Category:
Status: Approved
pk-protection-2.0-2014.docx
Editor: David Groep
Last updated: Wed, 22 November 2017
Total number of pages: 5

IGTF Private Key Protection Guidelines

Version 2.0-2014

Abstract

The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.

This document describes the requirements for the protection of private keys corresponding to end-user personal and robot certificates. Although it primarily aims to describe these user (personal) certificates, much will also apply to any other kind of end entity.

This document is an EUGridPMA Guidelines Document, to be referred to as the “Guidelines on Private Key Protection”.

Identifications

This document: **urn:oid:1.2.840.113612.5.4.1.1.1.5.4**

Table of Contents

1 About this document

This document describes the requirements for the protection of private keys corresponding to end-user personal and robot certificates. Although it primarily aims to describe these user (personal) certificates, much will also apply to any other kind of end entity.

In this document, we distinguish between the subscriber, the person who interacts with the CA/RA to obtain a certificate, and the subject, the entity named by the certificate. The subject and the subscriber may of course be the same entity – typically, if the certificate is a personal certificate.

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 is not the same entity.
5. Key storage – subject
6. Key activation
7. Deactivation of key
8. End of life of key

In this document, we distinguish between the subscriber, the person who interacts with the CA/RA to obtain a certificate, and the subject, the entity named by the certificate.

The private key is a secret, in public key cryptography, that allows the owner to prove affiliation with the public key. Activation data protects the confidentiality of the private key, and is typically password based encryption, but could also be access controls which provide equivalent (or better) levels of protection.

A CA MAY impose stronger restrictions than those required by this guideline.

The subscriber uses the private key to

- Prove possession of the private key as a part of the certificate request or rekeying process
- Request revocation of the certificate without the need for further investigation

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

As a guideline, the subscriber remains responsible for the private key throughout the lifetime of the key, but the profile allows for a handover where one subscriber hands over the responsibility for the certificate and private key to another - the person who gets this responsibility now becomes the subscriber (this is possible only if the subscriber is not the subject). The CA does not necessarily know about this handover process, and may not learn about it until the subscriber communicates with the CA proving possession of the private key. The handover process is described in more detail below. The CA must describe the permitted handover process(es) in its CPS.

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. The alternative is to trust the subscriber, to have the subscriber assert to the CA (or RA) that the requirements are fulfilled.

General principles:

- Unencrypted private keys SHALL NOT be transferred in clear
- Activation data SHALL NOT be transferred in clear
- Private key and activation data SHOULD NOT be stored together
- The encrypted private key SHOULD only be transferred via protected (encrypted and authenticated) channels
- Key material MUST be generated using trustworthy methods
- Activation SHOULD NOT persist beyond 24 hrs of inactivity (key is not being used) unless it is a short-lived credential

where transfer means the exchange of information between systems.

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 explained to relevant accrediting bodies to make an informed decision about accepting the exception, or the applicant must demonstrate to the accrediting bodies that an equivalent or better solution is in place.

2 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
- Infrastructure managed soft keys
- User managed soft keys

3 User managed secured keys

1. The subscriber generates a private key in an HSM certified to FIPS 140-2, operating at L2 or higher.
    a. The key MUST be generated in the HSM, not imported.
    b. The key MUST be protected by activation data.
    c. The cryptographic strength of the activation data SHOULD be checked and rejected if not strong enough. The check SHOULD follow IGTF recommendations for activation data, or be more stringent.
2. If the key is delivered to the subscriber, it is delivered in the token.
3. The 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:
    a. Giving control of the key to the subject by:
        i. Moving the HSM to a machine controlled wholly by the subject, and giving the subject the activation data, and/or
        ii. Giving the activation data controlling the key to the subject by some physical means, or by some equivalent means.
    b. The subscriber MUST ensure that the subject is authenticated by some trusted means.
5. The key remains stored in the HSM.
6. The activation data MUST be stored in a way which provides reasonable 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. Private keys MUST have a finite usable life time and this life time SHOULD be less than 60 months.

4 Infrastructure managed softkeys

1. The subscriber generates the key on a keystore, providing activation material to the generation process.
    a. 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 operations of the keystore MUST follow the data protection and security policies of the organisation hosting the service. The requirements of the Credential Store Operations guidelines for running a security sensitive service MUST be followed.
    b. 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.
    c. The subscriber MUST implement controls to ensure that only the authorised subject can make use of, or obtain, an activated key in the keystore.
    d. 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.
3. Keys on the keystore MAY be archived. In this case, the archive SHOULD NOT be accessible by anyone other than the trusted administrators.
4. Delivery of activation data to the subject MUST be done by secure means, and MUST authenticate the subject.
    a. Activation data MAY be used with other resources.
5. The Subscriber and the subject MUST protect activation data according to best practices.
6. Activation data MUST be provided to the keystore by secure means. In particular, it MUST NOT be sent in clear, and it MUST protect against machine-in-the-middle attacks, and SHOULD take measures to guard further against phishing.
7. The key SHOULD NOT remain activated for more than 24 hours of inactivity, unless its certificate(s) is (are) SLC(s).
8. The key SHOULD NOT be reused for applying for new certificates.

5 User managed softkeys

1. The subscriber MUST generate the key and activation material, on a trusted system which SHOULD be managed by trusted administrators.
2. If the private key and activation material are generated by the subscriber there is no key delivery. If the private key is generated by an external system:
   a. The generating system 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 operations of the keystore MUST follow the data protection and security policies of the organisation hosting the service. The requirements of the Credential Store Operations guidelines for running a security sensitive service MUST be followed.
   b. The generating system 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.
   c. The generating system MUST implement controls to ensure that only the authorised subject can make use of, or obtain, an activated key in the keystore.
   d. If the generating system 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.)
   e. The generating system MUST securely delete any generated key material after delivery to the subscriber
3. The key MAY be stored by the subscriber for archival purposes in which case it MUST be protected to prevent unauthorised use.
4. If the subscriber is not the same entity as the subject, the subscriber MUST deliver the key and the activation data separately by secure means.
5. The subscriber MUST implement controls[1] to prevent unauthorised use of the activated key - to ensure that only the subscriber and the subject use the private key, and only for permitted purposes.
6. The key SHOULD NOT be stored in activated form unless the CA allows it. If so, it MUST be stored on a secure system.
7. The key SHOULD NOT remain activated for more than 24 hours of inactivity, unless its certificate(s) is (are) SLCs or the CA permits storing keys in activated form.
8. The key SHOULD NOT be reused for requesting new certificates beyond the life time of the key.

[1] This protection, when taking the form of a passphrase, has conventionally been interpreted as being at least 12 characters in lengths and complying with best current practice in choosing high-quality password (equivalent to approximately 27 bits of entropy, according to 800-63-2 (revision 2, 2004))