EGI-InSPIRE

SECURITY ACTIVITY WITHIN EGI

EU MILESTONE: MS235

Document identifier:	EGI-MS235-FINAL
Date:	**22/03/2013**
Activity:	**NA2**
Lead Partner:	**EGI.eu**
Document Status:	**FINAL**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/1520

Abstract

The milestone provides an overview of the non-operational security activities from the SCG, SPG, SVG including description of EGI's participation in the international security policy bodies (e.g. EUGridPMA, IGTF). EGI security activities in the reporting period of EGI-InSPIRE project (Feb 2012- Jan 2013) were carried out as planned and EGI has confirmed its role as a leading force in international security policy bodies whereby EGI representatives were leading development of new policies and standards.



I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	Damir Marinovic Linda Cornwall David Kelsey David Groep	EGI.eu / NA2 STFC / SA1 STFC / NA2 FOM / NA2	
Reviewer:	Daniel Kouril	ICS	25/02/2013
Moderator	Peter Solagna	EGI.eu	21/2/2013
Approved	AMB		

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	11/01/2013	ToC	Damir Marinovic / EGI.eu
2	30/01/2013	First draft	Damir Marinovic / EGI.eu Linda Cornwall / STFC David Groep / FOM David Kelsey/ STFC
3	06/01/2012	Second draft	Damir Marinovic / EGI.eu Linda Cornwall / STFC David Groep / FOM David Kelsey/ STFC
4	06/03/2013	Final draft	Damir Marinovic / EGI.eu Linda Cornwall / STFC David Groep / FOM David Kelsey/ STFC

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 annual 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 annual report from EGI's representative in the International Grid Trust Federation (IGTF) and European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA).

EGI security activities in the third year of EGI-InSPIRE project were successfully carried out and EGI has strengthen its role as a leading partner in international security policy bodies (e.g. EUGridPMA, IGTF) where EGI representatives were a key factor in developing new policy standards, policies and guidelines.

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.
- Coordination of the Security Threat risk assessment.
- Security actions to ensure implementation of EGI Excellence Science Policy
- Revision of the Top-level Security Policy, Service Operations Security Policy and Acceptable Use Policy and expansion of the Accounting data protection policy
- Development of the Policy statement on proxy certificate and attribute certificate maximum lifetimes
- Leadership of the "Security for Collaborating Infrastructures (SCI)" activity, which has successfully defined a framework of policy and operational security standards for building trust between large-scale distributed computing infrastructures.
- Participation in the activity "Federated Identity Management for Research (FIM4R) where the paper was finalised expressing the joint vision and requirements for the use of Federated Identity
- Participation in the WLCG pilot project on the use of Federated Identity Management
- Twenty new vulnerabilities have been entered into the EGI report vulnerability tracker, eleven found to be vulnerabilities in the Grid Middleware.
- Nine advisories issued and provided input to one CSIRT alert concerning non-middleware.
- Decommissioning plans and decommissioning calendars were developed for software which is out of security support
- 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 OGF meetings in the CAOPS working group.
- Development of different assurance levels in IGTF being guided by the FIM4R requirements document, science portal scenarios and the availability of federated user credentials.
- Leadership of IGTF activities including preparation of the move to SHA-2, the tracking of IPv6 readiness, preparing guidelines for the protection of private authentication data by end-users in e-Infrastructures and the continuous monitoring of risks to the authentication infrastructure via a dedicated Risk Assessment Team.

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to describe non-operational security activities within the EGI. The milestone includes annual 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 annual report from EGI's representatives in the International Grid Trust Federation (IGTF) [R1] and European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA) [R2].

This milestone describes security activities within EGI from February 2012 to January 2013. Therefore, the milestone mostly covers the third 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 basis established on a new project – EGI-InSPIRE and a new organisation – EGI.eu. The second year was year of increased productivity after transitional year and increased number of meetings and activities. First year was described in MS214 Security Activity within EGI [R3], while the second year was described in MS224 Security Activity within EGI [R4]. The EGI security groups dealt well with security issues in the first two years, and provided a good foundation for the security activities in the third year. Therefore, security activities, initiatives and plans were carried out in the third year without any major obstacles or delays.

Out of ten EGI.eu policy groups, four EGI.eu policy groups deal with EGI security activities. This shows just how important security is considered within the infrastructure. All security groups have separate web pages on the EGI website [R5] and separate wiki pages [R6].

From the first milestone on security activity MS214 [R3] there was internal agreement among the Chairs of EGI security groups not to include the EGI CSIRT activities[1] since the milestone should describe the non-operational security activity within EGI.

However, in the case of SVG, we adopted a broader understanding of EGI security activities and included SVG activities. This is because SVG was participating in most of the security coordination work (for example work on the Security Threat Risk Assessment) and SVG activities have a significant impact on other security group activities.

The target group for the milestone consists of the people interested in EGI security activities and policies, EGI-InSPIRE project partners particularly NGI security officers, EGI.eu and NGIs Operation and Technology managers and officers etc.

The milestone content is structured as follows: Section 2 provides annual reports from different EGI security groups including annual report of EGI Representative at IGTF and EUGridPMA. Section 3

[1] The EGI Computer Security and Incident Response Team (EGI CSIRT) is a security team aimed at coordinating the operational security activities in the infrastructure, in particular the response to security incidents. The EGI CSIRT ensures the coordination with the NGIs and if applicable with NREN CSIRTs and security teams of peer Grids. In addition, the EGI CSIRT acts as a forum to combine efforts and resources from the NGIs in different areas, including Grid security monitoring, security training and dissemination, and improvements in responses to incidents.

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)

The purpose of the SCG is to bring 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. In addition, an aim of the SCG is to bring together security representatives with the operations and technological coordination representatives, when security issues have large operational or technical impact. The SCG provides:

- Information exchange between the SPG, SVG and other EGI security, operation and technology people
- Coordination of planning and response on EGI security issues [R7]

Two SCG meetings were held during reporting period (July and December 2012). On the SCG meeting in July gLite 3.2 and EMI 1 retirement plan were discussed. In coordination with EGI.eu Operations team certain actions were agreed including preparation gLite 3.2 retirement calendar advisory draft and coordinating actions with EMI people. At the second SCG meeting held in December 2012, the SCG participants were discussing the security actions needed to insure implementation of EGI Excellence Science Policy [R8] and developing appropriate mechanisms to implement them in terms of security policy documents. At both meetings next to the chairs of the EGI Security Groups and EGI.eu Director, the EGI.eu Technical Manager, EGI.eu Operations Manager and Officer and EGI.eu Strategy and Policy Manager and Officer were present.

Regular mail communication ensured continuous interaction between the Chairs of security groups (SCG, SPG, SVG and CSIRT) including the EGI Representative in IGTF and EUGridPMA and all other subscribers of SCG mailing list. Regular communications ensured agreement on common EGI position for various meetings in which EGI representative were participating and identification of gaps and needs for new EGI policies and procedures.

SCG members coordinated work on activities that need a common approach and the SCG's role of coordination body, for example work on Security Threat Risk Assessment [R9]. The Security Threat Risk Assessment was a risk assessment about threats to the assets in the EGI infrastructure. The Security Threat risk assessment was carried out in the first half of 2012 and led by the SVG chair. The team established to carry out the work identified 75 threats in 20 categories. This was carried out by starting from a draft from an assessment during EGEE and then discussing what should be the appropriate categories. Categories included operational and configuration threats, physical security threats, scientific and user data reliability, as well as illegal and general miss use. Each member of the team took one or two categories, proposed the detailed threats, and established the current situation for each. The team then had the opportunity to make suggestions on changes. Then each member of the team provided their estimation of 'Likelihood' and 'Impact' according to agreed guidelines. This was based on the current situation, with the current mitigation in place. The risk for each participant was computed as the product of the Likelihood and Impact. The average risk value was then computed. The group reported the 18 threats having the highest risk value, and 4 additional threats having the highest impact value.

Many of the threats having the highest risk values already had a lot of activity placed into their mitigation, for example 'Incident Spreads across the Grid' was one with a high risk value and a lot of effort was and still is put into preventing and mitigating this by CSIRT, including various training and simulation exercises.
Currently several of the higher risk threats have groups and teams working on them, for example the move to IPv6 was considered to have a high security risk and the IPv6 working group is looking at the impact and how to mitigate security risk.

During the reporting period, topics and achievements of the SCG meetings were the following:

- Coordination of work and development of on gLite 3.2 retirement calendar advisory draft for unsupported gLite 3.2 products.
- Initiation of security actions and policy statements needed to insure implementation of EGI Excellence Science Policy [R8].
- All the participants discussed various security issues that needed a common understanding. Regular communication with the OMB and TCB insured that the possibility of introduction of new functionalities will not cause security problems and if so they will be treated effectively and successfully.
- SCG members participated in reviewing the security policies developed by the SPG and operations procedures developed by the OMB
- Coordination of development of the document which summarizes the problems related to the usage of SHA1, the implications and actions needed for a safe migration towards SHA2 and RFC proxies.

2.2 Security Policy Group (SPG)

The Security Policy Group (SPG) produces and maintains policies that define the expected behaviour of sites and users to ensure a secure distributed computing infrastructure. An additional aim of the SPG is to develop general policies that could be applicable to e-infrastructures across the world in order to improve interoperability.

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 [R10].

During the year, SPG worked on a number of different policy issues including the following:

- Revision of the Service Operations Security Policy to clarify the requirement to upgrade old software with no on-going security support, to remove the statement on IPR as this is now covered in the OLA, and to add a new statement on emergency user suspension systems.
- Policy input to discussions on the implementation of the new central emergency user suspension system.
- Policy statement on proxy certificate and attribute certificate maximum lifetimes.
- Modification of the user Acceptable Use Policy to include the requirement for acknowledgment and record of use of the EGI infrastructure.
- Revision of the top-level Security Policy document to use new glossary terms and to generalise so as to address use of new technologies, e.g. federated Cloud services.
- Expansion of the Accounting data protection policy to also include storage accounting.

Formal approval and adoption of these new policy documents will be sought during 2013.

Only two face-to-face meetings of SPG were held during the year, one in February 2012 in Amsterdam and one during the EGI Technical Forum in Prague (September 2012). A general open session on SPG work was also held during the Technical Forum to inform the general audience and to invite feedback [R11]. SPG work continued outside of these formal meetings via the editorial teams or by email/phone.

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 of EUGridPMA and TAGPMA. One topic of particular concern here was consideration of the readiness of middleware and applications to move from SHA-1 to SHA-2 hashing and the related timetable. One of the great strengths of the IGTF organisation is that Relying Parties, i.e. those using the authentication technologies for controlling access to their resources, are full members of the PMAs. Active participation in EUGridPMA and TAGPMA gives EGI the ability to express requirements and to help steer the future direction of the work thereby ensuring that the IGTF trust fabric remains useful to EGI.
- Leadership of the "Security for Collaborating Infrastructure (SCI)" [R12]. SCI is a collaborative activity of information security officers from several large-scale distributed computing infrastructures, including EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE. SCI is developing a framework to enable interoperation of collaborating Grids with the aim of managing cross-Grid operational security risks and to build trust and develop policy standards for collaboration especially in cases where we cannot just share identical security policy documents. Different Grids are subject to many of the same threats and vulnerabilities as other infrastructures because of the use of common software and technologies. Moreover, there may be users who take part in more than one infrastructure and are thus potential vectors that can spread infection from one infrastructure to another. Finally, one infrastructure may want to extend rights to use its resources to users who are enrolled in a different infrastructure. In each of these situations, the infrastructures can benefit from working together and sharing information on security. This work will assist the EGI security teams, particularly the EGI CSIRT, in building trust with other infrastructures enabling cooperation on the handling of security issues. Two face-to-face meetings were held during the year, co-located with EUGridPMA meetings, during which a version 1 document was produced and agreed. In this document we lay out a series of numbered requirements in 6 areas (operational security, incident response, traceability, participant responsibilities, legalities, and data protection) that each infrastructure should address as part of promoting trust between infrastructures. At the SCI meeting in January 2013 an initial self-assessment of PRACE, EGI and CSC Finland was made. This exercise proved to be very useful as a way of tuning the assessment process.
- Continuing participation in the activity "Federated Identity Management for Research (FIM4R)". This is collaboration between several European research communities, including photon/neutron facilities, social science and humanities, high energy physics, climate science and bio-informatics. Two workshops were held in Taipei (March 2012) and Nijmegen (June 2012) and a paper was finalised expressing the joint vision and requirements for the use of Federated Identity. The joint vision presented in the paper expresses the need for a common policy and trust framework for Identity Management based on existing structures and federations either presently in use by or available to the communities. This framework must provide researchers with unique electronic identities authenticated in multiple administrative domains and across national boundaries that can be used together with community defined attributes to authorize access to digital resources. The paper also presents a number of

common requirements, across all the participating user communities, in areas such as usability, open standards, authorisation under the control of the communities, attribute management, levels of assurance, etc. The SPG chair presented this work to a REFEDs meeting (May 2012) and also the VAMP meeting (Sep 2012). The FIM4R collaboration is now negotiating with REFEDS, EduGAIN and GEANT on pilot projects and work to solve issues and find solutions to the higher priority requirements. The successful outcome of these pilot projects and the negotiations with the identity management providers will be very important for the future use of widely adopted common Identity Management deployments on the EGI infrastructure for the benefit of the EGI user communities.

- WLCG [R13] had an activity to plan the evolution of its technical services, including security. Kelsey participated in the pilot project on the use of Federated Identity Management and next year this will include work on policy and trust requirements, particularly with relation to Levels of Assurance in identity vetting and IDM systems.
- Participation in the work to produce the deliverable document on D4.4 EGI Security Risk Assessment [R9].

2.3 Software Vulnerability Group (SVG)

The main purpose 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 software for vulnerabilities, to pro-actively look for vulnerabilities.
3. Developer education, to help prevent new vulnerabilities from being introduced into the software.

The first activity is the largest activity of the EGI SVG, and is sometimes considered part of security operations. It is less “real time” than for example the incident handling carried out by CSIRT, and is carried out according to the agreed EGI Software Vulnerability Issue handling procedure [R14]. Between February 2012 and January 2013 20 new vulnerabilities were entered into the EGI report vulnerability tracker, 11 of these were found to be due to software vulnerabilities in the Grid Middleware affecting the production infrastructure. Others were either invalid or in software which was not in use in the EGI infrastructure or with limited use where the risk to EGI was considered negligible.

SVG issued 9 advisories [R15] on vulnerabilities concerning Grid Middleware, during this time, some of which refer to vulnerabilities reported as above, some for vulnerabilities reported prior to this reporting time which happened to be resolved during this time. In addition, SVG provided input to one CSIRT alert concerning non-middleware.

In one case, a ‘high’ risk vulnerability was found in a piece of middleware where a version was in widespread use which was no longer under security support. Although in that one case it was possible to produce a patch, it highlighted a problem where sites were still using software for which there was no longer any security support. In order not to find EGI in the position where it is necessary to instruct sites to stop running software immediately in the case of a critical vulnerability this led to the Operations Management Board producing decommissioning plans and decommissioning calendars for software which is out of security support. It also led to plans and strategies for handling the retirement of software which will come out of security support at dates in the future.

The Software vulnerability Issue handling procedure was not revised around PM 27 as originally planned, instead a new version is planned for around PM 35 or 36 which will include details of how to carry out the processes after the end of EMI and IGE in April 2013. Work on this began in January 2013.

The Vulnerability Assessment activity continues to be carried out by members of the University of Wisconsin, Universitat Autonoma de Barcelona Middleware security and testing group who developed the First Principles Vulnerability Assessment Techniques for assessing software for vulnerabilities. [R16]. Middleware is actively vetted for vulnerabilities using these techniques. This is a very labour intensive activity, as it takes several months to carry out a vulnerability assessment of one piece of middleware. Near the beginning of EGI a plan was formulated between SVG and EMI to define which pieces of middleware should be given priority for assessment using this technique. [R 19]

Since the start of EGI vulnerability assessments have been completed for Argus, VOMS Core, VOMS admin and glexec using these techniques. At the time of writing the assessment of WMS is still in progress, it was expected to be completed by now, but was delayed due to staff illness. The assessment of gLite's CREAM began in January 2013.

Much of the work of SVG continues to be carried out by e-mail. SVG also has monthly audio meetings which allow useful discussions.

The chair of the SVG was also the lead author of deliverable D4.4, the Security Risk Assessment of the EGI Infrastructure [R9] which included a plan for a detailed Security Threat Risk Assessment. This Security Threat risk assessment was carried out in the first half of 2012 and co-ordinated by the SVG chair.

2.4 IGTF and EUGridPMA

Through its participation in the European Policy Management Authority for grid authentication in e-Science (EUGridPMA) [R2] and the International Grid Trust Federation (IGTF) [R1], EGI helps to shape the management of identities for researchers in Europe, and ensures that the resources participating in EGI can rely on traceable and auditable identities on which access control and incident response are based.

The broadening of the user base leads to a continuous set of changes in assurance level. A wider range of resources (with a wider diversity in 'value' when seen from a risk management perspective) makes it possible to allow alternative forms of identity vetting. This wider diversity lead earlier to the development of the 'VO Portal Policy' work of the EGI SPG, but the increasing number of identity federations which can provide a light-weight form of identity vetting allows the IGTF to consider diversifying the identity vetting assurance levels defined for use by the relying parties. The wide interest by EGI, but also peer infrastructures such as PRACE-RI, OSG, and XSEDE provides a wide basis to define such additional levels. The Federated Identity Management for Research (FIM4R) requirements document, science portal scenarios, and availability of federated user credentials guide the developments of additional assurance levels. The widening divide in Europe between 'federation-enabled' researchers and those in countries without a federation (or with a federation without sufficient identity assurance) is a cause of concern to the EUGridPMA.

The practices developed for the IGTF in securing the infrastructure and managing assured credential data can be effectively re-used in EGI for the management of attribute authority systems, in particular community member directories and 'VOMS' virtual organisation management systems. A guideline for the deployment, operation and management of such services has been developed in the EUGridPMA for use by the VOMS service operators in EGI. It is foreseen that this initial version of the guideline will be iteratively refined through evaluation of existing services.

At the same time events in the authentication space outside the immediate scope of EGI require changes to the technical authentication infrastructure. Several prominent incidents related to commercial public key infrastructures (such as the infamous 'DigiNotar' incident) spurred rapid advances in assurance level for public CAs, and a more active role has been taken up by their coordination bodies such as the CA\Browser Forum [R17]. Although these improvements have been primarily in the vetting quality (where IGTF standards were already high), there have also been modifications to security algorithms and technical parameters. Since the EGI identity ecosystem leverages public PKI where possible, the improvements proposed for public PKI also influence the technical developments in the IGTF. Working closely with the EGI and Open Science Grid (US) operational teams, required software changes needed to accommodate these new security parameters (in particular the move to the 'SHA-2' message digest family and longer key lengths) are being implemented by middleware developers on request of the IGTF and the EGI-IGTF liaison function.

Further technical policy changes, including the move towards more timely identity status information, are foreseen in 2013. In addition the IGTF tracks IPv6 readiness, guidelines for the protection of private authentication data by end-users in e-Infrastructures, and continuously monitors risks to the authentication infrastructure through a dedicated Risk Assessment Team distributed globally.

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 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.

People who are interested in summaries of the PMA meetings can find more details on pages dedicated to the meetings at the EUGridPMA website [R18].

3 CONCLUSION

During the reporting period EGI security activities and processes were properly carried out with emphasis on improving efficiency and effectiveness. After the first transitional year and the second consolidation year, effectiveness of EGI security groups was improved during the third year, so there was no need for as many meetings as in the second year. Therefore, 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	• Security actions insuring implementation of EGI Excellence Science Policy • Coordination of work and development of gLite 3.2 retirement calendar advisory • SCG members participated in reviewing the security policies developed by the SPG and operations procedures developed by the OMB • Reaching common EGI position for various meetings in which EGI representative was participating and identified gaps for new EGI policies and procedures.
SPG	• Revision of the top-level Security Policy, Service Operations Security Policy and Acceptable Use Policy • Expansion of the Accounting Data Protection Policy • Development of the Policy statement on proxy certificate and attribute certificate maximum lifetimes • Successful open SPG session on SPG work held during the Technical Forum • Leadership of the “Security for Collaborating Infrastructure (SCI)” activity • Participation in the International Grid Trust Federation representing EGI and WLCG as a relying party of EUGridPMA and TAGPMA. • Participation in the activity “Federated Identity Management for Research (FIM4R) where the paper was finalised expressing the joint vision and requirements for the use of Federated Identity • Participation in the WLCG pilot project on the use of Federated Identity Management

Group	Major achievements
SVG	• Twenty new vulnerabilities have been entered into the EGI report vulnerability tracker, eleven found to be vulnerabilities in the Grid Middleware. • Nine advisories issued and input provided to one CSIRT alert concerning non-middleware. • 'High' risk vulnerability was found in a piece of middleware no longer under security support. • In collaboration with Operations Management board decommissioning plans and decommissioning calendars were developed for software which is out of security support. Initiated development of plans and strategies for software retirement for software which in future is comes out of security support. • The chair of the SVG was the lead author of deliverable D4.4 the Security Risk Assessment of the EGI Infrastructure. • Started revision of Software vulnerability Issue handling procedure. • The Vulnerability Assessment activity continues to be carried out.
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 OGF meetings in the CAOPS working group. • Participation in development of the Federated Identity Management for Research (FIM4R) requirements document, science portal scenarios, and availability of federated user credentials that are guiding the developments and diversifying of additional identity vetting assurance levels • Participation in development of the guideline for the deployment, operation and management of attribute authority systems, in particular community member directories and 'VOMS' virtual organisation management systemshas been developed in the EUGridPMA for use by the VOMS service operators in EGI • Software changes needed to accommodate these new security parameters implemented by middleware developers on request of the IGTF and the EGI-IGTF liaison function • Leadership of IGTF activities including preparation of the move to SHA-2, the tracking of IPv6 readiness, preparing guidelines for the protection of private authentication data by end-users in e-Infrastructures and the continuous monitoring of risks to the authentication infrastructure via a dedicated Risk Assessment Team

To conclude, EGI security activities in the third year of EGI-InSPIRE project were successfully carried out and EGI has deep-rooted its role as a leading partner in international security policy bodies (e.g. EUGridPMA, IGTF) where EGI representatives were a key factor in developing new policy standards, policies and guidelines.

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	MS224 Security Activity within EGI https://documents.egi.eu/document/965
R 5	EGI.eu Policy Groups http://www.egi.eu/policy/groups
R 6	Main EGI Wiki Page https://wiki.egi.eu/wiki/Main_Page
R 7	Security Coordination Group - Terms of Reference https://documents.egi.eu/document/119
R 8	Demonstrating Excellent European Science on EGI's shared resources https://documents.egi.eu/document/1415
R 9	D4.4 The Security Risk Assessment of the EGI Infrastructure https://documents.egi.eu/document/863
R10	SPG wiki page https://wiki.egi.eu/wiki/Security_Policy_Group
R11	Security Policy Group and EGI Security Threat Risk Assessment public reports http://indico.egi.eu/indico/contributionDisplay.py?contribId=8&sessionId=51&confId=1019
R12	Security for Collaborating Infrastructure (SCI) http://www.eugridpma.org/sci/
R13	Worldwide LHC Computing Grid (WLCG) http://wlcg.web.cern.ch/
R14	EGI Software Vulnerability Issue handling procedure https://documents.egi.eu/document/717
R15	SVG Advisories https://wiki.egi.eu/wiki/SVG:Advisories
R16	Vulnerability Assessment http://research.cs.wisc.edu/mist/includes/vuln.html
R17	CA\Browser Forum https://www.cabforum.org/
R18	Summaries from the PMA meetings https://www.eugridpma.org/meetings/2012-01/summary.txt https://www.eugridpma.org/meetings/2012-05/summary-eugridpma25.txt https://www.eugridpma.org/meetings/2012-09/eugridpma-26-lyon-summary.txt https://www.eugridpma.org/meetings/2013-01/eugridpma-rome-summary-20130117.txt
R19	The Security Assessement Plan https://documents.egi.eu/secure/ShowDocument?docid=563