EUGridPMA

P.O. Box 41882
NL 1009 DB Amsterdam
The Netherlands

Our Reference: EGP/090603/2 *Date: Thu, 04 June 2009* *Pages: 3*

The Management Board of EGI-DS and the EGI-DS Policy Board
c/o Ludek Matyska

Dear members of the EGI-DS Management Board and members of the EGI-DS Policy Board:

Greetings on behalf of the European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA). It has been brought to our attention that a specific interaction between the EGI council and the EUGridPMA has been proposed for inclusion in the Memorandum of Understanding for the establishment of the EGI.eu. In this context the EUGridPMA and the International Grid Trust Federation would like to clarify the role and aims of the EUGridPMA, the IGTF, and its Accredited Authorities and Relying Party members.

In summary, based on the arguments given in detail below, we would like to point out that:

- The aim of the IGTF is to enable interoperable open science, by reviewing authorities from any country based on technical merit;
- Relying parties are free to decide whether or not to trust any CA, IGTF accredited or not, and are thus free to remove or to add any additional CAs any time;
- Grid *authorisation* is the appropriate place to control access to resources, not the *authentication* as provided by the EUGridPMA and IGTF.

Specifically, we feel that each site and NGI itself should take decisions on exclusion of particular CAs, and that EGI should encourage full implementation of all IGTF accredited authorities to enable Interoperable Open Science. Excluding specific CAs at the EGI level is likely to impair bona fide collaboration between many NGIs and their own partners in projects in which they participate.
NGIs and sites within the country, or indeed within scientific projects, should retain both the right and technical means to decide who can use their resources. This will only work if someone else has not blocked the authentication at the EGI level.

In the remained of this letter, we would like to clarify these issue in more technical terms.

Background

The IGTF and the EUGridPMA establish common policies and guidelines for authentication management authorities that provide identity assertions to people, network systems and services for use in research and academic e-Infrastructure and grids. The IGTF and EUGridPMA ensure that, within the scope of its Charters, the assertions issued by accredited authorities of any of its member PMAs meet or exceed an authentication profile relevant to the accredited authority[1]. The Accreditation by the IGTF may be used by Qualified Relying Parties to make decisions about trust in the authorities accredited under a specific Authentication Profile.

The IGTF acknowledges and expects each individual resource owner or administrative domain (or ensembles thereof such as an NGI) to retain its full rights and autonomy with regards to its acceptance policy for authentication, like it has similar obvious authority over any authorization and access control policies. This can both be by adding additional trust anchors that are not accredited under any IGTF profile (such as training services, or CAs from countries whose authority is not or not yet accredited), as well as ignoring those authorities that violate local operational or security policies.

Apart from these individual veto's at the *authentication* level (trusting or not trusted a particular CA at a particular site), which every site and NGI can apply autonomously, the Grid software has additional *authorization* controls. These controls work both ways, protecting users from sites they do not trust, and sites from resources they do not trust.

- Users can use grid software mechanisms to direct their workload to particular destinations, and the user's organisation hosting grid brokering services can prevent un-trusted resources from being included in the resource matching list
- Resource owners and community managers can identify un-trusted individuals and prevent them from accessing their resources using per-user or per-community blacklisting facilities present in all Grid middleware.

With these two mechanisms, all grid participants can autonomously control their use of the Grid resources, and have resilience to a failure in any individual system.

[1] Individual authorities are accredited by any of the three members of the International Grid Trust Federation: the EUGridPMA covering Europe, the Middle East and Africa; the APGridPMA, covering the Australasian-Pacific region and the Indian subcontinent; and the TAGPMA, covering the Americas. There is no material difference between the accreditation by any of these three PMAs. For technical information regarding the Authentication Profiles or the accreditation process, we would like to refer you to the IGTF Web Site at http://www.igtf.net/

A close analogy in the 'real' world are passports: it is widely accepted to recognise passports issued by a nation state as authentic, but to still deny access to any individual holding such a passport. The Grid controls work in the same way, with *authorization* enforcing the vetoing discussed above.

In this context, it may also be illustrative to review the way in which two Relying Party members of the IGTF members (of both EUGridPMA and TAGPMA) use the accreditation: the Enabling Grids for E-Science project (EGEE) and the world-wide LHC Computing Grid Project (LCG) both have adopted a specific policy regarding the "Approval of Certification Authorities"[2]. In this policy, the Relying Parties approves the use of authorities accredited under several specifically names authentication profiles, and generally expects these authorities to be installed and maintained by all participants in their projects. At the same time it explicitly acknowledges that every individual resource owner may decide not to install or to subsequently remove an approved CA; in this case the only obligation a resource owner has is to inform (the project's) Grid Security Officer.
The EUGridPMA and IGTF support this use of the accreditation process, as it acknowledges that a trust decision always rests with the individual operational and administrative owners of the resources.
The EUGridPMA and the IGTF already work with and supports large scale Relying Parties on a national, European, and global basis, including EGEE, DEISA, TERENA, the US-based Open Science Grid, TeraGrid and PRAGMA. The EUGridPMA and its Members are willing and able to support the EGI infrastructure on the same basis as such support is currently given to all its Relying Parties.

The EUGridPMA looks forward to a fruitful collaboration with the EGI organisation and welcomes EGI as a Relying Party member to the PMA, in accordance with its Charter. The EUGridPMA continues to expect that, like today, national projects and infrastructures, including the individual National Grid Initiatives, will be represented through the Accredited Authority in their country.

With Kind Regards,

David Groep
Chair of the EUGridPMA.

[2] JSPG "Approval of Certification Authorities", https://edms.cern.ch/document/428038, adopted by EGEE and wLCG management August 2008