Joint Security Policy Group

Grid Security Traceability and Logging Policy

Date:	**28 August 2008**
EDMS Reference:	https://edms.cern.ch/document/428037
Internal Version:	**V2.0**
Status:	**Released**
Author:	**Joint Security Policy Group**

Document Log			
Issue	**Date**	**Author**	**Comment**
1.0	11 June 2003	Ian Neilson	Draft for Comment
1.1	18 June 2003	Ian Neilson	Some more details and add recommendations to GDB section
1.2	19 June 2003	Ian Neilson	Clarification of process accounting data volume. **Released version from this date on (until V2.0).**
1.3	15 February 2006	Romain Wartel	Policy simplified and made more generic
1.4	12 March 2007	Romain Wartel	Focusing on Resource Providers
1.5	15 March 2007	Romain Wartel	Integrated comments from JSPG
1.6	1 Nov 2007	JSPG	Changes agreed at the JSPG meeting of 29/30 Oct 2007. Includes the addition of draft section on "Motivation" still to be finalised. Title of the document also changed.
1.7	29 Jan 2008	JSPG	Changes agreed at the JSPG meeting today. Ready for wider distribution.
1.7a	2 Feb 2008	JSPG	Changes to section 4 to include the need for security logs to be put in a secure repository.
1.8	26 May 2008	JSPG	Addresses comments received on V1.7a.
1.8a 1.9 2.0	30 May 2008 26 June 2008 28 Aug 2008	JSPG JSPG David Kelsey	Changes agreed at today's JSPG meeting. Includes a MUST for service provider central logging. Address comments received during final call. No text changes from V1.9. Status set to "**Released**" following formal approval; WLCG MB (19 Aug 2008) and EGEE TMB (27 Aug 2008)

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.