Category:
Status: Public Consultation
IGTF-AP-SLCS-3.0.docx
Editor: Derek SimmelDavid Groep
Last updated: Thu, 01 October 2015
Total number of pages: 2

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

Version v3.0 (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 a Short Lived X.509 Credential Services (SLCS). SLCS X.509 Public Key Certification Authorities (SLCS PKI CAs) issue short-term credentials to end-entities, who themselves 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 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 EUGridPMA Classic Profile version 5.0 [ClaPro].

Identification

Title Authentication Profile for SLCS X.509 Public Key Certification Authorities with secured infrastructure
OID { igtf (1.2.840.113612.5) policy (2) authentication-profiles (2) SLCS (3) version-3.0 (3.0) }

This document: **urn:oid:1.2.840.113612.5.2.2.3.3.0**

Table of Contents

1 About this document

This document is an Authentication Profile (AP) of the Interoperable Global Trust Federation (IGTF). This AP defines Short-Lived Credential Service X.509 Public Key Certification Authorities (SLCS PKI CAs) that issue short-term credentials to end entities. Short-term credentials have a lifetime of at most one million seconds. These individual end-entities themselves control their key pair and their activation data.

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 SLCS PKI CA in a secure environment. The IGTF member PMAs will accredit a SLCS PKI CA according to 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 SLCS profile, identified as 1.2.840.113612.5.2.2.3, must comply with the latest endorsed version of

- the IGTF Level of Identity Assurance ASPEN (1.2.840.113612.5.2.5.1); and
- the IGTF PKI Technology Guidelines (1.2.840.113612.5.2.7).