Category: guidelines document
Status: DRAFT
Document: pk-protection-1.0-20091016.docx
Editor: davidg
Last updated: Fri, 16 October 2009
Total number of pages: 4

Protection of private key data for end-users in local and remote systems

Abstract

This document describes guidelines on the generation and storage of end-user private key material, using secure hardware tokens and appropriate computer systems. It applies to all systems that store key material on which certificates issued by IGTF accredited authorities are based, and may be used as guidance for any system that holds private key material.

This document is an EUGridPMA Guidelines Document, to be referred to as the "Guidelines on Private Key Protection", with OID 1.2.840.113612.5.4.1.1.1.5.

Table of Contents

1 Abstract

This document describes guidelines on the generation and storage of end-user private key material, using secure hardware tokens and appropriate computer systems. It applies to all systems that store key material on which certificates issued by IGTF accredited authorities are based, and may be used as guidance for any system that holds private key material. Footnotes are non-normative explanatory text, and may be removed or updated any time[1]

2 Protection of the end user private key data

This document describes guidelines on the generation and storage of end-user private key material, using secure hardware tokens and appropriate computer systems, the latter being only those computer systems that are physically intact and where the operating system is suitably patched and maintained. All pass phrases should be strong and chosen according to current best practice. Systems that can enforce pass phrase hygiene should do so.

2.1 Generation of private keys

The key material based on which a certificate is issued MUST only be generated by one of the following methods.

1. Inside a secure hardware token
2. Locally on an appropriate computer system of which the user is the sole user and administrator, and where
    a. The key material MUST be generated using trustworthy cryptographic software
3. On an appropriate computer system that is administered by the users home organisation[2], and where
    a. The key material MUST be generated using trustworthy cryptographic software
    b. Access MUST be limited to designated individuals who are subject to and aware of applicable privacy rules and a professional code of conduct[3]
    c. The private key SHALL NOT be sent in clear text over a network.
    d. The pass phrase SHALL NOT be sent in clear text over a network.
    e. The encrypted private key file SHOULD NOT be sent over the network unprotected. Network protections may be via encryption, or by physical control of the network in a trusted environment.
    f. A system SHOULD NOT persistently keep pass phrases or plain text private keys for longer than 24 hours, unless the key pair is used solely as a basis for Short Lived credentials, i.e. the certificate has a total validity of less than 1 Ms.
4. On an appropriate computer system that is administered by a third party4, and where[4]
    a. The key material MUST be generated using trustworthy cryptographic software
    b. Administrative access MUST be limited to designated individuals who are subject to and aware of applicable privacy rules and a professional code of conduct.
    c. The private key SHALL NOT be sent in clear text over a network.
    d. The pass phrase SHALL NOT be sent in clear text over a network.

[1] The aim of this document is to make a qualified trade-off between non-repudiation and current, actual practice. In the case of portals, or any third-party box, requesting certificates on the user's behalf based on key material generated or held by the third party, that box can use that key theoretically without the users' knowledge or consent. This document intends to provide guidelines for such systems, to countermand the loss of user binding by providing policies and operational guidelines.

[2] This covers the 'traditional' method of grid access from a desktop or specific user interface machine within the user's own organization.

[3] The 'professional code of conduct' means an accepted set of rules and behavior that lays down the way in which the administrator goes about business. It may be laid down in organisational policy and practice, by part of a contract, or a specific and defined ethics statement.

[4] This covers the 'traditional' method of grid access from a dedicated user interface hosted by an external computer centre, but also portals that procure certificates on behalf of a user.

e. The encrypted private key file SHOULD NOT be sent over the network unprotected. Network protections may be via encryption, or by physical control of the network in a trusted environment.
f. Key material MUST only be generated in the system as a result of a user action.
g. The host organisation MUST have a defined data privacy and security policy addressing confidentiality.
h. The systems MUST be located in a secure environment, where access is controlled and limited to only authorized personnel.
i. A system SHOULD NOT persistently keep pass phrases or plain text private keys for longer than 24 hours, unless the key pair is used solely as a basis for Short Lived credentials, i.e. the certificate has a total validity of less than 1 Ms[5].

2.2 Storage of key material

The private key for a natural person (user) MUST be stored only in one or more of the following:

1. On a secure hardware token from which it cannot be extracted, protected by a pass phrase
2. On a local file system on an appropriate computer system of which the user is the sole user and administrator, where
   a. the key MUST only ever stored persistently in encrypted form
3. On a local or networked file system on an appropriate computer system that is administered by the users home organisation, protected by a pass phrase. In this case,
   a. the key MUST only ever stored persistently in encrypted form
   b. Data needed to decrypt or use the private key MUST not be held by the system on persistent storage, and MUST not be held by the system administrators. It MUST only be present in the system as a result of a user action, and only for as long as the user is using the system. The activation data and any plain text private keys SHOULD be removed as soon as the user stops using the service, and MUST NOT be kept past 24 hours of inactivity
   c. Administrative access MUST be limited to designated individuals who are subject to and aware of applicable privacy rules and a professional code of conduct.
   d. The private key SHALL NOT be sent in clear text over a network.
   e. The pass phrase SHALL NOT be sent in clear text over a network.
   f. The encrypted private key file SHOULD NOT be sent over the network unprotected. Network protections may be via encryption, or by physical control of the network in a trusted environment.
   g. the system SHOULD NOT persistently keep pass phrases or plain text private keys for longer than 24 hours, unless the key pair is used solely as a basis for Short Lived credentials, i.e. the certificate has a total validity of less than 1 Ms.
4. On a local or networked file system on an appropriate computer system that is administered by third party, provided that
   a. the key MUST only be stored persistently in encrypted form
   b. Data needed to decrypt or use the private key MUST not be held by the system on persistent storage, and MUST not be held by the system administrators. It MUST only be present in the system as a result of a user action, and only for as long as the user is using the system. The activation data and any plain text private

[5] This text is written such that it allows for a portal to request a certificate on the user's behalf (e.g. by redirecting the users to a, potentially federated, SLCS service) and keep the key material in the portal. To off-set the risk of keeping unencrypted private keys on disk for long periods of time, the mechanism as used by, e.g., the ssh-agent system is intended to be used for protection: The portal can itself encrypt it with some other pass phrase and store the key on disk, but keep the (portal-private) activation data to re-read the private key only in-memory (so that it becomes a lot harder to sniff in case the box is broken, in the same way that ssh-agent does it and for the same reasons).

keys SHOULD be removed as soon as the user stops using the service, and MUST NOT be kept past 24 hours of inactivity[6].

c. Administrative access to the storage system MUST be limited to designated individuals. These persons must be subject to and aware of applicable privacy rules and a professional code of conduct.
d. The host organisation MUST have a defined data privacy and security policy.
e. The systems MUST be located in a secured environment, where access is controlled and limited to only authorized personnel.
f. The private key SHALL NOT be sent in clear text over a network.
g. The pass phrase SHALL NOT be sent in clear text over a network.
h. The encrypted private key file SHOULD NOT be sent over the network unprotected. Network protections may be via encryption, or by physical control of the network in a trusted, access-controlled environment.

[6] This text specifically allows for long-running and multi-step work flows to continue in the absence of physical user presence at the portal. The word 'inactivity' should be interpreted as “if a user logs in and starts a long work flow at 3PM, leaves the portal and goes home at 5 PM, but the work flow completes only 48 hours after that, it is perfectly legitimate for this third-party system to hang on to the private key activation data in memory for 56 hours”. If we were to limit the caching of activation data to just 6 (or 24) hours after the user as stopped clicking on the portal (i.e. at 11PM), we would never get any real work done. But if the portal gets rebooted, the activation data is lost and the work flow will terminate once the pending proxies expire (after ~ 12-24 hrs). The 6 or 24-hour period is somewhat arbitrary, and should be synchronised to the characteristic ‘session expiration’ period for most portal applications.