EGI-InSPIRE

SECURITY ACTIVITY WITHIN EGI

EU MILESTONE: MS224

Document identifier:	EGI-MS224-965-V3.doc
Date:	**06/03/2012**
Activity:	**NA2**
Lead Partner:	**EGI.eu**
Document Status:	**FINAL**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/965

Abstract

This milestone provides an overview of the non-operational security activities from the SPG, SVG and SCG including EGI's participation in the IGTF and EUGridPMA. EGI security activities in the reporting period of EGI-InSPIRE project (Feb 2011- Jan 2012) were successfully performed and EGI has confirmed its role as a leading force in International security policy bodies (e.g. EUGridPMA, IGTF) whereby EGI representatives were a key factor in developing new standards, policies and guidance.

I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	Damir Marinovic Linda Cornwall David Kelsey David Groep	EGI.eu / NA2 STFC / NA2 STFC / NA2 NIKHEF / NA2	08/02/2012
Reviewed by	Moderator: David O'Callaghan Reviewers: Jan Meizner	TCD ACC Cyfronet AGH	23/02/2012
Approved by	**AMB & PMB**		29/02/2012

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	13/01/2012	ToC	Damir Marinovic / EGI.eu
2	08/02/2012	First draft	Damir Marinovic / EGI.eu Linda Cornwall / STFC David Groep / NIKHEF David Kelsey/ STFC
3	24/02/2011	Final Draft	Damir Marinovic / EGI.eu Linda Cornwall / STFC David Groep / NIKHEF David Kelsey/ STFC
4	27/02/2012	Last version after reviews	Damir MArinovic et al

IV. APPLICATION AREA

This document is a formal deliverable for the European Commission, applicable to all members of the EGI-InSPIRE project, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the authors. The procedures documented in the EGI-InSPIRE "Document Management Procedure" will be followed:
https://wiki.egi.eu/wiki/Procedures

VI. TERMINOLOGY

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

VII. PROJECT SUMMARY

To support science and innovation, a lasting operational model for e-Science is needed − both for coordinating the infrastructure and for delivering integrated services that cross national borders.

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 user communities within the European Research Area.

EGI-InSPIRE will collect user requirements and provide support for the current and potential new user communities, for example within the ESFRI projects. Additional support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The objectives of the project are:

1. The continued operation and expansion of today's production infrastructure by transitioning to a governance model and operational infrastructure that can be increasingly sustained outside of specific project funding.
2. The continued support of researchers within Europe and their international collaborators that are using the current production infrastructure.
3. The support for current heavy users of the infrastructure in earth science, astronomy and astrophysics, fusion, computational chemistry and materials science technology, life sciences and high energy physics as they move to sustainable support models for their own communities.
4. Interfaces that expand access to new user communities including new potential heavy users of the infrastructure from the ESFRI projects.
5. Mechanisms to integrate existing infrastructure providers in Europe and around the world into the production infrastructure, so as to provide transparent access to all authorised users.
6. Establish processes and procedures to allow the integration of new DCI technologies (e.g. clouds, volunteer desktop grids) and heterogeneous resources (e.g. HTC and HPC) into a seamless production infrastructure as they mature and demonstrate value to the EGI community.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI-InSPIRE, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities (VRCs) − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

VIII. EXECUTIVE SUMMARY

The purpose of this document is to describe non-operational security activities within the EGI. The milestone includes reports from the EGI Security Policy groups - Security Coordination Group (SCG), Security Policy Group (SPG) and Software Vulnerability Group (SVG). In addition, the milestone includes report from EGI's representative in the International Grid Trust Federation (IGTF) and European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA).

The main focus during the reporting period was to ensure that EGI security activities and process were properly performed and followed. After the first transitional year, productivity rose during the second year of the EGI-InSPIRE project.

EGI security activities in the second year of the EGI-InSPIRE project were successfully performed and EGI has confirmed its role as leading force in International security policy bodies (e.g. EUGridPMA, IGTF) where EGI representatives were a key factor in developing new policy standards, policies and guidance.

To sum it up, some of the major achievements during the reporting period were:

- A common position was defined on interactions and relationships with other projects and organisations on a number of security issues.
- A number of policies and procedures were drafted, reviewed and put into effect (e.g. Service Operations Security Policy, the Security Policy for the Endorsement and Operations of Virtual Machine Images and Critical vulnerability operational procedure).
- Security Risk Assessment of the EGI infrastructure was developed.
- EGI leading role in a number of IGTF and EUGridPMA, OGF, TAGPMA meetings lead to development of new standards, policy and guidelines.
- 31 new vulnerabilities have been entered into the EGI report vulnerability tracker.

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to describe non-operational security activities within the EGI. The milestone includes reports from the EGI Security Policy groups - Security Coordination Group (SCG), Security Policy Group (SPG) and Software Vulnerability Group (SVG). In addition, the milestone includes report from EGI's representative in the International Grid Trust Federation (IGTF) [R1] and European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA) [R2].

The milestone is describing security activities within EGI from February 2011 to January 2012. Hence, the milestone mostly covers the second year of the EGI-InSPIRE project. The first year of EGI security activities was the year of transition, moving from the EGEE project to a more permanent foundation based on a new project – EGI-InSPIRE and a new organisation – EGI.eu. This transitional year was described in MS214 Security Activity within EGI [R3]. The EGI security groups dealt well with transition issues in the first year and routine security activities and plans were performed in second year without any major obstacles or bottlenecks. Therefore, this milestone is describing the regular security activities in the already established security environment.

Out of ten EGI.eu policy groups, four EGI.eu groups deal with EGI security activities. This fact shows just how important security is within EGI. All security groups have separate web pages on the EGI website [R4] and separate wiki pages [R5].

The target group for this milestone should primarily consist of the people interested in EGI security activities, partners of the EGI-InSPIRE project especially NGI security officers, Operation and Technology EGI officers and all those involved in delivering Europe-wide Distributed Computing Infrastructures (DCIs).

The milestone is organised as follows: Section 2 provides reports from different EGI security groups including report of EGI Representative at IGTF and EUGridPMA. Section 3 sums up the EGI security activities with concluding remarks and provides a table that highlights the major EGI security achievements.

2 REPORTS ON NON-OPERATIONAL SECURITY ACTIVITY

2.1 Security Coordination Group (SCG)

In the "Purpose and Responsibilities" section of the SCG Terms of Reference it is stated that: "*The SCG brings together representatives of the various security functions within the EGI to ensure that there is coordination between the operational security, the security policy governing the use of the production infrastructure and the technology providers whose software is used within the production infrastructure. The group provides:*

- *Information exchange between the various security groups*
- *A coordinated response and planning to EGI on security issues*" [R6]

In the related reporting period, four SCG meetings were held in February, August, October 2011 and January 2012. Regular meetings ensured continuous formal communication between the Chairs of security groups (SCG, SPG, SVG and CSIRT) together with the EGI Representative in IGTF and EUGridPMA. For the most of the meetings the EGI.eu Technical Manager, Technology Provider representatives, EGI.eu Operations Manager, EGI.eu Operations Officer and EGI.eu Policy Development Officer were present. For each meeting Chairs of EGI security groups, including the EGI Representative in IGTF and EUGridPMA, were requested to submit the report informing other participants of the meetings about latest activities in their domain.

Participants of SCG meetings in general discussed ways to improve coordination and flow of information between different security groups, In addition, SCG participants coordinated work on activities that need a common approach and the SCG's role of coordination body. During the reporting period, topics of the SCG meetings were the following:

- Various security issues were discussed that needed a common understanding by all the participants.
- Defining common position and opinion on interaction and relationship with other projects and organisations on security issues and discussing possibility of potential MoUs (e.g. Grid Canada, WLCG).
- Discussing common EGI position for various meetings in which EGI representative were participating.
- Nominating lead author to set up a team to work on drafting and delivery of D4.4. Security Risk Assessment of the EGI infrastructure [R15] (SVG Chair Linda Cornwall) including discussing the scope of this deliverable.
- Identifying gaps and discussing the need for new EGI policies and procedures.
- Analysing EGI compliance with ISO 27000 standards in security field
- Discussing scope and timeline for work on risk assessment and risk register and evaluating different options in order to gather more people to join risk assessment exercise (e.g. through NGI International Liaisons).
- Discussing formal responses needed on security related issues identified in Project Year 1 (PY1) review report and participation of Chairs of EGI security groups in PY2 review.

2.2 Security Policy Group (SPG)

The Security Policy Group (SPG) is responsible for developing the policies needed to provide NGIs with a secure, trustworthy distributed computing infrastructure. The SPG output defines the behaviour expected from NGIs, Resource Centres, Users and other participants to maintain a beneficial and effective working environment. One of the aims of the SPG is to develop policies that could be applicable to e-infrastructures across the world in order to improve interoperability [R7].

The security policy documents maintained by SPG are all published in the EGI Document Database and the list of currently approved policies may be found on the SPG wiki page [R8].

In 2010 SPG was established and its membership, terms of reference and procedures were all agreed. The real work started following a first formal face-to-face meeting of the full SPG held at Nikhef on 11-13 January 2011. The SPG work plan for 2011 agreed during that meeting included work on the following policy areas:

- Revision of the Grid Site Operations Policy (to be called "Service Operations Security Policy")
    - To include general service operation security policy - real and virtual services, where "real" means services running directly on the hardware and "virtual" services are running on virtual machines.
    - Include Resource Providers, VO managers, Virtual Machine managers, etc.
    - To exclude operational (non-security) items more correctly covered elsewhere.
- Generalise the HEPiX Security Policy on the Endorsement of Virtual Machine Images to include other types of trustworthy Virtual Machines.
- Full revision of the old top-level Security Policy document.
- Policy work related to Data privacy issues
    - Phase 1: expand the job-level accounting policy to include storage accounting.

It was agreed that SPG should give priority to the work on the "Service Operations Security Policy" [R9] and the "Security Policy for the Endorsement and Operations of Virtual Machine Images" [R10]. These two documents completed the three phases of SPG policy development and were approved and adopted by the EGI.eu Executive Board. These both come into effect on 1st February 2012. Work on the revision of the old top-level Security Policy document and on Data privacy issues was started in the second half of the year and will be completed in 2012.

Regular SPG meetings were held during 2011 [R8]. These included face-to-face meetings of the group at the EGI User Forum in Vilnius (April 2011) and the EGI Technical Forum in Lyon (September 2011). Several video meetings of the whole group were held during the year, as well as meetings of the Editorial Teams doing the work on the two main policy documents. A general session was held at the EGI Technical Forum in Lyon (Sep 2011) where the work of SPG was presented to a general EGI audience. Security policy development activities were presented and useful feedback was received.

Other security policy activities of the SPG Chair (David Kelsey, STFC, UK) on behalf of SPG and EGI during the period included:

- Active participation in the International Grid Trust Federation representing EGI and WLCG as a Relying Party, including:
    - Lead author on the production of a new Guidelines document addressing Attribute Authority Service Provider Operations. This document (V1 was finalised in January 2012) [R11] presents best practice and minimum requirements for the operation of trustworthy Attribute Authorities (e.g. VOMS services).
    - Participation in the face to face IGTF All Hands meeting in Taipei (March 2011) the face to face meetings of EUGridPMA in Prague (May 2011) and in Ljubljana (January 2012), in a face to face meeting of TAGPMA (Oakridge, TN, October 2011) and regular video conferences of TAGPMA.
- Participation in security area activities at the Open Grid Forum (OGF) meetings in Taipei (March 2011) and Lyon (September 2011)

Leadership of the "Security for Collaborating Infrastructures" activity. This is a collaboration between EGI, WLCG, OSG (and formerly DEISA and TeraGrid) to build a security policy framework to enable interoperation of collaborating Grids with the following aims:

- To manage cross-Grid operational security risks.
- To build Trust and develop policy standards for collaboration.
- In cases where we cannot just share policy documents build a standard framework for security policy for interoperation.

This work made good progress during the year. Work was initially done by phone conference but it was agreed that we needed to hold a 2-day face to face meeting. This was held at the Fermi National Accelerator Laboratory, near Chicago, in October 2011, chaired by Kelsey. By the end of this meeting we had produced a good draft document. This will be taken forward in 2012, hopefully with another face to face meeting, held this time in Europe.

- Participation in a new activity on Federated Identity Management for Scientific Collaborations. A number of research communities, including European photon/neutron facilities, social science and humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, held two workshops (CERN in June 2011 and RAL in November 2011) with an agreed objective of defining a common policy and trust framework for Identity Management. Kelsey helped organise the events, participated in a panel and chaired a session.

Towards the end of 2011, WLCG started an activity considering the evolution of a range of its technical services, including security. Kelsey participated in an exercise to revise the WLCG security risk assessment and in 2012 will lead an activity considering plans for the possible use of federated identity management in WLCG.

2.3 Software Vulnerability Group (SVG)

The main purposes of the EGI Software Vulnerability Group (SVG) is to eliminate existing vulnerabilities from the deployed infrastructure, primarily from the Grid Middleware, prevent the introduction of new ones and prevent security incidents.

This is carried out in 3 main ways:

1. Handling reported software vulnerabilities (or potential vulnerabilities).
2. Assessing the quality of software for vulnerabilities, to pro-actively look for vulnerabilities.
3. Developer education, to help prevent new vulnerabilities from being introduced into the software [R12].

The first activity is the largest activity of the EGI SVG, and is often considered to be part of security operations. It is less "real time" than for example incident handling carried out by CSIRT, and it is carried out according to the agreed EGI Software Vulnerability Issue handling Process [R13]. This was updated after one year's experience of using it, and with the clarification of some details concerning wiki locations and contacts that were not clear at the start of EGI [R13]. The new version was approved in October 2011. Between February 2011 and January 2012, 31 new issues were entered into the EGI report vulnerability tracker, 13 of these were found to be due to vulnerabilities in the Grid Middleware affecting the production infrastructure. Many of the others were due to problems in other software installed on the production infrastructure or in some of the tools used by EGI, some of which were handled by CSIRT some by SVG.

During the last year SVG has provided an opinion on the risk of some vulnerabilities in software which is not middleware, and worked more closely with CSIRT to provide a consistent opinion on the risk, whether a vulnerability is in middleware or in (for example) versions of the Linux kernels used in EGI. A number of SVG advisories have been published for Torque, which is not counted as part of the middleware [R14]. Also, the SVG risk assessment team has been involved in assessing e.g. the CVE-2010-3847 vulnerability in glibc, and the CVE-2010-3904 vulnerability in the Linux kernel, plus other similar OS vulnerabilities.

SVG issued 12 advisories on vulnerabilities concerning Grid Middleware; some of these refer to vulnerabilities reported as above, some from prior to this date [R14].

Part of the second SVG activity is eliminating vulnerabilities in the EGI infrastructure via Vulnerability Assessment. This activity is being carried out by members of the University of Wisconsin / Universitat Autonoma de Barcelona Middleware security and Testing Group who have developed manual First Principles Vulnerability Assessment Techniques for assessing software for vulnerabilities. [R15] This is a very effort intensive activity. The effort to carry out this work is partly funded by the European Middleware Initiative (EMI) and the "Security assessment plan" was developed [R16] one year ago with prioritization of these assessments largely proposed by the EGI SVG to ensure the most security critical pieces of Grid middleware used in EGI are assessed. During the last year three pieces for software were assessed according to this plan. gLexec was re-assessed and only 'Low' risk vulnerabilities were found, ARGUS was assessed and no problems found, VOMS core was assessed and only one 'Low' risk vulnerability found.

An additional aspect to assessing software for vulnerabilities is software from Technology providers with which EGI has a relationship and whose software is recommended for deployment on the EGI infrastructure. The EGI SVG is looking at how the security of the software should be assessed in order to provide adequate assurance that it is of sufficient quality.

Developer training is now primarily carried out in EMI, who have organised tutorials for their developers, including a tutorial on secure programming at the EGI 2011 Technical Forum [R17].

Members of the SVG are also active in the preparation of D4.4 Security Risk Assessment of the EGI Infrastructure [R18] (the lead author being the EGI SVG chair), and the EGI Security Risk Assessment described in this document, which is just starting. This is a comprehensive risk assessment of the EGI infrastructure and project; it includes threats arising from various sources including social engineering as well as technical threats.

Most of the work and discussions within SVG are carried out by e-mail. Since May 2011 SVG have been having monthly EVO meetings, as planned, which have allowed productive discussion. SVG also had a face to face meeting at the EGI Technical Forum in September 2011, and work over the past year was presented at this event.

Usually, Critical vulnerabilities are due to software vulnerabilities but they may be due to other problems, such as configuration of sites. The EGI Critical Vulnerability Operational procedure, which is a brief document describing the procedure for dealing with Critical Security issues where action needs to be taken by a single site or multiple sites, was completed by the SVG chair, reviewed by the OMB, and approved by EGI.eu Director and EGI.eu Executive Board..

2.4 IGTF and EUGridPMA

EGI has a strong involvement in the coordination of identity management for e-Infrastructures. Through its participation in the European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA) and the International Grid Trust Federation (IGTF) it has helped shape the required assurance levels for identities used.

With the emergence of new use cases (large-scale provisioning of systems identities in data centres, increased use of portal technology for new research domains), the assurance levels evolve to support a more distributed and tiered authentication model. For example, portals authenticate users based on federated home institution credentials, and subsequently the portal uses a 'robot' certificates to authenticate itself to the infrastructure as a single automated client. Similarly, automated installation systems for data centres can act as trusted software agents in the procurement of credentials for system devices in large coordinated deployments. Based on the technical assurance levels defined for identity provider systems, a comparable policy and practice statement for technical controls on authorization services was developed in the EUGridPMA, as mentioned in SPG section.

An auditing process for the quality and integrity of the authentication operations has been in place for some time, with the result that by now most of the authorities have been reviewed at least once. The review period is once every two years, and the PMA has an escalation process in place for remediation of late self-audits.
This is especially important for relying parties such as EGI, since with the more wide-spread use of e-Infrastructure there are many more identity providers and trust can only be maintained through a documented, open, and auditable process.

A coordinated effort to identify software implementation obstacles relating to new standards in the authentication domain was conducted in 2011, which resulted in a coordinated set of requirements being submitted to the EGI technology providers. EGI was the key driving force in identifying and

coordinating these requirements within the IGTF, which will improve standards compliance and compatibility with the evolving standards in PKIX and in the cryptology domain.

In the context of this activity, the EGI–EUGridPMA liaison function attended three EUGridPMA plenary meetings, three IGTF coordination meetings with the other continental PMAs in the Americas and the Asia-Pacific, and the OGF meetings where – in the CAOPS working group – the structure documents and standardization takes place. Both policy and technical feedback from these events is given back to the relevant EGI bodies.

3 CONCLUSION

The main focus during the reporting period was to ensure that EGI security activities and processes are properly performed and followed. After the first transitional year, effectiveness of EGI security groups was improved during the second year of the EGI-InSPIRE project. As a consequence of improved effectiveness, there was an increase in the number of achievements. Major achievements are summed up and listed in Table 1.

Table 1

Group	Major achievements
SCG	• Defined common position and opinion on interaction and relationship with other projects and organisations on security issues. • Monitoring EGI compliance with ISO27000 standards in security field. • Identified gaps and discussed need for new EGI policies and procedures. • Nominated lead author for D4.4. Security Risk Assessment of the EGI infrastructure (SVG Chair Linda Cornwall) and setup of team that worked on drafting and delivery of this deliverable. • Discussed scope and timeline for work on risk assessment and risk register and evaluated different options in order to gather more people to join risk assessment exercise. • Discussed formal response on security related issues identified in Project Year 1 (PY1) review report and participation of Chairs of EGI security groups in PY2 review.
SPG	• Service Operations Security Policy and the Security Policy for the Endorsement and Operations of Virtual Machine Images were approved and came into effect. • Started revision of the top-level Security Policy document and on Data privacy – user level accounting policy. • Successful "public information " session at EGI Technical Forum in Lyon. • SPG Chair was lead author on the production of a new Guidelines document addressing Attribute Authority Service Provider Operations. • Participation at OGF and TAGPMA meetings. • Leadership of the "Security for Collaborating Infrastructures" activity that resulted in Security policy framework draft between EGI, WLCG, OSG, DEISA/PRACE, and TeraGrid/XSEDE. • Participation in a new activity on Federated Identity Management for Scientific Collaborations. • SPG Chair participated in an exercise to revise the WLCG security risk assessment.

Group	Major achievements
SVG	• 31 new vulnerabilities have been entered into the EGI report vulnerability tracker, 13 found to be vulnerabilities in the Grid Middleware. 12 advisories issued. The issue handling process generally working smoothly. • 3 gLite middleware items assessed in detail by EMI, only Low Risk vulnerabilities found. • Finalized Critical Vulnerability Operational Procedure. • Agreed SVG detailed work plan for 2011.
IGTF and EUGridPMA	• Participation in the three EUGridPMA plenary meetings, three IGTF coordination meetings with the other continental PMAs in the Americas and the Asia-Pacific and in the CAOPS working group. • Participation in development of EUGridPMA policy and practice statement for technical controls on authorization services. • An auditing process for the quality and integrity of the authentication operations is in place. • EGI representatives were the key driving force within the IGTF in identifying and coordinating requirements submitted to the EGI technology providers in order to identify software implementation obstacles related to new standards in the authentication domain.

To conclude, EGI security activities in the second year of EGI-InSPIRE project were successfully performed and EGI has confirmed its role as a leading force in international security policy bodies (e.g. EUGridPMA, IGTF) where EGI representatives were a key factor in developing new policy standards, policies and guidance.

4 REFERENCES

R 1	International Grid Trust Federation (IGTF) http://www.igtf.net/
R 2	European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA) http://www.eugridpma.org/
R 3	MS214 Security Activity within EGI https://documents.egi.eu/document/307
R 4	EGI.eu Policy Groups http://www.egi.eu/policy/groups
R 5	Main EGI Wiki Page https://wiki.egi.eu/wiki/Main_Page
R 6	Security Coordination Group - Terms of Reference https://documents.egi.eu/document/119
R 7	Security Policy Group - Terms of Reference. https://documents.egi.eu/document/64
R 8	SPG wiki page https://wiki.egi.eu/wiki/Security_Policy_Group
R 9	Service Operations Security Policy https://documents.egi.eu/document/669
R10	Security Policy for the Endorsement and Operations of Virtual Machine Images. https://documents.egi.eu/document/771
R11	Guidelines for Attribute Authority Service Provider Operation http://www.eugridpma.org/guidelines/aaops/EUGridPMA-AASP-Operations-20120117-v1-0.pdf
R12	Software Vulnerability Group (SVG) - Terms of Reference https://documents.egi.eu/document/108
R13	EGI Software Vulnerability Issue Handling Process https://documents.egi.eu/document/717
R14	SVG Advisories https://wiki.egi.eu/wiki/SVG:Advisories
R15	Vulnerability Assessment http://research.cs.wisc.edu/mist/includes/vuln.html
R16	Security Assessment plan https://documents.egi.eu/document/563
R17	Tutorial on Secure Programming https://www.egi.eu/indico/contributionDisplay.py?sessionId=57&contribId=75&confId=452
R18	D4.4 Security Risk Assessment of the EGI Infrastructure https://documents.egi.eu/document/863