TAGPMA

The Americas Grid
Policy Management Authority

Category: authentication profiles
Status: PENDING-IGTF
Document: IGTF-AP-MICS-draft-1.1.doc
Editor: Tony J. Genovese
Last updated: September 15, 2006
Total number of pages: 7

Profile for Member Integrated Credential Services X.509 Certification Authorities with Secured Infrastructure

Version 1.1

Abstract
This is an Authentication Profile of the International Grid Trust Federation describing the minimum requirements for a Member Integrated X.509 PKI CAs. MICS X.509 Public Key Certification Authorities (MICS PKI CAs) issue credentials to end-entities, who will themselves posses and control their key pair and their activation data. These CAs act as an independent trusted third party for both subscribers and relying parties within the infrastructure. These issuing authorities will use a long-term signing key, which is stored in a secure manner as defined in the Profile.
This Authentication Profile is managed by the TAGPMA and is derived from the TAGPMA SLCS version 1.1.

Table of Contents

1 About this document

This document is an Authentication Profile (AP) of the International Grid Trust Federation (IGTF). This AP defines Member integrated Credential Service X.509 Public Key Certification Authorities (MICS PKI CAs) that issue X.509 credentials to end entities based on an external primary source of identity, with a credential life time of at most 1 year and 1 month. These individual end-entities will themselves posses and control their key pair and their activation data. PKI CAs of this type will act as an independent trusted third party for both subscribers and relying parties within a defined user community.

These authorities will use a long-term signing key, which is stored in a secure manner. This profile defines the minimum requirements for operating a MICS in a secure environment. The IGTF member PMAs will accredit a MICS operated by sites by using this profile.

In this document, the key words `must', `must not', `required', `shall', `shall not', `should', `should not', `recommended', `may', and `optional' in this document are to be interpreted as described in RFC 2119.

1.1 Identification

Document title:	Profile for Member Integrated Credential Services X.509 Certification Authorities with Secured Infrastructure
Document version:	1.1
Document date:	15 September, 2006.
OID:	1.2.840.113612.5 = IGTF
OID:	IGTF.policies.authentication-profiles.mics.1.0
Document OID:	1.2.840.113612.5.2.2.5.1.0

2 General Architecture

A MICS is an automated system to issue X.509 formatted identity assertions (certificates) based on pre-existing identity data maintained by a federation or large organization – the end-entity certificate is thus based on a membership or authentication system maintained by the organization or federation, and is not the primary identity of the end-entity.

The goal is to leverage any existing, well-established identity management system, in most cases for identifying human individuals, in some cases including automated or networked entities, and generate X.509 certificates for these entities that are fully compatible with certificates that would be issued to similar end-entities as primary identity tokens.

A MICS can be based on any primary authentication service to produce a Grid identity, as long as this primary authentication service meets the requirements of this Profile; the MICS will then map this primary identity to a Grid identity. In the CP/CPS that covers the MICS, the following processes must be described, and must be compliant with this Profile:

- The procedures and policies that govern the initial, primary, identity validation;
- How the primary identity management system is managed and secured;
- How the primary identity management system is connected to the MICS;
- How the primary identity is translated to the X.509 certificate;
- How the chain of trust is protected during the translation process.

To achieve sustainability, it is expected that the CAs will be operated as a long-term commitment by institutions or organizations rather than being bound to specific projects.

3 Identity

Any single subject distinguished name (DN) in a certificate must be linked to one and only one entity within the whole of the service. Over the entire lifetime of the Service it must not be linked to any other entity. However, entities may have more then one credential assigned to them. Private keys must not be shared between entities.

To insure that the subject DN used in a certificate is assigned to one and only one person, service, or networked system, once a certificate request has been verified, the ownership of the DN validated, and a certificate issued, the owner is considered to be the "registered owner" of the DN. The DN owner is the human individual or organizational group that has valid rights to exclusive use of a subject name in a certificate. The process of registering the end entity of a certificate request is what maintains the binding between an owner and the subject name (DN). This is to insure that the name is reissued to the same person it was issued to the first time.

3.1 Identity vetting rules for the primary identity management system

The initial vetting of identity for any entity in the primary authentication system must be based on a face-to-face meeting where the binding of the entity to the subject DN is confirmed via photo-identification and/or similar valid official documents. Sufficient information must be recorded and archived such that the association of the entity and the subject DN can be confirmed at a later date. In case of host or service entities, the initial registration should ensure that the association between the registered owner and the FQDN is correct, and sufficient information should be recorded to contact the registered owner.

In case the initial identity vetting is a distributed operation, these rules shall apply for all registration points and all identity validations that result in primary identities that can be translated by the MICS.

The primary identity management system may contain other entities that do not qualify based on the above mentioned conditions, but it must not be possible for such entities to obtain valid credentials from the MICS.

3.2 Identity translation rules

All identities used to create grid identity certificates will be based on the described primary identity management system. A MICS authority must identify the organizational or federated identity management service that will be used to provide the authenticated identity to the MICS. The organization or federation must provide details of how the identity management system creates and validates identities for its users, and this information must be detailed in the CP/CPS of the MICS.

A MICS must describe in their CP/CPS:

1. How the identity (DN) assigned in the certificate is unique within the namespace of the issuer.
2. How it attests to the validity of the identity.
3. How it provides accountability, show that they have verified enough identity information to get back to the physical person any time now and in the future

The identity management (IdM) system containing the identity information of the organization or federation must also meet the following conditions:

1. Re-usable private information used to authenticate end-entities to the IdM system must only ever be sent encrypted over the network when authenticating to any system (including any non-certificate issuing systems) that are allowed to use the IdM for authentication.
2. A second authentication factor not published and not normally used to authenticate to the IdM (i.e. a reasonable private factor) must be used to authenticate the end-entity for any certificate issuance.
3. The end-entities must be notified of any certificate issuance, using contact information previously registered in the IdM (for example by electronic mail).

4. From the information stored in the IdM it must be possible to determine if the requestor's identity has originally been validated using all initial vetting requirements described above.

The IdM used by the CA should be a identity management system that is also used to protect access to other critical resources – e.g. payroll systems, for use in financial transactions, granting access to highly-valuable resources – and be regularly maintained. Alternatively, equivalent security mechanisms must be provided and described in detail and presented to the PMA and are subject to PMA agreement.

3.3 End-entity certificate expiration, renewal and re-keying

Credentials issued by a MICS must not be renewed or re-keyed: any and all certificate issuance must follow the identity translation requirements described above, and be based on the primary identity management system.

Possible local site/organization identity management systems that could be used with a MICS:

1. Kerberos
2. Windows Domain
3. One Time passwords
4. LDAP User Account DB

3.4 Removal of an authority from the authentication profile accreditation

An accredited authority should be removed from the list of authorities accredited under this profile if it fails to comply with this authentication profile document, or with the IGTF Federation Document, via the voting process described in the Charter of the PMA to which this authority is accredited.

4 Operational Requirements

The MICS CA computer, where the signing of the grid identity certificates will take place, needs to be a dedicated machine, running no other services than those needed for the MICS CA operations. The CA computer must be located in a secure environment where access is controlled, limited to specific trained personnel.

The MICS CA system is an on-line system, i.e. the issuing machine is connected (directly or indirectly) to a network or other computer device. It must be equipped with at least a FIPS 140-2 level 3 capable Hardware Security Module or equivalent, and the CA system must be operated in FIPS 140-2 level 3 mode to protect the CA's private key. The CA computer must only be connected to a highly protected/monitored network, which can and will be accessible from the Internet. The secure environment must be documented and approved by the PMA, and that document or an approved audit thereof must be available to the PMA.

Known compliant architectures (with details described in the "on-line CA Guideline Document") include:

- an authentication/request server, suitably protected and connected to the public network, and a separate signing system, connected to the front-end via a private link, that only processes approved signing requests and logs all certificate issuances (model A);
- an authentication/request server containing also the HSM hardware, connected to a dedicated network that only carries traffic destined for the CA and is actively monitored for intrusions and is protected via a packet-inspecting stateful firewall (model B); or equivalence of the protection level must be demonstrated to the PMA.

The on-line CA architecture should provide for a tamper-protected log of issued certificates.

The MICS CA Key must have a minimum length of 2048 bits. The MICS CA signing certificate lifetime should not be more than 20 years.

4.1 Certificate Policy and Practice Statement Identification

Every MICS CA must have a Certification Policy and Certificate Practice Statement (CP/CPS Document) and assign it a globally unique object identifier (OID). CP/CPS documents should be structured as defined in RFC 3647. Whenever there is a change in the CP/CPS the OID of the document must change and the major changes must be announced to the accrediting PMA and approved before signing any certificates under the new CP/CPS. All the CP/CPS under which valid certificates are issued must be available on the web.

4.2 Certificate and CRL profile

The accredited MICS authority must publish a X.509 certificate as a root of trust.

The MICS CAs must issue and publish CRLs, unless the life time of all end entity certificate is less then 1 million seconds (~ 11 days).

The MICS CA certificate must have the extensions keyUsage and basicConstraints marked as critical.

The MICS authority shall issue X.509 certificates to end entities based on cryptographic data generated by the applicant, or based on cryptographic data that can be held only by the applicant on a secure hardware token.

The end-entity certificates keys must be at least 1024 bits long and have a maximum lifetime less than 1 year and one month, and may eb as short as the authority will support.

The short lived certificates must be in X.509v3 format and compliant with RFC3280 unless explicitly stated otherwise. In the certificate extensions:

- a Policy Identifier must be included and must contain at least one OID and only OIDs
- if any end-entity certificates with a life time longer than 1Ms exist or have existed, the CRLDistributionPoints extension must be included and contain at least one http URL
- keyUsage must be included and marked as critical
- basicConstraints may be included, and when included it must be set to ‘CA: false’ and marked as critical so it conforms to general CA and ASN.1 practice.
- if an OCSP responder, operated as a production service by the issuing CA, is available, AuthorityInfoAccess must be included and contain at least one URI
- for certificates bound to network entities, a FQDN must be included as a dnsName in the SubjectAlternativeName

If a commonName component is used as part of the subject DN, it should contain an appropriate presentation of the actual name of the end-entity.

The message digests of the certificates must be generated by a trustworthy mechanism, like SHA1 (in particular, MD5 must not be used).

4.3 Host certificates

Host certificates can be issued to members if that member is authorized to manage the specified host. Every Host certificate DN must include the FQDN of the host.

4.4 Revocation

Revocation requests can be made by certificate holders, Site identity managers and the MICS CA. These requests must be properly authenticated. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key.

Individual holders of a MICS certificate must request revocation if the private key pertaining to the certificate is lost or has been compromised, or if the data in the certificate are no longer valid.

4.5 CA key changeover

When the MICS CA's cryptographic data needs to be changed, such a transition shall be managed; from the time of distribution of the new cryptographic data, only the new key will be used for certificate signing purposes. The overlap of the old and new key must be at least as long as the time an issued certificate will be valid.

5 Site and authority issuing system security

The primary IdM system(s) of the organization or federation must be well protected, and all communications between the IdMs and the certificate issuance setup must be well secured.

Typically, the IdM is considered well-protected if this same IdM used by the CA is also the identity management system that is also used to protect access to other critical resources – e.g. payroll systems, for use in financial transactions, granting access to highly-valuable resources – and be regularly maintained. Alternatively, equivalent security mechanisms must be provided and described in detail and presented to the PMA and are subject to PMA agreement.

Re-usable private information used to authenticate end-entities to any IdM systems involved in certificate issuance must only ever be sent encrypted over the network when authenticating to any system (including any non-certificate issuing systems) that are allowed to use the IdM for authentication.

The certificate issuance setup must comply with the on-line CA setup requirements specified in Section 4.

6 Publication and Repository responsibilities

Each MICS authority must publish for their subscribers, relying parties and for the benefit of distribution by the PMA and the federation:

- a http or https URL of the web page of the CA for general information;
- a MICS CA root certificate or set of CA root certificates up to a self-signed root;
- a http or https URL of the PEM-formatted CA certificate;
- If revocation is supported, a http URL of the PEM or DER formatted CRL;
- the CP and CPS documents;
- an official contact email address for inquiries and fault reporting
- a physical of postal contact address

The MICS CA should provide a means to validate the integrity of their root of trust.
Furthermore, the MICS CA must provide their trust anchor to a trust anchor repository, specified by the accrediting PMA, via the method specified in the policy of the trust anchor repository.

The repository must be run at least on a best-effort basis, with an intended continuous availability.

The originating authority must grant to the PMA and the Federation – by virtue of its accreditation – the right of unlimited re-distribution of the above list of published information.

7 Audits

The MICS CA must record and archive all requests for certificates, along with all the issued certificates, all the requests for revocation and the login/logout/reboot of the issuing machine.

The MICS CA must keep these records for at least three years. These records must be made available to external auditors in the course of their work as auditor.

Each MICS CA must accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document.

The MICS CA should perform operational audits of the CA/RA staff at least once per year. A list of CA and site identity management personnel should be maintained and verified at least once per year.

The identity management system on which the MICS CA relies should undergo a periodic review or audit. This review should be conducted by persons other than the system operators.

8 Privacy and confidentiality

Accredited MICS CAs must define a privacy and data release policy compliant with the relevant national legislation. The MICS CA is responsible for recording, at the time of validation, sufficient information to identify the person getting the certificate. The CA is not required to release such information unless provided by a valid legal request according to national laws applicable to that MICS CA.

9 Compromise and disaster recovery

The MICS CA should have an Business Continuity and Disaster Recovery plan, and be willing to discuss this procedure in the PMA. The procedure need not be disclosed in the CP/CPS.

10 Due diligence for subscribers

The MICS CA should make a reasonable effort to make sure that people realize the importance of properly protecting their private data. For credentials with a life time longer than 1 Ms that are issued to human individuals, it is upon the user to protect the private key with a strong pass phrase.