**Private Key Protection**

This document describes the requirements for the protection of private keys corresponding to end entity certificates. It primarily aims to describe user (personal) certificates, but much of the key management will also apply to robots or hosts, or other end entities.

The following describes the private key protection profiles. It is important to describe the *full lifecycle* of the key. For each profile, the following are described:

1. Key generation
2. Key delivery to subscriber
3. Key storage – subscriber
4. Key deployment (delivery to subject) – if the subject and the subscriber are not the same entity.
5. Key storage – subject
6. Key activation
7. Deactivation of key
8. End of life of key

In the profile, we distinguish between the subscriber, the person who interacts with the CA to obtain a certificate, and the subject, the entity named by the certificate. At any given time, there SHOULD be a well-defined subscriber for each certificate.

The private key is a secret, in public key cryptography, which consists not just of the key but also of the activation material in case the key is encrypted. Activation data can also cover other types of protection, if permitted by the profiles: including, but not limited to, smartcards, protected by filesystem (readable only by root or a service system user account accessible only by the subject), multi-person controls, etc. [TODO: expand.]

In the case of each profile, a CA MAY impose stronger restrictions than those required by the profile.

The subscriber uses the private key to

* Prove possession of the private key, as a part of the certificate request process
* Rekey the certificate
* Revoke the certificate

The subject uses the private key for the purposes encoded in the certificate and described in the relevant CP/CPS.

The subject and the subscriber may of course be the same entity – typically, if the certificate is a personal certificate.

As a guideline, the *subscriber* remains responsible for the private key throughout the lifetime of the key (which may be longer than the lifetime of the certificate), but the profile allows for a handover where one subscriber hands over the responsibility for the certificate to another. The handover process is described in more detail below. There MUST be a subscriber associated with a key whenever there are valid certificates associated with the key; there SHOULD be no more than one subscriber.

In order to make an assertion regarding the strength of the private key protection, the CA may need to witness some or all parts of the processes described in each profile[[1]](#footnote-1). The alternative is to trust the subscriber, to have the subscriber assert to the CA (or RA) that the requirements are fulfilled. [TODO: expand]

General principles:

* Private key SHALL NOT be transferred in clear
* Activation data SHALL NOT be transferred in clear
* Private key and activation data SHOULD NOT be stored together
* Protected Private key SHOULD NOT be transferred over a network [?]
* Key material MUST be generated using trustworthy methods
* Activation SHOULD NOT persist beyond 24 hrs (unless it’s a SLC) [?]

**Profiles**

The profiles are described here in order of their assurance, with the highest assurance first, but it should be emphasised that they are all acceptable for the IGTF.

**User managed secured keys**

1. The subscriber generates a private key in an HSM certified to FIPS 140-2, operating at L2 or higher.
   1. The key MUST be generated in the HSM, not imported.
   2. The key MUST be protected by activation data.
   3. The cryptographic strength of the activation data SHOULD be checked and rejected if not strong enough. The check SHOULD implement IGTF recommendations for activation data, or stronger.
   4. The CA SHOULD witness the key generation.
2. As the key generation in the HSM is controlled by the subscriber, there is no key delivery to the subscriber – the key remains in the HSM.[[2]](#footnote-2)
3. They key remains stored in the HSM. There is a backup of the key only if the HSM provides backups.
4. The key is deployed to the subject, if the subscriber is not the subject, by:
   1. Giving control of the key to the subject by:
      1. Physically moving the HSM to a machine controlled wholly by the subject, and giving the subject the activation data, OR
      2. Giving the activation data controlling the key in the HSM by some physical means, OR
      3. Giving the activation data controlling the key to the subject by some equally, or more, secure means.
   2. The subscriber MUST ensure that the subject is authenticated by some trusted means.
5. The key remains stored in the HSM.
6. Activation data must be stored in a documented way which provides reasonably assurance that only the subject can access the activation data.
7. This profile does not require a time limit on the duration of the activation.
8. There is no requirement on key destruction. The key MAY be used for renewal.

**Infrastructure managed softkeys**

1. The subscriber generates the key on a keystore, providing activation material.
   1. The keystore MUST be run according to best practices by trusted system administrators.The system MUST be located in a secure environment where access is controlled and limited to authorised personnel, and the organisation running the service MUST have a defined data protection and security policy.
   2. The keystore MUST be run on a dedicated system which runs no services other than those pertaining to the key management and the monitoring of their management.
   3. The activation material MUST NOT be stored on the keystore, nor on the host running the keystore.
   4. The key MUST NOT be stored in activated form on the keystore.
   5. If the keystore communicates with the CA, it MUST do so by securely authenticated means. (This link is necessary if the keystore is to assert the level of protection of the key, and/or to generate and submit a CSR.)
2. The private key SHOULD NOT leave the keystore. If the private key leaves the keystore, it MUST be delivered to the subscriber by secure means, ie.
   1. Ensure that the subscriber is authenticated to the keystore with a level of assurance equivalent to, or better, than the level of assurance associated with the identification of the subject with the certificate associated with the key.
   2. Key delivery to subscriber MUST be logged using secure means.
   3. The keystore MAY destroy the key after delivery to subscriber. If it does, the destruction of the key MUST be logged and MUST be done using best practices for destruction of information for the type of storage where the key is stored.
   4. A destroyed key MAY be archived for backup or escrow purposes. See 3.1.
   5. If a key is delivered to the user and the keystore copy subsequently destroyed by the keystore, it MUST subsequently be managed according to the softkey profile, except that stipulations in this profile regarding the access to the archived copy still hold.
3. Keys stored on the keystore SHOULD be archived. The archive SHOULD NOT be accessible by anyone other than the trusted administrators.
   1. The recovery of the archived copy MUST require privileged access by keystore administrators.
   2. If the archived copy is used for any purpose other than recovery (e.g. escrow), the CA SHOULD be consulted and permit the use.
4. Activation data can be delivered to the subject by the subscriber. This MUST be done either in physical form or by other secure means, and MUST authenticate the subject to the subscriber.
   1. Activation data MAY be used with other resources, so an infrastructure MAY implement single sign-on to the keystore.
5. The Subscriber MUST protect activation data according to best practices.
6. If the subject activates the key in the keystore, the activation data MUST be provided to the keystore by secure means. In particular, it MUST NOT be sent in cleartext, and it MUST protect against MIM attacks, and SHOULD take measures to guard further against phishing and replay attacks.
7. The key SHOULD NOT remain activated in the keystore for more than 24 hours, unless its certificate(s) is/are SLC(s).
8. The key SHOULD NOT be reused beyond the lifetime of the first end entity certificate associated with the key, and it is RECOMMENDED to destroy the non-archival copies of the key. The keystore MAY retain the archival copy beyond the expiry of all certificates associated with the key.

**User managed softkeys**

1. The Subscriber generates the key and activation material, on a system managed by trusted administrators.
2. If the private key is generated remotely, it MUST follow the stipulations for key generation and delivery to the subscriber described in the infrastructure key profile. If the private key and activation material are generated by the Subscriber locally, there is no key delivery to the Subscriber.
3. The key MAY be stored by the subscriber for archival purposes. In this case, the key SHOULD be stored without activation data, and the activation data for the archived copy, if different, SHOULD be at least as strong as the activation data of the original key.
4. If the Subscriber is not the same entity as the Subject, the Subscriber delivers the key and the activation data separately by secure means.
5. The subject MUST store the private key in a form where access or use is protected against other non-privileged users and other services, by using best practices (or specifically those required by the CA).
6. Activation of the subject’s private key MUST ensure that only the subject can activate the key with a strong[[3]](#footnote-3), and documented, level of assurance.
7. The key SHOULD NOT remain activated for more than 24 hours, unless its certificate(s) is (are) SLCs.
8. The key SHOULD NOT be reused, and it is RECOMMENDED to destroy the non-archival copies of the key. If the certificate is personal, it is RECOMMENDED that the subscriber retain the archival copy.

1. Usually by delegation, ie the CA defines a role of Registration Authority or similar, who witnesses the key generation. [↑](#footnote-ref-1)
2. The HSM may be handed over physically to the subscriber, but this is equivalent to the change of subscriber, where the first generates the key pair and the second takes over responsibility for the key. [↑](#footnote-ref-2)
3. “Strong” level of assurance means a compromise of the key (unauthorised leakage of key information) will require wilful circumvention of the protection rules by the subject, or compromise of privileged accounts on the system, or similar. [↑](#footnote-ref-3)