

Profile for Short Lived Credential Services X.509 Public Key Certification Authorities with secured infrastructure

Version 1.1

Abstract

This is an Authentication Profile of the International Grid Trust Federation describing the minimum requirements on a Short Lived Credential Service (SLCS) X.509 PKI CAs. SLCS X.509 Public Key Certification Authorities (SLCS PKI CAs) issue short-term credentials to end-entities, who will themselves possess 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 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 EUGridPMA Guidelines Document on minimum requirements, version 4.0.

Table of Contents

1	About this document.....	2
1.1	Identification	2
2	General Architecture.....	2
3	Identity.....	2
3.1	Identity translation rules.....	3
3.2	Removal of an authority from the authentication profile accreditation	3
4	Operational Requirements	3
4.1	Certificate Policy and Practice Statement Identification	4
4.2	Certificate and CRL profile	4
4.3	Revocation	4
4.4	CA key changeover	5
5	Site security.....	5
6	Publication and Repository responsibilities	5
7	Audits	5
8	Privacy and confidentiality.....	6
9	Compromise and disaster recovery.....	6
9.1	Due diligence for subscribers.....	6

1 About this document

This document is an Authentication Profile (AP) of the International Grid 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 Entities¹. These individuals 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 federation.

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 in a secure environment. The IGTF member PMAs will accredit a SLCS 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 Short Lived Credential Services X.509 Public Key Certification Authorities with secured infrastructure
Document version: 1.1
Document date: November 15, 2005.
OID: 1.2.840.113612.5 = IGTF
OID: IGTF.Policies.Authentication Profiles.SLCS.version
Document OID: 1.2.840.113612.5.2.3.1.1

2 General Architecture

A SLCS is an automated system to translate the local site identity into a Grid identity. End entity identity validation is based on the local site authentication system.

SLCS will be operated by large sites or large organizations. The goal is to leverage the existing site/organizations' User Identity management systems. Sites have established identity management systems for their normal business operations. It would benefit these sites to be able to reuse their infrastructure with Grids. In Grids we use X.509 Certificates for identity. A SLCS can be used with a number of local authentication services to produce a short lived Grid identity. A SLCS will map this local site identity to a Grid identity. How the Site manages this process must be described in the CP/CPS that covers the SLCS.

The SLCS must describe how the site/organization identity management system is connected to the SLCS. It must describe how the site/organizations' identity is translated into a Grid Certificate based identity by the SLCS. It must describe 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

Every DN in a short lived certificate must be linked to one and only one End Entity at the Site/Organization. End Entities may have more than one credential assigned to them. Private keys must not be shared between people.

¹ Short-term is defined as lasting less than 1 million seconds, i.e., less than approx. eleven days.

To insure that the DN used in a certificate is assigned to one and only one person/service. 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 translation rules

All identities used to create a Short Lived Certificate will be based on the local Site/Organization identity system.

A SLCS must identify the Site/Organization identity management service that will be used to provide the authenticated identity to the SLCS. The Site/Organization must provide details of how the site identity management system creates and validates identities for its users. This information must be detailed in the CP/CPS of the SLCS

A SLCS 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

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

1. Kerberos
2. Windows Domain
3. One Time passwords
4. Long term certificates
5. LDAP User Account DB

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

The SLCS CA computer should be equipped with at least a FIPS 140-2 level 3 Hardware Security Module or equivalent, to protect the CA's private key. If accessible from the Internet, the local network to which the CA computer is attached must be a highly protected/monitored network. The secure environment must be documented and that document or an approved audit thereof must be available to the PMA.

SLCS CA's that do not have a FIPS 140-2 level 3 Hardware Security Module, must describe the security precautions taken to protect the SLCS CA private key.

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

The private key of the SLCS CA must be protected using a modern secure crypto algorithm used in a safe manner (ex: 3DES, AES) and that is known only by specific personnel of the Certification

Authority, except in the case of an HSM where an equivalent level of security must be maintained. Copies of the encrypted private key must be kept on offline media in secure places where access is controlled.

4.1 Certificate Policy and Practice Statement Identification

Every SLCS 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 SLCS authority must publish a X.509 certificate as a root of trust. SLCS CAs are not expected to issue CRLs.

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

The SLCS authority shall issue X.509 short lived 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 personal short lived certificates keys must be at least 1024 bits long. The personal short lived certificates must have a maximum lifetime less than 1 million seconds (1 Msec).

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 an OID and an OID only
- 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

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 Revocation

It is assumed that the Short Lived Certificates will not need to be revoked because their life time is shorter than the update cycle of most CRLs.

If revocation is supported, then revocation requests can be made by certificate holders, Site identity managers and the SLCS 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 SLCS 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.

4.4 CA key changeover

When the SLCS 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 security

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

6 Publication and Repository responsibilities

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

- a SLCS 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;
- a http or https URL of the web page of the CA for general information;
- the CP and CPS documents;
- an official contact email address for inquiries and fault reporting
- a physical or postal contact address

The SLCS CA should provide a means to validate the integrity of their root of trust. Furthermore, the SLCS CA shall 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 SLCS 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 SLCS 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 SLCS 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 SLCS 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 SLCS 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 SLCS CAs must define a privacy and data release policy compliant with the relevant national legislation. The SLCS 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 SLCS CA.

9 Compromise and disaster recovery

The SLCS CA must have an adequate compromise and disaster recovery procedure, and we will discuss this procedure in the PMA. The procedure need not be disclosed in the policy and practice statements.

9.1 Due diligence for subscribers

The SLCS CA should make a reasonable effort to make sure that people realize the importance of properly protecting their private data.