



EUGridPMA
dr D.L. Groep, Chair

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

Our Reference: EGI-response-20080731.docx

Date: Thu, 31 July 2008

Pages: 5

The EGI-DS Project

Dr Dieter Kranzmueller

Altenbergerstr. 69

A-4040 Linz, AUSTRIA

Dear Dieter Kranzmueller:

Greetings on behalf of the European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA). We write to you in response to your public call for comments on the EGI-DS Blueprint Proposal.

- Considering that the EGI-DS Blueprint Proposal references the EUGridPMA and proposes that a future EGI participates in the EUGridPMA and IGTF work;
- considering that the Blueprint Proposal leverages the existence of the EUGridPMA and IGTF coordinated trust fabric for specific elements of its operational and administrative procedures;
- considering that the EUGridPMA seeks to encourage and engage in a fruitful collaboration with the EGI-DS project, the NGIs, and the future EGI organisation;
- considering that the EGI Blueprint Proposal makes or implies certain specific assumptions about the structure and operations of the IGTF trust fabric that are not in line with current state and future developments of the trust fabric;

we would like to clarify the structure of the current IGTF trust fabric and its future development, and point out the inconsistencies we perceive between the current EGI-DS Blueprint Proposal and the IGTF trust fabric. We hope this letter will both improve the understanding of the trust fabric as well as foster a fruitful collaboration between EGI-DS and the EUGridPMA.

The IGTF Trust Fabric Model in the EUGridPMA

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 grid use. It ensures compliance to these guidelines amongst the participating CAs by peer review, by implementing audit mechanisms, and the promotion of current best

practices. It implements these goals by accrediting authorities according to these guide lines, aiming to serve the largest possible community with a small number of stable Authorities that are operated as a long-term commitment.

These Authorities may use several mechanisms to assert identity: either through a 'classic' Public Key Infrastructure with direct identification of the users, or through other identity management technologies (such as Short Lived or Member-integrated Credential Services that leverage existing or emerging federations based on Shibboleth, eduGAIN, and similar technologies).

National and Regional Authorities

The EUGridPMA aims to accredit a single Authority per country or large region. In several cases, these authorities have direct support from their national ministry (usually of research and education), whilst others are associated with an (emerging) national grid initiative, or are the de-facto centre of grid authentication in their country.

At this point in time, the EUGridPMA covers 25 of the 27 EU member states (all except for Luxemburg and Malta) with a national or regional CA as well as 14 other countries in and around Europe and Africa.

In all cases, the national authorities are committed to support the entire research and educational community in their country, even though they may be funded and operated by more narrowly-scoped organisations. Some authorities go beyond that and offer 'catch-all' services for a larger constituency, such as Grid-FR (operated by CNRS), SEE-GRID (operated by GRNET), and the Italian CA (operated by INFN).

In several cases, multiple countries have joined forces and together use the services of a *regional* Authority: the most prominent ones being the NorduGrid CA (serving Denmark, Sweden, Finland, Norway and Iceland) and the BalticGrid CA (serving Estonia, Latvia and Lithuania). These regional CAs are a welcome and permanent feature of the IGTF and EUGridPMA.

Some countries have adopted national identity cards that are in themselves capable of bearing an electronic identity assertion. The Estonian ID card for example has a very large national coverage and is suitable for grid authentication. In the near future we may see such national ID cards being used for grid authentication, in lieu of a separate 'grid authority' in these selected countries.

Identity assertions for guests, visitors and expatriates

At the same time, national authorities serve all people resident in a country, foremost including any guests and temporary visitors that reside in a country for a longer or shorter

period of time. As such, not all users that have their identity asserted by a specific CA actually have an association with the country in which the issuing authority resides.

Conversely, national CAs may and will issue assertions to their nationals, even though they are no longer resident in their country and may be employed by organisations in entirely different countries. In this case, their employment and the responsibility therefore resides with their new country of work, not the country in which the issuer CA is residing.

Subject naming of users and other end-entities

There may be a ill-advised tendency to infer from the subject name of a certificate attributes of the user such as nationality or national affiliation. In some cases, authorities assign subject names that contain a country name or another identifier that suggests such a national scope. However, increasingly subject and issuer identifiers are entirely opaque, and are opaque on purpose. Especially for the regional CAs and catch-all CAs (such as operated by NorduGrid, BalticGrid, Grid-FR, ESnet, etc.) the subject name contains only the name of the person, plus a randomly-generated number to ensure uniqueness. These subject names *do not* contain any hint about the country of origin, affiliation or citizenship.

About inferring NGI affiliation from issuer or subject name

In no case may 'NGI affiliation' may be induced from the issuing CA or the assigned subject name of the user. Issuer and subject names must be treated as opaque identifiers that uniquely identify a user, are guaranteed to be unique, and are traceable for the validity period of the assertion (although exercising the traceability may require court orders in certain jurisdictions).

Attempting to rigidly keep the association between the country of the issuing CA and the chosen country of employment would require that these users give up their national citizenship, which is clearly unacceptable. This is especially true for those CAs that (also) leverage national identity cards.

Future development of the trust fabric

Increasingly, identity management is being organised based on federations or user home organisations (universities, research laboratories, and other institutes of higher education). These federations themselves subsequently confederate to form trans-national trust domains (such as envisioned in the eduGAIN approach). It is likely that in the longer-term future, the issuance of also PKI identity certificates will be closely linked to these federations and confederations. In particular, it is conceivable that a single X.509 Certificate Authority will front an entire confederation, serving multiple or even the majority of countries in Europe.

EGI-DS Blueprint Proposal assumptions on the Trust Fabric

In several places the EGI-DS Blueprint Proposal makes specific assumptions about the trust fabric that are not aligned with its current or future structure. We would like to point out these inconsistencies:

- In section 5.1.6, “NGI Resource Estimates” task O-N-7, mandates the existence of an “NGI Certification Authority to distribute X.509 certificates to users and servers in the region”.

Bearing in mind the aim of the EUGridPMA to serve the community with a small number of stable CAs, this phrasing appears to imply that the NGI must establish a CA, even when an existing CA inside that country already exists (e.g. supported by a different ministry, having been the de-facto grid CA in good standing for a long period of time, or being operated by a nationally recognised entity supporting research and education, such as a National Research and Educational Network organisation), and is willing and able to serve the NGI.

We consider the needless duplication of overlapping CAs that could ensue to be detrimental to the trust fabric, and recommend that in such cases adequate support is given to the existing accredited national authority.

- In section 8.3 “NGI notice of leaving EGI.ORG”, states that when an NGI leaves EGI.org, virtual organisations (VOs) can “remove all users with certificates issued by the NGI country from their VO”

From the description of the IGTF and EUGridPMA trust fabric structure given, it will be apparent that the assumed association between ‘certificates issued’ and ‘the NGI country’ does not exist. The IGTF and the EUGridPMA member authorities cannot determine or define NGI membership, and neither issuer nor subject name of a certificate may be used to infer such an association. In the future, when trans-national confederations will be more prominent, any perceived association today will only weaken.

We consider the suggested association between certificate issuance and NGI to be incompatible with the current and future structure of the IGTF trust fabric.

- Section 8.4 “Transition of the accounting and resource system from EGEE to EGI.ORG” states on page 62: “There is the issue of the catch all CA, currently operated in France, for NGI who do not currently host a CA themselves which need to be addressed by the NGI if they wish to host a CA to overcome this anachronism.”

Since this line appears in the context of a section on accounting and resource usage measurement, it implies that either the issue or the subject name of users (or

resources) will be used to assign resource usage to NGIs. As stated earlier, the IGTF and EUGridPMA member authorities cannot determine or define NGI membership, and neither issuer nor subject name of a certificate may be used to infer such an association. We therefore also do not see how, in a model that correctly assigns roles and responsibilities for determining NGI membership, the use or absence of a catch-all CA affects the accounting and resource system in either EGEE or EGI.ORG

We consider the suggested association between certificate issuance and NGI to be incompatible with the current and future structure of the IGTF trust fabric.

Furthermore, we deplore your choice of the term “anachronism” in relation to the catch-all CAs.

We appreciate the fact that a catch-all CA services is explicitly mentioned in the EGI-DS Blueprint Proposal, and that the Proposal foresees supporting this activity (O-E-5, p. 28), as well as the encouragement for NGIs to support the trust fabric.

Summary

We appreciate the support for the EUGridPMA and IGTF that is eminent from the EGI-DS Blueprint Proposal. The EUGridPMA is willing and prepared to work with the EGI-DS Project and a future EGI Organisation to provide a robust and reliable trust fabric for authentication in collaboration with our IGTF partners and our members. We see clearly shared goals for a future authentication and authorization, and are pleased to see that the EGI-DS Blueprint Proposal acknowledges the importance of existing and emerging national authentication and authorization federations and their confederation at a trans-national scale.

We realize that resolving the issues and misalignments identified may require technical discussions for which there is insufficient time available given the mile stones of the EGI-DS project. In that case, we propose that the specifics about how NGI membership for users is defined is left for a future technical document and that such specifics as identified above be rephrased such that they are at least not known-inconsistent with the IGTF trust fabric.

With Kind Regards,



David Groep

Chair of the EUGridPMA.