual researchers and small laboratories who - opposed to large, expensive collaborations - do not have access to computational resources and online services to manage and analyse large amount of data.

The users of the LTOS generally are not interested in long-term and continuative collaboration with EGI, but more in a spot usage of the EGI resources, to accommodate bursts of computing capacity requirements.

Processes are well established for several years in EGI to allocate resources for user communities, in particular well established and organized collaborations. However individual researchers and small research teams perceive some barriers accessing grid and cloud compute and storage resources from the network of NGIs. Examples of these barriers are:

* Obtain an IGTF personal certificate
* Set-up a virtual organization or join an existing one
* Have the VO enabled in the resources, and use resources

Although EGI has processes and solutions to overcome these barriers, to some users the overhead associated is enough to discourage users and make them look for alternatives. Users who need to user computing resources for few weeks want to get access to resources in an order of days, to cope with their deadlines.

Recognising the need for simpler and more harmonised access for users of the LTOS, the EGI community started to designed a prototype for a new platform to support these users and to reduce, if not eliminate, the barriers above. The platform main features are:

* Allow users registered with username/password to access EGI resources
* Use a catch-all VO
* Aggregate an initial pool of resources already configured to support the LTOS VO.

This EGI platform allows individual researchers and small research teams to perform compute and data-intensive simulations on large, distributed networks of computers in a user friendly way.

The platform, besides the technical services, aims at creating communication channels between EGI and the NGIs who have already implemented processes and services for the LTOS users, and who could better support their national users. Through the platforms users will be able to get in contact with the user support of their NGIs, in case their use case could be better supported locally.

This document provides an overview of the architecture of the LTOS platform, which are the components and how they interconnect between each others, the processes that support the workflows and how its modular nature can evolve to expand the services offered to the users.

In summary the LTOS platforms is designed to be an almost zero barriers access to the EGI services.

# Architecture of the Long Tail of science Platform

The LTOS platform is composed by the following main technical components, as shown in Figure 1:

* A user registration portal (access.egi.eu)
* A catch-all VO
* A pool of resources where the catch-all VO is pre-enabled
* A set of science gateways and portal
* A X509 credentials factory

**

Figure , high level architecture of the LTOS platform

The **user registration portal** is composed by a website (access.egi.eu) which allows users to authenticate using either social credentials or EGI SSO IdP[[1]](#footnote-1), providing information about their contacts, institutions, and research topic. The website is the initial human interface for both the end users and the support team who will approve and manage the user registrations and request.

The user registration portal has also an interface for the services, such as the science gateways, in the form of an identity provider (IdP) which is used by the science gateways to get user authorization data and attributes. While the user interface has been developed ad-hoc, the IdP interface is using Unity[[2]](#footnote-2), a pre-existing authentication and authorization management solution using OpenID Connect as standard interface.

The **catch-all VO** is a Virtual Organization (called vo.access.egi.eu) that is used to collect the activities performed by the LTOS users. This VO can be used only by users owning credentials authorized by the LTOS platform.

The **pre-allocated pool of resources** is a number of EGI sites, both cloud and HTC, that accepted to enable the vo.access.egi.eu VO in their resources. The services in these sites are configured to recognize the X509 per-user sub-proxies, and handle these credentials according to the LTOS procedures and policies.

The **science gateways** (SG) are user interfaces, usually web portals, which provide a set of tools for the user to have an easy access to the EGI services. Command-line access to HTC or cloud resources may be too complicated to new users, SGs provide a user friendly interface to work with the pool of resources devoted to the LTOS VO.

Science gateways must be integrated with the LTOS platform, specifically to consume authorization information form access.egi.eu and to implement the use of the per-user sub proxies through the credential factory. These developments have proven to be not heavy developments for a SG portals.

The **X509 credentials factory** is a service which is directly contacted by the science gateways to get a per-user-sub-proxy from a robot certificate. Only the science gateways integrated in the LTOS platform can ask for robot certificate proxies through this service, and only if the user accessing the SG is authorized in the LTOS platform. The purpose of a per-user sub-proxy (PUSP) is to allow identification of the individual users that operate using a common robot certificate. This is achieved by creating a proxy credential from the robot credential with the proxy certificate containing user-identifying information in its additional proxy CN field. The user-identifying information may be anonymised where only the portal knows the actual mapping.

The interaction between the components is described in Figure 2, the steps represented are the following:

1. User registers in the access.egi.eu portal, a user ID is associated to the user and kept in the user database of the portal
2. The user, once approved, can log into the SG, to access EGI resources
3. The SG confirms that the user is authorized with the IdP provided by the access.egi.eu portal and retrieves the UID of the user.
4. The SG generated a PUSP from the credential factory (not in the picture), including the UID information in the sub-proxy, and use it to submit the payloads of the users to HTC or cloud resources in the LTOS pool.

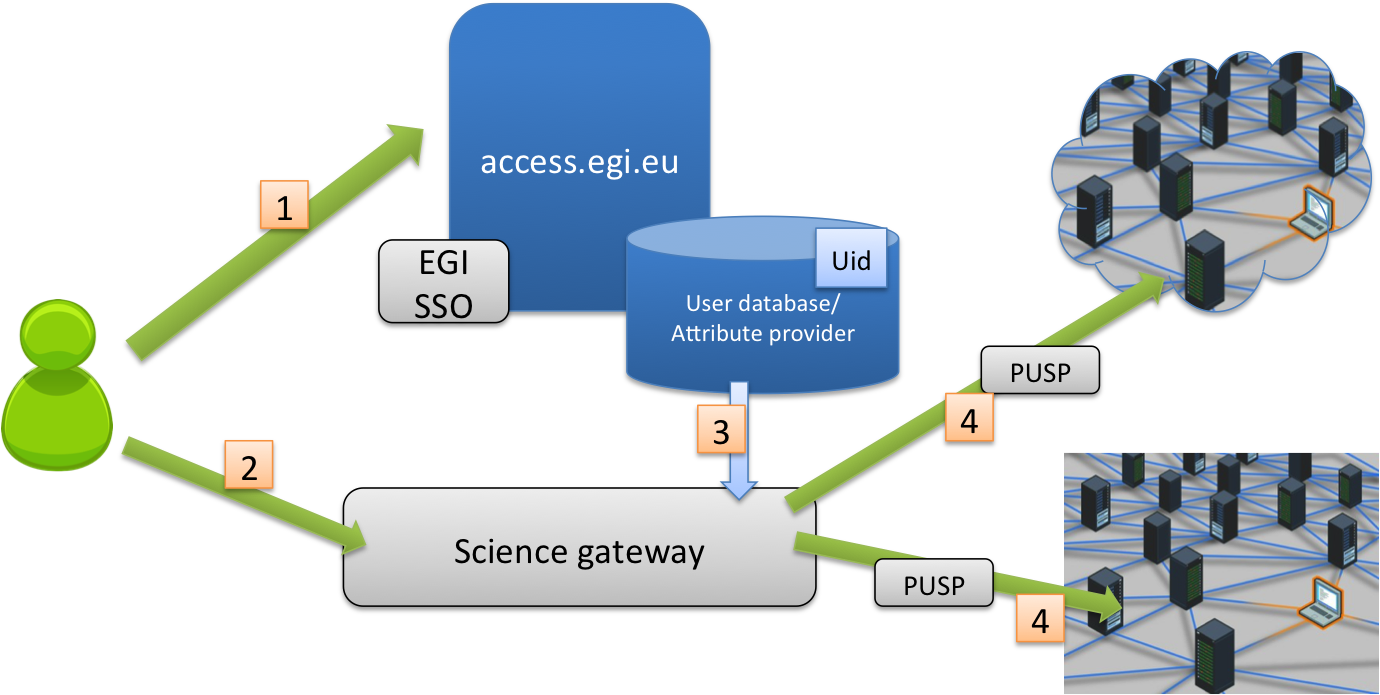


Figure , Interactions between the components of the LTOS

The advantages of the centralised user management are multiple, for example:

* EGI can have control on the users’ activities from a unique entry point
  + Users are associated to a persistent unique identifier which is used in all the services accessed through the platform
  + Users can be quickly suspended in case of a security issue
* Science Gateways do not have to keep a users database or manage authorization, since these information are hosted centrally

# Operational processes and business model

This section analyses the policies and processed that have been developed to support the LTOS, providing an overview of the non-technical components of the platform.

## User validation and user management

New users register in the user management portal (access.egi.eu), as described in the previous sections, providing information about their institution, referee and topic of the research for which they would like to use EGI resources.

New users registration required validation, and this is a manual process that must be performed by either the EGI user support team, in collaboration with the NGI user support representatives. The process of validation filters out users who are not eligible of using the EGI services, and provides an additional level of assurance to the service providers who enable the LTOS VO trusting EGI in authorizing the right users.

The process for validating a user must be limited to the essential steps to reduce any additional overhead and therefore the resources requested to handle the LTOS community. The necessary checks to be implemented are:

* The user is affiliated to a research institution, or is collaborating with someone affiliated to a research institution.
* The user has no other active accounts in the LTOS platform.
* The topic of the research that will use the EGI resources is relevant.

The checks that the user support team member will verify are the following:

1. Is the institution reported by the user a research institution, or another legal entity with research purposes?
   1. If not, the request will be rejected.
2. Has a user with the same name, or with the same email another account on the LTOS platform?
   1. In case the users already has another account the new one will not be approved.
3. Has the user registered with an institutional email, and/or has the user provided the link to a contact page on the website of their institution containing the user’s contacts?
   1. Using an institutional email, verified during the registration process, and reported on the contacts page is usually enough to provide the minimum level of assurance to access the LTOS platform. To confirm this requirements, user supporters can call on the phone the requester is they have a work phone number that is available on their institution website.
4. If the user suggests a referee in a research institution, this reference must be checked by phone.
5. Has the user previously used the LTOS, has they properly acknowledged EGI and reported results to be associated to their use of EGI services (e.g. publications)?
   1. User must provide an explanation for not following this policy, before being approved again.
6. Is the research topic relevant?
   1. This step is not a review of the quality of the research, but only checks that the resources devoted to the user will be used for research and non for profit goals.

Although not fully implemented, the LTOS platform is implementing some simple mechanisms for filtering notifications of new registrations, so the NGI representatives can subscribe receive notifications about users coming from their NGI, and either approve the access to the EGI platform, or redirect the user to the services provided by their NGI.

The future integration with eduGAIN will streamline the authorization process, since through an eduGAIN federation users can be easily associated to the research and education area, and the main information, for example the institution, can be validated directly by the Identity Provider. After a initial test/pilot period eduGAIN users could be automatically approved.

Once the user has been approved they can access EGI resources, as long as the approved status does not change. Currently the reasons for which a user can be suspended are:

* The user has used the maximum amount of resources allocated to LTOS users
  + Temporary suspension in order to understand if the allocation of more resources is enough or if the user would benefit by joining a VO. EGI has different mechanisms to grant resources for use cases where larger capacity is involved.
* The user has been approved 12 or more months ago
  + Temporary suspension in order to confirm the validity of the data reported by the users 12 months ago.
* The user behaviour does not comply with the EGI policies
  + Depending on the severity of the non-conformity suspension can be permanent.

## Security policy and AUP

The deployment of the LTOS platform required policy work to support the technical solutions. The existing EGI VO portal policy[[3]](#footnote-3) limits science gateways in the actions that can be performed on behalf of the user with a robot certificate.

A **LTOS security policy** has been developed as part of the activities of the project to define what services integrated with the LTOS are allowed to do on behalf of the user, and what the EGI requirements are. The policy also describes the risk envelope of the LTOS platform, and it suggests what mitigations the resource providers should implement.

The main points in the security policy are:

1. User access should be subject to explicit approval.
2. User affiliation must be verified at the moment of the approval, and verified every 13 months
3. User information must be kept in the platform for at least 13 months after the user’s last access
4. The resource providers shall accept the risks introduced by supporting the LTOS users, and shall protect the rest of the infrastructure by that additional risk

The security policy also suggests a list of implementation guidelines for the resource providers, to be compliant with the policy and minimize any risk associated to the LTOS to an acceptable level.

The security policy allows users of the LTOS to access a set of features that are similar to the capabilities offered to users owning a personal certificate, for example submitting arbitrary binaries. The verification of the user identity, although acceptable, is not as strong as it is performed by a certification authority who releases certificates. This introduces the additional risk that is evaluated in the policy and that should be mitigated throught he implementation recommendation.

The second policy document produced to support the LTOS activities is the **Acceptable Use Policy and Conditions of Use of the EGI Platform for the Long-tail of Science**. It is an expansion of the general AUP for the EGI users, which implements the specifics requirements and limitations of the platforms from a user’s perspective. Every user is required to accept the AUP during registration in the portal.

The main points in the LTOS VO AUP are:

1. The user is authorized to use the EGI resources through the LTOS platform only for the purposes described during the registration.
2. Access is suspended after the usage of resources exceeded the assigned allocation (the same for every user), or the time limits.
3. User must provide appropriate acknowledgement of the EGI support in the outputs of their work
4. Contact information must be kept up-to-date in the access.egi.eu portal
5. The LTOS platform, and the resource providers, are allowed to track user’s activities to be kept confidential and used only for operational and security purposes
6. User accepts the risk that their access to the LTOS platform can be suspended and is provided without any guarantee

Both policies have been approved by the EGI bodies and are in production.

## Business model

**Zero barrier access**

The first use case of the platform is to support the users, in this sense LTOS platform is an easy zero-barrier access gate to EGI general purpose services. EGI now has a scalable process to use with the individual users, who can begin use EGI resources with a minimum effort and minimum bureaucracy. The platform should contain, in the future evolution, all the documentation/tools and resources to support very small collaborations who do not need specific software of complex platforms but who can benefit from compute/storage or cloud in their daily work, and – possibly – from more higher level tools that can be used out-of-the-box without need for specific user-level customisations.

For NGIs who do not have existing processes to support their LTOS users, enabling the LTOS platform would be as easy as enabling a new VO in their resources, and redirect their users on the EGI LTOS platform.

**Enabling access to existing tools**

Existing services provided by the NGIs or by the Virtual Organizations can benefit from the LTOS as well. In case of a service that needs to be open and easy to access, for example to provide access to open data, the service provider can delegate user management to EGI and to the LTOS platform, since it is already providing the features that would need to be implemented by the existing tool.

In particular platforms or Virtual research environment that are using the EGI resources to run users’ tasks would highly benefit from the out of the box provision of X.509 credentials already enabled with the PUSP and a pre-allocated pool of resources.

VOs or communities who are developing tools for a specific research discipline, which can though be used independently by individual users without the original community, may want to make the tool available to as many users as possible, to increase the use base of their software. Integrating it with the LTOS, will both achieve the results of creating a short-cut for new users to join, and advertise the tool in the LTOS platform portal.

**Integration with the EGI Marketplace**

LTOS is gateway for new users approaching the EGI infrastructure, an access mode to EGI services, though it is not a service by itself. The integration with the marketplace under development can be done by adding a LTOS “flavour” to the services advertised. For example:

* HTC computing
  + VO Access
  + LTOS Acces
* Cloud computing
  + VO Access
  + LTOS access

Where "VO access” means the traditional access mode with dedicated agreements between resource providers and the VO. The LTOS flavour can be associated to other types of services on top of HTC and Cloud, as described in the other sections of the documents, as long as they can be technically integrated as described in section 3.4. LTOS access could be also used as a “trial version” of the service, which can subsequently evolve in a continuous collaboration (e.g. through an SLA) based on the user’s needs.

## Integration of new services in the platform

As described in previous sections the LTOS platform has developed a user registration and management process, and associated a pre-allocated pool of resources. The link between the users and the resources are the science gateways or other services that can help users in easily use the resources.

The requirements for the platforms and the services (called SG for simplicity) are the following:

* The SG must authenticate the users through the LTOS platform, using access.egi.eu
* The SG must allow the users to act on the EGI resources only if they are authorized in the access.egi.eu portal
* SG must use the UID provided by access.egi.eu to log user activity
* If X.509 credentials are required for some actions or to access other services, the SG must use robot certificates and per-user sub-proxies. The PUSP must contain the UID provided by access.egi.eu

To fulfil these requirements the development work for a SG is relatively limited.

* The SG should implement OpenID Connect authentication, since the unity service releases user information through the OIDC interface. Many portal framework already have OIDC plugins that can be used out of the box.
* The SG should retrieve the X.509 credentials from the credential factory. This can be done as easily as with a HTTP call through a REST interface. Credential factory (token service) can provide robot certificate proxies already in the PUSP format (UID is provided by the SG in the REST call), and already with the VO extensions for the LTOS VO.

The steps required for the integration on the LTOS side are very simple as well:

* Authorize the SG to retrieve authentication and authorization information from access.egi.eu
* Add a link of the list of SG in the pages of access.egi.eu

The integration process is tracked in a helpdesk ticket[[4]](#footnote-4) by the Operations support unit. Before the technical implementation, the operations and the user support team evaluate the new SG in terms of maturity and effectiveness to support LTOS users.

# Services integrated or evaluated for integration

At the moment of writing only the Catania science gateway has been fully integrated with the EGI LTOS platform, but other services are undergoing the integration and will be integrated in the coming weeks.

## Catania science gateway

The Catania Science Gateway Framework (CSGF) has been developed by INFN-Catania, to provide application developers with a tool to create Science Gateways (SGs) in short time and in a very easy way. CSGF is made of a set of libraries to manage Authentication & Authorization mechanisms and to interact with several different kinds of DCIs (grid, cloud, HPC, local, etc.). The CSGF is based on well established and widely adopted standards, such as SAGA, SAML, OCCI, JSR 286, etc. and it is fully compliant with both the EGI.eu VO Portal and User Traceability policies.

The CSGF allows users to execute applications on the EGI Federated Cloud and HTC resources, through web portals/SGs. The Science Gateways based on CSGF provide users with intuitive web interface to execute applications on the Cloud as jobs and to manage these jobs during their running (check the status and download the output). The SGs takes care of starting the VMs on the EGI Federated Cloud, transfer the needed files (e.g. executable, input files, etc.), stop the VMs and download the output in behalf of the user.

The LTOS users can exploit the CSGF features to:

* Execute applications already integrated in one of the existing Science Gateways
* Add their applications in one of the existing Science Gateways
* Deploy a new Science Gateway

## Services under integration

The following science gateways are in the pipeline for the integration with the LTOS:

**WS-PGRADE[[5]](#footnote-5)**

WS-PGRADE is an open source science gateway framework that enables users to access grid and cloud infrastructures. gUSE is developed by the Laboratory of Parallel and Distributed Systems (LPDS) at Institute for Computer Science and Control (SZTAKI) of the Hungarian Academy of Sciences.

WS-PGRADE is a Web portal hosted in a standard portal framework, using the client APIs of gUSE services to turn user requests into sequences of gUSE specific Web service calls. A graph editor component can be downloaded from WS-PGRADE and can be used to define the static skeleton of workflows, while the HTML pages of WS-PGRADE provide interfaces to add content to graphs, to generate complete Grid/Web service applications. The members of gUSE community can access WS-PGRADE via ordinary web browsers. Application developers can access to all the advanced workflow features (graph, abstract workflow, template, application and project) to develop new workflow applications and upload them to the gUSE repository. For scientific end-users WS-PGRADE gives full access to the parameterization and execution of applications downloaded from the gUSE repository.

WS-PGRADE is in a very advanced status of integration, at the moment of writing.

**QCG[[6]](#footnote-6)**

The QCG middleware is an integrated system offering advanced job and resource management capabilities to deliver to end-users supercomputer-like performance and structure. By connecting many distributed computing resources together, QCG offers highly efficient mapping, execution and monitoring capabilities for variety of applications, such as parameter sweep, workflows, MPI or hybrid MPI-OpenMP. Thanks to QCG, large-scale applications, multi-scale or complex computing models written in Fortran, C, C++ or Java can be automatically distributed over a network of computing resources with guaranteed QoS. The middleware provides also a set of unique features, such as advance reservation and co-allocation of distributed computing resources.

The integration of QCG has started.

# Assessment of the requirements of the long tail of science users

The evolution of the LTOS platform need to implement enough SGs to get a critical mass of functionalities and tools to be attractive to the users, and start to grow.

Identify the services that would be needed by potential users of the LTOS is one of the major challenges of this activity. LTOS users are – by definition – very diverse, and not being organized in communities is also very difficult to identify interlocutors to gather requirements. In other words, a survey could have been easily prepared, but we would not have known to whom it should have been submitted.

The chosen approach has been to prepare the questionnaires addressing the service providers in EGI, the NGIs, not addressing directly the users, but gathering indirectly the users’ requirements from the services providers who have been supporting the LTOS users for years.

The questionnaire was very short, three questions questions asking which services the NGI considers important to be provided to the LTOS users, or which services have been most popular among their LTOS users, general purpose or discipline specific. It has been circulated through the NGI user support (NIL) and Operations contacts.

Some NGIs, who have been more active in the past in structuring the support for the LTOS in their countries, have been addressed directly to discuss more in details their experience.

The following sub-sections summarize the information that we could gather in this process about the users’ expectations.

## Services for data management

## Computing services

## Discipline specific services

Although supporting

## Roadmap for the integration

1. EGI SSO identity provider: https://www.egi.eu/sso/ [↑](#footnote-ref-1)
2. http://www.unity-idm.eu/ [↑](#footnote-ref-2)
3. <https://documents.egi.eu/document/80> [↑](#footnote-ref-3)
4. helpdesk.egi.eu [↑](#footnote-ref-4)
5. http://guse.hu/about/architecture/ws-pgrade [↑](#footnote-ref-5)
6. http://www.qoscosgrid.org/trac/qcg [↑](#footnote-ref-6)