Minimum CA Requirements

Here we discuss the minimum requirements for traditional offline PKI CAs. These have evolved over a period of three years in an iterative discursive fashion – largely as a result of the numerous difficulties that arise when interoperating between different linguistic, administrative, networking and security domains as occur over national boundaries. In this section, 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 PKI Structure

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. 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 country 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 when necessary.

2 Certification Authority

2.1 Computer Security Controls

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 and must be kept disconnected from any kind of networks at all times. In case the CA computer is equipped with at least a FIPS 140-1 level 3 Hardware Security Module or equivalent, to protect the CA's private key, the CA computer can be connected to a highly protected/monitored network, possibly accessible from the Internet. The secure environment must be documented and that document or an approved audit thereof must be available to the PMA.

2.2 CA Namespace

Each CA must sign only a well-defined namespace that does not clash with any other CA.

2.3 Policy Document & Identification

Every CA must have a Certification Policy and Certificate Practice Statement (CP/CPS Document) and assign it an O.I.D. Whenever there is a change in the CP/CPS the O.I.D. of the document must change and the major changes must be announced to the EUGridPMA and approved before signing any certs under the new CP/CPS. All the CP/CPS under which valid certs are issued MUST be available on the web.

2.4 CA Key

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 which is known **only** by specific personnel of the Certification Authority. Copies of the encrypted private key must be kept on offline mediums in secure places where access is controlled.

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.

2.5 CA Certificate

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

2.6 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.

End-entities 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.

2.7 Records Archival

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.

2.8 Key changeover

The CA's private signing key must be changed periodically; from that time on 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.

2.9 Repository

The repository must be run at least on a best-effort basis, with an intended availability of 24x7.

2.10 Compliance Audits

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.

2.11 Operational Audits

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.

2.12 Shutdown

3 Registration Authority

3.1 Entity Identification

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 CSR be delivered to the RA by the person in charge of the specific entities using a secure method.

3.2 Name Uniqueness

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.

3.3 Records and Archival

The RAs must record and archive all requests and confirmations.

3.4 RA Obligations

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)

4 End Entity Certificates

The EE keys must be at least 1024 bits long and must not be generated by the CA or the RA. The EE certificates must have a maximum lifetime of 1 year plus 1 month and must not be shared among end entities.

The CA should make a reasonable effort to make sure that end-entities realize the importance of properly protecting their private data. It's upon the user to protect his private key with a pass phrase at least 12 characters long.

4.1 Certificate profile

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

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