TPM Key Backup and Recovery

For Trusted Platforms

White paper for understanding and support proper use of backup and recovery procedures for Trusted Computing Platforms.

Contents

Executive Summary

The complete trust and security functionality of a Trusted Computing Platform (TCP) is based on the Trusted Platform Module (TPM) silicon chip and its capabilities to store a set of keys safely inside. These keys and certificates have different tasks and usage scenarios:

A. Signing and verifying other key material to show its validity and its integrity within the TP usage and application scenario.

A1 Signing data and keys which belong to this specific TPM and should not be used or are not useful on another TPM (Non migratable keys, e.g. certificate tree inside the TPM based on TPM specific root keys).

A2 Signing data and keys which are referenced to specific users and their application fields (migratable keys, e.g. user specific certificates like mail signing and encryption, user specific SW authentication or service access keys and similar. It could be even necessary that such migratable keys are required on different platforms, which are handled by a user alternatively. This is especially the case for access rights or licenses for SW and similar use areas, where the user wants to have access independently of the platform and related TPM, where he is currently working.

The most dangerous, assumable accident which could happen with a TP is either the defect of a TPM itself or even any damage of a motherboard. It is unusual to repair single components of a motherboard in a maintenance situation; usually the whole motherboard will be replaced. And this is also valid for the TPM on such a motherboard.

If critical data e.g. in a PC are secured by encryption and the related user key is stored in the TPM which can not be replaced in a maintenance situation, a loss of complete information could occur in such a situation. This is even more problematic because one of the ideas behind the TPM is the protection of any key material inside the TPM against all type of attacks and damage and also against denial of service by hardware defects.

To prevent such problems and solve critical situations the TCG standardization group has created some protocol elements to do a secure backup on such critical TPM data and store the backup data on an external storage device. These procedures encrypt all the TPM data for external storage, store them on a safe location selected by the owner and decrypt them again during a recovery procedure.

1. Introduction

The Backup Procedures are designed to offer large scale support not only for standard work flows, but especially also for recovery operations on the system in case of a severe error situation (Motherboard or even TPM damage and replacement).

The worst kind of problem is damage to the Trusted Platform Module (TPM) Security Chip or even with a much higher probability the replacement of a motherboard where out of repair policy the replacement of the old PC will not be possible. A situation with the loss of the TPM would also result in a loss of the TPM Owner key, which is the physical root for secrets as well as the logical root for all User specific keys. Whenever the TPM Security Chip must be replaced, a new Owner key is created, as there is no way to transfer an existing key from one Embedded Security Chip to another. This transfer is not possible due to the digital signing of the owner key which chip specific credentials (like the handle to the chip individual Endorsement key). A transfer of such an SRK to another TPM would disable signature verification with the new TPM and produce loss of validity of all keys and certificates within the chips internal certificate chain.

To overcome this potential problem, an Emergency Recovery mechanism is available together with the Infineon TPM professional SW package. This backup and migration capability is one of the cornerstones to allow the user a comfortable use of the applications without the danger of total data loss due to system errors and missing backup support.

For a simple integration and activation of all this backup and migration features the necessary keys and TPM backup storage reservation will be made already during the TPM activation and take ownership procedure during the installation and set up phase. For an easy handling all the required activities are handled by the TPM owner (usually the system administrator by using the Initialization Wizard.

The restoration in case of emergency is done using the Backup Wizard.

1.1 Implementation:

All these functions are implemented within the Infineon Professional Package which is available as an OEM product and is part of a PC package outfitted with an Infineon TPM. This OEM package will be delivered from nearly every PC manufacturers, which integrates and sells trusted Computing (PC)-Platforms based on an Infineon TPM chip.

In an organization with a large PC fleet and a dedicated IT department it is also advisable to handle these backup versions by a centralized Backup-Server under the control of the IT department, which also initiates the necessary backup, recovery and migration tools and procedures. For planning and installation of such backup infrastructure either the PC manufacturer or also Infineon may have made available some implementation examples and hints.

1.2 Emergency Recovery Token, Password and Archive

The Emergency Recovery concept is similar to Password Reset concerning the usage of token, password and archive.

Restoring user keys in case of emergency requires some information stored in an archive. Emergency Recovery data in this archive can only be used in combination with a recovery token which is protected with a dedicated password.

The archive contains encrypted copies of Basic User keys in order to allow restoration in case of Embedded Security Chip failure. If Emergency Recovery is not set up, users may not be able to restore their encrypted data in case of Embedded Security failure. Emergency Recovery is set up once, and the concerned archive is automatically accessed later by Embedded Security components. The archive file must be accessible for all users of this Embedded Security.

For some general aspects on handling Emergency Recovery refer to the Frequently Asked Questions.

2 Tokens, Archives and other TPM security management files

The Trusted Security SW package uses several files for management tasks such as backup, Emergency Recovery or Password Reset (e.g. tokens and archives). Some of them are for the TPM Owner or Administrator, others are for TPM Security Users. Please make sure not to mix up these file types.

The following table gives an overview of TPM Security management files.

File	Used by...	Purpose/Explanation
Archives used for restoration, Emergency Recovery and Password Reset	Administrator/User	Contain TPM Security credentials, TPM Security settings and Personal Secure Drive backups. Created by automatic and manual backup. Required for restoration in case of a broken hard disk or lost data, exchange of complete motherboard or a broken TPM Security Chip. The Password Reset data in an archive is required to reset Basic User Passwords.
Emergency Recovery Token	Administrator	Created during the configuration of Trusted Security Features. Required for restoration, if Emergency Recovery is needed (broken TPM Security Chip).
Password Reset Token	Administrator	Created during the configuration of Trusted Security Features. Required to prepare the Password Reset for a specific user.
Migration Archive	User	Contains user keys and certificates to be migrated to another Trusted Computing Platform. Created during the *Export* step of migration. Required during the *Import* step of migration.
Personal Secret for Password Reset	User	Created during the configuration of Trusted Security User Settings. Required to reset a user's Basic User Password.
Reset Authorization Code File	Administrator/User	Contains the Reset Authorization Code which is needed to reset a user's Basic User Password. Created during the administrative steps of Password Reset. Required during the user steps of Password Reset.
PKCS #12 file (Personal Information Exchange file)	User	Contains a user's private key and certificate. Needed to import a certificate.

3 Initialize or restore a Trusted Security Platform

There exists a wizard (Application advise and support routine) for supporting you for this feature. The wizard page asks whether you want to initialize or restore the trusted Security SW and data package.

Wizard Page Element	Explanation
Initialize a new Trusted Security	Click here if you want to set up a new Trusted Security. In this case new platform and user credentials will be created.
Restore a Trusted Security from a Backup Archive	Click here if you want to restore a Trusted Security package after a failure, replacement or reset of hardware, storage media or Trusted Platform Module (TPM) Chip. Trusted Security Platform Restoration reestablishes access to Trusted Security Platform Software features for all users.

4 Generating Emergency Recovery Data

Availability of function: This function is only available, if you have selected to configure automatic Trusted Security backups.

This functionality is supported by a wizard (Application advise and support routine) for supporting you for this feature. This wizard is accessible via the Trusted Security management menu.

4.1 Wizard Page Elements

Note that your options within this wizard page may be restricted depending on system policies.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
Create new recovery token	Select this option, if you want to create a new token to be used for Emergency Recovery. The token will be written to the location you have specified. You will have to set a new token password.
Use existing recovery token	Select this option, if the following conditions are met: • In case of emergency, you want to restore your system using an Emergency Recovery Token which was created before. • This token and the token password are currently accessible. You will have to verify the token password, i.e. you need to enter the password only once.
Use existing recovery archive	Select this option, if the following conditions are met: • In case of emergency, you want to restore your system using an Emergency Recovery Token which was created before. • You have access to an archive containing the token's public key. You will not need to enter the token password now. Configuring Emergency Recovery to use an existing token requires only the token's public key. Performing a restoration including Emergency Recovery requires access to the token and knowledge of the token password in any case.
File location Browse...	If your policy settings permit a manual specification of the file location, you may change file name and path. Type in path and file name or browse for it. This file has XML format, the extension *.xml must be used.

If you selected *Create new recovery token*: The Emergency Recovery Token should be saved in a secure location such as a removable media stored in a secure environment. Do not store the recovery token on your hard drive. Otherwise in case of system or hard drive failure, your token will not be accessible and will result in data loss. Store the recovery token on a backup medium like a memory drive or a CD in order to prevent loss of this token and ensure that only you have access to this recovery token.

If you selected *Create new recovery token*, you need to set a new token password. Enter a password for the Emergency Recovery Token.
Consider general hints regarding passwords.

Password If you selected *Use existing recovery token*, you need to verify the token password. Enter the existing token's password.

If you selected *Use existing recovery archive*, you do not need to enter a password.

Confirm Password If you selected *Create new recovery token*, you need to confirm your new password. Enter the password again to confirm.

5 Restore Emergency Recovery Data Step by Step

With the Emergency Recovery data you can restore the main data from the TPM (which contains all user specific key material) in case of failure and subsequent replacement of your TPM Security Chip. The restoration process has two parts:

Part to be performed by an Embedded Security Administrator:

- Recreation of the fundamental TPM functionality (includes the activation of the TPM Security Chip, initialization of the TPM Security Management Functions and restoring Emergency Recovery data).

Performed by all Embedded Security Users:

- Restoration of Basic User Keys in order to gain access to protected data again, or generation of new Basic User Keys (which will result in overwriting existing key material and therefore loss of all existing protected data).

Preconditions:

- **Backup Archive including Emergency Recovery data:** This file is created when the Trusted Security feature Backup is configured. Configuring Backup including Emergency Recovery is highly recommended in order to preserve user data in case of severe system failure. The Backup Archive must be accessible for the restoration process. It should be stored in a fail safe location like a network folder with regular backup. If located on a local hard disk, it is recommended to include this file in a periodical backup. The frequently asked questions cover additional tips on setting up Emergency Recovery data correctly.
- **Emergency Recovery Token:** This file protects Emergency Recovery data in an encrypted form from unauthorized use and requires knowledge of a separate password. It is created when the Embedded Security feature Backup is configured. It should be stored separately from the Backup Archive on a removable storage device in a secure environment. The Emergency Recovery Token must be accessible for the restoration process.

5.1 Administrative Steps

Step 1 - Preparation of the TPM Security Chip	How To:
One possible restoration reason is a failure of your TPM Embedded Security Chip. If this happens, the new chip must be enabled in the system BIOS first. If other hardware caused the malfunction (e.g. hard disk failure), the system must be set up properly (operating system restored, user profile and protected data restored) before the Trusted Security SW can be restored.	This operation is performed by a system administrator. A specific description on how to enable the chip is available here:
Step 2 - Initialization and Restoration of Emergency Recovery Data	How To:
After the TPM Security Chip has been enabled, you must initialize the Security SW package and restore the Emergency Recovery data. Both the Backup Archive file and Emergency Recovery Token file must be accessible to perform this step.	Only the Trusted platform Owner (usually the system Administrator can restore Emergency Recovery data. Start the Trusted Computing TPM Initialization Wizard and select *Restore an Embedded Security from a backup archive*.

5.2 User Step

Recovery of Trusted Computing TPM User and data	How To:
After the administrative operations are finalized, restoration operation for TPM Users can be performed. Restoration must be done for each individual User in a separate step.	Start the Embedded Security User Initialization Wizard. The wizard automatically detects the recovery state immediately after it is started. It offers the choice of creating a new Basic User Key or restoring an existing key from a Backup Archive. Usually an existing key should be recovered, because otherwise all previously encrypted data (still protected by the old Basic User Key) will not be accessible. Follow the on screen directions to finish the process.

Background Information:

Forced User Initialization when Backup Archive is not available:

If the Basic User Key cannot be loaded (for example as a result of clearing Embedded Security Chip ownership and taking ownership again) then Embedded Security User Initialization Wizard does not allow to proceed with user initialization.
The correct step in this situation is to restore Emergency Recovery data.

If for some reason the Backup Archive is not available (for example it was lost or corrupted) then the Basic User Key cannot be restored. To proceed with the creation of a new Basic User Key in this situation the Embedded Security User Initialization Wizard must be started with command line parameter: *SpUserWz.exe /forceinit*.

Note: A new Basic User Key will be created and therefore all previously protected data will be lost.

6 Frequently Asked Questions (FAQ)

6.1.1 Is it a security problem to store Emergency Recovery data on a remote machine?

There is no security problem. The data is protected (encrypted) by the Emergency Recovery Token, which in turn is protected by the Emergency Recovery Token password.

6.1.2 What information is left on a system after a successful uninstallation of the Trusted Security SW package?

If the Trusted Security Software is uninstalled, some TPM backup information and similar data is left on the system. Keeping the platform and user settings and credentials, after a re-installation the system will have the same state as before. Thus no previously encrypted data will be lost after a re-installation of the Trusted Security Software.

However, if this data is no longer needed and the system is to be completely cleaned up, the following data should be deleted.

Backup Archives: The location of automatically written Backup Archives is specified by the administrators. Please note that an automatically written Backup Archive is represented on the file system by an XML file and a folder with the same name, e.g. file `SPSystemBackup.xml` and folder `SPSystemBackup`. Additionally, there may be some manually written Backup Archives.

Emergency Recovery Token: The location is specified by the Embedded Security Owner during Embedded Security initialization.

Emergency Restoration Archive: `\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\RestoreData\<Machine SID>\Users\<User SIDs>\SHTempRestore.xml`

System Data and System Keys Files:

```
\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software
2.0\PlatformKeyData
IFXConfigSys.xml
IFXFeatureSys.xml
TCSps.xml
```

Local Shadow Backup Files:

```
\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software
2.0\BackupData\<Machine SID>\System\SHBackupSys.xml
\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software
2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml
```

User Key Files: `\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TSPps.xml`

TPM Cryptographic Service Provider Container: `\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMcp.xml`

TPM PKCS #11 Provider File: `\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMck.xml`

User Configuration Files: `\%AppData%\Infineon\TPM Software 2.0\UserKeyData\`
`IFXConfig.xml`
`IFXFeature.xml`

Registry keys:
`HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software`
`HKEY_CURRENT_USER\Software\Infineon\TPM software`

The following **Personal Secure Drive** registry keys have to be deleted manually, when the Personal Secure Drive security feature is uninstalled:
`[HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]`
`[HKEY_CURRENT_USER\SOFTWARE\Infineon\TPM Software\PSD]`
`[HKEY_USERS\.DEFAULT\Software\Microsoft\SystemCertificates\PSD]`
`[HKEY_USERS\S-1-5-18\Software\Microsoft\SystemCertificates\PSD]`

Personal Secure Drive Directories: Additionally, the following directories have to be deleted manually:
`x:\Embedded Security\Personal Secure Drive\System Data`
where x: is the drive where Personal Secure Drives are located. This drive is either selected during Personal Secure Drive creation and can therefore be any local hard disk or else is defined by the Personal Secure Drive local user policy.

Miscellaneous:
Registered TPM Embedded Security Chip based certificates
Scheduled Backup Task (e.g. `C:\WINDOWS\Tasks\Embedded Security Backup Schedule`)

6.1.3 How can a Trusted Security Platform be prepared for a successful system backup? Which files are essential for a successful restoration of a Trusted Security Platform using system mechanisms?

The core files of the Trusted Security Platform do not include the applications of the Trusted Security SW package. It can be re-installed after a system backup has been restored.

The Trusted Security Platform Software specific data is backed up using the Trusted Security Platform Backup Wizard.
The Trusted Security Platform Backup Wizard does not backup protected data like your encrypted files or e-mail which have to be backed up utilizing other backup tools. You should include the Backup Archive of the Trusted Security Platform in your routine mass data backup.

Automatic system backups set up by the Embedded Security Administrator include also Emergency Recovery data.

If you do not use the Trusted Security Platform Backup Wizard for the Software specific data, then please make sure to backup all the data listed in the section What information is left on a system after a successful uninstallation?.

6.1.4 How has the Backup Archive to be configured and handled, especially with respect to the policy settings?

You can configure all your enterprise Trusted Platforms to use a common Backup Archive by setting a policy.

In case a new Backup Archive file has to be created, it is very important not to import the policies before the Trusted Security Platform Software has been setup using the Trusted Security Platform Software Initialization Wizard.

The Backup Archive has to be a file with the extension *.xml. This is checked by the system. Any other extension will result in an error situation.

After this, the policy administration has to be started and the policy has to be configured correctly by setting the location of the previously created Backup Archive. Finally the configured file will be used by the Trusted Security Platform Software Initialization Wizard automatically while enrolling the enterprise Embedded Securities.

7 Annex 1: Trusted Platform Module: Security Key and Data Hierarchy

A1.1 Key and certificate chain in the TPM as starting point of the “chain of trust”

As the TPM Specification in accordance with the trust requirements of the TCG is completely public and accessible to all, someone could clone their own TPM on a processor in conformance with this Specification. If e.g. secure e-commerce processes are then transacted, the owner of this "special" TPM could easily modify the internal data to his advantage: such a module would certainly enjoy the full trust of its owner, but would be totally unsuitable for exchanging trusted processes. A trust structure has therefore been implemented which is already known from high-security bank cards:

A1.1.1 Endorsement Key

At the end of TPM chip fabrication (after final testing), the manufacturer generates a 2048 bit private/public key pair in the TPM, the so-called Endorsement Key. This is stored in such a way that the private key (PK) can no longer be read out, but can only be used internally in the TPM. The EK is additionally protected by a special certificate. The manufacturer thereby confirms electronically that this TPM has been produced in a trusted process by an inspected manufacturer and meets the requirements of the Specification. The trustworthiness of the entire TPM system is based for the most part on this process and the uniqueness of the EK. The user must trust the manufacture that the private part of the key is not stored anywhere, and that it is not accessible to anyone else. This aspect is also intensively tested as part of the security evaluation. In the case of qualified manufacturers such as Infineon, this fundamental process is performed in the same certified high-security area as for smart cards.

A1.1.2 Storage Root Key (SRK)

The SRK forms the root of a key hierarchy in which other lower-order keys, but also data (blobs), are securely stored, their trustworthiness therefore depending on the SRK. The SRK is automatically generated by the owner in a “Take Ownership” operation. If the owner of a TPM gives up this ownership, this also deletes the SRK and also makes all the keys protected by it completely unusable, which is welcome for data protection purposes.

A1.1.3 Basic User Key (BUK)

The SRK forms the root of a key hierarchy in which other lower-order keys, but also data (blobs), are securely stored, their trustworthiness therefore depending on the SRK. The SRK is automatically generated by the owner in a “Take Ownership” operation. If the owner of a TPM gives up this ownership, this also deletes the SRK and also makes all the keys protected by it completely unusable, which is welcome for data protection purposes.

A1.1.4 Certificates

Additional confidence in the correctness of the platform is created using further cryptographic certificates which are likewise stored in the TPM:

The **Endorsement Certificate** confirms that the TPM originates from a trusted source. It contains the public key (PK) of the EK and is used for forming the AIK.

The **Platform Certificate** is brought in by the motherboard/PC manufacturer and confirms that a valid TPM has been mounted in a correct platform. It is likewise used for forming AIKs.

The **Conformance Certificate** is issued by a test laboratory and confirms that the security functions of the TPM and motherboard have been positively checked and are compliant with the protection profile of the TCG.

The concatenation of these various certificates, credentials and keys in order to be able to make various security declarations constitutes a highly sophisticated logical system. The interested reader is referred to [TCG01] TCG Specification Architecture Overview, Sect. 4.2.5.

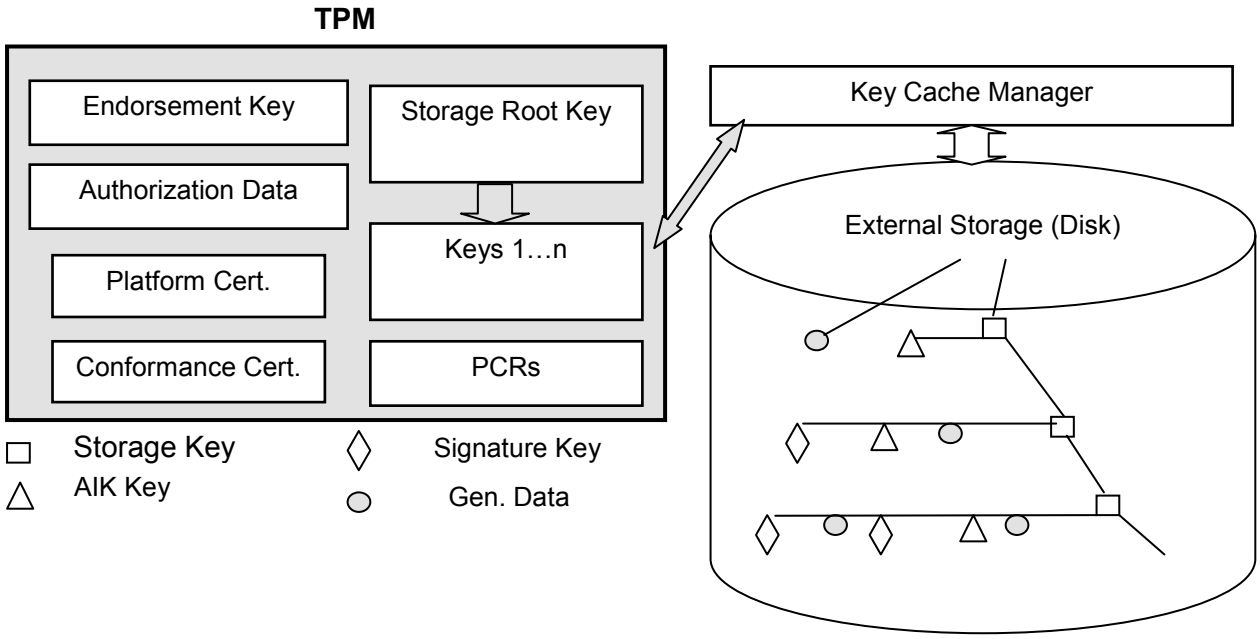

Fig. 5: Certificate chain

A1.2 Key migration

As both platform-related and person-related keys (user keys) can be stored via the TPM, the need arises to transfer the user keys securely to other platforms. For this purpose the TCG has defined a set over rules under the term *migration*:

A1.2.1 Non-migratable keys

(bound to the platform)

Examples :
- EK: Endorsement Key of the TPM manufacturer
- SRK: Storage Root Key

These keys basically cannot be transferred to other TPMs as they are platform-specific. Under the rules, backup (maintenance) is possible as provided for in the Specification.

A1.2.2 Migratable keys

(transferable to other platforms)

Example:
- All the keys (if generated in a migratable manner) and data employed by the user and stored under the storage key.

A1.3 Transport modes

A1.3.1 Migration

(Transfer to other TPMs)

For migration a special authorization process is used and the data material is transported in a password-protected container for security purposes. In practical terms this can be accomplished by a special migration server

A1.3.2 Maintenance

(backing up and restoring key material)
This feature is used for data/key backup in the event of a hardware defect (recommendation only). Implementation by backup server or e.g. smart cards

References

[TCG01] Trusted Computing Group Website: http://www.trustedcomputinggroup.org

Published by:
Infineon Technologies AG
St.-Martin-Strasse 53
81669 Munich, Germany
Phone: +49-89-234-80000
www.infineon.com/TPM
security.chipcards.ics@infineon.com