TAGPMA

The Americas Grid
Policy Management Authority

Category: authentication profiles
Status: FINAL-TAGPMA
Document: IGTF-AP-MICS-1.1.pdf
Editor: Margaret Murray
Last updated: 2 May 2009

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

Version 1.1

Abstract

This is an Authentication Profile of the International Grid Trust Federation describing the minimum requirements for Member Integrated X.509 Credential Services (MICS). MICS X.509 Public Key Certification Authorities (MICS PKI CAs) issue credentials to end-entities who themselves possess and control their key pair and activation data. These CAs will act as independent trusted third parties for both subscribers and relying parties within the infrastructure. MICS CAs 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

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 possess 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', `recommended', `may', and `optional' are to be interpreted as described in RFC2119. 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.

1.1 Identification

Document title:	Profile for Member Integrated X.509 Credential Services with Secured Infrastructure
Document version:	1.1
Document date:	2 May 2009
OID:	1.2.840.113612.5 = IGTF
OID:	IGTF.policies.authentication-profiles.mics.1.1
Document OID:	1.2.840.113612.5.2.2.5.1.1

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.

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 under the Classic Authentication Profile.

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 with one and only one entity for the whole lifetime of the service. However, entities may have more than one credential assigned to them. The subject DN used in a certificate may be assigned to a person, service, or networked system. The registered owner of the subject DN is the human individual or organizational group that has valid rights to exclusive use of that subject name in the certificate. Validation of the certificate request establishes the permanent binding between the end-entity, the registered owner, and the subject DN name. This is to ensure that the name when subsequently reissued refers to the same end-entity.

The private key associated with any certificate must not be disclosed to or shared with end-entities other than the one to which the certificate was issued.

3.1 Identity vetting rules for the primary identity management system

A MICS PKI CA should define the role of Registration Authority (RA) and how these RAs interact with the IdM system process. The initial vetting of identity for any entity in the primary authentication system that is valid for certification should be based on a face-to-face meeting and should be 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 the 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 the case where the initial identity vetting is a distributed operation, these rules shall apply for all registration authority (RA) points and all identity validations that result in primary identities that can be translated by the MICS. Any distributed RA must have formal authority to recognize and establish end-entity identity.

All communications between the CA and the RA regarding certificate issuance or changes in the status of a certificate must be by secure and auditable methods. The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate.

In all cases, the certificate request submitted for certification must be bound to the act of identity vetting.

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 end-entity certificates must be based on a 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 the identity (DN) assigned in the certificate will never be re-issued to another end-

entity during the entire lifetime of the CA,

4. How it provides DN accountability, showing how they can verify enough identity information to enable traceback to the physical person for at least as long as the certificate is valid and in keeping with audit retention requirements. In the event that documented traceability is lost, the DN must never be reissued.

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. The end-entities must be notified of any certificate issuance, using contact information previously registered in the IdM (for example by electronic mail).
3. 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.

A second authentication element not published and not normally used to authenticate to the IdM (i.e. a reasonable private identity verification element) may be used to authenticate the end-entity for any certificate issuance. The CP/CPS must describe how the 'private element' maps to the IdM identity and how it increases identity assurance. Answers to 'private element' questions get collected either at initial F2F registration or out-of-band with RA verification.

The IdM used by the CA should be an identity management system that is also used to protect access to other critical resources – e.g. payroll systems; financial transaction support; access control for highly-valuable resources – and should be regularly maintained. Alternately, equivalent security mechanisms must be provided and described in detail and presented to the PMA with acceptance subject to PMA agreement.

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

For any renewal or rekeying of the certificate by the MICS:

- The registered owner must authenticate to the IdM and
- The MICS must follow the same identity translation requirements described above.

Certificates associated with a private key restricted solely to a hardware token may be renewed for a period of up to 5 years (for equivalent RSA key lengths of 2048 bits) or 3 years (for equivalent RSA key lengths of 1024 bits). Otherwise, the certificate must be re-keyed.

3.4 Removal of an authority from the authentication profile accreditation

An accredited certificate authority (CA) 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 appropriate PMA.

4 Operational Requirements

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

The MICS CA system is designed to be an on-line system, i.e. the issuing machine may be connected (directly or indirectly) to a network or other computer device. If so, it must be equipped with at least a FIPS 140 level 3 capable Hardware Security Module (HSM) or equivalent, and the CA system must be operated in FIPS 140 level 3 mode to protect the CA's private key. The CA computer must only be connected to a highly protected/monitored network, which may 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/certificate self-service system, 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);

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. A MICS CA that does not employ a FIPS 140 level 3 Hardware Security Module, should describe the security precautions taken to protect the MICS CA private key.

The MICS CA Key must have a minimum length of 2048 bits. Copies of the encrypted private key must be kept on off-line media in secure places where access is controlled. 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 RFC3647. 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 documents 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.

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 (e.g., on a secure hardware token; generated from a transient yet unique session handle retrieved from the applicant's encrypted session).

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 be as short as the authority will support.

The end-entity certificates must be in X.509v3 format and compliant with RFC5280 unless explicitly stated otherwise. In the certificate extensions:

- A ***Policy Identifier*** containing only OIDs must be included and must contain at least one OID;
- the *policyIdentifier* must include the OID for this profile: 1.2.840.113612.5.2.2.5
- If any end-entity certificates with a life time longer than 1 million seconds 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 that it conforms to general CA and ASN.1 practice;
- If the issuing CA operates a production service OCSP responder, ***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 if and only if the applicant is authorized to manage the specified host. Such authorization must be described in the CP/CPS. Every Host certificate DN must include the FQDN of the host.

4.4 Revocation

If the MICS implements revocation, revocation requests can be made by certificate holders, IdM 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. The IdM manager must revoke a certificate if the data changes or the traceability to the person is lost.

The CRL should comply with RFC5280.

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.

The CA must react as soon as possible, but within one working day, to any revocation request received. After determining its validity, a CRL must be issued immediately. For CAs issuing certificates to end-entities, the maximum CRL lifetime[1] must be at most 30 days. The CA must issue a new CRL at least 7 days before the time stated in the *nextUpdate* field for off-line CAs, at least 3 days before the time stated in the nextUpdate field for automatically issued CRLs by on-line CAs, and immediately after a revocation. The CRLs must be published in a repository at least accessible via the World Wide Web, as soon as issued.

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.

[1] The CRL life time is defined as the difference between the times stated in *nextUpdate* and *thisUpdate.*

5 Site and authority issuing system security

5.1 Site CA Security

The pass phrase of the encrypted private key must be kept also on an offline medium, separated from the encrypted keys and guarded in a safe place where only the authorized personnel of the Certification Authority have access. Alternatively, another documented procedure that is equally secure may be used.

5.2 Identity Management Security

The 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.

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 certificates up to a self-signed root;
- a http or https URL of the PEM-formatted CA certificate;
- an 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 internal operational audits of the CA/RA staff and IdM interfaces at least once per year to verify its compliance with the rules and procedures specified in its CP/CPS document. Audit results shall be made available to the PMA upon request. A list of CA and site identity management personnel should be maintained and verified at least once per year.

In order to establish the trust of the IdM itself, it is recommended that the IdM system make their periodic audits and reviews available to the MICS CA.

8 Privacy and confidentiality

Accredited MICS CAs must define and follow 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 a 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 subscribers realize the importance of properly protecting their private data. When using software tokens, the private key must be protected with a strong pass phrase, i.e., at least 12 characters long and following current best practice in choosing high-quality passwords. Private keys pertaining to host and service certificates may be stored without a passphrase, but must be adequately protected by system methods.

Subscribers must request revocation as soon as possible, but within one working day after detection of loss or compromise of the private key pertaining to the certificate, or if the data in the certificate is no longer valid.