

Trusted Platform Module (TPM) Quick Reference Guide

System builders/integrators should give this Guide to the system owners to assist them in enabling and activating the Trusted Platform Module.

Warning of Potential Data Loss	3
Trusted Platform Module (TPM)	5
System Requirements	5
Security Precautions	5
Password Procedures	6
Emergency Recovery File Back Up Procedures	7
Hard Drive Image Backup Procedures.....	7
Clear Text Backup (Optional)	7
Trusted Platform Module Ownership.....	8
Trusted Platform Module Software Installation..	8
Enabling the Trusted Platform Module	8
Assuming Trusted Platform Module Ownership..	9
Recovery Procedures	10
How to Recover from a Hard Drive Failure	10
How to Recover from a Desktop Board, coin battery or TPM Failure.....	10
Clearing Trusted Platform Module Ownership ...	11
Support Links	12

E48197-001



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel products are not intended for use in medical, life saving, life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Intel is a trademark of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2008 Intel Corporation

Warning of Potential Data Loss

IMPORTANT USER INFORMATION. READ AND FOLLOW THESE INSTRUCTIONS PRIOR TO TRUSTED PLATFORM MODULE INITIALIZATION.

System integrators, owners, and end users must take precautions to mitigate the chance of data loss. Data encrypted by any program utilizing the Trusted Platform Module (TPM) may become inaccessible or unrecoverable if any of the following occurs:

- **Lost Password:** Loss of any of the passwords associated with the TPM will render encrypted data inaccessible. No password recovery is available. **Read the Security Precautions for Password Procedures.**
- **Removal or draining of coin battery:** The coin battery is required to maintain the TPM's monotonic counters. One major function of the monotonic counters is for anti-replay protection of the internal Intel TPM data. If the battery is removed or exhausted, the Intel TPM data will be deleted in accordance to Trusted Computing Group guidelines. **Read the Security Precautions for Emergency Recovery File Back Up Procedures.**
- **Hard Drive Failure:** In the event of a hard disk (or other storage media) failure that contains encrypted data, an image of the hard disk (or other storage media) must be restored from backup before access to encrypted data may become available. The owner/user should backup the system hard disk on a regular basis. **Read the Security Precautions below for Hard Drive Backup Procedures.**
- **Platform Failure:** In the event of a platform failure and/or replacement of the desktop board, recovery procedures may allow migratable keys to be recovered and may restore access to encrypted data. All non-migratable keys and their associated data will be lost. Both the Wave Systems* EMBASSY* Security Center and Wave Systems EMBASSY Trust Suite utilize migratable keys. Please check any other software that accesses the TPM for migratability. **Read the Security Precautions for Emergency Recovery File Back Up Procedures.**
- **Loss of Trusted Platform Module Ownership:** Trusted Platform Module Ownership/contents may be cleared (via a BIOS switch) to allow for the transfer of a system to a new owner. If TPM ownership is cleared, either intentionally or in error, recovery procedures may allow the migratable

keys to be recovered and may restore access to encrypted data. **Read the Security Precautions for Emergency Recovery File Back Up Procedures.**

Trusted Platform Module (TPM)

The Trusted Platform Module is a component on the desktop board that is specifically designed to enhance platform security above-and-beyond the capabilities of today's software by providing a protected space for key operations and other security critical tasks. Using both hardware and software, the TPM protects encryption and signature keys at their most vulnerable stages—operations when the keys are being used unencrypted in plain-text form.

The TPM is specifically designed to shield unencrypted keys and platform authentication information from software-based attacks.

System Requirements

- Intel® Desktop Boards Executive or Extreme Series
- Microsoft Windows* XP Professional (SP2) or Microsoft Windows Vista* operating system
- NTFS file system
- Microsoft Internet Explorer 5.5 or later
- Adobe* Acrobat* 5.0 or later

Security Precautions

Security, like any other aspect of computer maintenance, requires planning. What is unique about security has to do with understanding who "friends" are and who adversaries are. The TPM provides mechanisms to enable the owner/user to protect their information from adversaries. To provide this protection, the TPM effectively puts "locks" around the data. Just like physical locks, if keys or combinations are lost, the assets (data) may be inaccessible not only to adversaries, but also to the asset owner/user.

The TPM provides two classes of keys: migratable and non-migratable. Migratable keys are designed to protect data that can be used (unencrypted) on more than one platform. One advantage is allowing the key data to be replicated (backed-up and restored) to another platform. This may be because of user convenience (someone uses more than one platform, or the data needs to be available to more than one person operating on different platforms). Another advantage to this type of key is that it can be backed-up and restored from a defective platform onto a new platform.

However, migratable keys may not be the appropriate level of protection needed for the application when the user wants the data restricted to a single platform. This requires a non-migratable key. Non-migratable keys carry with them a usage deficit in that while the key may be backed-up and restored (protected from hard disk failure) they are not protected against system or TPM failure. The very nature of a non-migratable key is that they can be used on one and only one TPM. In the event of a system or TPM failure, all non-migratable keys and the data associated with them will be inaccessible and unrecoverable.

The following precautions and procedures may assist in recovering from any of the previously listed situations. Failure to implement these security precautions and procedures may result in unrecoverable data loss.

Password Procedures

The Wave Systems EMBASSY Security Center software allows users to configure passwords from 8 to 255 characters.

A good password should consist of:

- At least one upper case letter (A to Z)
- At least one numerical character (0 to 9)
- At least one symbol character (!, @, &, etc.)

Example Passwords: "I wear a Brown hat 2 work @ least once-a-month" or "uJGFak&%)adf35a9m"



NOTE

Avoid using names or dates that can be easily guessed, such as birthdays, anniversaries, family member names, or pet names.

All passwords associated with the EMBASSY Security Center (owner, TPM Key Archive, and other archives) as well as the EMBASSY Trust Suite are NOT RECOVERABLE and cannot be reset without the original text. The system owner should document all passwords, store them in a secured location (a vault, safe deposit box, or off-site storage), and have them available for future use.

These documents should be updated after any password changes are made.

Emergency Recovery File Back Up Procedures

Use the EMBASSY Security Center to create the TPM Key Archive file (**keyarchive.xml**) onto a removable media (a floppy, CDR, or flash media). Once this is completed, the removable media should be stored in a secure location. **DO NOT LEAVE ANY COPIES** of the TPM Key Archive on the hard drive or within any hard drive image backups. If a copy of the TPM Key Archive remains on the system, it could be used to compromise the Trusted Platform Module and platform.

This procedure should be repeated after any password changes or the addition of a new user.

Hard Drive Image Backup Procedures

To allow for emergency recovery from a hard drive failure, frequent images of the hard drive should be created and stored in a secure location. In the event of a hard drive failure, the latest image can be restored to a new hard drive and access to the encrypted data can be re-established.



All encrypted and unencrypted data that was added after the last image was created will be lost.

Clear Text Backup (Optional)

It is recommended that system owners follow the Hard Drive Image Backup Procedures.

This option is not recommended because the data is exposed during backup and restores. To backup select files without creating a drive image, files can be moved from secured programs or drive letters to an unencrypted directory. The unencrypted (clear text) files may then be backed up to removable media and stored in a secure location. The advantage of the clear text backup is that no TPM key is required to restore the data.

Trusted Platform Module Ownership

The Trusted Platform Module is disabled by default when shipped and the owner/end customer of the system assumes “ownership” of the TPM. This permits the owner of the system to control initialization of the TPM and create all the passwords associated with the TPM that will be used to protect their keys and data.

System builders/integrators may install both the Wave Systems EMBASSY Security Center and the Wave Systems EMBASSY Trust Suite, but SHOULD NOT attempt to use or activate the TPM or either software package.

Trusted Platform Module Software Installation

The software package for the TPM can be installed from the Intel Express Installer DVD.

Enabling the Trusted Platform Module

The Trusted Platform Module is disabled by default when shipped to insure that the owner/end customer of the system initializes the TPM and configures all security passwords. The owner/end customer should use the following steps to enable the TPM.

1. While the PC is displaying the splash screen (or POST screen), press the <F2> key to enter BIOS.
2. Use the arrow keys to go to the Advanced Menu, select Peripheral Configuration, and then press the <Enter> key.
3. Select the Trusted Platform Module, press <Enter>, and select Enabled and press <Enter> again (display should show: Trusted Platform Module [Enable]).
4. Press the <F10> key, and press Y.
5. The system should reboot and start Microsoft Windows.

Assuming Trusted Platform Module Ownership

Once the TPM has been enabled, ownership must be assumed by using the EMBASSY Security Center. The owner/end user should follow the steps listed below to take ownership of the TPM:

1. Start the system.
2. Launch the EMBASSY Security Center.
3. Select the Owner tab and click on the Establish button.
4. Create the Owner password (before creating any password, review the Password Recommendations made earlier in this document).
5. After successfully taking ownership of the TPM, select the User tab and click on the Initialize button.
6. Enter the Windows login password to create and synchronize the TCG Security Vault Password.
7. To create an archive of the TPM keys, select the Key Manager icon on the left side of the EMBASSY Security Center and click on the Archive button.
8. Choose a location to save the TPM Key Archive file (removable media recommended; see Emergency Recovery File Back Up Procedures for more information).
9. Create a password to protect the TPM Key Archive (this password should not match the Owner password or any other password).
10. Enter the Owner password when prompted.
11. After completing the archive function, the TPM Key Archive (**keyarchive.xml**) that is now on a removable media should be stored in a secure location. No copies of the **keyarchive.xml** should remain on the system. This procedure should be repeated after any password changes or the addition of new users or TPM enabled software.
12. All passwords associated with the EMBASSY Security Center Software (owner, TPM Key Archive, and other passwords) are not recoverable and cannot be reset without the original password. These passwords should be documented and stored in a secured location (vault, safe deposit box, or off-site storage) in case they are needed in the future. These documents should be updated after any password changes.

Recovery Procedures

How to Recover from a Hard Drive Failure

Restore the latest hard drive image from backup to the new hard drive – no TPM specific recovery is necessary.

How to Recover from a Desktop Board, coin battery or TPM Failure

This procedure may restore the migratable keys from the TPM Key Archive, but does not restore any previous keys or content to the TPM. This recovery procedure may restore access to the EMBASSY Trust Suite that is secured with migratable keys.

Requirements

- TPM Key Archive file (**keyarchive.xml** file created with the EMBASSY Security Center)
- TPM Key Archive password (created with the EMBASSY Security Center)
- Owner password
- Working original operating system installation, or a restored image of the hard drive

This recovery procedure may restore the migratable keys from the previously created TPM Key Archive.

1. Replace the desktop board with the same model as the failed board.
2. Start the original operating system or restore the original hard drive image.
3. Start the EMBASSY Security Center.
4. Take ownership of the Trusted Platform Module (see Assuming Trusted Platform Module Ownership, steps 3 and 4 only).
5. To restore a TPM Key Archive, select the Key Manager icon on the left side of the EMBASSY Security Center and click on the Restore button.
6. Enter the password for the TPM Key Archive when prompted.
7. Enter the Owner password when prompted.
8. Restoring the keys may take as long as 5 minutes and you may be prompted for your Windows password.

After the keys have been successfully restored, you should be able to access previously encrypted files.

Clearing Trusted Platform Module Ownership



WARNING

Disconnect the desktop board's power supply from its AC power source before you connect or disconnect cables, or install or remove any board components. Failure to do this can result in personal injury or equipment damage. Some circuitry on the desktop board can continue to operate even though the front panel power switch is off.



CAUTION

DATA ENCRYPTED BY ANY PROGRAM UTILIZING THE TPM WILL BECOME INACCESSIBLE IF TPM OWNERSHIP IS CLEARED. *Recovery procedures may allow the migratable keys to be recovered and might restore access to encrypted data. (Review the Recovery Procedures for detailed instructions).*

Follow the steps below to clear the TPM to transfer ownership of the platform to a new owner.

1. Observe the precaution in the WARNING above before opening the system case.
2. Move the BIOS configuration jumper on the board to pins 2-3.
3. Restore power to the PC and power on.
4. System should automatically enter BIOS setup.
5. Use the arrow keys to select `Clear Trusted Platform Module`, press `<Enter>`.
6. Select `Yes` and press `<Enter>`.
7. Press the `<F10>` key to save and exit, and press `Y`.
8. Power off the system.
9. Review the precaution in the WARNING above.
10. Restore the BIOS configuration jumper on the board to pins 1-2.

When cleared, the TPM module is disabled by default.

Support Links

- For assistance with the Wave System* EMBASSY* Trust Suite visit: <http://www.wave.com/support/ets.html>
- For additional information about TPM and enhancing PC security, visit: <https://www.trustedcomputinggroup.org>