IGTF POLICY FOR HIGH-LEVEL CERTIFICATION AUTHORITIES

Non-End Entity Issuing CAs

1. PREAMBLE

This document describes the IGTF (http://www.gridpma.org/) recommendations for Certificate Policies (CPs) for Grid Certification Authorities (CAs) that issue certificates to subordinate CAs.

1.1 Document Identification

Document OID	TBD
GGF Identifier	GGF-CAOPS-blah-blah
Status	DRAFT
Contact	info@gridpma.org
URL	

1.2 Document History

Version	Date	Circulation	Comment
0.1	2006-08-14	TAGPMA	Initial version by Jens Jensen, UK e-Science CA, CCLRC Some bits based on an email from Michael Helm, DoEScienceGrid, ES-NET, sent to TAGPMA 2006-07-11.
0.2	2006-08-15	TAGPMA	Contributions and suggestions from David Groep, DutchGrid CA, NIKHEF.

1.3 Document Change and Approval

This document must be modified in such a way that existing section numbers do not change.

Change procedure and approval TBD.

2. INTRODUCTION & TERMINOLOGY

With current (2006) Grid middleware, it is necessary to review and deploy not just the accredited CAs but also the higher level ones, even when the higher level CAs have other subordinates that are not issuing Grid certificates, or are not meant to be accepted (defined below) by an IGTF PMA. Other Grid CAs are themselves switching to hierarchies for various reasons, some of which are discussed informally below (section 2.1).

This document describes the IGTF recommendation and requirements for the policy of such a high level CA, and for review and PMA acceptance of such a CA. The CAs are referred to as "High Level Certification Authorities" (**HLCA**s) throughout this document, mainly for lack of

a better word. A HLCA is thus a *root* CA (self-signed), or an *intermediate* CA (part of a validation chain up to a root, but not issuing EE certificates).

It is generally assumed throughout this document that the PKI forms a *tree* with a single Root, and thus that all validation chains can build one and only one path to the Root.

2.1 The Role of the HLCA

The role and *raison d'être* of the HLCA is usually one or more of the following. A CA Manager who writes the CP for a HLCA may consider these points.

1. A HLCA should define a common community for all its subordinates, and can impose policy restrictions on their policies.

2. In certain cases, a resource provider may review the CP/CPS of the HLCA and decide to implicitly trust all its subordinates. For this purpose, for some types of middleware, it is sufficient to install the certificate of the HLCA itself. The HLCA may forbid this implicit trust in its own policy, in which case a resource provider must review each individual subordinate.

3. HLCAs allow different subordinates to have different assurance levels, or serve different purposes in the same community, but there is usually some modest advantage in tying them under a common HLCA.

4. In practical terms, running and supporting a production Grid CA is always a lot more effort than anyone (who hasn't done it before) ever estimates. One should think carefully whether a hierarchy is really needed. For example, if distributed sites wish to issue their own certificates, but all to roughly the same assurance level, it is often better to make them RAs.

   Having said that, non-EE CAs and credential conversion CAs (like SLCS and MICS(?)) are sometimes easier to run and support than Classic EE-issuing CAs. A hierarchy is often more manageable if there are only few such CAs.

2.2 Accreditation and Trust

Usually PMAs *accredit* CAs. In this document we shall distinguish between *Accreditation* and *Trust*. The purpose of this document is that HLCAs should not be Accredited, but only Trusted, by the IGTF PMAs. A CA is either Trusted or Accredited (or neither), never both: although the Trusted state can be seen as a subset of Accredited, an Accredited CA is not considered Trusted in this terminology. For convenience, we introduce the word *Accepted* to mean "Trusted or Accredited". In this respect, terminology differs from that used in the PMA charters.

The CAs to which the HLCA issues certificates are referred to as its **Subject CA**s. Any CA in the hierarchy below the HLCA is referred to as a **Subordinate CA**, i.e., Subordinate CA is a CA whose certificate validation chain contains the certificate of the HLCA.

Acceptance refers to a CA whose CP/CPS has been reviewed by a PMA according to the applicable profiles, and has been declared either *Accredited* or *Trusted*.

Accreditation refers to the case described in the IGTF charter and covered in the charters of the PMAs where a CA is:

- A full member if its accrediting PMA, with voting rights, represented by its CA Manager who shall attend PMA meetings according to the PMA's requirements; and,

- Its certificate is made available from the PMA's repository, along with pointers to the all necessary documentation and information (CP/CPS, CRL if applicable, etc); and,

- Its CP/CPS has been reviewed by the PMA according to the applicable AP, and found acceptable; and, in particular,

- The CA is trusted by the PMA to issue certificates in its designated namespace.

Trusted refers to the limited case where a CA is:

- Not a member of the accrediting PMA, and has no voting rights; and,

- Its certificate and other relevant information is published by the PMA's repository, as in the case of an accredited CA; and,

- Its CP/CPS has been satisfactorily reviewed by the PMA according to ***this document***; and,

- At the PMA's discretion, depending on the CA's policy, each Subject CA certificate issued by the CA may itself be subject to PMA review and Acceptance.

- The CA is trusted by the PMA to issue certificates in its designated namespace.

The rationale behind this is that the middleware needs to build a trust chain to a root, but each CA above the Accredited CA need not itself be Accredited, but they do need to be Trusted.

In particular, Trust leaves it to the PMA to decide whether each of the Subject CA certificates issued by the HLCA is itself subject to an acceptance review by the PMA. Such a requirement shall normally be imposed if the Subject CAs have significantly different communities, policies (in particular, assurance levels), or purposes. Conversely, if the HLCA imposes sufficient restrictions upon its Subject CAs that the PMA feels that they can all be trusted, e.g., if they all have the same CP but just happen to be geographically distributed, the PMA can at its discretion decide to trust *all* Subject CAs issued by the HLCA.

We shall refer to the former case – each Subject CA is reviewed for Acceptance – as **Explicit Acceptance** of the Subject CA. This PMA policy is expressed in RP name space restrictions by explicitly naming all trusted subject DNs.

Conversely, we refer to the latter case – a (possibly proper) subset of Subject CAs is automatically accepted – as **Implicit Acceptance** of the Subject CA. This is encoded in RP namespace restrictions using a string followed by a wildcard (in the default OpenSSL stringification – see section 3.2.3).

2.3 Other Terminology

Standard Grid CA terminology and abbreviations are not explained in this document.

RFC Terminology:

1. In this document, the keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL, NOT", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119.

2. The keywords "SHOULD" and "RECOMMENDED" are to be interpreted as follows: there may exist valid reasons in particular circumstances to ignore a particular item; in that case the full implications must be understood and, for a CA to be Accepted by its PMA, or to remain Accepted, the CA manager must explain the reasons before the PMA.

3. The keywords "SHOULD NOT" and "NOT RECOMMENDED" are to be interpreted as follows: there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful; in that case the full implications must be understood and, for a CA to be Accepted by its PMA, or to remain Accepted, the CA manager must explain the reasons before the PMA.

4. A requirement that a PMA "SHOULD" (resp., "SHOULD NOT") do a particular action, means that the PMA should decide in quorum whether it is acceptable to not do (resp., do) this action.

3. REQUIREMENTS AND RECOMMENDATIONS

This section describes the requirements and recommendations for the policy of a root or intermediate CA; one that does not itself issue certificates to EEs – hereinafter referred to as "HLCA".

To some extent, this document relies on being recursive: if a HLCA is intermediate, its own issuer is itself a HLCA, and this document applies to it, too. However, there are cases where IGTF CAs are issued by HLCAs which are not themselves IGTF CAs. Nevertheless, it is the purpose of this document that even non-Grid HLCAs SHALL be satisfactorily reviewed according to this document prior to being Trusted by a PMA.

3.1 CP and CPS

1. A HLCA must have a CP, and a CPS conforming to the CP. New CAs SHOULD structure them according to RFC3647.

2. A HLCA MUST publish its CP and its CPS, and its own certificate.

3. A HLCA MUST be a Classic CA, except as amended by this document, and in particular section 3.3 below.

4. A HLCA's CP MUST be consistent with the CP of its Issuer, and that of its Issuer's Issuer, and so on, up to the Root. A HLCA SHOULD describe the hierarchy into which it fits; at least the path up to the Root.

5. A HLCA SHOULD define its community consistently (i.e., to have the same community for all its Subordinates). The community of a HLCA MAY be a proper subset of that of its issuer.

6. A HLCA MAY impose restrictions on the CP and CPS of its Subordinates, other than those described and required by this document. A HLCA MUST NOT impose restrictions on a HLCA that is not a Subordinate of itself.

3.2 Namespaces

1. A HLCA MUST document its namespace, both its own name and those of all certificates it issues.

2. A HLCA MUST impose the restriction on all its Subordinates that they issue in distinct namespaces. This requirement MAY be imposed by the HLCA's policy only, but MUST be reflected accordingly in the policies of the Subordinate CAs (cf. item 1).

3. A HLCA and all its subordinates MAY have a common namespace root, i.e. RDNs which are common to DNs issued. If so, they MUST be the leftmost, when written in default OpenSSL format (rightmost by RFC2253).

4. An HLCA MUST publish, and provide to the PMA for review, its namespace restriction (for use by RPs) consistent with the PMA's decision whether to Accept its Subject CAs Implicitly or Explicitly, and consistent with item 3.2.1 and 3.2.3.

3.3 Certificates and Revocation

1. Normal IGTF practices and policy requirements for a Classic CA SHOULD apply to any HLCA, except as stated and amended in this section.

2. A HLCA SHOULD NOT issue EE certificates. If it does, they MUST be the minimum necessary for its own operation.

3. If the HLCA is a Root, it SHOULD keep its private key and associated signing entirely offline.

4. If the HLCA is a Root, its own certificate SHOULD have a lifetime not exceeding 20 (twenty) years, and no less than 10 (ten) years.

5. Certificates issued by the HLCA SHOULD have a lifetime no less than 2 (two) years and no more than 5 (five).

6. The CRL SHOULD be refreshed at least once every year.

3.4 Acceptance Procedure

Briefly, for any CA seeking Accreditation, the CA Manager must ensure that a Trusted chain is built up to a Root. For this purpose, the CA Manager of the CA seeking Accreditation may represent all the HLCAs of the CA seeking Accreditation, if the HLCAs themselves are not to be Accredited, but only Trusted, by the PMA.

1. Each PMA MAY introduce stricter requirements upon HLCAs than those described in this document. If so, they MUST be documented and published by the PMA, and the PMA MUST ensure that those requirements are reviewed, and updated if necessary, whenever this document changes.

2. The CA Manager of ***any*** CA seeking Accreditation from a PMA MUST ensure that ***all*** HLCAs above it in a suitable chain up to a Root, are Accepted by the PMA.

3. The CA Manager of ***any*** CA seeking Accreditation MAY represent HLCAs above the CA before the PMA ***if*** the HLCAs in question are to be Trusted by the PMA.

4. If applying for Accreditation for a HLCA,

    a. The CA Manager MUST appear before the PMA to present the HLCA's CP/CPS.

    b. The CA Manager MUST in particular get agreement from the PMA whether Subject CAs are Implicitly or Explicitly Accepted.

5. The CA Manager MUST ensure that the HLCA issues in a namespace, and MUST supply a signing policy file, such that ***all*** Explicitly Accepted Subject CAs are admitted, and ***no*** Subject CA which has not been approved for Implicit Acceptance by the PMA is admitted.

6. This document does not require that all Subject CAs of an Accepted HLCA should themselves be Accepted.

    Nor does this document require that all Accepted Subordinates of an Accredited HLCA should themselves be Accredited – they MAY be Trusted.

4. EXAMPLE

Non-normative examples of structuring a hierarchical Grid PKI.

4.1 Descriptive picture here

4.2 Extensive PKI example

TODO