



GridPP
UK Computing for Particle Physics

GridPP Project Management Board

GridPP3 Milestone 2.2.12 - Security Recommendations

Document identifier :	GridPP-PMB-153- SecurityRecommendations
Date:	31/03/2011
Version:	V1.0
Document status:	Final
Author	D. P. Kelsey/STFC-RAL

Introduction

GridPP3 milestone 2.2.12

Milestone 2.2.12 (31 Jan 2011) was to produce “*Security recommendations for the future*”. The main thrust of this milestone is to ensure that security operations, procedures and policies are well established for GridPP operations in the GridPP4 era.

“Security” is an ongoing process, i.e. one that has no end-point. Operational procedures and policies require constant implementation, feedback, review and maintenance. Security Operations and Policy activities were firmly established during GridPP3 and EGEE-III. The simple “recommendation” is to build on these successes and to take the various activities forward into GridPP4, WLCG and EGI.

The future plans for GridPP security were agreed during 2010 and described in the GridPP4 proposal (http://www.gridpp.ac.uk/docs/gridpp4/GridPP4_Proposal_Final.pdf). GridPP/EGI security activities, many of which are led by GridPP staff, were established during 2010 and reviewed in GridPP3 milestone 2.2.11 (<https://edms.cern.ch/document/1058629/2>).

A brief overview of Security Operations and Security Policy during GridPP4 is presented here. The UK NGI security team leads many of the international security activities (EGI and WLCG). Security in the UK NGI (and hence in GridPP4) implements the local national security operations and policies required by EGI and WLCG. More details are in the referenced documents. This document, in particular, does not cover security middleware services.

The milestone was completed on time (as recommendations were in place and used in the planning of GridPP4 and our involvement in EGI) but the production of this document was delayed by two months (until 31 March 2011) because of the funding uncertainties following CSR2010; we were waiting for notification from STFC of the full GridPP4 Award (this happened on 11 March 2011) and also hoping that more information about future funding for the UK NGS beyond October 2011 would be forthcoming (this did not happen and is now not expected before May 2011).

The UK NGI Security Team in the GridPP4 era

The GridPP4 proposal contains the following words:

“The existing GridPP3 security officer provides coordination that has proved invaluable as the number of identified kernel, package and middleware vulnerabilities affecting GridPP sites has increased, and has ensured that GridPP meets wLCG security requirements. However, as the overall number of UK Grid sites increases, this operational security must be integrated into the larger NGI-based security team. Also, by operating within the NGI this levers matching EU funding for additional staff that cover the additional work.”

It also goes on to say:

“In addition to operational security, GridPP foresees an advantage from working within an NGI in the area of international security policy, a topic where GridPP has established international leadership in the development of wLCG and EGEE security policy. This is recognised in the EGI-InSPIRE proposal where the UK would be funded to provide this work as an EGI Global Task, leveraging matching funding and maintaining the UK’s position at the centre of security work. If EGI does not proceed as planned, or if NGS future funding is not assured, there is still an ongoing requirement in wLCG for GridPP to provide leadership of the global security policy activity. Thus, it is proposed to fund 1.5 FTE in GridPP4 as part of an NGI-based security team. This will cover operational security (1.0 FTE) and security coordination and international policy development (0.5

FTE). This is a reduction from 2.3 FTE funded by GridPP3 in the security area and focuses our effort on the key areas.”

EGI did subsequently proceed as planned. The international security operations and security policy work, with leadership by GridPP members, includes the following activities:

- EGI-CSIRT (see https://wiki.egi.eu/wiki/EGI_CSIRT)
The EGI CSIRT covers all aspects of operational security aimed at achieving a secure infrastructure within EGI and relies on site and NGI security contact information maintained in the GOCDB by each NGI. The EGI CSIRT ensures both the coordination with peer grids and with the NGIs and NREN CSIRTs. 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 (e.g. security drills). Each NGI appoints an NGI Security Officer in order to provide the NGI CSIRT function. The resulting group of NGI Security Officers collaborate as part of the EGI CSIRT.
- EGI SVG (see <https://wiki.egi.eu/wiki/SVG>)
The Software Vulnerability Group has been established to eliminate existing vulnerabilities from the deployed middleware, prevent the introduction of new ones and prevent security incidents. A Risk Assessment Team (RAT) is the core working group within SVG and the main purpose is to handle specific software vulnerabilities reported in the EGI infrastructure. Most of the activities and responsibilities of SVG are done by RAT since software issue handling is by far the largest activity in the SVG.
- EGI SPG (see <https://wiki.egi.eu/wiki/SPG>)
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.
- WLCG Security Policy Coordination (also led by GridPP) is aimed at maintaining "trust" between WLCG participants. The mandate includes:
 - Prepare and maintain WLCG Security Policy covering participants (including Sites, users and VOs) in coordination with EGI, OSG, NDGF, VOs, Sites, etc.
 - Represent WLCG as "relying party" on IGTF (EUGridPMA and TAGPMA). Feed in requirements and report back.
 - Coordinate WLCG and EGI security policy strategy to ensure that common policies are used wherever possible. This work to include the investigation of the production of Security Policy Standards to ease interoperation.
 - Provide advice to WLCG management on any security policy-related issue.

Funding of the UK NGI Security Team in the GridPP4 era

The funding for the UK NGI security team comes from 3 sources; GridPP4, EGI and the UK NGS. The following table shows details of the activities and funding sources. This table is the plan for FY 2011-12 showing effort expressed in Full Time Equivalent (FTE). GridPP4 funding continues at the same rate for all 4 years of the funding. EGI funding currently continues at the same rate until 30 April 2014. NGS4 funding beyond 30 Sep 2011 is not yet known so this will need to be reviewed later.

UK NGI Security Funding (FTE)	EGI funding	GridPP4 funding	NGS3 funding	Total Effort
EGI/GridPP/NGS Security Operations (EGI Global)	0.36	0.36		0.73
EGI/GridPP/NGS Security Operations (International)	0.03	0.24		0.27
EGI/GridPP/NGS Security Operations		0.40	0.21	0.61
EGI SVG (Global)	0.04		0.04	0.08
EGI SPG (Global)	0.20	0.20		0.40
WLCG/GridPP Security Policy		0.30		0.30
TOTALS	0.64	1.50	0.25	2.39