Category:
Status: Public Consultation
IGTF-AP-classic-5-0.docx
Editor: David Groep
Last updated: Tue, 10 May 2016
Total number of pages: 2

Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure

Version v5.0 (rev 20160510)

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 International Grid Trust Federation describing the minimum requirements on traditional X.509 PKI CAs. Traditional X.509 Public Key Certification Authorities (traditional PKI CAs) issue long-term credentials to end-entities, who will themselves possess and control their key pair and their activation data. These CAs act as independent trusted third parties for both subscribers and relying parties within the infrastructure. These authorities will use long-term signing keys, which is stored in a secure manner as defined in the Profile.

This Authentication Profile is managed by the EUGridPMA.

Identification

Title Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure
OID { igtf (1.2.840.113612.5) policy (2) authentication-profiles (2) classic (1) version-5.0 (5.0) }

This document: **urn:oid:1.2.840.113612.5.2.2.1.5.0**

Table of Contents

1 About this document

This document is an Authentication Profile (AP) of the International Grid Trust Federation (IGTF). This AP defines traditional X.509 Public Key Certification Authorities (traditional PKI CAs) that issue long-term credentials to end-entities, who will themselves possess and control their key pair and their activation data. These CAs act as independent trusted third parties for both subscribers and relying parties within the infrastructure. These authorities will use long-term signing keys that are stored in a secure manner.

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 “Classic” profile, identified as 1.2.840.113612.5.2.2.1, must comply with the latest endorsed version of

- the IGTF Level of Identity Assurance CEDAR (1.2.840.113612.5.2.5.3); and
- the IGTF PKI Technology Guidelines (1.2.840.113612.5.2.7).