

# Trusted Platform Module (TPM) Quick Reference Guide

---

System builders/integrators should pass this Guide on to the system owner to assist them in enabling and activating the TPM.

- Warning of Potential Data Loss ..... 3**
- Trusted Platform Module (TPM)..... 4**
- System Requirements..... 4**
- Security Precautions..... 4**
  - Password Procedures.....5
  - Emergency Recovery File Back Up Procedures.....5
  - Hard Drive Image Backup Procedures .....6
  - Clear Text Backup (Optional) .....6
- Trusted Platform Module Ownership ..... 6**
- Enabling the Trusted Platform Module ..... 6**
- Assuming Trusted Platform Module Ownership ..... 7**
- Recovery Procedures ..... 8**
  - How to recover from a hard drive failure .....8
  - How to recover from a desktop board or TPM failure .....8
- Clearing Trusted Platform Module Ownership ..... 10**
- Support Links ..... 10**

C64174-002



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 or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

Copyright © 2004 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.**
- **Hard Drive Failure:** In the event of a failure of a hard disk (or other storage media) 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 motherboard, 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 Infineon\* Security Platform software 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

- Boxed Intel® Desktop Board D915GEV with Gigabit Ethernet solution or Boxed Intel® Desktop Board D915GUX with Gigabit Ethernet solution
- Microsoft Windows® 2000 Professional (SP4) or Microsoft Windows XP Professional (SP1)
- NTFS file system required
- Microsoft Internet Explorer® 5.5 or later
- Adobe® Acrobat® 5.0 or later (included on Intel® Express Installer CD)

## Security Precautions

Security, like any other aspect of computer maintenance requires planning. What is unique about security has to do with understanding who "friends" and 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 (i.e., data) may be inaccessible not only to adversaries, but also to 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 (i.e., unencrypted) on more than one platform. This has the advantage of 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). This type of key also has the advantage in 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 (e.g., the user wants the data restricted to a single platform) needed for the application. 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 (i.e., 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 Infineon Security Platform software allows users to configure passwords from 6 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: birthdays, anniversaries, family member names, pet names, etc.*

All passwords associated with the Infineon Security Platform software (Owner, Emergency Recovery Token, and User passwords) and the Wave Systems 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 (vault, safe deposit box, off-site storage, etc.), and have them available for future use. These documents should be updated after any password changes.

## Emergency Recovery File Back Up Procedures

The Emergency Recovery Token (**SPEmRecToken.xml**) must be saved or moved to a removable media (floppy, USB drive, CDR, flash media, etc). Once this is done, the removable media should be stored in a secure location. DO NOT LEAVE ANY COPIES of the Emergency Recovery Token on the hard drive or within any hard drive image backups. If a copy of the Emergency Recovery Token remains on the system, it could be used to compromise the Trusted Platform Module and platform.

After completing the Infineon Security Platform User Initialization Wizard, a copy of the Emergency Recovery Archive (**SPEmRecArchive.xml**) should be

copied to a removable media and stored in a secure location. 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 may be re-established.



### NOTE

*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. 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 a 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. This option is not recommended because the data is exposed during backup and restore.

## 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 is used to protect their keys and data.

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

## 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 [Enabled]).
4. Press the <F10> key, select Ok and press <Enter>.
5. 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 Infineon Security Platform Software. The owner/end user should follow the steps listed below to take ownership of the TPM:

1. Start the system.
2. Launch the Infineon Security Platform Initialization Wizard.
3. Create Owner password (before creating any password, review the Password Recommendations made earlier in this document).
4. Create a new Recovery Archive (note the file name and location).
5. Specify a Security Platform Emergency Recovery Token password and location. (this password should not match the Owner password or any other password).
6. Define where to save the Emergency Recovery Token (note the file location and name).
7. The software will then create recovery archive files and finalize ownership of the TPM.
8. After completing the Infineon Security Platform Initialization Wizard, the Emergency Recovery Token (**SPEmRecToken.xml**) must be moved to a removable media (floppy, CDR, flash media, etc) if the file was not saved to a removable media during installation. Once this is done, the removable media should be stored in a secure location. No copies of this Emergency Recovery Token file should remain on the system. If a copy remains on the system, it could be used to compromise the security of the platform.
9. Launch the Infineon Security Platform User Initialization Wizard.
10. Create a Basic User password (this password is the most frequently used and should not match any other password).
11. Select and configure Security Platform features for this user.
12. After completing the Infineon Security Platform User Initialization Wizard, a copy of the Emergency Recovery Archive (**SPEmRecArchive.xml**) should be copied to a removable media and stored in a secure location. This procedure should be repeated after any password changes or the addition of new users.
13. Restart the system.

14. To backup the keys for the EMBASSY Trust Suite, the Key Transfer Manager software must be configured. Launch the Key Transfer Manager from the program menu.
15. Follow the instructions and create and document the locations for both the archive and restoration key files. The key archive should be located on a removable media and stored in a secure location when not in use.
16. Create and document the password to protect the key archive.
17. Provide the TPM Owner password to allow the Key Transfer Manager to create the archive and restoration key files.
18. Upon completing the configuration of the Key Transfer Manager, it will place an icon in the task bar and automatically back up all new and updated keys associated with the EMBASSY Trust Suite. If the removable media that contains the archive file is not present when a new key is generated, then keys will have to be manually backed up using the Key Transfer Manager when the removable media is available.
19. All passwords associated with the Infineon Security Platform Software (Owner, Emergency Recovery Token, and User passwords) and Wave Systems EMBASSY Trust Suite and Key Transfer Manager are not recoverable and cannot be reset without the original text. These passwords should be documented and stored in a secured location (vault, safe deposit box, off-site storage, etc.) in case they are needed in the future. These documents and files 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 or TPM failure

This procedure may restore the migratable keys from the Emergency Recovery Archive, and does not restore any previous keys or content to the TPM. This recovery procedure may restore access to the Infineon Security Platform software and Wave Systems EMBASSY Trust Suite that are secured with migratable keys.

#### Requirements

- Emergency Recovery Archive (created with the Infineon Security Platform Initiation Wizard)
- Emergency Recovery Token (created with the Infineon Security Platform Initiation Wizard)



- Emergency Recovery Token Security Password (created with the Infineon Security Platform Initiation Wizard)
- Working original operating system (OS) installation, or a restored image of the hard drive
- Wave Systems Key Transfer Manager archive password
- TPM Ownership password

**This recovery procedure only restores the migratable keys from the previously created Recovery Archives.**

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 Infineon Security Platform Initialization Wizard and check the “I want to restore the existing Security Platform” box.
4. Follow the instructions during the Security Platform Initialization, and append the Emergency Recovery Archive to the existing archive.
5. Provide all the necessary passwords, files, and file locations as requested. It may take up to 20 minutes for Security Platform Initialization Wizard to restore the security platform settings.
6. Start User Initialization Wizard. Select “Recover your Basic User Key” when prompted. Specify the original Basic User Key password and proceed with the wizard.
7. When re-configuring the Personal Secure Drive, select “I want to change my Personal Secure Drive setting”, confirm the drive letter and name are correct, and then proceed through the rest of the wizard.
8. Restart the system when requested.
9. To restore access to the EMBASSY Trust Suite, right mouse click on the Key Transfer Manager icon located in the taskbar in the lower right corner of the screen, and select Restore TPM Keys.
10. Provide all the necessary passwords, files, and file locations as requested by the Key Transfer Manager.

Upon successful completion of all steps, 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).*

The TPM may be cleared to transfer ownership of the platform to a new owner.

1. Observe precautions in the above WARNING then open the system case.
2. Move the 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. If you agree to the warning message select Ok and press <Enter>.
7. Press the <F10> key to save and exit, select Ok and press <Enter>.
8. Power off the system.
9. Review precautions in the WARNING above.
10. Restore the configuration jumper on the board to pins 1-2.

When cleared, the TPM module is disabled by default.

## Support Links

- For assistance with the Infineon Security Platform Software visit:  
<http://www.infineon.com>
- 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:  
<http://www.trustedcomputinggroup.org/home>