EGI-InSPIRE

GRID SECURITY TRACEABILITY AND LOGGING POLICY

Document identifier	EGI-SPG-Traceability-V1_0
Document Link	https://documents.egi.eu/document/81
Last Modified	14/07/2010
Version	1.0
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	**David Kelsey/STFC, UK**
Document Status	Submitted
Approved by	EGI.eu Executive Board
Approved Date	10/09/2010

Policy Statement

This policy defines the minimum requirements for traceability of actions on Grid Resources and Services as well as the production and retention of security related logging in the Grid.



I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Body	Date
Approved by	EGI.eu Executive Board	10/09/2010

III. DOCUMENT LOG

Issue	Date	Comment	Author/Organization
1.0	14/07/2010	Imported from JSPG policy document with the same title. No change was made to any wording. See https://edms.cern.ch/document/428037 (V2.0, dated 28 Aug 2008) for the old JSPG document.	David Kelsey/STFC
2.0			
3.0			
4.0			

IV. 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 the 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 the ESFRI projects. 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 − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

TABLE OF CONTENTS

1 INTRODUCTION

This policy defines the minimum requirements for traceability of actions on Grid Resources and Services as well as the production and retention of security related logging in the Grid.

2 NOTATION

This document occasionally uses terms that appear in capital letters.

When the terms "MUST", "SHOULD", "MUST NOT", "SHOULD NOT", and "MAY" appear capitalized, they are being used to indicate particular requirements of this specification. A definition of the meanings of these terms may be found in IETF RFC 2119.

3 REQUIREMENTS FOR TRACEABILITY AND LOGGING

The management of risk is fundamental to the operation of any Grid. Identifying the cause of incidents is essential to prevent them from re-occurring. In addition, it is a goal to contain the impact of an incident while keeping services operational. For response to incidents to be acceptable this needs to be commensurate with the scale of the problem.

The minimum level of traceability for Grid usage is to be able to identify the source of all actions (executables, file transfers, pilot jobs, portal jobs, etc) and the individual who initiated them. In addition, sufficiently fine-grained controls, such as blocking the originating user and monitoring to detect abnormal behaviour, are necessary for keeping services operational. It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user.

The aim is to be able to answer the basic questions who, what, where, and when concerning any incident. This requires retaining all relevant information, including timestamps and the digital identity of the user, sufficient to identify, for each service instance, and for every security event including at least the following: connect, authenticate, authorize (including identity changes) and disconnect.

4 PRODUCTION AND RETENTION OF LOGGING DATA

In order to satisfy the traceability requirements, software deployed in the Grid MUST include the ability to produce sufficient and relevant logging, and to collect logs centrally at a Site. The software SHOULD follow any security guidelines on logging defined by the Grid.

The level of the logging MUST be configured by all service providers, including but not limited to the Sites, to produce the required information which MUST be retained for a minimum of 90 days. Grid Security Operations MAY define longer periods of retention for specific services and/or operational requirements. The logs MUST be collected centrally at the service provider level.

5 IMPLEMENTATION

The security architecture and software used in the Grid is under constant change. Grid Security Operations provides detailed requirements on the implementation of this policy. Participants MUST abide by the detailed implementation instructions.