International Grid Trust Federation
c/o D.L. Groep

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

Our Reference: EGP/DG/060502.01 Date: Tue, 02 May 2006 *Pages: 2*

To the Grid Middleware Providers

Amsterdam, May 2nd, 2006

THIS IS A DRAFT FOR DISCUSSION ONLY –AT THE CAOPS-WG IGTF SESSION #2 FRIDAY

Greetings!

The International Grid Trust Federation, IGTF, is the overarching federation of Grid Authentication Policy Management Authorities that insures global harmonization amongst identity providers for identity tokens in the scientific and academic world. The members of the IGTF are the Asia Pacific Grid PMA, the European PMA for Grid Authentication in e-Science, and The Americas Grid PMA. The membership of the PMAs, the Issuing Authorities, provides the vast majority of identity certificates for the Grid today. These identity certificates are of approximate parity with respect to quality, strength of underlying identity vetting, and protection of the private data held by the users and services.

Over the past years, the 'trust fabric' managed by the IGTF members has grown significantly. Currently it is estimated that over 50 000 identity certificates are valid concurrently, and this number is growing steadily. In the near future, the advance of credential translation services based on the Short-Lived Credential Services (SLCS) Authentication Profile, and the introduction of classic Certification Authorities (CAs) based on large-scale distribution of hardware tokens will give rise to additional complexity in the trust fabric. In particular, we expect:

- a larger number of identity providers, possibly exposed to the Grid relying parties by 'proxy' authorities based on the SLCS Profile;
- a wider variety in the 'quality' of the user-held private data used to protect their identity certificates (i.e. by the use of USB hardware tokens, or integrated smart cards issued by either an institution or by the national or regional government);
- coupling and clustering of identity providers via bridging technology, in the latter case likely supported by a single proxy authority to hide complexity
- more variation in the quality of the identity tokens (different levels), as can be seen in other large-scale identity management deployments[1]

At the same time, current issues such as the coordination of a globally unique namespace for subject identifiers, and the enforcement thereof by our relying parties, will remain essential.

To manage this complexity, the Issuing Authorities within the IGTF will soon have to start employing additional technical means of conveying credential quality information and specific

[1] In particular, we refer to schemes such as the e-Authentication standards as in use in the U.S.A. for their 'Federal Bridge' system, see for example NIST SP-800-63.

assertions to relying parties. But for this information to be useful to the relying parties, they will need to have software that supports discrimination based on these attributes and guidelines.

We therefore ask you, the developers and packagers of the software used for authentication by our Relying Parties (RPs), to provide mechanisms for our RPs to:

- enforce externally-defined namespace constraints, such that relying parties can uniquely assign namespaces for subject identifiers to specific issuing authorities.

  This one the one hard enables RPs to ensure that there are no overlaps, and it also enables relying parties to restrict the namespace they accept from any the issuing authority to only those identifiers that are agreed to be subject to a specific Authentication Profile. Note that the identifier namespace is used for this purpose to allow interoperation between general-purpose (commercial) Authorities and the trust fabric.

- make validation and subsequent authorization decision based on the (set of) Policy Object Identifiers embedded in any of the certificates that are part of the certificate chain used to authenticate end-entities.

  The Policy OIDs (X.509 version 3 extension OID 2.5.29.3) are multi-values sets of OIDs that enumerate the policies under which a certificate was issued. Accredited Authorities currently supply at least one Policy OID that refers to their own CP/CPS. In the near future, the Policy OID extension will be multi-valued, and contain OIDs for

  - *the IGTF Authentication Profile under which the issuing authority has been accredited (in end-entity certificates)*
  - *zero or more identifiers for One-Statement Certificate Policies (1SCPs), that may for example indicate whether the private key pertaining to the certificate is stored and fixed to a specific hardware storage (USB key, smart card) and cannot be extracted*
  - *authentication level (e.g. with respect to NIST SP800-63) for the underlying identity assertion associated with a certificate*

  These policy OIDs, and ranges thereof, should be interpretable by the software used by RPs in order to make validity and subsequent authorization decisions.

We kindly ask you to consider implementing software that enables decision making based on these additional capabilities, such that our relying parties can inspect and act upon these qualifiers and thus make more informed authentication decisions. We feel that having such controls is essential for the Grid to grow and prosper and reach the ever larger audience, whilst retaining the authentication quality we have today.

It would be highly appreciated if the syntax in which these decisions are expressed would be coordinated amongst the software providers via the usual channels.