EGI-InSPIRE

SECURITY ACTIVITY WITHIN EGI

EU MILESTONE: MS246

Document identifier:	EGI-MS246-V4.1tf.doc
Date:	**17/03/2014**
Activity:	**NA2**
Lead Partner:	**STFC**
Document Status:	**FINAL**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/2066

Abstract

This milestone provides an overview of the non-operational security activities from the SPG, SVG and SCG including EGI's participation in the international security policy bodies (e.g. EUGridPMA, IGTF) for the reporting period of EGI-InSPIRE project (Feb 2013- Jan 2014).



I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	Linda Cornwall David Groep David Kelsey	STFC/SA1 FOM/NA2 STFC/NA2	25-01-2014
Reviewed by	Peter Solagna Daniel Kouril	EGI.eu/SA1 CESNET/SA2	10-02-2014
Approved by	**AMB and PMB**		14-03-2014

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	14 Jan 2014	Table of Contents	David Kelsey/STFC
2	4 Feb 2014	SCG, SPG, SVG, and IGTF/EUGridPMA sections added	Linda Cornwall/STFC, David Groep/FOM, David Kelsey/STFC
3	5 Feb 2014	Add introduction, summary and conclusions – start of external review	David Kelsey/STFC
4	3 March 2014	Addressed reviewers comments	Linda Cornwall/STFC
5	12 March 2014	AMB and PMB review	

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), Software Vulnerability Group (SVG), and from EGI's representative(s) in the International Grid Trust Federation (IGTF) and European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA).

EGI security activities in this final year of the EGI-InSPIRE project were successfully carried out, the production infrastructure continued to provide secure and available services for the benefit of its users and EGI continues to demonstrate its role as a leading partner in international security policy bodies (e.g. EUGridPMA, IGTF, FIM4R and Security for Collaborating Infrastructures - SCI) 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:

- Ensuring the continuing operation of a secure and available EGI infrastructure, in collaboration with the EGI CSIRT;
- Maintenance and development of EGI security policy and procedures including a new policy for emergency central suspension of users in case of compromised user credentials[1];
- Engagement with the EGI federated cloud task force towards an agreed understanding on the required changes to security policies and procedures and cloud operations to provide secure and available services;
- Successful handling of 38 new software vulnerabilities reported to SVG, thereby avoiding security incidents that could have happened;
- Successful tuning of the SVG procedures to cope with the end of the EMI and IGE projects;
- Completion of the vulnerability assessment of CREAM and fixing the problems identified;
- Leadership of and publication of version 1 of the Security for Collaborating Infrastructures SCI document describing the requirements for a collaborative trust framework in security policy;
- Leadership of the development of version 2 of the SCI document;
- Participation in the Federated Identity Management for Research activities with clear specification of joint policy requirements and negotiation with identity federations and providers towards a single sign-on AAI for Research
- Ever closer collaboration between the security teams within EGI and with security experts in PRACE and EUDAT including planning for security beyond the end of EGI-InSPIRE
- Continuing close collaboration with the OSG;
- Dissemination of all our activities in the EGI Technical Forum and several international conferences;
- Revision of the EGI security risk assessment and planning of a security threat risk assessment for cloud infrastructures;
- Successful leadership of EUGridPMA and presentation of EGI requirements resulting in the development of new IGTF profiles and guidelines including:
    - The Identifier-Only Trust Assurance Profile,
    - Guidelines on trusted credential stores,

[1] Operational Procedure for Compromised Certificates and Central Security Emergency suspension (https://documents.egi.eu/document/1018).

  - Attribute Authority Operations Guidelines
  - Guidelines on Private Key Protection
- Participation in several OGF security working groups, including the revision of the OGF GFD.125 certificate profile,
- Handling of the policy issues and timetable related to the move of IGTF to the use of SHA-2 hash algorithms,
- Contributions to successful security training events in several international conferences and workshops.

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to describe the non-operational security activities within 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 an 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 2013 to January 2014. The first year of EGI-InSPIRE was described in MS214 Security Activity within EGI, while the second and third years were described in MS224 and MS235 [R3]. The security activities, initiatives and plans were carried out in this 4th year without any major obstacles or delays.

The milestone content is structured as follows: Section 2 provides annual reports from the different EGI security policy groups including the annual report of the EGI Representative at IGTF and EUGridPMA. Section 3 sums up the EGI security activities with concluding remarks and provides a list of the major EGI security achievements. All references are listed in Section 4.

2 REPORTS ON NON-OPERATIONAL SECURITY ACTIVITY

2.1 Security Coordination Group (SCG)

The purpose of the SCG [R4] is to bring together representatives of the various security functions within EGI to ensure that there is coordination between the operational security, the security policy governing the use of the production infrastructure and the general operations management. 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.

Regular communication ensured continuous interaction between the Chairs of security groups (SCG, SPG, SVG, CSIRT and EUGridPMA) and all other subscribers of the SCG mailing list. This also ensured agreement on a common EGI position for various meetings in which EGI representatives were participating and the identification of gaps and the need for new EGI policies and procedures.

During 2013 all chairs of the EGI security groups have worked ever more closely together and wherever possible we hold join meetings with security experts from other infrastructures, including PRACE, EUDAT, WLCG, XSEDE, OSG etc. We have lost some key members of the various groups during the year and now find that the membership of the various activities overlaps much more than in the past. Beyond the end of the EGI-InSPIRE project we see a growing need to collaborate more closely for efficiency reasons and to make the best possible use of the available expertise and funding. This will be reflected in e-Infrastructure collaborative structures that will be defined in the remainder part of 2014.

We have held several very successful security training events in public conferences and in a new development a joint security training event and workshop was held in Linkoping, Sweden between EGI, EUDAT and PRACE in October 2013 [R5]. This included an examination at the end of the training and the award of certificates to the successful participants. We plan to build on this during 2014, assuming that we can find sufficient funding for the trainers to travel to future events.

2.2 Security Policy Group (SPG)

The Security Policy Group (SPG) produces and maintains policies that define the expected behaviour of sites, service operators and users to ensure a secure and available distributed computing infrastructure. Important and growing aims of the SPG include the development of general policies that could be applicable to e-infrastructures across the world in order to improve interoperability and to contribute to the development of policies in the world of federated identity management for researchers.

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 [R6].

During the year three revisions of EGI security policy documents were made:

- The Grid Policy on the Handling of User-level Job Accounting [R7] was updated to increase the allowed period of retention of accounting data containing personal identifying information from one year to 18 months as operational problems had been experienced with the shorter deadline. This new version was adopted on 19 March 2013.
- The Service Operations Security Policy [R8] was updated to add the policy requirement for services to implement the central emergency suspension system. This new version was adopted on 1 June 2013.
- The Grid Acceptable Use Policy [R9] was revised to add a requirement for users to acknowledge the use of EGI/NGI resources and services. This has not yet been formally adopted as we are also modifying the AUP so that it also applies to the EGI Federated Cloud services.

No formal meetings of SPG were required during the year as most of the general policy discussions took place in SCI and various federated identity management meetings (see below) or in joint meetings of the operational security team with PRACE and EUDAT. Discussions on policy issues also took place on the SPG mail list. A general open session on EGI security, including the work of SPG, was held during the EGI Technical Forum in Madrid in September 2013 to inform the general audience and to invite feedback [R10].

Engagement with the EGI Federated Clouds activity has now started with two members of the EGI security team attending a meeting of the working group in Oxford UK (January 2014) and becoming members of the EGI Federated Cloud initiative. Presentations were given on the importance of operational security and a draft security questionnaire for Cloud providers has been produced. It is clear that considerable work still needs to be done on security policies and procedures for the federated cloud service. New procedures[2] for certification of cloud providers are required and are been experimented to prepare for the start of the EGI Federated Cloud production phase starting in May 2014. We need to develop a new security test suite to check basic traceability of actions and further developments in security monitoring are likely to be required.

The SPG Chair continued to lead and members of SPG participated in the "Security for Collaborating Infrastructures" (SCI) [R11] activity building a standard trust framework for security policy between EGI, EUDAT, PRACE, XSEDE and others. Two formal meetings of the SCI group were held during the year, in Boulder, Colorado, USA in May 2013 and in January 2014 in Abingdon, UK [R12]. Version 1 of the document was presented at the ISGC2013 conference in Taipei in March 2013 and has been published in the conference proceedings [R13]. The work of SCI was also presented to the WLCG Grid Deployment Board in July 2013 and to the CHEP2013 conference in Amsterdam in October 2013 [R14]. The SCI group is close to producing version 2 of their document. It has been agreed that we will investigate publishing this in OGF as an informational document.

An important topic during this year has been the general move towards the provision of federated identity management for research communities. The discussions and work takes place in several fora; the Federated Identity Management for Research (FIM4R) activity [R15], the IGTF (see below), REFEDS, VAMP and other joint TERENA/EGI/Geant meetings. The SPG chair presented the work of FIM4R at a Latin America Video meeting (19 Jun 2013) [R16]. All of this work is aimed at linking

[2] https://wiki.egi.eu/wiki/PROC18



together the AAI infrastructure required by EGI and distributed computing for Research in general with the existing national education federations and eduGAIN. The policy issues are often much more complex than the technical ones and this will be an important topic during 2014.

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 three main ways:

- Handling reported software vulnerabilities (or potential vulnerabilities),
- Assessing software for vulnerabilities (pro-actively looking for vulnerabilities and arranging their resolution),
- Developer Education, to prevent new vulnerabilities being introduced into the software.

This has continued to be the case over the past year, but there has been less emphasis on developer education, and more on dealing with vulnerabilities reported.

Handling vulnerabilities reported has always been the largest activity, and is sometimes considered part of security operations. Generally it is less 'real time' than more general operational security, but there are times when SVG needs to issue an advisory urgently asking sites to take action to secure their sites against a serious vulnerability. Vulnerabilities are handled according to the approved EGI Software vulnerability issue handling procedure [R17]. Between February 2013 and January 2014 38 new vulnerability issues were entered in the tracker, 24 were found to be software vulnerabilities in the Grid middleware and 3 in 3rd party software widely used in the infrastructure. Others were either invalid, or required no action from SVG.

SVG issued 12 advisories publicly [R18] during this time. 3 others were released but not made public on the wiki, either due to being vulnerabilities in 3rd party software or the problem was not fixed in all versions of the software. Some of these refer to the vulnerabilities above, some refer to vulnerabilities reported earlier. Also, some refer to more than one vulnerability, if for example more than one vulnerability concerning a piece of software is fixed in the same release, usually only one advisory is sent referring to all the vulnerabilities.

Prior to the end of EMI and IGE, EGI had a Service Level Agreement with these projects to handle middleware vulnerabilities according to [R17]. The end of EMI and IGE meant that there were discussions on how to continue with the general maintenance of the software as well as vulnerability issue handling. In effect, less has changed than expected, some contact details have been revised but generally the fixing of vulnerabilities in middleware has continued largely supported by various institutes supporting the product teams. There have been less active members of SVG, and at times there have been fewer members of SVG providing their opinion on the risk than we have had before. On a couple of occasions we have set the risk resulting from the opinion of 2 experienced people, whereas we have stated that 3 is the minimum. However, we have been able to continue the issue handling activity effectively due to a handful of dedicated members of SVG.

During the year SVG also handled several vulnerabilities in TORQUE, which is a batch system developed by the cluster resources company. It was found that suitable secure versions were not available for EGI. It was decided to provide an additional 'SVG fixes' repository in the EGI UMD

and SVG members made 2 versions of Torque available in this repository, which were suitable for the EGI infrastructure, and contained no known vulnerabilities.

The Vulnerability Assessment of CREAM by the Universitat Autonoma de Barcelona Middleware security and testing group was completed. This reported 5 vulnerabilities in CREAM. Near the beginning of EGI a plan was formulated between SVG and EMI to define which pieces of middleware should be given priority for Vulnerability assessment [R19] and assessment of all the software in this plan are either completed (Argus, gLexec, VOMS core, CREAM) or in progress (WMS, Unicore TSI and Gateway).

In 2012 a security threat risk assessment was carried out. The chair of the EGI SVG also provided a brief update on status of some of the higher risk and higher impact threats as input to the EGI review in June 2013. One of the threats of highest risk value mentioned was "Insufficient staff may be available to carry out security activities", and it was agreed that most of the security activities are 'Critical' to the continuation of the EGI infrastructure. A partial funding of these 'critical' activities has been agreed until further funding (e.g. through Horizon 2020 or other sources) can be found in order to reduce the likelihood of losing critical staff. Another threat which was considered 'high' risk was "an incident spreads across the Grid", and various activities were carried out to further reduce this risk, such as emergency suspension of a credential, and the operational security service challenges. Another high risk threat was "The move to more use of Cloud technologies may lead to security problems". The various security teams (EGI SVG, EGI CSIRT and EGI SPG) have engaged with the EGI Federated task force in order to bring their expertise and adapt the activities to mitigating the security risks in the EGI federated cloud.

EGI SVG has requested a session at the EGI Community Forum, in order to update on the status of SVG and describe some of the work being carried out to evolve this activity in the future in particular for cloud technology.

2.4 IGTF and EUGridPMA

Having a world-wide system to identify participants of the e-Infrastructure in a trustworthy way is of key importance for an open and interoperable system that harnesses high-value resources like those offered in EGI and its peer infrastructures outside Europe. Through its participation in the IGTF (the International Grid Trust Federation) and the EUGridPMA EGI can ensure its requirements are met with regards to traceable and auditable identities on which access control and incident response are based. It can also help shape the direction in which identity management for distributed e-Infrastructures develops worldwide.

As the e-Infrastructure expands to include a more diverse user base, EGI worked within the IGTF alongside other infrastructures such as PRACE in Europe, and XSEDE and Open Science Grid in the USA, on guidelines for differentiated assurance levels, on best practices for operating attribute services by research communities, and on trusted credential stores and credential translation services.

The set of these guidelines taken together prepares the EGI infrastructure for the more heterogeneous assurance levels and evolving technology choices that today are found in the research and education AAI federations. The following policies were completed in this project year to further the aims of EGI in this area:

- **Collaborative trust assurance through the Identifier-Only Trust Assurance (IOTA) Profile**

  End-to-end integrity of authentication and authorisation has traditionally been achieved by strong identity vetting by trusted external partners (Authorities) that profile extensive traceability and vetting capabilities. By re-distributing the vetting and traceability requirements amongst the participants (identity providers, research community registrars, resource centres and portal operators), more lower-assurance identity assertions can be incorporated in the trust fabric – but only on the explicit provision that the information that is subsequently lacking in these lower-assurance assertions is compensated by additional controls residing in the other participants (e.g. a stronger community registration process, resource-centre specific vetting), or the over-all risk is lowered (e.g. by allowing only read-only access to data).

  EGI already has the VO portal policy in place to support lower-risk applications. The new IOTA Profile [R20] introduces lower-assurance identity assertions, which – when used together with strong community vetting – could in principle allow more Identity Providers to qualify for the trust fabric. It has the potential in Europe to permit orders-of-magnitude more users from existing AAI federations for selected use cases (restricted services or in conjunction with highly trusted community registries). Highly detailed feedback was received from PRACE, XSEDE and OSG, and through a multi-stage convergence process the concerns of (primarily) PRACE and the abilities of prospective IOTA accreditable CAs (in particular CILogon InCommon Basic) were reconciled. Feedback was also received from the UK SARoNGS service and from several portal development groups in EGI. PRACE has expressed interest in supporting IOTA or specific (restricted) use cases, and - alongside the current VO portal policy - the IOTA profile was deemed useful for portals in EGI.

  If, and if so how, other services in the EGI ecosystem can make use of IOTA is yet to be determined. Presentations to the EGI Community Forum as well as the technical forum in 2013 were used to disseminate information about the IOTA profile to potentially interested relying parties.

- **Trusted Credential Stores**

  Credential generators and credential stores are likely to play an important role in bridging the multitude of AAI technologies in use throughout Europe and throughout the application area. It is unlikely that a single AAI technology emerges that can address all use cases (in particular the wide gap between Web-based single sign-on systems and those involving non-web, command-line and brokering services is unlikely to be solved with a single technology). Also the Web-SSO is continuously changing, with new technologies (OAuth, OpenID Connect) emerging prominently – especially outside the research and academic domain. Developments in national e-Identity systems in Europe are also likely to change the AAI landscape. Trusted credential stores, when deployed widely, are likely to aid interoperability.

  In order to prepare for the emergence of these systems and pave the way for their secure deployment, the IGTF with important contributions from EGI as well as others, drafted the first version of the policy on Guidelines for Trusted Credential Stores [R21]. It is foreseen that this first version will evolve as more experience in operating such stores is gained in the coming period.

- Attribute Authority Operations (AAOPS) Guidelines

  The practices developed for the IGTF in securing the infrastructure for attribute authority operations can be effectively used in EGI for the management of attribute authority systems,

in particular community member directories and 'VOMS' virtual organisation management systems. A guideline [R22] 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.

An update to the Key Protection guidelines [R23] further clarifies the way sensitive authentication data can be managed by or on behalf of the user.

The changes in technical deployment policy related to cryptographic integrity of authentication, initiated by the IGTF and supported by EGI, have by the end of this project year ensured operational readiness of all public-key infrastructure authentication and authorization software in EGI. Through its engagement with the IGTF, EGI could also ensure the global migration proceeded in pace with the EGI requirements. EGI can now face the transition to the modern standard "SHA-2" with confidence.

Further technical policy changes, including the move towards more timely identity status information, was re-scheduled for 2014 and beyond to allow software providers and resource centres to focus on the SHA-2 migration. In addition the IGTF continues to tracks IPv6 readiness, guidelines for the protection of private authentication data by end-users in e-Infrastructures, and risks to the trust infrastructure.

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 feed-back from these events is given back to the relevant EGI bodies. A revised version of the technical policy on PKI Certificate Profiles, updating the current Community Practice document GFD.125 to a Recommendation, has been completed [R24]. It is likely to have applicability also to the new 'cloud' infrastructure management systems that also often employ PKI technology for management access control.

3 CONCLUSION

During the reporting period EGI security activities and processes were properly carried out with emphasis on improving efficiency and effectiveness. We have successfully coped with a reducing number of security experts by holding joint meetings wherever possible, not only within the EGI security groups but by also strengthening our collaborations with infrastructures such as PRACE and EUDAT.

The main achievements of the year include:

- Ensuring the continuing operation of a secure and available EGI infrastructure, in collaboration with the EGI CSIRT,
- Maintenance and development of EGI security policy and procedures,
- Leadership of and publication of version 1 of the Security for Collaborating Infrastructures document describing the requirements for a collaborative trust framework in security policy,
- Leadership of the development of version 2 of the SCI document,
- Participation in the Federated Identity Management for Research activities with clear specification of joint policy requirements and negotiation with identity federations and providers towards a single sign-on AAI for Research,
- Ever closer collaboration between the security teams within EGI and with security experts in PRACE and EUDAT including planning for security beyond the end of EGI-InSPIRE,
- Dissemination of all our activities in the EGI Technical Forum and several international conferences,
- Successful handling of 38 new software vulnerabilities reported to SVG, thereby avoiding security incidents that could have happened,
- Successful tuning of the SVG procedures to cope with the end of the EMI and IGE projects,
- Completion of the vulnerability assessment of CREAM and fixing the problems identified,
- Revision of the EGI security risk assessment,
- Successful leadership of EUGridPMA and presentation of EGI requirements resulting in the development of new IGTF profiles and guidelines including:
    - The Identifier-Only Trust Assurance Profile
    - Guidelines on trusted credential stores
    - Attribute Authority Operations Guidelines
    - Guidelines on Private Key Protection
- Participation in several OGF security working groups, including the revision of the OGF GFD.125 certificate profile,
- Handling of the policy issues and timetable related to the move of IGTF to the use of SHA-2 hash algorithms,
- Engagement with the EGI federated cloud task force working towards an agreed understanding on the required changes to security policies and procedures and cloud operations to provide secure and available services,
- Contributions to successful security training events in several international conferences and workshops.

From Mau 2014 EGI policy-related security activities as well as the coordination of EGI security operations will continue in order for the EGI infrastructure through the EGI core activities[3], which will be funded through EGI Council Participants membership fees. In addition, security experts are engaging with the EGI Federated Cloud task force to take their expertise and develop methods to ensure the secure sharing of resources using this new technology. This also means that it is important to keep the security experts available and funded in order that they are able to carry out the work.

[3] https://wiki.egi.eu/wiki/2013-bidding/Security_monitoring_and_security_operations_support_tools

4 REFERENCES

R 1	The International Grid Trust Federation, http://www.igtf.net/
R 2	EUGridPMA, https://www.eugridpma.org/
R 3	EGI milestone documents on Security Activity within EGI: MS214 (March 2011), https://documents.egi.eu/document/307 MS224 (March 2012), https://documents.egi.eu/document/965 MS235 (March 2013), https://documents.egi.eu/document/1520
R 4	EGI Security Coordination Group, https://wiki.egi.eu/wiki/SCG
R 5	Joint EGI/PRACE/EUDAT security training and workshop, Linkoping, Sweden 7-9 Oct 2013, https://www.nsc.liu.se/joint-sec-training/
R 6	EGI adopted security policies, https://wiki.egi.eu/wiki/SPG:Documents
R 7	Grid Policy on the Handling of User-Level Job Accounting Data, https://documents.egi.eu/document/85
R 8	Service Operations Security Policy, https://documents.egi.eu/document/1475
R 9	Grid Acceptable Use Policy, https://documents.egi.eu/document/1779
R10	Security at Madrid EGI Technical Forum, 18 Sep 2013, https://indico.egi.eu/indico/sessionDisplay.py?sessionId=49&confId=1417#20130918
R11	Security for Collaboration among Infrastructures, http://www.eugridpma.org/sci/
R12	SCI meetings in 2013: Boulder, Colorado USA, 7-8 May 2013, https://indico.cern.ch/conferenceDisplay.py?confId=246253 Abingdon, UK, 15-16 Jan 2014, https://indico.cern.ch/conferenceDisplay.py?confId=293705
R13	Version 1 of the SCI document published in the proceedings of The International Symposium on Grids and Clouds (ISGC) 2013, March 17-22, 2013, Academia Sinica, Taipei, Taiwan, http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf
R14	SCI at the 20th International Conference on Computing in High Energy and Nuclear Physics (CHEP2013) 14-18 Oct 2013, Amsterdam, https://indico.cern.ch/contributionDisplay.py?contribId=336&sessionId=8&confId=214784
R15	FIM4R paper (https://cdsweb.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf) and most recent meeting of FIM4R (joint with REFEDS and VAMP), https://refeds.org/meetings/oct13/
R16	RedCLARA Virtual Federations Day – presentation on FIM4R by David Kelsey, http://eventos.redclara.net/indico/conferenceDisplay.py?confId=247
R17	EGI Software Vulnerability Issue handling procedure https://documents.egi.eu/document/717
R18	EGI SVG advisories on the wiki https://wiki.egi.eu/wiki/SVG:Advisories
R19	The Security Assessment Plan https://documents.egi.eu/secure/ShowDocument?docid=563
R20	Identifier-Only Trust Assurance Profile, https://www.eugridpma.org/guidelines/IOTA/

R21	Guidelines on the Operation of Credential Stores, https://www.eugridpma.org/guidelines/trustedstores/
R22	Guidelines for Attribute Authority Service Provider Operations, https://www.eugridpma.org/guidelines/aaops/
R23	Private Key Protection Guidelines, https://www.eugridpma.org/guidelines/pkp/
R24	OGF Grid Certificate Profile, GFD.125, https://www.ogf.org/documents/GFD.125.pdf Revised version of this profile (still not finalised) at: http://redmine.ogf.org/issues/65