EGI-InSPIRE

SECURITY ACTIVITY WITHIN EGI

EU MILESTONE: MS214

Document identifier:	EGI-MS214-307-V6.doc
Date:	**30/03/2011**
Activity:	**NA2**
Lead Partner:	**EGI.eu**
Document Status:	**FINAL**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/307

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. To conclude, transition from EGEE to EGI security framework was successfully completed while improving collaboration between EGI security groups. Involvement of EGI security representative in international security policy bodies was intensified, resulting in EGI taking a leading role in a number of actions including developing new policy standards and guidance.

I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	Damir Marinovic	EGI.eu / NA2	01/03/2011
Reviewed by	**Moderator:** Peter Solagna **Reviewers:** Tomasz Szepienec	EGI.eu SA1	 21/02/2011
Approved by	**AMB & PMB**		01/03/2011

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	27/01/2011	ToC	Damir Marinovic / EGI.eu
2	15/02/2011	First draft	Damir Marinovic / EGI.eu Linda Cornwall / STFC David Groep / NIKHEF David Kelsey/ STFC
3	19/02/2011	Second draft	Damir Marinovic / EGI.eu Steven Newhouse / EGI.eu
4	01/03/2011	Final Draft	Damir Marinovic

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 in within the EGI ecosystem. Hence, the document includes reports from the EGI Policy groups in the security field - Security Policy Group (SPG), Security Coordination Group (SCG) and Software Vulnerability Group (SVG). In addition, the milestone describes EGI's participation in the International Grid Trust Federation (IGTF) and European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA).

The basic motivation for writing the milestone is to examine activity over the last 9 months (starting from the beginning of the EGI-InSPIRE project) and to see what was done in security area in these formative months of the new EGI security model. During this period the groups were in transition from the EGEE security framework to the new EGI model (described in EGI-InSPIRE Description of Work), as part of EGI-InSPIRE project and the EGI.eu organisation. Thus, dedicated effort was required in order to ensure that transition of security activities and process ran smoothly and without interruption and obstacles. Some of the specific transition issue included clarification of the responsibilities of the groups by establishing and finalising Terms of References (ToRs), transition of security policy and procedures to a new format and adoption by EGI.eu Executive Board, the membership of the groups renewal, creation and populating new wiki pages for the all groups; furthermore, for some of the groups (e.g. SVG) moving to the EGI infrastructure included using the EGI RT to track issues. This also included establishing contact details, including who to contact in which situation, with the various software providers who supply software that will be included in EGI's Unified Middleware Distribution. Meetings of all these groups were held during this period.

Therefore, to sum up the major achievements:

- successful transition into the new EGI security framework
- the ToRs finalised and adopted for all EGI security groups
- a number of policies and procedures were developed, drafted and reviewed.
- during this period the groups defined work plan for 2011
- participation and shown leadership in a number of IGTF and EUGridPMA meetings

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to provide an overview of the non-operational security activities in EGI. The document includes report from Security Policy Group (SPG), Security Coordination Group (SCG) and Software Vulnerability Group (SVG). Furthermore, the document describes EGI's participation in International Grid Trust Federation (IGTF), and European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA).

The milestone is of descriptive nature and describe activities from the beginning of the EGI-InSPIRE project (May 2010) to the January 2011. Thus, the document will cover first nine month of the EGI-InSPIRE project.

Non-operational security activities are part of six EGI.eu's organisational functions: Technology, Operations, User Services, Administration and Policy. Thus, Security Policy Group and Security Coordination Group are part of the Policy organisational function [R11]. During first nine months the SCG, SPG and SVG were in transition, moving from the EGGE project to more permanent basis as a part of a new project – EGI-InSPIRE and a new organisation – EGI.eu. Thus, these months of transition required dedicated effort in order for transition to run smoothly. Therefore, this milestone describes how the EGI security groups dealt with this transition issues and whether regular security activities and plans went well, without any major obstacles and bottlenecks.

The target audience should primarily consist of the partners of EGI-InSPIRE project, and those involved in delivering European wide Distributed Computing Infrastructures.

The document is structured as follows: Section 2 provides reports from different security groups including information about participation in international security bodies; while Section 3 draws up conclusion and provides a synthetic view of the policy groups' activity within and outside the EGI.

2 REPORTS ON NON-OPERATIONAL SECURITY ACTIVITY

2.1 Security Coordination Group (SCG)

The SCG brings together representatives of the various security functions within and outside EGI, including Chairs of SPG, SVG, EGI.eu CSIRT and security representatives of technology providers (e.g. EMI representative). The purpose of the SCG is 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 [R5]

The first formal SCG meeting was held in December 2010 following informal communication between the different activities during the preceding months of the project. The chairs of all security groups were present together with the EGI Representative in EUGridPMA, EGI.eu Technical Manager and EGI.eu Policy Development Manager. Focus of the discussion was on the ways to improve coordination between different security groups and the decision was made to prepare a poster for the User Forum explaining the responsibilities for the various security policy groups within EGI. It was decided to have regular meetings on a monthly basis. These monthly meetings have continued continuing the coordination of the different activities.

2.2 Security Policy Group (SPG)

The purpose of SPG [R7] is as follows: *"The Security Policy Group is charged with developing and maintaining Security Policy for use by EGI and the NGIs. This EGI Security Policy defines the expected behaviour of NGIs, Sites, Users and other participants, required to facilitate the operation of a secure and trustworthy distributed computing infrastructure. SPG may also provide policy advice on any security matter related to the operation of the EGI infrastructure. SPG should, wherever possible, aim to prepare and maintain simple and general policies which are not only applicable to EGI/NGIs but that are also of use to other Grid infrastructures and DCIs in Europe and across the world. The adoption of common policies by multiple infrastructures eases the problems of interoperability"* [R3].

Each participant and associate participant of EGI.eu is entitled to nominate one voting member of SPG. In addition to the voting members, SPG should also aim to include expertise in its deliberations from other stakeholders, including site security officers, site system administrators, operational experts, middleware experts, VRCs and other DCIs.

Much of the activity of SPG during 2010 has been to define its Terms of Reference [R7] and to recruit members. An EGI-InSPIRE Milestone 209 [R4] was reached in October 2010 by defining the SPG procedures for developing new policies and for consulting the stakeholders so as to arrive at policies ready for approval by the EGI management bodies. The transition from the old EGEE/WLCG Joint Security Policy Group was completed. All the existing security policies inherited from EGEE-III have

been imported into standard EGI policy document templates and have been approved and adopted by the EGI Executive Board. The policy documents are all published in the EGI Document Database and the list of SPG policy documents with links you can find on a dedicated SPG wiki page [R10].

Several meetings of SPG have taken place during the period under consideration:

- A subset of the members of SPG met on 18-19 May 2010 at Nikhef to complete the security policy "Glossary of Terms" [R8] and to start work on the development of a standard security policy framework for possible future use in EGI.
- The members of SPG and the wider community were consulted during an SPG session at the EGI Technical Forum in Amsterdam (14-17 Sep 2010). The SPG Terms of Reference and proposals for SPG procedures were discussed. A draft work plan for SPG during the next year was also discussed and the general aims were agreed
- The first formal face-to-face meeting of the full SPG was held at Nikhef on 11-13 Jan 2011. The group (approximately 25 members were able to attend) discussed many important topics with the main aim of understanding which new security policies are needed and which of the current policies are most in need of revision. A work plan for 2011 was agreed including the creation of several editorial teams [R9].

The agreed SPG work plan for 2011 includes work on the following policy areas:

- Full revision of the old top-level Security Policy document.
- Policy related to Data privacy.
    - Phase 1: expand the job-level accounting policy to include storage accounting.
    - Phase 2: even more general data privacy policy and its relationship with the EU Digital Agenda.
- Revision of the Grid Site Operations Policy.
    - To include general service operation security policy (real and virtual services).
    - Include Resource Providers, Virtual Machine managers, etc.
    - This will now exclude operational (non-security) items to be considered by EGI-InSPIRE SA1 and the Operations Management Board (OMB).
- Generalise the HEPiX Security Policy on the Endorsement of Virtual Machine Images to include other types of trustworthy Virtual Machines.
- SPG Glossary (as a contribution to the more general EGI Glossary).

Other activities of the SPG Chair (David Kelsey, STFC, UK) during the period included:

- A presentation on "Federating the Grid" at the annual TERENA Networking Conference in Vilnius (2 June 2010).
- Participation in all security area activities at the OGF29 meeting in Chicago (20-22 June 2010).
- Acceptance of an invitation to a joint DEISA/PRACE security workshop in Helsinki on 14-15 October 2010. The work of SPG was presented. This achieved statements of intent from members of both DEISA and PRACE to collaborate with SPG in the future production of security policies, with the aim of producing interoperable policies.
- Participation in the EUGridPMA meetings on 20-22 September 2010 (Zagreb) and 24-26 January 2011 (Utrecht).

- Symposium on Authentication Technologies for Education and Research and TAGPMA meeting 4-7 October 2010 in Lubbock, Texas, USA. Kelsey gave a talk on the history of the old Joint (EGEE/WLCG) Security Policy Group and the EGI SPG and its plans to try to encourage participation by Grids in the USA in SPG deliberations.
- Leadership of an activity in WLCG to define a draft security policy for the endorsement of trusted virtual machine images. This work for the particle physics community should be of use to EGI in the future and is now part of the agreed work plan for SPG in 2011.
- Draft of a Security Policy Standard for interoperating infrastructures on Security Operations, Traceability and Incident Handling with Romain Wartel (WLCG Security Officer)
- At the EGI Technical Forum (14-17 Sep 2010, Amsterdam) Kelsey co-organised the one-day TERENA NRENs and Grids workshop and spoke on Policy Issues for Identity Management.

2.3 Software Vulnerability Group (SVG)

The main purpose of the Software Vulnerabilities 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 [R6]. In addition, some of the specific activities provided during related time period included software vulnerability issue handling, vulnerability assessment, vulnerability prevention etc.

The largest activity of the Software Vulnerability Group is the Software vulnerability issue handling, which is largely seen as an Operational Security activity. A description of the Software Vulnerability issue handling procedure is part of MS405, the Operational Security Procedures [R1]. Since this has been written the contact details for the various software providers, and more details of how the process is carried out have been established. Since the start of EGI 18 new vulnerabilities have been entered into the EGI report-vulnerability tracker, and 8 were found to be due to vulnerabilities in Grid Middleware affecting the production infrastructure.

Another activity for eliminating vulnerabilities in the EGI infrastructure is Vulnerability Assessment. This activity is being carried out by Members of the University of Wisconsin / Universitat Autònoma de Barcelona Middleware Security and Testing Group who have developed manual First Principles Vulnerability Assessment techniques for assessing software for vulnerabilities [R2]. The effort to carry out these assessments is partly funded by the European Middleware Initiative (EMI). A Vulnerability Assessment plan is being written, jointly between EMI and the EGI SVG on which pieces of software are to be assessed and when. The prioritisation of these assessments has been largely proposed by the EGI SVG to ensure the most security critical pieces of Grid middleware used in EGI are assessed.

The other activity is vulnerability prevention; that is attempting to prevent new vulnerabilities being introduced. SVG has been discussing the possibility of checking for world writeable files (from which some vulnerabilities derive) as part of the certification process, and the usage of safe file libraries for file handling. Developer training is now largely carried out within EMI, but the EGI SVG does attempt to raise awareness of the need for developers to be aware of secure programming and how to avoid

introducing some of the most common types of vulnerability, such as those resulting from file permission problems or failure to validate user input.

In regard to SVG meetings up to now most of the discussions have been carried out by e-mail. There was an SVG meeting/session at the EGI TF in Amsterdam, which was chaired by the Group Chair Linda Cornwall. The issue handling process in EGI was presented and discussed. The vulnerability assessment was presented by Elisa Heymann and priorities for which packages should undergo Vulnerability Assessment were discussed. The Group Chair had face-to-face meeting with Barton Miller (University of Wisconsin) and Elisa Heymann (University of Barcelona). During the meeting Vulnerability Assessment plan was discussed, which is completed from SVG side; a small re-arrangement of the order of assessments due to an imminent CREAM re-write to comply with EMI-ES (Execution Service) specification.

Much of the work during the first six months of EGI consisted of the transition from the EGEE to the EGI vulnerability handling process. This included expanding the RAT to cope with the increased scope of the activity in EGI, and moving to the EGI infrastructure, including using the EGI RT to track issues, and the writing of the SVG Wiki page https://wiki.egi.eu/wiki/SVG. This also including establishing contact details, including who to contact in which situation, with the various software providers who supply software that will be included in the EGI UMD.

The Group Chair has produced the issue handling process which was part of MS405. The other procedures the Group Chair has drafted are:

- The critical security operational procedure. This is an operational/CSIRT process, NOT SVG so it is probably not relevant to this document. This requires some change to sort out the site suspension procedure. Other than that it has been provisionally approved by the OMB.
- The Critical Software vulnerability handling procedure. This is a joint SVG/CSIRT document, with details on how both teams handle critical software vulnerabilities but requires change to fit the above which should be done in the next few weeks.

Plan for 2011 is to:

- Have monthly telephone or EVO meetings of the Group
- Produce an updated vulnerability handling process as part of the milestone Operational Security Procedures
- Update critical software vulnerability handling procedure, which is a joint CSIRT/SVG document
- Handle Vulnerabilities reported to the EGI software vulnerability group. For vulnerabilities in the Middleware distributed in the Unified Middleware Distribution collaborate with members of the EGI Technology Unit to help ensure that a version of the software where the vulnerability is absent is available in the UMD for installation across EGI in time for the Target Date set by SVG, and that the release notes refer to the advisory provided by the SVG
- Improve the smooth running and efficiency of the issue handling process, including automation of some aspects of the issue handling using the EGI RT tracker such as reminders, and the establishment of matrices and output from the tracker to compute the matrices

- Collaborate on Vulnerability prevention, including advising on checking for common vulnerability types in the certification process, developer education, and the usage of safe libraries for carrying out common actions

2.4 IGTF and EUGridPMA

The EUGridPMA in Europe, and the International Grid Trust Federation - IGTF at the global level, coordinate a common authentication trust domain that is used to persistently identify all Grid participants. First and foremost this trust domain provides the basis for authorization, the assignment of access privileges to users, and a means of differentiating the qualities of service provided by the Infrastructure. But the ability to persistently identify the participants in the infrastructure is also the basis for auditing, operational security and incident response, and can be used for accounting and settlement purposes.

EGI engages with the EUGridPMA as a recognized Major Relying Party, alongside other e-Infrastructures such as PRACE RI, the US based Open Science Grid, and other large cross-national infrastructures.

The IGTF implements the global trust fabric by ensuring compliance to authentication guidelines amongst the participating national and regional authorities via the mechanisms of peer review, by implementing audit mechanisms, and by the promotion of current best practices.

It implements these goals by accrediting authorities according to specific authentication guide lines. The EUGridPMA and the IGTF assert that the identity assertions issued by the member's authorities meet or exceed the minimum requirements in said guidelines.

Currently, three distinct types of authorities are recognised by the IGTF:

- Classic X.509 Certification Authorities with Secured Infrastructure ("classic") authorities perform identity vetting of their subscribers at the first time an identity assertion is issued to a subscriber. This authority is the most prevalent in the current trust fabric, and usually applied to small and medium-scale authentication operations
- Short-Lived Credential Services ("slcs") authorities issue identity assertions based on existing records, usually held by a single organisation or federation. These assertions are short-lived (at most 10 days), such that the underlying organisations or federation do not need to provide revocation capabilities for their members
- Member-Integrated Credential Services ("mics") authorities, like "slcs" ones, issue their assertions based on existing records, usually held either by large organisations where the accredited authority is tightly and completely integrated in its own business processes, or where a national research and educational federation mediates between the authority and the organisations that hold the identity vetting records. Through policy and by contractual relationships, a strong binding between the issuing authority and the underlying identity providers is maintained.

Identities that expire from the underlying systems result in timely revocation of the issued assertions. Therefore, assertions issued by “mics” authorities may be valid for up to 13 months.

The IGTF nor the PMAs do not themselves issue identity assertions (“certificates”), which is a task for the accredited authorities. In general, there is one such authority per country or region, although for some countries or regions more than one authority has been accredited to account for local variations or accommodate the geographic, topical or economic extent of an authority within a country or region.

The EGI participation in the IGTF has led to a number of new guidelines and policies that address the needs of our increasingly heterogeneous infrastructure. This includes guidance on the way end-users protect security sensitive materials, and two infrastructure providers can aid in ensuring this security by managing sensitive material on behalf of the end user. This at the same time promotes ease of use for such end-users by making access less complicated. A new guideline on the operation of attribute authorities (such as VO management servers) has been drafted with strong EGI participation and is now being extended to include more diverse access methods to the infrastructure and being scoped to a global audience. Next IGTF meetings will be All-Hands meeting in Taipei on 21-22 March 2011.

In the context of this activity EGI attended the two Plenary EUGridPMA meetings, four IGTF meetings and the Open Grid Forum (CAOPS Working Group) where the foundational documents for the working of the IGTF are defined and developed. Policy guidance with respect to identity management and the trust fabric was disseminated to the EGI TF and the Council in its assessment of policy mechanisms to address sensitive use of the EGI infrastructure.

David Kelsey, Chair of SPG participated in the EUGridPMA meetings on 20-22 September 2010 (Zagreb) and 24-26 January 2011 (Utrecht). At both of these meetings, Kelsey led sessions working on new policy standards for general Attribute Authorities, thereby expanding the work of IGTF beyond pure identity management to the management of attributes in general, e.g. for Authorisation of access to Grid services.

In 2011 it is expected to develop policies and guidance for the further integration of federated access (based on the educational and research federations that have emerged in the web environment) and automated and transparent access to the EGI infrastructure. Also further expansion of the trust fabric is foreseen in regions that are relevant to EGI, in particular in those areas where other EU FP7 support projects are under way.

3 CONCLUSION

The main focus during first 9 months was EGI transition from the EGEE security framework to the EGI security framework (as described in EGI-InSPIRE Description of Work) [R11]. Furthermore, special attention was dedicated to ensuring that security activities and process are performed without interruption and obstacles between the EGEE and EGI.

The transition included clarification of the responsibilities of the groups by establishing and finalising ToRs, transition of security policy and procedures to a new format and adoption by EGI.eu Executive Board. In addition, the membership of the groups were renewed and updated and new wiki pages for the all groups were created. Furthermore, for some of the groups (e.g. SVG) moving to the EGI infrastructure included using the EGI RT to track issues. This also included establishing contact details, including who to contact in which situation, with the various software providers who supply software that will be included in the UMD. Initial meetings of the groups were held during applied period.

Therefore, to sum up the major achievements, some of them are listed in Table 1.

Table 1

Groups	Major achievements
SCG	• finalised and adopted ToR • improved coordination between different EGI security groups and security representatives of other DCI projects
SPG	• finalised and adopted ToR • defined SPG procedures for developing new policies and for consulting the stakeholders • started drafting new and reviewing old security policies (e.g. full revision of old top-level Security Policy document • leadership of an activity in WLCG to define a draft security policy for the endorsement of trusted virtual machine images • participation at TERENA, DEISA/PRACE, OGF, TAGPMA events • agreed SPG detailed work plan for 2011

Groups	Major achievements
SVG	• finalised and adopted ToR • 18 new vulnerabilities have been entered into the EGI report-vulnerability tracker, and 8 were found to be due to vulnerabilities in Grid Middleware affecting the EGI infrastructure. • finalised Vulnerability Assessment plan • finalised Security Incident handling procedure and Vulnerability issue handling process and drafting critical security operational procedure and critical Software vulnerability Handling procedure • agreed SVG detailed work plan for 2011
IGTF and EUGridPMA	• participation of SPG Chair David Kelsey on 2 EUGridPMA meetings where he led sessions working on new policy standards for general Attribute Authorities, thereby expanding the work of IGTF beyond pure identity management to the management of attributes in general, e.g. for Authorisation of access to Grid services. • participation at four IGTF meetings and the Open Grid Forum (CAOPS Working Group) where the foundational documents for the working of the IGTF are defined and developed • starting to develop policies and guidance for the further integration of federated access (based on the educational and research federations that have emerged in the web environment), automated and transparent access to the EGI infrastructure and further expansion of the trust fabric is foreseen in regions that are relevant to EGI

To conclude, transition from EGEE to EGI security framework was successfully done; furthermore, as a direct consequence, new EGI security architecture improved coordination between security groups. Finally, participation in international security policy bodies was intensified, whereby EGI representatives took a leading role in a number of initiatives and actions including developing new policy standards, policies and guidance.

4 REFERENCES

R 1	MS405 Operational Security Procedures https://documents.egi.eu/document/47
R 2	Manual First Principles Vulnerability Assessment techniques for assessing software for vulnerabilities. http://www.cs.wisc.edu/mist/includes/vuln.html
R 3	ToR Security Policy Group https://documents.egi.eu/document/64
R 4	MS209 Security Policies within EGI https://documents.egi.eu/document/210
R 5	ToR Security Coordination Group https://documents.egi.eu/document/119
R 6	ToR Software Vulnerability Group https://documents.egi.eu/document/108
R 7	Security Policy Group Wiki site https://wiki.egi.eu/wiki/SPG
R 8	Security Policy Group – Glossary of Terms https://documents.egi.eu/document/71
R 9	Security Policy Group meeting – January 2011 https://www.egi.eu/indico/conferenceDisplay.py?confId=263
R10	Security Policy Wiki Page with the list of policy documents https://wiki.egi.eu/wiki/SPG:Documents
R11	EGI-InSPIRE Description of Work https://documents.egi.eu/document/10