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.

C52834-002

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.

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 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 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* Trusted 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 Board D865GRH
- 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 are "friends" and who are adversaries. 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 available for future use. These documents should be updated after any password changes.

Emergency Recovery File Back Up Procedures

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). 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 can 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 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 procedures.

Trusted Platform Module Ownership

The Trusted Platform Module ships disabled by default and the owner/end customer of the system assume “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 ships disabled by default 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 location and name).
5. Create a Security Platform Emergency Recovery Token password (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 removable media (floppy, CDR, flash media, etc). Once this 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 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 removable media and stored in a secure location. This procedure should be repeated after any password changes or the addition of new user.
13. All passwords associated with the Infineon Security Platform Software (Owner, Emergency Recovery Token, and User passwords) 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 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

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

1. Replace the desktop board with the same model as the failed board.
2. Start the original OS or restore the original hard drive image.
3. Start the Infineon Security Platform Initialization Wizard.
4. During the Security Platform initialization, DO NOT overwrite the existing Emergency Recovery Archive or Emergency Recovery Token. Upon completion, DO NOT start User Initialization Wizard.
5. Start the Infineon Security Platform Initialization Wizard in recovery mode (C:\Program Files\…\SpTPMWz.exe -restore).
6. Specify the location of the Emergency Recovery Archive, Emergency Recovery Token to restore (from backup), and original Emergency Recovery Token password. Select the original machine name (it should match the current machine name). Finish the Wizard.
7. Start User Initialization Wizard. Select “Recover your Basic User Key” when prompted. Specify the original Basic User Key password. Finish Wizard.

You should be able to access previously encrypted files now.

Clearing Trusted Platform Module Ownership

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

⚠ **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).*

⚠ **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.

1. Observe precautions in the above WARNING then open the system case.
2. Move the configuration jumper (J9J4) 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 (J9J4) 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* Trusted Suite visit:
http://www.wave.com/support/ets.html

For additional information about TPM and enhancing PC security, visit:
https://www.trustedcomputinggroup.org

Schnellreferenz zum Trusted Platform Module (TPM)

Systemhersteller/-integratoren sollten diese Schnellreferenz zum Trusted Platform Module dem Systembesitzer übergeben, um diesen beim Aktivieren und Initialisieren des TPM zu unterstützen.

DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN IN VERBINDUNG MIT INTEL®-PRODUKTEN ZUR VERFÜGUNG GESTELLT. DIE BEREITSTELLUNG DIESES DOKUMENTS STELLT WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND ODER DURCH RECHTSVERWIRKUNG ODER AUF SONSTIGE WEISE EINE GEWÄHRUNG EINER LIZENZ AN GEISTIGEN EIGENTUMSRECHTEN DAR. MIT AUSNAHME DER BESTIMMUNGEN IN DEN ALLGEMEINEN GESCHÄFTSBEDINGUNGEN VON INTEL ÜBERNIMMT INTEL KEINE WIE AUCH IMMER GEARTETE HAFTUNG UND GEWÄHRT WEDER EINE AUSDRÜCKLICHE NOCH EINE STILLSCHWEIGENDE GARANTIE BEZÜGLICH DES VERKAUFS UND/ODER DER VERWENDUNG VON INTEL-PRODUKTEN, EINSCHLIESSLICH HAFTUNG UND GEWÄHRLEISTUNG BEZÜGLICH DER ANWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK, VERKÄUFLICHKEIT ODER VERLETZUNG VON PATENT- UND URHEBERRECHTEN. Intel-Produkte sind nicht für die Verwendung in medizinischen, lebensrettenden oder lebenserhaltenden Anwendungen vorgesehen.
Intel behält sich das Recht vor, die Spezifikationen und Produktbeschreibungen jederzeit ohne Ankündigung zu ändern.

Intel ist eine Marke bzw. eingetragene Marke der Intel Corporation oder ihrer Tochterunternehmen in den Vereinigten Staaten und anderen Ländern.

* Andere Namen und Marken können das Eigentum Dritter sein.

Warnung vor möglichem Datenverlust

WICHTIGE ANWENDERINFORMATION! LESEN UND BEFOLGEN SIE DIE ANWEISUNGEN, BEVOR SIE DAS TRUSTED PLATFORM MODULE INITIALISIEREN.

Systemintegratoren, Besitzer und Endanwender müssen Vorsichtsmaßnahmen treffen, um das Risiko eines Datenverlustes zu mindern. Daten, die durch ein beliebiges Programm unter Verwendung des Trusted Platform Module (TPM) verschlüsselt wurden, können in den folgenden Fällen unzugänglich und/oder nicht wiederherstellbar werden:

- Verlust des Passworts: Wenn ein beliebiges Passwort im Zusammenhang mit dem TPM verloren gegangen ist, kann auf die verschlüsselten Daten nicht mehr zugegriffen werden. Eine Wiederherstellung des Passworts ist nicht möglich. **Lesen Sie die Sicherheitsvorkehrungen für Passwortprozeduren.**
- Ausfall der Festplatte: Wenn eine Festplatte (oder ein anderes Speichermedium) mit verschlüsselten Daten ausfällt, muss ein Abbild der Festplatte (oder des Speichermediums) aus einer Sicherheitskopie wiederhergestellt werden, bevor der Zugriff auf verschlüsselte Daten möglich ist. Besitzer/Anwender sollten regelmäßig Sicherheitskopien der Systemfestplatte erstellen. **Lesen Sie die folgenden Sicherheitsvorkehrungen für Festplattensicherungen.**
- Ausfall der Plattform: Wenn die Plattform einen Defekt aufweist oder das Motherboard ausgetauscht wird, können Wiederherstellungsprozeduren migrationsfähige Schlüssel zurückgewinnen und erneut Zugriff auf verschlüsselte Daten ermöglichen. Alle nicht migrationsfähigen Schlüssel und damit verbundene Daten gehen verloren. Sowohl die Infineon* Security Platform-Software als auch die Wave Systems EMBASSY* Trusted Suite verwenden migrationsfähige Schlüssel. Prüfen Sie andere Software, die auf das TPM zugreift, auf Migrationsfähigkeit. **Lesen Sie die Sicherheitsvorkehrungen für Datenwiederherstellungen im Notfall.**
- Verlust der Besitzerkennung des TPM: Die Besitzerkennung/Inhalte des TPM können durch einen BIOS-Schalter gelöscht werden, um das System auf einen anderen Besitzer zu übertragen. Wird die Besitzerkennung des TPM gelöscht (absichtlich oder versehentlich), können Wiederherstellungsprozeduren die migrationsfähigen Schlüssel zurückgewinnen und den Zugriff auf verschlüsselte Daten wiederherstellen. **Lesen Sie die Sicherheitsvorkehrungen für Datenwiederherstellungen im Notfall.**

Trusted Platform Module (TPM)

Das Trusted Platform Module ist eine Komponente auf dem Desktop Board, welche speziell zur Erhöhung der Sicherheit der Plattform entwickelt wurde. Diese Komponente übertrifft die heutigen Möglichkeiten der Software, indem sie einen geschützten Speicher für Schlüsseloperationen und andere sicherheitskritische Aufgaben bereitstellt. Das TPM bedient sich sowohl der Software als auch der Hardware, um Schlüssel und Signaturen in deren kritischster Phase zu schützen: Operationen, zu denen diese Daten unverschlüsselt in Klartextform verwendet werden. Das TPM wurde speziell dazu entwickelt, unverschlüsselte Schlüssel und Authentifikationsdaten der Plattform vor softwarebasierten Angriffen zu schützen.

Systemanforderungen

- Intel® Desktop Board D865GRH
- Microsoft* Windows* 2000 Professional (SP4) oder Microsoft Windows XP Professional (SP1)
- NTFS-Dateisystem erforderlich
- Microsoft Internet Explorer* 5.5 oder höher
- Adobe* Acrobat* 5.0 oder höher (auf Intel® Express Installer CD enthalten)

Sicherheitsvorkehrungen

Sicherheit erfordert wie jeder andere Aspekt des Unterhalts eines Computers Planung. Grundlegend für die Sicherheit ist das Verständnis für die Unterscheidung zwischen "Freunden" und "Gegnern". Das TPM stellt dem Besitzer/Anwender Mechanismen zur Verfügung, um dessen Daten vor Gegnern zu schützen. Hierzu schließt das TPM bildlich gesehen die Daten ein. Wie bei echten Türschlössern sind die Dinge dahinter (hier: die Daten) nicht nur für Gegner unzugänglich, sondern auch für die Besitzer/Anwender, wenn Schlüssel oder Kombinationen verloren gehen.

Das TPM stellt zwei Klassen von Schlüsseln zur Verfügung: migrationsfähige und nicht migrationsfähige. Migrationsfähige Schlüssel sind dafür konzipiert, Daten zu schützen, die auf mehreren Plattformen verwendet werden sollen. Daher können die Schlüsseldaten selbst auf einer anderen Plattform dupliziert (gesichert und zurückgelesen) werden. Dies kann aus Bequemlichkeitsgründen so gestaltet sein (jemand arbeitet z. B. auf mehreren Plattformen oder die Daten müssen für mehrere Personen auf verschiedenen Plattformen zugänglich sein). Schlüssel dieses Typs haben darüber hinaus den Vorteil, dass sie von einer defekten Plattform gesichert und auf eine neue zurückgelesen werden können. Allerdings bieten migrationsfähige Schlüssel möglicherweise nicht den erforderlichen Sicherheitsgrad für den gewünschten Anwendungszweck (z. B. wenn ein Anwender die Daten nur auf eine einzige Plattform beschränken will). Dies erfordert einen nicht migrationsfähigen Schlüssel. Nicht migrationsfähige Schlüssel können zwar gesichert und zurückgelesen werden (z. B. im Falle defekter Festplatten), haben aber den inhärenten Nachteil, nicht gegen Versagen des Systems oder des TPM geschützt zu sein. Ein nicht migrationsfähiger Schlüssel kann bestimmungsgemäß nur für ein einziges TPM verwendet werden. Fällt das System oder das TPM aus, sind sowohl alle nicht migrationsfähigen Schlüssel als auch alle damit verschlüsselten Daten unzugänglich und nicht wiederherstellbar.

Folgende Sicherheitsvorkehrungen und Prozeduren helfen Ihnen, Daten aus einer der vorstehend beschriebenen Situationen wiederherzustellen. Wenn Sie diese Sicherheitsvorkehrungen und Prozeduren nicht treffen bzw. durchführen, kann irreversibler Datenverlust eintreten.

Passwortprozeduren

Unter der Infineon Security Platform-Software können Anwender Passwörter mit einer Länge von 6 bis 255 Zeichen definieren.

Ein gutes Passwort sollte bestehen aus:

- mindestens einem Großbuchstaben (A bis Z)
- mindestens einer Ziffer (0 bis 9)
- mindestens einem Sonderzeichen (!, @, & usw.)

Passwortbeispiele: “Ich esse 1 Ei bei DeR @rbeiT mindestens 1x-im-monat” oder “uJGFak&%)adf35a9m”

HINWEIS

Vermeiden Sie Namen oder Daten, die leicht zu erraten sind: Geburtstage, Jubiläen, Namen von Familienmitgliedern, Haustiernamen usw.

Alle mit der Infineon Security Platform-Software sowie mit der Wave Systems* EMBASSY* Trust Suite verknüpften Passwörter (Besitzer, Notfall-Token, Anwender) sind NICHT ERSETZBAR und können nicht ohne die Originale zurückgesetzt werden. Der Systembesitzer sollte alle Passwörter dokumentieren und an einem sicheren Ort für zukünftige Nutzung zugänglich aufbewahren (Wertschrank, Tresor oder an einem entfernten Ort). Die dokumentierten Passwörter müssen nach jeder Passwortänderung aktualisiert werden.

Sicherheitsvorkehrungen für Datenwiederherstellungen im Notfall

Nach dem Festigstellen des Initialisierungsassistenten der Infineon Security Platform muss das Notfall-Token (**SPEmRecToken.xml**) auf einen entnehmbaren Datenträger verschoben werden (Diskette, CD-R, Flash-Medium usw.). Danach sollte der entnehmbare Datenträger an einem sicheren Ort aufbewahrt werden. Belassen Sie KEINERLEI KOPIEN des Notfall-Token auf der Festplatte oder innerhalb von Festplattensicherungen. Wird eine Kopie des Notfall-Token auf dem System belassen, kann sie dazu verwendet werden, die Sicherheitsfunktionen des TPM und der Plattform zu umgehen.

Nachdem Sie den Anwender-Initialisierungsassistenten der Infineon Security Platform fertig gestellt haben, sollten Sie eine Kopie des Notfallarchivs (**SPEmRecArchive.xml**) auf einen entnehmbaren Datenträger kopieren und diesen an einem sicheren Ort aufbewahren. Diese Prozedur muss nach jeder Passwortänderung und nach jedem Hinzufügen eines neuen Anwenders wiederholt werden.

Prozeduren zur Festplattensicherung

Um im Notfall Daten bei Versagen der Festplatte wiederherzustellen, sollten in kurzen Abständen Datenabbilder der Festplatte erstellt und an einem sicheren Ort aufbewahrt werden. Das letzte Abbild kann somit im Fall des Ausfalls der Festplatte auf eine neue zurückgelesen werden, und die verschlüsselten Daten können zurückgewonnen werden.

HINWEIS

Alle verschlüsselten und unverschlüsselten Daten, die nach der letzten Sicherung hinzugefügt wurden, gehen dabei verloren.

Klartext-Sicherung (optional)

Es wird empfohlen, dass Systembesitzer nach den Prozeduren zur Festplattensicherung vorgehen. Um einzelne, ausgewählte Dateien ohne Abbilderstellung zu sichern, können diese von gesicherten Programmen oder Quellpfaden in einen unverschlüsselten Ordner kopiert werden. Die unverschlüsselten (Klartext-) Dateien können dann auf ein Wechselmedium gesichert und an einem sicheren Ort aufbewahrt werden. Die Klartext-Sicherung hat den Vorteil, dass kein TPM-Schlüssel zum Wiederherstellen der Daten benötigt wird. Diese Option wird nicht empfohlen, weil die Daten dem Risiko des unberechtigten Zugriffs während der Sicherungs- und Wiederherstellungsvorgänge ausgesetzt sind.

Trusted Platform Module - Besitzerkennung

Das Trusted Platform Module ist im Auslieferungszustand deaktiviert, und der Besitzer/Anwender des Systems erlangt den “Besitz” des TPM. Dies erlaubt dem Besitzer des Systems, die Initialisierung des TPM zu steuern und alle damit verknüpften Passwörter zu erstellen, die zum Schutz der Schlüssel und der Daten dienen.

Systemintegratoren und -hersteller können zwar sowohl die Infineon Security Platform-Software als auch die Wave System EMBASSY Trust Suite installieren, sollten aber NICHT VERSUCHEN, die Software oder das TPM zu aktivieren oder zu verwenden.

Trusted Platform Module aktivieren

Das Trusted Platform Module ist im Auslieferungszustand standardmäßig deaktiviert, um sicherzustellen, dass der Besitzer/Endanwender des Systems das TPM initialisiert und alle seiner Sicherheitspasswörter konfiguriert. Der Besitzer/Endanwender sollte nach folgenden Schritten vorgehen, um das TPM zu aktivieren:

1. Während der PC den Splash-Bildschirm (oder POST-Bildschirm) anzeigt, drücken Sie <F2>, um ins BIOS-Setup-Programm zu gelangen.
2. Verwenden Sie die Pfeiltasten, um zum Menü “Advanced” zu gelangen, wählen Sie “Peripheral Configuration” und drücken Sie die <Eingabetaste>.
3. Wählen Sie den Eintrag “Trusted Platform Module”, drücken Sie die <Eingabetaste> und wählen Sie “Enabled”. Bestätigen Sie die Wahl mit der <Eingabetaste>; die Anzeige sollte folgende Meldung zeigen: `Trusted Platform Module [Enabled]`).

4. Drücken Sie <F10>, wählen Sie OK und drücken Sie die <Eingabetaste>.
5. Das System sollte erneut starten und Microsoft Windows laden.

Besitzerkennung des TPM annehmen

Nach der Aktivierung des TPM muss die Besitzerkennung angenommen werden, indem die Infineon Security Platform-Software gestartet wird. Der Besitzer/Endanwender sollte nach folgenden Schritten vorgehen, um die Besitzerkennung des TPM zu übernehmen:

1. Starten Sie das System.
2. Starten Sie den Initialisierungsassistenten der Infineon Security Platform.
3. Erstellen Sie das Besitzerpasswort (lesen Sie vor dem Erstellen von Passwörtern die obigen Empfehlungen hierzu).
4. Erstellen Sie ein neues Wiederherstellungsarchiv (notieren Sie sich den Speicherort und den Namen der Datei).
5. Erstellen Sie das Notfall-Token der Security Platform (dieses Passwort darf nicht identisch mit dem Besitzer- oder einem anderen Passwort sein).
6. Geben Sie an, wo das Notfall-Token gespeichert werden soll (notieren Sie sich den Speicherort und den Namen der Datei).
7. Die Software erstellt daraufhin die Wiederherstellungs-Archivdateien und schließt die Besitznahme des TPM ab.
8. Nach dem Festigstellen des Initialisierungsassistenten der Infineon Security Platform muss das Notfall-Token (**SPEmRecToken.xml**) auf einen entnehmbaren Datenträger verschoben werden (Diskette, CD-R, Flash-Medium usw.). Danach sollte der entnehmbare Datenträger an einem sicheren Ort aufbewahrt werden. Auf dem System sollten keine Kopien dieses Notfall-Token verbleiben. Verbleibt eine Kopie auf dem System, kann diese dazu verwendet werden, die Sicherheitsmaßnahmen der Plattform zu umgehen.
9. Starten Sie den Anwender-Initialisierungsassistenten der Infineon Security Platform.
10. Erstellen Sie ein Benutzerpasswort (dieses Passwort ist das meistverwendete und sollte mit keinem anderen Passwort übereinstimmen).
11. Wählen und konfigurieren Sie die Eigenschaften der Security Platform für diesen Anwender.
12. Nachdem Sie den Anwender-Initialisierungsassistenten der Infineon Security Platform fertiggestellt haben, sollten Sie eine Kopie des Notfallarchivs (**SPEmRecArchive.xml**) auf einen entnehmbaren Datenträger kopieren und diesen an einem sicheren Ort aufbewahren. Diese Prozedur muss nach jeder Passwortänderung und nach jedem Hinzufügen eines neuen Anwenders wiederholt werden.
13. Alle mit der Infineon Security Platform-Software verknüpften Passwörter (Besitzer, Notfall-Token, Anwender) sind NICHT ERSETZBAR und können nicht ohne die Originale zurückgesetzt werden. Diese Passwörter sollten dokumentiert und an einem sicheren Ort aufbewahrt werden (Wertschrank, Tresor oder an einem entfernten Ort), falls sie zukünftig benötigt werden. Die dokumentierten Passwörter müssen nach jeder Passwortänderung aktualisiert werden.

Wiederherstellungsprozeduren

So stellen Sie Daten nach Ausfall der Festplatte wieder her:

Schreiben Sie das letzte Datenabbild aus der Sicherung auf die neue Festplatte; ein TPM-spezifisches Wiederherstellen ist nicht erforderlich.

So stellen Sie Daten nach einem Ausfall des Desktop Board oder des TPM wieder her:

Mit dieser Prozedur können migrationsfähige Schlüssel aus dem Notfallarchiv wiederhergestellt, aber keinerlei vorherige Schlüssel oder TPM-Inhalte wiederhergestellt werden. Mit dieser Wiederherstellungsprozedur kann der Zugang zur Infineon Security Platform-Software und zur Wave Systems EMBASSY Trust Suite wieder gewährleistet werden, sofern diese mit migrationsfähigen Schlüsseln abgesichert wurden.

Anforderungen

- Notfall-Archiv (erstellt mit dem Initialisierungsassistenten der Infineon Security Platform)
- Notfall-Token (erstellt mit dem Initialisierungsassistenten der Infineon Security Platform)
- Sicherheitspasswort zum Notfall-Token (erstellt mit dem Initialisierungsassistenten der Infineon Security Platform)
- Funktionierende Originalinstallation des Betriebssystems (OS) oder wiederhergestelltes Datenabbild der Festplatte

Diese Wiederherstellungsprozedur stellt lediglich die migrationsfähigen Schlüssel aus der vorher erstellten Archivdatei wieder her.

1. Ersetzen Sie das defekte Desktop Board durch ein gleiches Modell.
2. Starten Sie das Original-Betriebssystem, oder stellen Sie das Datenabbild der Festplatte wieder her.
3. Starten Sie den Initialisierungsassistenten der Infineon Security Platform.
4. Überschreiben Sie während der Initialisierung der Security Platform NICHT das bestehende Notfallarchiv und das Notfall-Token. Starten Sie danach NICHT den Anwender-Initialisierungsassistenten.
5. Starten Sie den Initialisierungsassistenten der Infineon Security Platform im Wiederherstellungsmodus (C:\Programme\…\SpTPMWz.exe -restore).
6. Geben Sie den Speicherort des Notfallarchivs, des wiederherzustellenden Notfall-Token (aus der Sicherung) und das ursprüngliche Passwort zum Notfall-Token ein. Wählen Sie den ursprünglichen Namen des Computers (dieser sollte mit dem aktuellen Namen des Computers übereinstimmen). Beenden Sie den Assistenten.
7. Starten Sie den Anwender-Initialisierungsassistenten. Wählen Sie “Recover your Basic User Key”. Geben Sie das ursprüngliche Benutzerpasswort ein. Beenden Sie den Assistenten.

Nun sollten Sie Dateien entschlüsseln können.

Trusted Platform Module – Besitzerkennung löschen

Das TPM kann gelöscht werden, um den Besitz der Plattform auf einen neuen Besitzer zu übertragen.

⚠ **VORSICHT**

WENN DIE BESITZERKENNUNG GELÖSCHT WURDE, SIND DIE MIT EINEM BELIEBIGEN PROGRAMM UNTER VERWENDUNG DES TPM VERSCHLÜSSELTEN DATEN NICHT MEHR ZUGÄNGLICH. *Wiederherstellungsprozeduren können migrationsfähige Schlüssel und den Zugriff auf verschlüsselte Daten wiederherstellen. (Detaillierte Anweisungen hierzu finden Sie unter Wiederherstellungsprozeduren.)*

⚠ **WARNUNG**

Ziehen Sie den Netzstecker vom Netzteil für das Desktop Board ab, bevor Sie Kabel anschließen oder entfernen oder Komponenten des Board installieren oder entfernen. Wenn Sie den Computer vor dem Öffnen des Gehäuses nicht vom Stromnetz trennen, kann dies zur Verletzung von Personen oder Beschädigung von Sachgut führen. Bestimmte Schaltkreise auf dem Desktop Board können weiterhin Strom führen, auch wenn das System am Netzschalter auf der Vorderseite ausgeschaltet wurde.

1. Öffnen Sie unter Beachtung der Vorkehrungen in der obigen Warnung das Systemgehäuse.
2. Bringen Sie die Steckbrücke (J9J4) auf dem Board in die Position 2-3.
3. Stellen Sie die Stromversorgung wieder her, und schalten Sie das System ein.
4. Das System sollte automatisch das BIOS-Setup-Programm aufrufen.
5. Wählen Sie mit den Pfeiltasten “Clear Trusted Platform Module”, und drücken Sie die <Eingabetaste>.
6. Bestätigen Sie die Warnmeldung, indem Sie “OK” wählen und die <Eingabetaste> drücken.
7. Drücken Sie <F10> zum Speichern und Beenden, wählen Sie “OK” und drücken Sie die <Eingabetaste>.
8. Schalten Sie das System aus.
9. Beachten Sie die Vorkehrungen in der obigen WARNUNG.
10. Bringen Sie die Steckbrücke (J9J4) auf dem Board in die Position 1-2.

Nach dem Löschen ist das TPM standardmäßig deaktiviert.

Links zur Unterstützung

Unterstützung zur Infineon* Security Platform Software erhalten Sie auf der Webseite: http://www.infineon.com

Unterstützung der Wave System* EMBASSY* Trusted Suite erhalten Sie auf der Webseite: http://www.wave.com/support/ets.html

Zusätzliche Informationen zum TPM und zur Erhöhung der PC-Sicherheit erhalten Sie unter: https://www.trustedcomputinggroup.org

Guía de referencia rápida del Módulo de plataforma fiable (TPM)

Los desarrolladores e integradores de sistemas deberán pasar esta guía al propietario del sistema con el fin de facilitarle la activación e inicialización del TPM.

LA INFORMACIÓN DE ESTE DOCUMENTO SE SUMINISTRA JUNTO CON LOS PRODUCTOS DE INTEL®. EL PRESENTE DOCUMENTO NO OTORGA NINGÚN TIPO DE LICENCIA, EXPLÍCITA O IMPLÍCITA, POR IMPEDIMENTO LEGAL O DE CUALQUIER OTRA ÍNDOLE, SOBRE NINGÚN DERECHO DE PROPIEDAD INTELECTUAL. A EXCEPCIÓN DE LO QUE SE INDIQUE EN LOS TÉRMINOS Y CONDICIONES DE VENTA DE CADA PRODUCTO, INTEL NO ASUME RESPONSABILIDAD DE NINGUNA ÍNDOLE NI OTORGA NINGUNA GARANTÍA, EXPLÍCITA O IMPLÍCITA, EN RELACIÓN CON LA VENTA O USO DE LOS PRODUCTOS DE INTEL, INCLUIDA LA RESPONSABILIDAD O GARANTÍA RELACIONADA CON LA IDONEIDAD PARA UN PROPÓSITO DETERMINADO, COMERCIABILIDAD O INFRACCIÓN DE CUALQUIER PATENTE, COPYRIGHT U OTRO DERECHO DE PROPIEDAD INTELECTUAL. Los productos de Intel no están diseñados para utilizarse en aplicaciones médicas, de rescate o mantenimiento. Intel se reserva el derecho a realizar modificaciones en las especificaciones y las descripciones de los productos, en cualquier momento y sin previo aviso.

Intel es una marca comercial o registrada de Intel Corporation o de sus subsidiarias en Estados Unidos y en otros países.

* El resto de los nombres y marcas pueden ser propiedad de terceros.

Advertencia sobre posible pérdida de datos

INFORMACIÓN IMPORTANTE PARA EL USUARIO. LEA Y SIGA ESTAS INSTRUCCIONES ANTES DE PROCEDER A LA INICIALIZACIÓN DEL MÓDULO DE PLATAFORMA FIABLE.

Los integradores de sistema, propietarios y usuarios finales deberán tomar todas las precauciones posibles con el fin de eliminar la posibilidad de pérdida de datos. Los datos codificados por cualquier programa que utiliza el Módulo de plataforma fiable (TPM) pueden llegar a quedar inaccesibles o irrecuperables si se presenta cualquiera de las situaciones que se describen a continuación:

- Contraseña perdida: La pérdida de cualquiera de las contraseñas asociadas con el TPM hará que los datos codificados no estén accesibles. La recuperación de la contraseña no es posible. **No deje de leer las precauciones de seguridad para procedimientos de contraseña.**
- Fallo en la unidad de disco duro: En el caso de que se produzca un fallo en el disco duro (u otro medio de almacenamiento) que contenga datos codificados, deberá recuperarse una imagen del disco duro (u otro medio) de la copia de seguridad antes de que se pueda acceder a los datos codificados. El propietario / usuario deberá realizar una copia de seguridad del disco duro del sistema con regularidad. **No deje de leer las precauciones de seguridad que aparecen a continuación acerca de los procedimientos de copia de seguridad de la unidad de disco duro**.
- Fallo en la plataforma: En el caso de que se produzca un fallo en la plataforma y/o se requiera la sustitución de la placa madre, el procedimiento de recuperación permite restablecer las claves de migración y el acceso a los datos codificados. Se perderán todas las claves que no puedan migrarse, así como los datos asociados. Tanto el software para plataformas de seguridad Infineon* como Wave Systems EMBASSY* Trusted Suite utilizan claves con posibilidad de migración. Compruebe cualquier otro software que acceda al TPM para determinar la capacidad de migración de claves. **No deje de leer las precauciones de seguridad para procedimientos de copia de seguridad de archivos de recuperación de emergencia.**
- Pérdida de la propiedad del módulo de plataforma fiable: La propiedad / contenido del módulo de plataforma fiable puede borrarse (mediante un conmutador del BIOS) con el fin de permitir la transferencia de un sistema a un nuevo propietario. Si se borra la propiedad del TPM, bien de forma intencionada o por error, los procedimientos de recuperación pueden recuperar las claves de migración y restablecer el acceso a datos codificados. **No deje de leer las precauciones de seguridad para procedimientos de copia de seguridad de archivos de recuperación de emergencia**.

Módulo de plataforma fiable (TPM)

El módulo de plataforma fiable (TPM, Trusted Platform Module) es un componente de la tarjeta de sobremesa que se ha diseñado específicamente para mejorar la seguridad de las plataformas más allá de las posibilidades del software actual; con este fin, facilita un espacio protegido para las operaciones de claves y otras tareas de seguridad importantes. Mediante el uso de hardware y software, el TPM protege las claves de codificación y firma en las fases más vulnerables, cuando las claves se utilizan sin codificar en formato de texto.

El TPM está específicamente diseñado para proteger claves sin codificar, así como información de autentificación de plataformas de ataques a software.

Requisitos del sistema

- Tarjeta de sobremesa Intel® D865GRH
- Microsoft* Windows* 2000 Professional (SP4) o Microsoft Windows XP Professional (SP1)
- Sistema de archivos NTFS necesario
- Microsoft Internet Explorer* 5.5 o posterior
- Adobe* Acrobat* 5.0 o posterior (incluido en el CD de Intel® Express Installer)

Precauciones de seguridad

La seguridad, como cualquier otro aspecto del mantenimiento de un equipo, requiere una planificación. Lo más elemental en cuanto a seguridad es la capacidad de distinguir claramente quién es "amigo" y quién es "enemigo". El TPM proporciona mecanismos que permiten al propietario / usuario proteger su información de los enemigos. Para conseguir esta protección, el TPM establece "bloqueos" alrededor de los datos. Al igual que los bloqueos físicos, si las claves o combinaciones se pierden, los datos pueden quedar inaccesibles no sólo para los adversarios, sino también para el propietario / usuario.

El TPM ofrece dos clases de claves: de migración y de no migración. Las claves de migración están diseñadas para proteger datos que pueden utilizarse en más de una plataforma (es decir, sin codificar). Tienen la ventaja de que los datos claves pueden duplicarse (copia de seguridad y recuperación) en otra plataforma. Esto puede depender del usuario (alguien utiliza más de una plataforma, o hay distintas personas que tienen que acceder a los datos y que trabajan en distintas plataformas). Este tipo de clave presenta la ventaja de que permite la realización de copias de seguridad y la recuperación desde una plataforma defectuosa. Sin embargo, es posible que las teclas de migración no dispongan del nivel de protección adecuado necesario para la aplicación (por ejemplo, el usuario desea que los datos se restrinjan a una sola plataforma). Esto requiere una clave de no migración. Las claves de no migración llevan consigo un inconveniente; aunque se puede hacer una copia de seguridad de la clave o recuperarla (es decir, protegerla de un fallo del disco duro), no estará protegida contra un fallo del sistema o del TPM. La naturaleza de las claves de no migración sólo permite utilizarlas en un TPM. En el caso de que se produzca un fallo en el sistema o en el TPM, todas las claves de no migración y los datos asociados no estarán accesibles ni podrán recuperarse.

Las precauciones y procedimientos siguientes pueden ayudarle a recuperarse de cualquiera de las situaciones descritas anteriormente. De no respetar estas precauciones y procedimientos de seguridad, podría producirse una pérdida irrecuperable de los datos.

Procedimientos de contraseña

El software para plataformas de seguridad Infineon permite a los usuarios configurar contraseñas de 6 a 255 caracteres.

Una contraseña apropiada debería consistir en:

- Al menos una letra en Mayúscula (de la A a la Z)
- Al menos un carácter numérico (de 0 a 9)
- Al menos un carácter de símbolo (!, @, &, etc.)

Ejemplos de contraseñas: "Llevo 1 Sombrero verde al trabajO por lo menos una vez / mes" o "uJGFak&%)adf35a9m"

✏ **NOTA**

Evite el uso de nombres o fechas que puedan adivinarse fácilmente: fechas de cumpleaños, aniversarios, nombres de miembros de su familia, nombres de mascotas, etc.

Todos las contraseñas asociadas con el software para plataformas de seguridad Infineon (propietario, token de recuperación de emergencia y contraseñas de usuario) y Wave Systems EMBASSY* Trust Suite NO PUEDEN RECUPERARSE y no pueden, por lo tanto, restablecerse sin el texto original. El propietario del sistema deberá registrar todas las contraseñas y almacenarlas en una ubicación segura (caja fuerte, caja de seguridad, un lugar externo, etc.) y tenerlas disponibles para su posible utilización. Estos documentos deben actualizarse tras modificar las contraseñas.

Procedimientos de copia de seguridad de archivos de recuperación de emergencia

Tras finalizar el Asistente de inicialización de la plataforma de seguridad Infineon, debe moverse el token de recuperación de emergencia (**SPEmRecToken.xml**) a un medio extraíble (disquete, CD-ROM, dispositivos flash, etc). Una vez hecho esto, el medio extraíble debe almacenarse en una ubicación segura. NO DEJE NINGUNA COPIA del token de recuperación de emergencia en la unidad de disco duro o dentro de cualquier copia de seguridad de imagen del disco duro. Si se deja una copia del token de recuperación de emergencia en el sistema, ésta podría utilizarse para atentar contra el módulo de plataforma fiable y la plataforma.

Tras finalizar el Asistente de inicialización de la plataforma de seguridad Infineon, debe realizarse una copia del archivo de recuperación de emergencia (**SPEmRecArchive.xml**) en un medio extraíble y almacenarla en una ubicación segura. Este procedimiento debe repetirse siempre que se modifiquen contraseñas o se incorpore un nuevo usuario.

Procedimientos de copia de seguridad de imagen de la unidad de disco duro

Para permitir la recuperación de emergencia tras un fallo de la unidad de disco duro, deberán crearse imágenes frecuentes de la unidad de disco duro y almacenarlas en una ubicación segura. En el caso de que se produzca un fallo en la unidad de disco duro, puede recuperarse la última imagen en un nuevo disco duro y restablecerse los datos codificados.

NOTA

Los datos codificados y sin codificar que se hayan añadido tras la creación de la última imagen se perderán.

Copia de seguridad de texto normal (opcional)

Es recomendable que los propietarios del sistema sigan los procedimientos de copia de seguridad de imagen de la unidad de disco duro. Para realizar una copia de seguridad de archivos seleccionados sin crear una imagen de la unidad, éstos pueden moverse de programas o letras de unidad seguros a un directorio sin codificar. A continuación, puede hacerse una copia de seguridad de los archivos sin codificar (texto normal) en un medio extraíble y almacenarla en una ubicación segura. La ventaja de la copia de seguridad de texto normal es que no se requiere la clave del TPM para recuperar los datos. No se recomienda la utilización de esta opción, ya que se corre el riesgo de que los datos queden expuestos durante los procesos de copia de seguridad y de recuperación.

Propiedad del Módulo de plataforma fiable

El Módulo de plataforma fiable se encuentra desactivado por defecto, y el propietario / cliente final del sistema asume la "propiedad" del TPM. Esto permite al propietario del sistema controlar la inicialización del TPM y crear todas las contraseñas asociadas con el TPM que se utilice para proteger sus claves, datos y privacidad.

Los desarrolladores e integradores de sistemas pueden instalar tanto el software para plataformas de seguridad Infineon como Wave System EMBASSY Trust Suite, aunque NO DEBERÍAN intentar utilizar ni activar el TPM o el paquete de software.

Activación del Módulo de plataforma fiable

El Módulo de plataforma fiable se encuentra desactivado por defecto con el fin de asegurar que el propietario / cliente final del sistema inicialice el TPM y configure todas las claves de seguridad. Para activar el TPM, el propietario / cliente final deberá seguir los pasos que se indican a continuación:

1. Cuando el PC muestra la pantalla de bienvenida (o pantalla POST), pulse la tecla <F2> para acceder al BIOS.
2. Utilice las teclas de flecha para desplazarse hasta el menú Advanced (Opciones avanzadas), seleccione Peripheral Configuration (Configuración de periféricos) y pulse la tecla <Intro>.
3. Seleccione Trusted Platform Module (Módulo de plataforma fiable), pulse <Intro>, elija Enabled (Activado) y pulse <Intro> de nuevo (la pantalla deberá mostrar: `Trusted Platform Module [Enabled]`).

4. Pulse la tecla <F10>, seleccione Ok (Aceptar) y pulse <Intro>.
5. Se debe reiniciar el sistema e iniciar Microsoft Windows.

Obtención de la propiedad del Módulo de plataforma fiable

Una vez que se ha activado el TPM, debe obtenerse la propiedad mediante el software para plataformas de seguridad Infineon. Para obtener la propiedad del TPM, el propietario / usuario final deberá seguir los pasos que se indican a continuación:

1. Inicie el sistema.
2. Abra el Asistente de inicialización de la plataforma de seguridad Infineon.
3. Cree una contraseña de propietario (antes de crear cualquier contraseña, consulte las recomendaciones indicadas anteriormente en este documento).
4. Cree un nuevo archivo de recuperación (anote la ubicación y el nombre del archivo).
5. Cree una contraseña de token de recuperación de emergencia de plataforma de seguridad (esta contraseña no debe coincidir con la contraseña de propietario ni con cualquier otra contraseña).
6. Defina la ubicación en la que va a guardar el token de recuperación de emergencia (anote la ubicación y nombre del archivo).
7. El software creará, a continuación, archivos de recuperación y con ello finalizará el proceso de obtención de la propiedad del TPM.
8. Tras finalizar el Asistente de inicialización de la plataforma de seguridad Infineon, debe moverse el token de recuperación de emergencia (**SPEmRecToken.xml**) al medio extraíble (disquete, CD-ROM, dispositivo flash, etc). Una vez hecho esto, el medio extraíble debe almacenarse en una ubicación segura. No se debe dejar ninguna copia de este token de recuperación de emergencia en el sistema. De lo contrario, ésta podría utilizarse para atentar contra la seguridad de la plataforma.
9. Abra el Asistente de inicialización de usuario de la plataforma de seguridad Infineon.
10. Cree una contraseña de usuario (esta contraseña es la que se utiliza con más frecuencia y no debe coincidir con ninguna otra).
11. Seleccione y configure las funciones de plataforma de seguridad para este usuario.
12. Tras finalizar el Asistente de inicialización de la plataforma de seguridad Infineon, debe realizarse una copia del archivo de recuperación de emergencia (**SPEmRecArchive.xml**) en el medio extraíble y almacenarla en una ubicación segura. Este procedimiento debe repetirse siempre que se modifiquen contraseñas o se incorpore un nuevo usuario.
13. Todas las contraseñas asociadas con el software para plataformas de seguridad Infineon (propietario, token de recuperación de emergencia y contraseñas de usuario) no pueden recuperarse y no pueden, por lo tanto, restablecerse sin el texto original. Dichas contraseñas deben registrarse y almacenarse en una ubicación segura (caja fuerte, caja de seguridad, un lugar externo, etc.) y tenerlas disponibles en caso de que se necesiten. Estos documentos deben actualizarse tras modificar las contraseñas.

Procedimientos de recuperación

Procedimiento de recuperación tras un fallo en la unidad de disco duro

Recupere la imagen más reciente de la unidad de disco duro de la copia de seguridad al nuevo disco duro (no es necesario una recuperación específica del TPM).

Procedimiento de recuperación tras un fallo en la tarjeta de sobremesa o en el TPM

Este procedimiento puede recuperar las claves de migración del archivo de recuperación de emergencia y no restablece ninguna clave o contenido anterior a la activación del TPM. Este procedimiento de recuperación puede restablecer el acceso al software para plataformas de seguridad Infineon y Wave Systems EMBASSY Trust Suite, que están protegidos con claves de migración.

Requisitos

- Archivo de recuperación de emergencia (creado con el Asistente de inicialización de la plataforma de seguridad Infineon)
- Token de recuperación de emergencia (creado con el Asistente de inicialización de la plataforma de seguridad Infineon)
- Contraseña de seguridad de token de recuperación de emergencia (creado con el Asistente de inicialización de la plataforma de seguridad Infineon)
- Instalación del sistema operativo original en funcionamiento o una imagen recuperada de la unidad de disco duro

Este procedimiento sólo restablece las claves de migración del archivo de recuperación creado anteriormente.

1. Sustituya la tarjeta de sobremesa defectuosa por una del mismo modelo.
2. Inicie el SO original o recupere la imagen del disco duro original.
3. Inicie el Asistente de inicialización de la plataforma de seguridad Infineon.
4. Durante la inicialización de la plataforma de seguridad, NO sustituya el archivo o el token de recuperación de emergencia existentes. Una vez finalizada, NO abra el Asistente de inicialización de usuario.
5. Ejecute el Asistente de inicialización de la plataforma de seguridad Infineon en modo de recuperación (C:\Archivos de programa\…\SpTPMWz.exe -restore).
6. Indique la ubicación del archivo de recuperación de emergencia, el token de recuperación de emergencia que se va a restablecer (de la copia de seguridad) y la contraseña del token de recuperación de emergencia original. Seleccione el nombre del equipo original (debe coincidir con el nombre actual del equipo). Finalice el Asistente.
7. Abra el Asistente de inicialización de usuario. Seleccione “Recover your Basic User Key” (Recuperar clave de usuario básica) cuando el sistema lo indique. Escriba la contraseña de clave de usuario básica. Finalice el Asistente.

Ahora podrá acceder a los archivos anteriormente codificados.

Eliminación de la propiedad del Módulo de plataforma fiable

El TPM puede borrarse con el fin de transferir la propiedad de la plataforma a un nuevo propietario.

⚠ **PRECAUCIÓN**

LOS DATOS CODIFICADOS POR CUALQUIER PROGRAMA QUE UTILIZA EL TPM PUEDEN LLEGAR A QUEDAR INACCESIBLES SI SE BORRA LA PROPIEDAD DEL TPM. *Es posible que los procedimientos de recuperación permitan restablecer las claves de migración y recuperar el acceso a datos codificados. (Consulte los procedimientos de recuperación para obtener instrucciones detalladas al respecto.)*

⚠ **ADVERTENCIA**

Desconecte la tarjeta de sobremesa de la fuente de alimentación de CA antes de conectar o desconectar cables, así como antes de instalar o retirar cualquiera de los componentes de la tarjeta. De no hacerlo, podría sufrir daños personales o dañar el equipo. Algunos circuitos de la tarjeta pueden continuar funcionando a pesar de que se haya apagado el sistema mediante el interruptor del panel frontal.

1. Antes de abrir la cubierta del sistema, tenga en cuenta las precauciones descritas en el apartado ADVERTENCIA.
2. Mueva el puente de configuración (J9J4) de la tarjeta a las patillas 2-3.
3. Restablezca la alimentación del PC y enciéndalo.
4. El sistema abrirá automáticamente el programa Setup del BIOS.
5. Utilice las teclas de flecha para seleccionar Clear Trusted Platform Module (Borrar Módulo de plataforma fiable) y pulse <Intro>.
6. Si está de acuerdo con el mensaje de advertencia, seleccione Ok (Aceptar) y pulse <Intro>.
7. Pulse la tecla <F10> para guardar y salir, seleccione Ok (Aceptar) y pulse <Intro>.
8. Apague el sistema.
9. Revise las precauciones descritas en el apartado ADVERTENCIA.
10. Restablezca el puente de configuración (J9J4) de la tarjeta a las patillas 1-2.

Una vez borrado, el TPM se desactiva por defecto.

Enlaces de soporte

Para obtener ayuda sobre el software para plataformas de seguridad Infineon*, visite el sitio Web: http://www.infineon.com

Para obtener ayuda sobre Wave System* EMBASSY Trusted Suite, visite el sitio Web: http://www.wave.com/support/ets.html

Para obtener información adicional sobre el TPM y acerca de cómo mejorar la seguridad del PC, visite el sitio Web: https://www.trustedcomputinggroup.org