Category: authentication profiles
Status: PENDING-AP-TAG
Document: IGTF-AP-classic-20050930-4-1-b3.doc
Editor: David Groep
Last updated: Mon, 09 October 2006
Total number of pages: 6

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

Version 4.1-b3

Abstract
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 posses 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 EUGridPMA.

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[1], who will themselves posses and control their key pair and their activation data. These PKI CAs act as a independent trusted third party for both subscribers and relying parties within an infrastructure.
These authorities will use a long-term signing key, which is stored in a secure manner

In this document, the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' in this document 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

There should be a single Certification Authority (CA) organisation per country, large region or international organization. The goal is to serve the largest possible community with a small number of stable CAs.[2] To achieve sustainability, it is expected that the CAs will be operated as a long-term commitment by institutions or organisations rather than being bound to specific projects.

The CA structure within each region should not follow the conventional hierarchical model, but there should be a single end-entity issuing CA. A wide network of Registration Authorities (RA) for each CA is preferred. The RAs will handle the tasks of validating the identity of the end entities and authenticating their requests, which will then be forwarded to the CA. The CA will handle the actual tasks of issuing CRLs, signing Certificates/CRLS and revoking Certificates.

3 Identity

Any single subject distinguished name must be linked to one and only one entity. Over the entire lifetime of the CA it must not be linked to any other entity.
It is not contrary to the above requirement for a single entity to have more than one associated subject name, e.g., for different key usages.
Certificates must not be shared among end entities.

3.1 Identity vetting rules

A PKI CA must define the role of registration authority (RA), and these registration authorities are responsible for the identity vetting of all end-entities, such as natural persons and network entities.

In order for an RA to validate the identity of a person, the subject should contact the RA face-to-face and present photo-id and/or valid official documents showing that the subject is an acceptable end entity as defined in the CP/CPS document of the CA.
In case of host or service certificate requests, the RA should validate the identity of the person in charge of the specific entities using a secure method. The RA must ensure that the requestor is appropriately authorized by the owner of the FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate.
The RA must validate the association of the certificate signing request.

The RAs must record and archive all requests and confirmations.
The CA is responsible for the continued archival and audit-ability of these records.

[1] Long-term is defined as lasting more than 1 million seconds, i.e., more than approx. ten days.
[2] This constituency definition is going to be moved to the accreditation guidelines adopted by the individual PMAs in a future revision of this AP.

The RA must communicate with the CA with secure methods that are clearly defined in the CP/CPS. (e.g. Signed emails, voice conversations with a known person, SSL protected private web pages that are bi-directionally authenticated). The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate.

In all cases, the certificate request submitted for certification must be bound to the act of identity vetting.

3.2 End-entity certificate expiration, renewal and re-keying

For credentials based on software tokens credentials should only be re-keyed, not renewed. For those based on hardware tokens, these may be renewed for a period of up to 5 years (for equivalent RSA key lengths of 2048 bits) or 3 years (for equivalent RSA key lengths of 1024 bits).
No credentials can be renewed or re-keyed for more than 5 years without a form of identity and eligibility verification, and this procedure must be described in the CP/CPS.

3.3 Removal of an authority from the authentication profile accreditation

An accredited authority must be removed from list of accredited authorities 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 CA computer, where the signing of the certificates will take place, needs to be a dedicated machine, running no other services than those needed for the CA operations. The CA computer must be located in a secure environment where access is controlled, limited to specific trained personnel. The CA computer may be either

- on-line: the certificate issuing machine is directly or indirectly connected (by wire, wireless or any other means) to any other computer device (this includes peripherals that themselves are connected to devices not integral part of the certificate issuing machine); or
- completely off-line: kept disconnected from any kind of networks at all times.

4.1 On-line CAs

In case the CA computer is equipped with at least a FIPS 140-2 level 3 capable Hardware Security Module or equivalent, and the CA system is operated in FIPS 140-2 level 3 mode to protect the CA's private key, the CA computer may be connected to a highly protected/monitored network, possibly accessible from the Internet. 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.
Known compliant architectures (with details described in the "on-line CA Guideline Document") include

- an authentication/request server, suitably protected and connected to the public network, and a separate signing system, connected to the front-end via a private link, that only processes approved signing requests and logs all certificate issuances (model A);
- an authentication/request server containing also the HSM hardware, connected to a dedicated network that only carries traffic destined for the CA and is actively monitored for intrusions and is protected via a packet-inspecting stateful firewall (model B);

or equivalence of the protection level must be demonstrated to the PMA.

The on-line CA architecture should provide for a (preferably tamper-protected) log of issued certificates.

The CA Key must have a minimum length of 2048 bits and for CAs that issue end-entity certificates the lifetime must be no less than two times of the maximum life time of an end entity certificate and should not be more than 20 years.

The private key of the CA must be protected with a pass phrase of at least 15 elements 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 mediums in secure places where access is controlled.

4.2 Certificate Policy and Practice Statement Identification

Every 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.

4.3 Certificate and CRL profile

The accredited authority must publish a X.509 certificate as a root of trust.

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

The authority shall issue X.509 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 EE keys must be at least 1024 bits long. The EE certificates must have a maximum lifetime of 1 year plus 1 month.

The end-entity 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
- CRLDistributionPoints must be included and contain at least one http URL
- keyUsage must be included and marked as critical
- basicConstraints should be included, and when included it must be set to ‘CA: false’ and marked as critical
- 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
- for certificates bound to network entities, a FQDN shall be included as a dnsName in the SubjectAlternativeName

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 CRLs must be compliant with RFC3280, and is recommended to be version 2.
The profile of the CA certificates, the end-entity certificates and the CRLs must also comply with the current IGTF and OGF certificate profile guidelines before being included in any distribution of certificates.

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

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. For CAs issuing certificates to end-entities, the maximum CRL lifetime must be at most 30 days and the CA must issue a new CRL at least 7 days before expiration and 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.

4.5 CA key changeover

When the 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 the longest time an end-entity cert can be valid. The older but still valid certificate must be available to verify old signatures – and the secret key to sign CRLs – until all the certificates signed using the associated private key have also expired.

5 Site security

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

6 Publication and Repository responsibilities

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

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

The CA should provide a means to validate the integrity of their root of trust.
Furthermore, the 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 this information.

7 Audits

The CA must record and archive all requests for certificates, along with all the issued certificates, all the requests for revocation, all the issued CRLs and the login/logout/reboot of the issuing machine.

The 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 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 CA should perform operational audits of the CA/RA staff at least once per year. A list of CA and RA personnel should be maintained and verified at least once per year.

8 Privacy and confidentiality

Accredited CAs must define a privacy and data release policy compliant with the relevant national legislation. The CA is responsible for recording, at the time of validation, sufficient information regarding the subscribers to identify the subscriber. The CA is not required to release such information unless provided by a valid legal request according to national laws applicable to that CA.

9 Compromise and disaster recovery

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

9.1 Due diligence for end-entities

The CA should make a reasonable effort to make sure that end-entities realize the importance of properly protecting their private data. When using software tokens, it is upon the user to protect his private key with a strong pass phrase, i.e., at least 12 characters long and following current best practice in choosing high-quality passwords.

End-entities must request revocation as soon as possible, but within one working day after detection of loss or compromise of the private key pertaining to the certificate, or if the data in the certificate are no longer valid.