Category:
Status: Public Consultation
IGTF-AP-MICS-2.0.docx
Editor: Derek SimmelDavid Groep
Last updated: Thu, 01 October 2015
Total number of pages: 2

# Authentication Profile for Member Integrated Credential Services (MICS) X.509 Public Key Certification Authorities with secured infrastructure

## Version v2.0 (rev 20151001)

**Abstract**
The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.

This is an Authentication Profile of the Interoperable Global 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 incorporates parts of the EUGridPMA Classic version 5.0 and TAGPMA SLCS version 3.0 authentication profiles.

**Identification**
Title Authentication Profile for MICS X.509 Public Key Certification Authorities with secured infrastructure
OID { igtf (1.2.840.113612.5) policy (2) authentication-profiles (2) MICS (5) version-2.0 (2.0) }

This document: **urn:oid:1.2.840.113612.5.2.2.5.2.0**

**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 lifetime 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 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

Authorities accredited under this IGTF MICS profile, identified as 1.2.840.113612.5.2.2.5, must comply with the latest endorsed version of

- the IGTF Level of Identity Assurance BIRCH (1.2.840.113612.5.2.5.2); and
- the IGTF PKI Technology Guidelines (1.2.840.113612.5.2.7).