Category: guidelines document
Status: DRAFT
Document: AP-HLCA-1.0beta-20110805.doc
Editor: davidg
Last updated: Mon, 09 May 2011, revision 12
Total number of pages: 7

Authentication Profile for Higher Level Certification Authorities

Abstract
When an issuing CA is Accredited under any of the Authentication Profiles for issuing CAs, the certificate with which it signs end-entity certificates is published in the IGTF distribution along with any certificates in a Trust Path to a self signed Root. However, these high-level authorities are only trusted in a very limited sense, especially when IGTF-recommended Relying Party Defined Namespace Constraints ('signing policies') are applied that limit the effective scope of these authorities in a trust anchor store. As such, different considerations with respect to trust apply to these CAs.

Table of Contents

1 About this document

In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119. If a 'should' or 'should not' is not followed, the reasoning for this exception must be explained to the PMA to make an informed decision about accepting the exception, or the applicant must prove to the PMA that an equivalent or better solution is in place.

2 General Architecture

When an issuing CA is Accredited under any of the Authentication Profiles for issuing CAs, the certificate with which it signs end-entity certificates is published in the IGTF distribution along with any certificates in a Trust Path to a self signed Root. Although not strictly needed for trust establishment, nevertheless the majority of software constructing trust paths, in absence of the client providing a trust chain, requires the CAs needed to construct a trust path up to a self-signed CA certificate to be pre-installed.

2.1 Reasons for pre-provisioning trust paths

Requiring the full Trust Path in the trusted certificate store is a good idea for the following reasons:

- Having the Trust Path in the trusted store prevents attacks that aim to subvert certificates by faking CA certificates.
- All CRLs associated with certificates in the Trust Path are refreshed regularly and cached locally.
- Namespace enforcement: Relying Parties can restrict namespaces of CAs to a subset of its normal namespace (see [RPDNC]).

The CAs in the Trust Path, excluding the Accredited CA, 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). This document describes the IGTF requirements for such CAs.

Unless mentioned otherwise, it is 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. Indeed, Trust Paths are usually built based on the names of the CAs.

It is assumed that a CA operates with a single certificate. If a CA operates with more than one certificate, then for the purpose of this document, each such certificate is considered an independent CA.

2.2 HLCA Policy Considerations

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. If the policy of a HLCA is strong enough, a resource provider may decide to implicitly Accept all its Subordinates (i.e., Accept any Subordinate without having reviewed it individually.) In this case, they can be added directly to the distribution, thus creating a slightly more dynamic hierarchy.
   [Rationale: to some extent we can already dynamically deploy new CAs into trust anchors. If in the future we support TAMP [TAMP], or some other process for dynamically deploying

middleware – or support "traditional" security infrastructures which permit clients to send intermediate CA certificates on authentication – in these cases in may be beneficial to have a "fast track" approval for a new Trust Anchor, similar e.g. to the deployment of a rollover certificate. If the *issuer* constrains the Subject to such an extent as to ensure that the Subject itself is accreditable, the Subject CA can obviously be deployed immediately without passing through a lengthy review.]

3. HLCAs may allow different subordinates to have different assurance levels, or serve different purposes in the same community.

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) would think. 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 such as 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 Classic EE-issuing CAs.

5. A CA certificate can be revoked if it is signed by a HLCA. Otherwise the CA will have to revoke itself, and the efficacy of this obviously relies on whether the middleware checks the CA certificate against *its own CRL* at the time of reliance. If there are circumstances where the IGTF considers it necessary to be able to revoke a CA (e.g. if it is Online), it is best to make it Subordinate to a Root.

6. A CA whose Subjects are themselves CAs can be used to define a common purpose or community for those Subject CAs.

Bridging is not considered in this document.

3 HLCA Policies

3.1 Terminology

In this document we distinguish between *Accreditation* and *Trust*. PMAs *Accredit* CAs. 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 CAs*. Any CA in the hierarchy below the HLCA is referred to as a *Subordinate CA*, i.e., Subordinate CA of a HLCA is a CA whose certificate validation chain contains the certificate of the HLCA somewhere in the chain.

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 means 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,
- It has passed an operational review according to the practices of the relevant PMA; and,
- The CA is trusted by the PMA to issue certificates in its designated namespace.

Trusted means 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 the most recent version of *this document*; and,
- It has passed an operational review to determine whether it meets the operational requirements imposed by *this document*; and,
- The PMA has decided whether to implicitly Accept any or every Subordinate CA of the CA being reviewed, or whether any Subject CA should itself be subject to an Acceptance review; and,
- The CA is trusted by the PMA to issue certificates in its designated namespace.

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 – some or all Subject CAs are automatically Accepted – as *Implicit Acceptance* of these Subject CAs. This is encoded in RP namespace restrictions using a string followed by a wildcard (in the default OpenSSL stringification).

The following terms are used throughout this document

Acceptance	means Trusted or Accredited, as defined in section 2.2.
Accredited	means accredited by a PMA as defined in section 2.2.
AP	IGTF Authentication Profile, a set of requirements for CAs issuing EE certificates.
CA	CA, for the purposes of this document, means a Trust Anchor according to [PKIX]: "A trust anchor is an authoritative entity represented by a public key and associated data."
EE	End Entity (qv).
End Entity	means an entity whose certificate is not a CA certificate.
HLCA	means a CA which issues certificates to CAs, as defined in section 2.
IGTF	International Grid Trust Federation (www.igtf.net)
Intermediate	of a CA, means a HLCA which is not a Root.
Namespace	See the IGTF RPDNC document.
Offline	of a physical machine, means that it is not, and has not been, connected to any network at any time with the operating system that it is currently running. See also section 3.3.

Online	means not Offlline.
PMA	Policy Management Authority, the formal members of IGTF (qv). CAs are reviewed by a PMA and become members of it once they are Accredited.
Root	means a self-signed certificate, or a CA with self-signed certificate, depending on context.
Subject CA	of a CA, means a CA certificate signed by the CA's certificate.
Subordinate CA	of a CA, means another CA whose certificate validation chain to a Root contains the certificate of this CA.
Trusted	means trusted for the purpose of being distributed with the PMA distributions according to the definition in section 2.2.
Trust Path	means the certification path (i.e., a chain of certificates) from a given certificate to a Root *as defined by the subject distinguished names* of the CAs in this path.

3.2 Policy Requirements

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". The references to sections of RFC3647 are meant as a guide; they do not impose the requirement that the information be described fully or in part in those sections.

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 Grid 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.

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

   It is RECOMMENDED to format according to RFC3647 and leave out the sections saying "no stipulation" (if there are many of those) but keep the numbering.

2. Repository obligations {2.1, 2.4}. The CP and the certificate of a HLCA, MUST be published {2.1, 6.1.4}. The CPS SHOULD be published. The PMA SHOULD be given access to the CPS for the purpose of reviewing it. If not, the PMA MUST have a report from an approved auditor sufficient to verify that the CPS implements the CP, and is being followed, and complies with the requirements of this document. A fee MUST NOT be charged for access to CP or CPS.

3. 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. [Rationale: a CA MAY impose restrictions on its Subordinates (item 6); in this case this item says Subordinates MUST comply with them.]

4. A HLCA SHOULD describe hierarchy or hierarchies into which it fits {1.1, 1.3.1}. A HLCA MUST describe its Trust Path.

5. A HLCA MAY define a consistent community for all its Subordinates {1.1, 1.3.3}. The community of a HLCA MAY be a proper subset of that of its issuer – if so, it is RECOMMENDED that the HLCA describes this. [Rationale: this is one of the use cases (above) for HLCAs.]

6. A HLCA MAY impose restrictions on the CP and CPS of its Subordinates, other than those described in and required by this document. In particular, Subordinates MAY be covered by the same CP and/or CPS as the HLCA.

3.3 IGTF Recommended Relying Party Defined Namespace Constraints

1. The Trust Path from the Root to the EE-issuing CA MUST be documented {1.3.1}. Names SHOULD be X.500 distinguished names {3.1.1}. The Namespace of the HLCA SHOULD be documented {3.1.4 }. [It should be possible to write a signing policy for the HLCA describing the Trusted Path from the Root to the EE-issuing CA.]

2. Any single Subject distinguished name MUST be linked to one and only one Subject over the entire lifetime of the HLCA it MUST NOT be linked to any other Subject {3.1.5}. [A Subject by definition is a single Subject CA possessing a single certificate, except when rolling over.]

3. A HLCA with implicitly Accredited Subject CAs MUST ensure that the Subject CAs between them do not issue the same DN to different entities {3.1.5}.

4. For an HLCA with explicitly Accepted Subject CAs, these MUST be Accepted explicitly by Subject name.

3.4 Acceptance Process

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. 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.

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

3. 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 get agreement from the PMA whether Subject CAs are Implicitly or Explicitly Accepted. [The signing policy file must be approved by the PMA]

4. The CA Manager MUST ensure that the HLCA issues in a well defined 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.

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

4 Operational Requirements

4.1 Protection of the Private Key

1. The private key, if based on RSA, MUST have a key length of no less than 2048 bits, or equivalent strength in other ciphers {6.1.5}.

2. Subject CA certificates in the Trust Path SHOULD NOT be generated without human intervention {section 4}.

   If the HLCA is a Root, its signing machine SHOULD be Offline {6.5.1}.

3. A CA SHOULD have a single private key except when rolling over {5.6}.

4.2 Revocation

1. A HLCA SHOULD NOT issue EE certificates {1.3.3}. If it does, they MUST be the minimum necessary for its own operation.

2. The HLCA MUST publish a CRL {4.9.7} using a HTTP URL, and MAY use other means of publishing certificate status information. The CA MUST NOT charge a fee for certificate status information for certificates in the Trust Path

3. The certificate of the HLCA SHOULD comply with GFD.125 [ref]

5 Site Security

6 Publication and Repository Responsibilities

7 Audits

8 Privacy and Confidentiality

9 Compromise and Disaster Recovery

10 Subscriber Obligations