Summary: the Guidelines for On-line PKI Certification Authorities apply to those PKI CAs where the certificate issuing machine is directly or indirectly connected to any other computer device. The architecture should protect against the very harmful leaking of private keys, since there is no viable possibility to quickly withdraw a compromised root CA from trust anchor distributions. This is a draft of a document describing the recommendations for the operation of on-line Certification Authorities.

Table of Contents

- About this document
- Scope of this document
- Operational requirements
  - Network controls
  - Key generation
  - Key storage
  - Key Activation
  - Key Deactivation
  - Key End of Life
  - Procedural Controls
- Site Security
- Publication and repository responsibilities
- Audits
- Compromise and disaster recovery

About this document

This is a draft document of the IGTF managed by the EUGridPMA.

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 documented such that relying parties can decide whether to accept the exception.

Scope of this document

The Guidelines for On-line PKI Certification Authorities apply to those PKI CAs where the certificate issuing machine is directly or indirectly connected (by wire, wireless or any other means) to any other computer device (including the connection of any peripherals(1) of the certificate issuing machine that themselves are connected to devices not an integral part of the certificate issuing machine)

The architecture should protect against the very harmful leaking of private keys, since there is no viable possibility to quickly withdraw a compromised root CA from trust anchor distributions.

Any on-line CA architecture shall be documented at the systems level, and this documentation shall be available to the accrediting body for assessment and subject to review.

Operational requirements

Network controls

On-line CA architectures must ensure that only legitimate traffic related to certificate issuing opertions will ever reach the on-line CA issuing system. This can be ensured in various ways:

1. (A) 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;
2. (B) 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;

where it is noted that model A type designs are more readily secured and usually need less components and effort to maintain and operate.

Key generation

The key must be generated in a controlled and secure environment:

- generated inside a FIPS 140-2 level 2* or level 3 certified HSM in which it is thereafter stored and retained and not exported in plain-text, or
- in a 'key generation ceremony', in an environment providing equivalent integrity and confidentiality protection guarantees. In

such cases, the key generation shall be:
- done using a strong source of random numbers
- using a trustworthy cryptographic algorithm and an implementation thereof which has been reviewed
- performed in a way that all potential copies of the private key material shall be accounted for
- shall be done on an off-line system which is known to be run a true and unaltered copy of the intended software and operating system

The key generation ceremony protocol shall be documented beforehand, there ceremony shall be witnessed by independent auditors, and a written record as well as any audiovisual records of the ceremony shall be archived.

Following the key generation ceremony, the key shall be imported into the HSM module(s) for storage and operational use. All other copies of the private key shall be securely archived and each copy shall be accounted for. It is strongly advised that 'n-of-m' multi-person control is used to control access to the copies of the private key that shall be held outside of an HSM.

Key storage

The private key of a CA which is used for signing purposes must be held in a HSM certified to FIPS 140-2.

The HSM used should be certified at FIPS140-2 level 3. A level-2 certified HSM, or a level-3 HSM operated in level-2 mode, may be permissible provided additional compensatory controls are in place to mitigate the increased risk of theft and unauthorized access:
- controls to make it physically hard to remove the HSM from the secured location and to detect in a timely manner any attempt at tampering with the HSM at the secured location.
  Since the HSM is not tamper-proof, once it is removed off-premises or left unguarded, its key material can be taken and the activation data brute-forced;
- additional controls to identify the operator or operators involved in activating the key material, e.g. through automated logging and on-site monitoring, or by implementing multi-person controls.

Key material used at the time of signing must only ever be stored inside an HSM.

Archival and back-up key material must be held in a secure location in a dedicated safe deposit box to which only authorized CA personnel with a key recovery role has access. It is strongly advised that 'n-of-m' multi-person control is used to control access to the copies of the private key that shall be held outside of an HSM.

Key Activation

The private key of the CA must be encrypted within the HSM. Key activation must involve the intervention of a human operator entering the activation data locally on the machine. Activation data must never be sent over a network, not even in encrypted form.

The passphrase used to protect the private key must have at least 15 elements with high entropy, and must only be known by designated personnel of the CA.

Keys can remain activated inside the system for as long as the system is powered on and remains in the secure environment.

Key Deactivation

Loss of power and loss of connectivity between the on-line CA issuing system and the HSM must result in key de-activation. The system architecture should allow for a way to de-activate the key remotely.

Key End of Life

No stipulation yet.

Procedural Controls

To further protect the issuing CA and permit revocation thereof, it is strongly advised that all on-line issuing CAs be a subordinate of an off-line root or higher-level CA, where the off-line root may have a long-lived (one year or longer) CRL.

Site Security

The site security measures must ensure that neither the HSM nor the on-line CA system can be removed from the secured location without evidence being left that permits identifying the actor(s). It must not be possible to remove the on-line system from the secured location without de-activating the private key in the HSM.

Archival copies and key material fragments must be kept in a secure location where access is controlled to designated CA personnel with a key management role.

Publication and repository responsibilities

The CA shall inform the accrediting body that the issuing machine holding the key material is an on-line system.

Audits

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.

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

Compromise and disaster recovery

Any on-line CA shall have a disaster recovery and business continuity plan. For CAs where the key material has been generated inside the HSM, this plan should include regular tests of the capability to recover the key in the HSM from archival material.

-- DavidGroep - 2014-05-11

Notes

1 : Including peripherals intended for remote operation and management of the issuing computer system, such as out-of-band management boards, remotely-accessible KVM systems, remotely-operable (USB) peripherals switching equipment, etc. However, remotely-operated PSU, or PSUs that have remote-read-out functionality are not considered peripherals of the issuing machine.

This topic: Main > WebHome > PolicyDrafts > GuidelinesForOnLineCAs
Topic revision: r3 - 2014-06-05 - DavidGroep