EGI-InSPIRE

APPROVAL OF CERTIFICATION AUTHORITIES

Document identifier	EGI-SPG-CAs-V1_0
Document Link	https://documents.egi.eu/document/83
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	Approved
Approved by	EGI.eu Executive Board
Approved Date	10/09/2010

Policy Statement

This document describes the procedure by which the list of trusted Certification Authorities for use in EGI should be created and maintained.

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 changes to wording were made. See https://edms.cern.ch/document/428038 (V3.0, 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

Authentication decisions on the *Grid* are currently based on X.509 Public Key Infrastructures. *Grid* participants, e.g. users, virtual organisations and resources, trust Certification Authorities (CAs) to issue credentials in a manner which unambiguously and securely binds the identity of the *Grid* entity to the issued credential. As such, the set of CAs providing credentials which are accepted by the *Grid* form a fundamental basis on which security within the infrastructure is built.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.

2 INTERNATIONAL GRID TRUST FEDERATION

The *Grid* endorses the work of the International Grid Trust Federation (IGTF) as a body for the accreditation of Certification Authorities. The *Grid* MAY participate in the accreditation standards process of the IGTF through formal membership of the IGTF member Policy Management Authorities.

3 DEFINITION OF APPROVED CERTIFICATION AUTHORITIES

The *Grid* approves the use of authentication credentials issued by:

a) a CA accredited to the IGTF Classic Authentication Profile
b) a CA accredited to the IGTF Short Lived Credential Service (SLCS) Profile
c) a CA accredited to the IGTF Member Integrated Credential Services (MICS) Profile
d) other CAs which MAY be approved by the appropriate Grid management bodies. These SHOULD normally be temporary, pending IGTF accreditation.

Credentials issued by authorities other than those listed above are not approved.

4 OPERATIONAL MATTERS

The *Grid* deployment team SHALL maintain its own repository containing all approved CA root certificates (see section 3) synchronised promptly with each IGTF release.

All *Grid* resources SHOULD promptly install the full list of approved CAs from the repository as packaged, updated and announced from time to time by the deployment team. Decisions not to install or to subsequently remove an approved CA MUST be communicated immediately to the Grid Security Officer.

Individual Grid resources MAY deploy other non-approved CAs for their own local use, providing this is allowed by their local policy and that they take care of the potential problems arising from non-uniqueness of certificate subject distinguished names.