TAGPMA

The Americas Grid
Policy Management Authority

Profile for SLCS X.509 Public Key Certification Authorities with Secured Infrastructure

Version 2.2

Abstract

This is an Authentication Profile of the International Grid 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 4.2 [ClaPro].

Table of Contents

1   About this Document

(RFC3647: §1)

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 entities. Short-term credentials have a lifetime of at most one million seconds, or about twelve days[1] [GFDI032].   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', `SHOULD, `SHOULD NOT', `RECOMMENDED, `MAY, and `OPTIONAL are to be interpreted as described in RFC 2119 [RFC2119].

1.1   Identification

(RFC3647: §1.2)

Document title:	Profile for SLCS X.509 Public Key Certification Authorities with Secured Infrastructure
Document version:	2.2
Document date:	6 October 2010
OID:	1.2.840.113612.5 = IGTF
OID:	IGTF.Policies.AuthenticationProfiles.SLCS.MajorVersion.MinorVersion
Document OID:	1.2.840.113612.5.2.2.3.2.2

2   General Architecture

(RFC3647: §3, §4.2)

The SLCS CA translates credentials (usually authentication tokens) issued from a large site or federation into the X.509 format suitable for use on Grids. The SLCS is intended for situations where identity tokens are available from an existing identity service that may not be suitable as the foundation for the creation of long-lived certificates. It is expected that the SLCS CA will issue X.509 certificates automatically, based on a successful authentication using existing identity tokens, although additional authorization may be required by the SLCS CA.   Kerberos [KERB] infrastructures issue short-lifetime authentication tokens (tickets). Other legacy authentication and identity services may have uncertainties about revocation, or other management issues, that preclude translating them into long-term credentials. The relationships between site or federation identity management and the SLCS CA must therefore be carefully described. A SLCS CA can be integrated with any primary authentication service to produce a Grid identity, as long as this authentication service meets the requirements of this Profile. In the SLCS CA CP/CPS, the following processes must be described to the accrediting regional policy management authority of the IGTF ("the PMA"), and must be compliant with this Profile:

1.   The procedures and policies that govern the initial identity validation
2.   How the primary identity management systems are managed and secured
3.   How the primary identity management systems are connected to the SLCS CA
4.   How the primary identity is translated to the X.509 certificate
5.   How the chain of trust is protected during the translation process

---

[1] A definition ascribed to Matt Crawford (FNAL), also found in [GFDI032]

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

(RFC3647: §3.1)

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 be generated and stored according to best practices documented in "Guidelines on Private Key Protection" version 1.1 [EUGridPKP]

3.1   Identity Vetting Rules for the Primary Identity Management System

(RFC3647: §3.2)

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.

Qualifying IdMs must suspend or revoke authorization to use the service if the traceability to the person is lost. Suspension or revocation must last until identity is updated and confirmed according to IdM policies.

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

3.2   Identity Translation Rules

(RFC3647: §3.1, §3.2)

All identities used to create a Short-Lived Certificate must be based on one or more described primary identity management systems. A SLCS must identify the Site/Organization/Federation 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 CA.   The CP/CPS must describe:

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 trace back to the physical person for at least one year from the date of certification, and in keeping with audit retention requirements. In the event that documented traceability is lost, the DN must never be reissued.

Many authentication services, identity management systems, identity federation protocols, and other techniques may be used to support a SLCS CA, provided these services can support the identification requirements listed above. A non-exhaustive list:

1. Kerberos-based authentication service
2. Windows Domain
3. One Time password service
4. Another PKI with long term certificates
5. LDAP User Account service
6. Shibboleth-based federation

3.3   End-entity Certificate Expiration, Renewal and Re-keying

(RFC3647: §4.6, §4.7)

Certificates issued by a SLCS CA SHOULD NOT be renewed.   End entities normally re-authenticate to the SLCS CA and are issued a new certificate. The subject DN for new certificates must remain constant for account holders over time to support Grid authorization services.

3.4   Removal of an Authority from the Authentication Profile Accreditation

It is RECOMMENDED that an accredited authority 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 secure environment must be documented and approved by the PMA, and that document or an approved audit thereof must be available to the PMA. This secure environment minimally includes the following:

1. The SLCS CA computer SHOULD be equipped with at least a FIPS 140 level 2 rated Hardware Security Module or equivalent, and the CA system operated substantially in FIPS 140 level 2 mode [FIPS140], to protect the CA's signing key. Additionally, the private key should not be exportable in plaintext form. Alternative configurations must demonstrate how the security precautions taken to protect the SLCS CA signing key meet the functional security objectives of FIPS 140 and substantially meet the security requirements of security level 2, to the satisfaction of the accrediting PMA. (RFC3647: §6.2)
2. The CA computer must only be connected to a highly protected/monitored network, which may be accessible from the Internet. (RFC3647: §6.7)
3. The SLCS CA computer, where the signing of the short-lived certificates will take place, must be a dedicated machine, running no other services than those needed for the CA operations. ((RFC3647: §6.5.1)
4. The SLCS CA computer must be located in a secure environment where access is limited to specific trained personnel. (RFC3647: §5.1)
5. The SLCS CA signing key must have a minimum length of 2048 bits. (RFC3647: §6.1.5)
6. Copies of the encrypted signing key must be kept on off-line media in secure places where access is controlled. (RFC3647: §5.1.6, §6.2.4, §6.2.7)
7. The SLCS CA signing certificate lifetime should not be more than 20 years. (RFC3647: §6.3.2)

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) (RFC3647: §1.2)

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. (RFC3647: §1.5.4, §9.12.2 and §9.12.3)

CP/CPS documents should be structured as defined in RFC 3647 [RFC3647]. (RFC3647: §1)

Every CP/CPS document under which valid certificates are issued must be available on the web. (RFC3647: §2.2)

4.2   Certificate and CRL Profile

The accredited authority must provide and allow distribution of a (sufficient collection of) X.509 certification authority certificates to enable validation of end-entity certificates. All certificates, including all end-entity certificates subject to this Authentication Profile, must comply with the Grid Certificate Profile as defined by the Open Grid Forum [GFD125]. (RFC3647: §2.2 and §4.10.1)

The SLCS CA must issue and publish CRLs .(RFC3647: §4.9.7)

The SLCS CA certificate must have the extensions **keyUsage** and **basicConstraints** marked as critical. (RFC3647: §7.1.2)

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 (e.g., on a secure hardware token; generated from a transient yet unique session handle retrieved from the applicant's encrypted session). (RFC3647: §6.1)

The end-entity certificate RSA keys must be at least 1024 bits long and have a maximum lifetime less than 1 million seconds (1 Msec). (RFC3647: §6.1.5 and 6.3.2)

The short-lived certificates must be in X.509v3 format and compliant with RFC5280 [RFC5280] unless explicitly stated otherwise. In the certificate extensions: (RFC3647: §7.1.2)

1. a **Policy Identifier** containing only OIDs must be included and must contain at least one OID
2. **cRLDistributionPoints** extension must be included in end entity certificates
3. **keyUsage** must be included and marked as critical
4. **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
5. **SubjectAlternativeName** extension must include a dnsName containing a FQDN, for certificates bound to network entities
6. **commonName** component should contain an appropriate presentation of the actual name of the end-entity. (RFC3647: §3.1.2)

The message digests of the certificates must be generated by a trustworthy mechanism, like SHA1 (in particular, MD5 must not be used). (RFC3647: §7.1.3)

All SLCS certificates must comply with the Grid Certificate Profile as described in Open Grid Forum document GFD.125 [GFD125].

4.3   Host Certificates

Although use cases are not known at this time, 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 subject DN must include the FQDN of the host.

4.4   Revocation

The CA must publish a CRL. 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. The CA must issue a new CRL at least 3 days before expiration of the current CRL or immediately after a revocation. The CRLs must be published in a repository at least accessible via the World Wide Web, as soon as issued.

Revocation requests can be made by end-entities, Registration Authorities and the CA. These requests must be properly authenticated. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key. (RFC3647: §4.9)

4.5   CA Key Changeover

(RFC3647: §5.6)

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

(RFC3647: §6.4.2 or §5.1.2)

A copy of the pass phrase of the encrypted CA signing 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

(RFC3647: §2)

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

1.   http or https URL of the web page of the CA for general information
2.   SLCS CA root certificate or set of CA root certificates up to a self-signed root
3.   http or https URL of the PEM-formatted CA certificate
4.   http URL of the PEM or DER formatted CRL
5.   CP and CPS documents
6.   Official contact email address for inquiries and fault reporting
7.   Physical or postal contact address

It is RECOMMENDED that the SLCS CA provide a means to validate the integrity of its root of trust. (RFC3647: §6.1.4)

Furthermore, the SLCS CA shall provide its 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. (RFC3647: §5.4.1)

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. (RFC3647: §5.4.3, §8)

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. (RFC3647: §8.3)

The SLCS CA should perform operational audits of the CA/RA staff and IdM interfaces at least once per year to verify 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 either site or federation identity management personnel should be maintained and verified at least once per year. (RFC3647: §8)

8   Privacy and Confidentiality

(RFC3647: §9.4)

Accredited SLCS CAs must define a privacy and data release policy compliant with the relevant national legislation. Accredited SLCS CAs must follow a privacy and data release policy consistent with the policy of the underlying accounts database or IdM. In the case where no such policy exists, then the CPS must disclose this. The SLCS CA is responsible for recording, at the time of validation, sufficient information for unique identification of the person getting the certificate.

9   Compromise and Disaster Recovery

(RFC3647: §5.7)

The SLCS CA is RECOMMENDED to 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

(RFC3647: §4.5.1)

The SLCS CA is RECOMMENDED to make a reasonable effort to ensure that subscribers realize the importance of properly protecting their private data, as described in "Guidelines on Private Key Protection" version 1.1 [EUGridPKP]. Private keys must not be shared.

References

[ClaPro] "Authentication Profile for Classic X.509 Public Key Certification Authorities with secure infrastructure version 4.2". EUGridPMA. http://www.eugridpma.org/guidelines

[EUGridPKP] "Protection of private key data for end-users in local and remote systems version 1.1". EUGridPMA. D Groep. http://www.eugridpma.org/guidelines/pkp/

[FIPS140] "Security Requirements for Cryptographic Modules". NIST.   May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[GFD125] GFD-C.125: Grid Certificate Profile. OGF. D Groep, M Helm, J Jensen, M Sova, S Rea, R Karlsen-Masur, U Epting, M Jones. March 2008. http://www.ogf.org/documents/GFD.125.pdf

[GFDI032] GFD-I.032: Site Requirements for Grid Authentication, Authorization and Accounting. GGF. S Mullen et al. 2004. http://www.ogf.org/documents/GFD.32.pdf

[KERB] RFC4120: The Kerberos Network Authentication Service (V5). C Neuman et al. IETF. http://www.ietf.org/rfc/rfc4120.txt

[RFC2119] RFC2119: Key words for use in RFCs to Indicate Requirement Levels. IETF. S. Bradner. 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC3647] RFC3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. IETF. S Chokhani et al. 2003. http://www.ietf.org/rfc/rfc3647.txt

[RFC5280] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF. D Cooper, S Santesson, S Farrell, S Boeyen, R Housley and W Polk. May 2008. http://www.ietf.org/rfc/rfc5280.txt

Acknowledgements

The Americas Grid Policy Management Authority   http://www.TAGPMA.org/