Guida all’installazione v3.3.0

TPM (Trusted Platform Module)

computers.toshiba-europe.com

TOSHIBA

Leading Innovation

Indice generale

Copyright

Marchi

1 Introduzione

Il computer è dotato di un modulo TPM (Trusted Platform Module) integrato. Per attivare TPM, è necessario abilitare o installare il software Infineon Security Platform Tools. Questa Guida all'installazione descrive le procedure di installazione e configurazione di TPM e deve essere letta attentamente prima di utilizzare il software.

1.1 Convenzioni

Per descrivere, identificare ed evidenziare i termini e le procedure operative, vengono utilizzate le convenzioni riportate di seguito.

Icone di sicurezza

Questo manuale contiene importanti istruzioni sulla sicurezza alle quali è necessario attenersi al fine di evitare possibili rischi di lesioni personali, danni al computer o perdita di dati. Le istruzioni per la sicurezza sono state classificate in base alla gravità del rischio ed evidenziate con le icone descritte di seguito.

Indica l'esistenza di un potenziale rischio che, se non viene evitato, può provocare danni agli oggetti.

Fornisce informazioni importanti.

1.2 Panoramica di TPM

Il controller di sicurezza incorporato TPM è basato sulle specifiche Trusted Computing Group. TPM protegge i dati del computer utilizzando chiavi di crittografia segrete anziché formule (algoritmi) di crittografia segrete. Se la crittografia è basata esclusivamente sul software, esiste il rischio che una chiave di crittografia salvata su file o registrata nella memoria del computer venga letta e decifrata. Al contrario, l'archiviazione della chiave di crittografia in TPM garantisce una maggiore protezione dei dati.

Poiché TPM adotta specifiche pubbliche e standardizzate, è possibile costruire un ambiente protetto per il computer utilizzando la soluzione di sicurezza corrispondente.

Per ulteriori informazioni sulle specifiche TCG, visitare il relativo sito Web all'indirizzo http://www.trustedcomputinggroup.org/

Crittografia, certificati e password

- *TPM offre la possibilità di creare e impostare un numero indefinito di chiavi di crittografia, certificati e password. Una volta effettuate le impostazioni, è importante mettere al sicuro le password ed eseguire il backup dei file delle chiavi di crittografia. Qualora tali impostazioni venissero perse o dimenticate, infatti, non sarebbe più possibile decifrare i file cifrati mediante TPM né accedere ai dati cifrati.*

TPM

- *Pur se dotato di funzioni di sicurezza di ultima generazione, TPM non può garantire una protezione assoluta di dati e hardware. Toshiba non è responsabile di eventuali errori o danni derivanti dall'uso di questo software.*

Se la configurazione di Microsoft® Windows® prevede più account utente, ciascuno dei quali utilizzerà TPM, è necessario che ogni singolo utente esegua il login in Windows® e si registri individualmente.

2 Uso di TPM per la prima volta

Questo manuale contiene solo indicazioni di carattere generale. Dopo l'installazione di TPM Professional Package, si consiglia di consultare la Guida in linea di TPM.

Quando si utilizza TPM per la prima volta, è necessario configurarlo nel modo descritto di seguito. (Per configurare le impostazioni 1 - 3, effettuare il login come amministratore di *Windows*®.)

1. Abilitare TPM.
2. Installare **Infineon TPM Professional Package**.
3. Registrare il proprietario e gli utenti in TPM.

2.1 Abilitazione di TPM

Per abilitare TPM, effettuare le seguenti impostazioni nel BIOS:

1. Accendere il computer tenendo premuto il tasto **Esc**.
2. Viene visualizzato un messaggio. Premere il tasto **F1.**
3. Viene visualizzata la schermata di configurazione del BIOS.
4. Premere il tasto **Pg Giù** per visualizzare la schermata successiva.
5. Impostare **TPM** in **SECURITY CONTROLLER** (Controller di sicurezza) su **Enabled** (Abilita).

In alcuni modelli la schermata di configurazione del BIOS comprende anche l'opzione **Hide TPM** *(Nascondi TMP). Se per il sistema in uso è disponibile l'opzione* **Hide TPM**, *impostarla su* **No** *prima di impostare* **TPM** *su* **Enabled**. *In caso contrario, non sarà possibile modificare* **TPM**.

6. Premere il tasto **End**, salvare le modifiche delle impostazioni del BIOS e premere il tasto **Y**.

La coerenza interna dei dati di TPM non può essere garantita quando il computer viene sottoposto a interventi di riparazione. In questi casi, prima di mandare il computer in riparazione, creare una copia di backup non solo dei file presenti nel disco rigido ma anche dei dati di TPM, utilizzando l'apposita funzione di backup. (Per ulteriori informazioni, consultare il capitolo 8 - Ripristino di TPM*.) Le funzioni di sicurezza che utilizzano TPM non possono funzionare correttamente in caso di perdita dei dati di TPM. (Ad esempio, non sarebbe più possibile aprire i file cifrati con TPM.) In assenza di un backup, potrebbe verificarsi una perdita di dati.*

- ***TPM** potrebbe essere impostato su **Disabled** anche quando il computer viene restituito all'utente dopo una riparazione. In questi casi è necessario riconfigurare TPM e abilitarlo di nuovo.*
- *Per impedire a persone diverse dall'amministratore e dagli utenti del computer di modificare le impostazioni del BIOS, si consiglia vivamente di impostare una password utente e una password supervisore per il BIOS. Per informazioni sull'impostazione di queste password, consultare il manuale del computer.*

2.2 Installazione di Infineon TPM Professional Package

Installare **Infineon TPM Professional Package** da `C:\TOSHIBA\Drivers\TPM Utility`.

Infineon TPM Professional Package comprende i componenti e le funzioni elencate di seguito:

- Guida in linea di Security Platform
- Security Platform Setting Tool
- Security Platform Initialization Wizard
- Security Platform User Initialization Wizard
- Security Platform Initialization Wizard
- Security Platform Backup Wizard
- Security Platform Password Reset Wizard
- Security Platform PKCS #12 Import Wizard
- Security Platform Certificate viewer e Certificate Selection
- Icona Security Platform Taskbar Notification
- Servizi integrativi di Security Platform
  - Integrazione di Microsoft® Outlook®
  - Integrazione di Netscape®
  - Integrazione di EFS (Encrypted File System)
  - Personal Secure Drive
  - Policy Administration
- Servizi Security Platform
  - TSS (TCG Software Stack) Service Provider
  - TSS Core Service
  - TSS Device Driver Library

2.3 Registrazione dei proprietari e degli utenti in TPM

1. Fare clic sull'icona **Security Platform** nella barra delle applicazioni e selezionare **Security Platform Initialization** (Inizializzazione piattaforma di sicurezza).

2. TPM viene avviato e appare la schermata principale del programma. Fare clic sul pulsante **Next** (Avanti).
3. Nella schermata **Initialization** (Inizializzazione), selezionare Initialize a new Security Platform (Inizializza una nuova piattaforma di sicurezza). Quindi, fare clic sul pulsante **Next** (Avanti).
4. Nella schermata **Create Security Platform Owner** (Crea proprietario piattaforma di sicurezza) per l'autenticazione del proprietario, inserire la password nelle caselle di testo **Password** e **Confirm Password** (Conferma password) e fare clic sul pulsante **Next** (Avanti).
5. Viene visualizzata la finestra **Features** (Funzioni). Selezionare la funzione da impostare e fare clic sul pulsante **Next** (Avanti).
   Per informazioni dettagliate sulle funzioni della piattaforma di sicurezza, consultare la Guida in linea.

Si raccomanda vivamente di impostare il **backup automatico***. Se non è impostato, i dati utente crittografati potrebbero andare persi in condizioni anomale.*

6. Nella schermata **Backup**, specificare il percorso in cui deve essere creato e salvato il file di backup. Fare clic sul pulsante **Next** (Avanti).
7. Nella schermata **Emergency Recovery** (Ripristino di emergenza), selezionare **Create a new Recovery Token** (Crea nuova chiave di ripristino) e specificare il percorso in cui deve essere creata e salvata la chiave di ripristino (**Emergency Recovery Token**).
8. Nella schermata **Emergency Recovery** (Ripristino di emergenza) per l'autenticazione della chiave di ripristino di emergenza, inserire la password nelle caselle di testo Password e Confirm Password (Conferma password) e fare clic sul pulsante **Next** (Avanti).

Si consiglia vivamente di creare una chiave di ripristino di emergenza per garantire che, in caso di seri problemi al sistema, le informazioni di TPM e i dati utenti relativi a TPM siano al sicuro. In caso contrario, potrebbe verificarsi una perdita di dati.

9. Nella schermata **Password Reset** (Ripristino password), selezionare **Create a new Token** (Crea nuova chiave) e specificare il percorso in cui deve essere creata e salvata la chiave di ripristino della password (**Password Reset Token**).

10. Nella schermata **Password Reset** per l'autenticazione della **chiave di ripristino della password**, inserire la password nelle caselle di testo Password e Confirm Password (Conferma password) e fare clic sul pulsante **Next** (Avanti).

Si consiglia vivamente di creare e salvare la **chiave di ripristino della password** *su un supporto di archiviazione che sia accessibile in caso di malfunzionamento del sistema (ad esempio un dischetto). Conservare il supporto in un luogo sicuro per un possibile uso futuro.*

- Se TPM viene utilizzato su più computer, ogni computer ha una chiave diversa che deve essere conservata separatamente.
- Non è possibile ricreare la chiave di ripristino del proprietario* registrato di TPM. Per evitare di perdere la chiave, è consigliabile crearne e salvarne più copie, come indicato nella nota precedente.

  *È possibile ricreare lo stesso nome del proprietario di TPM inizializzando TPM nel menu del BIOS e registrando un nuovo proprietario; tuttavia, poiché in questo caso il proprietario è in realtà diverso da quello precedentemente registrato, i file cifrati in precedenza non potranno essere decifrati.
- Una persona non autorizzata che venisse in possesso sia della chiave che della password potrebbe accedere ai dati cifrati. Di conseguenza si raccomanda di conservare chiavi e password con la massima attenzione.

  Per ulteriori informazioni, consultare il capitolo 8 - *Ripristino di TPM*.

11. Viene visualizzato il riepilogo (**Summary**). Verificarlo e fare clic su **Next** (Avanti).
12. Potrebbero trascorrere alcuni minuti prima che venga visualizzato il messaggio **Wizard completed successfully** (Procedura guidata completata correttamente). Successivamente, fare clic sulla casella di controllo **Start Security Platform User Initialization Wizard** (Avvia inizializzazione guidata utente della piattaforma di sicurezza), quindi fare clic sul pulsante **Finish** (Fine).
13. Nella schermata **User Initialization Wizard** (Inizializzazione utente guidata), fare clic sul pulsante **Next** (Avanti).
14. Nella schermata **Basic User Password** (Password utente base) per l'autenticazione dell'utente, inserire la password nelle caselle di testo **Password** e **Confirm Password** (Conferma password) e fare clic sul pulsante **Next** (Avanti).
15. Nella schermata **Basic User Password Reset** (Ripristino password utente base), verificare che sia selezionata l'opzione **Enable the resetting of my Basic User Password in case of an emergency** (Abilita ripristino password utente base in caso di emergenza). Specificare il percorso in cui deve essere creato e salvato il file **Personal Secret**.

Salvare questo file in una posizione sicura. In caso di necessità, verrà richiesto di ripristinare la password utente di base.

16. Viene visualizzata la finestra **Password and Authentication** (Password e autenticazione). Verificare il contenuto visualizzato e fare clic sul pulsante **Next** (Avanti).

La visualizzazione della schermata Security Platform Features (Funzioni piattaforma di sicurezza) potrebbe richiedere diversi minuti.

17. Verificare che siano selezionate le opzioni desiderate nella schermata **Security Platform Features** (Funzioni piattaforma di sicurezza), quindi fare clic sul pulsante **Next** (Avanti).

- *Per utilizzare la funzione* **Secure E-mail** *(Protezione e-mail), è necessario configurare adeguatamente il* **software e-mail**. *Per informazioni dettagliate sulla funzione Secure E-mail, consultare il capitolo 4 -* Secure E-Mail.
- *La funzione* **File and Folder encryption (EFS)** *(Crittografia file e cartelle) non è disponibile in Windows Vista® Home.*
- *Per poter utilizzare questa funzione, è necessario che l'unità disco rigido sia formattata in NTFS.*

Le impostazioni descritte in questa sezione possono anche essere modificate in un secondo momento.

18. Se l'opzione **Secure E-mail** (Protezione e-mail) è selezionata nella schermata **Security Platform Features** (Funzioni piattaforma di sicurezza), viene visualizzata la schermata seguente. Fare clic sul pulsante **Next** (Avanti).

Se si fa clic sul pulsante **Outlook®, Windows Mail/Outlook Express** *o* **Netscape®** *in questa schermata, viene visualizzata la Guida in linea di* **Secure E-mail** *per il corrispondente* **software e-mail**. *(La Guida in linea può essere consultata anche dopo il completamento della procedura guidata.)*

19. Nella schermata **Security Platform Features** (Funzioni piattaforma di sicurezza), viene visualizzato il messaggio Encryption Certificate (Certificato di crittografia). Selezionare il certificato da utilizzare e fare clic su **Next** (Avanti). Generalmente, per creare e selezionare il certificato si fa clic sul pulsante **Create** (Crea).

Il valore predefinito di **Maximum Basic User Password age** *(Durata massima password utente base) è impostato su* **[Disabled]** *(Disattivato). Per modificare questo valore, è possibile utilizzare l'opzione* **User** *(Utente) in* **Security Policy** *(Criteri di protezione).*

20. Se l'opzione **Personal Secure Drive (PSD)** (Unità protetta personale) è selezionata nella schermata **Security Platform Features** (Funzioni piattaforma di sicurezza), viene visualizzata la schermata seguente. In questa schermata, selezionare l'unità da assegnare a PSD, quindi specificare l'etichetta di tale unità e fare clic sul pulsante **Next** (Avanti). Per informazioni dettagliate sulla funzione Personal Secure Drive (PSD), consultare il capitolo 3 - *Personal Secure Drive*.
21. Nella schermata **Security Platform Features**, specificare il volume dello spazio di archiviazione da assegnare a PSD, quindi selezionare l'unità e fare clic sul pulsante **Next** (Avanti).
22. Viene visualizzata la schermata di conferma delle impostazioni. Fare clic sul pulsante **Next** (Avanti).

- *Si consiglia vivamente di specificare un'unità disco rigido incorporata (generalmente C) nel menu a discesa* **My Personal Secure Drive will be saved on this drive** *(L'unità protetta personale sarà salvata in questa unità).*
- *Lo spazio disponibile nell'unità specificata deve essere superiore a quello specificato in* **My Personal Secure Drive will have [XX] MB of storage space** *(L'unità protetta personale avrà [XX] MB di spazio di archiviazione).*

23. Dopo qualche momento, viene visualizzato il messaggio **Wizard completed** (Procedura guidata completata). Fare clic sul pulsante **Finish** (Fine).

Se la configurazione di Windows® prevede più account utente, ciascuno dei quali utilizzerà TPM, è necessario che ogni singolo utente esegua il login in Windows® e si registri individualmente. Dopo aver eseguito il login in Windows® per effettuare la registrazione dell'utente, fare clic sull'icona **Security Platform** *nella barra delle applicazioni e selezionare* **Security Platform User initialization** *(Inizializzazione utente della piattaforma di sicurezza).*

Dopo aver modificato la configurazione, fare clic sull'icona **Security Platform Setting Tool** (Strumento di impostazione di Security Platform) nella barra delle applicazioni ed effettuare le modifiche necessarie nella schermata di configurazione.

- *inizializzazione*
  - *Quando si utilizza Infineon TPM Professional Package, non è necessario inizializzare prima TPM in Windows Vista® mediante* **TPM Management on Local Computer** *(Gestione TPM su computer locale).*
  - *Quando TPM viene inizializzato in Infineon TPM Professional Package, non è necessario inizializzarlo in Windows Vista® mediante* **TPM Management on Local Computer** *(Gestione TPM su computer locale).*
- *Metodo di inizializzazione*

Quando si utilizza Professional Package V3.0 dopo che TPM è stato inizializzato in Windows Vista® mediante la funzione **TPM Setting** *(Impostazione TPM), la normale inizializzazione della piattaforma viene eseguita come segue:*

1. *Dopo l'installazione di Professional Package V3.0, viene visualizzato il messaggio "*`Initialized other OS`*" (Altro sistema operativo inizializzato) dall'icona* **TPM** *della barra delle applicazioni.*

   ** Questo non indica anomalie del funzionamento di TPM.*
2. *Quando si esegue* **Infineon Security Platform Setting Tool** *(Strumento di impostazione di Infineon Security Platform) nello stato del punto 1, l'opzione* **[Security Platform State:]**, **[Owner:]** *(Stato Security Platform - Proprietario:) della scheda* **Info** *(Informazioni) viene visualizzata come "*`Initialized (Failure Mode 2)`*" (Inizializzato - Modalità errore 2).*

   ** Questo non è un errore ma l'inizializzazione della piattaforma non è stata completata.*
3. *Quando viene eseguito* **Security Platform User Initialization Wizard** *(Avvia inizializzazione guidata utente della piattaforma di sicurezza), viene visualizzata la schermata* **Initialization** *(Inizializzazione). Anche se è stata selezionata l'opzione* **Security Platform restoration form a Backup Archive** *(Ripristino piattaforma di sicurezza da un archivio di backup), selezionare* **Security Platform Initialization** *(Inizializzazione piattaforma di sicurezza).*
4. *Nella schermata successiva in* **Initialize Security Platform** *(Inizializza piattaforma di sicurezza) immettere la password impostata in Windows Vista® mediante* **TPM Management on Local Computer** *(Gestione TPM su computer locale). In questo periodo, non è possibile utilizzare il* **file di backup della password del proprietario TPM** *salvato in* **TPM Management on Local Computer** *(Gestione TPM su computer locale).*
5. *Quando la password utente viene modificata da Infineon TPM Professional Package, non è possibile utilizzare* **TPM Owner Password Backup file** *(File di backup password proprietario TPM) creato in Windows Vista® mediante* **TPM Management on Local Computer** *(Gestione TPM su computer locale).*

3 Personal Secure Drive

La funzione **Personal Secure Drive** (Unità protetta personale) consente di creare uno spazio di archiviazione per il salvataggio delle informazioni (file), di cifrare i file di dati e di salvarli nell'unità virtuale creata. I file non vengono semplicemente cifrati e archiviati nel disco rigido; poiché sono protetti da TPM, il livello di sicurezza è superiore rispetto alla crittografia basata su software. La dimensione dell'unità PSD può essere impostata su un valore non inferiore a 10 MB. La dimensione massima dipende dal file system utilizzato per la creazione di tale unità. Per informazioni dettagliate, consultare la Guida.

3.1 Vantaggi di Personal Secure Drive

- Crittografia dell'unità virtuale mediante protezione con chiave AES (Advanced Encryption Standard).
- Algoritmo RSA per la generazione di chiavi cifrate.
- Crittografia e decrittografia automatica dei dati di sicurezza trasparenti.
- Protezione semplificata dei file.
- Funzionamento semplice: Personal Secure Drive funziona come una normale unità di *Windows*®.
- Gestione e configurazione semplificata mediante procedure guidate.

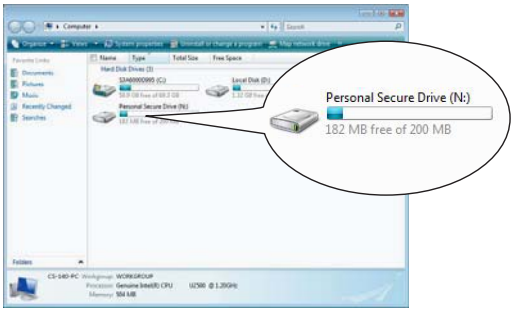
3.2 Personal Secure Drive (PSD) - Operazioni principali

1. Se nella schermata **Security Platform Features** (Funzioni piattaforma di sicurezza) è selezionata l'opzione PSD, fare clic sull'icona **Security Platform** nella barra delle applicazioni dopo aver effettuato l'accesso a Windows e selezionare [**Personal Secure Drive**] - [**Load**] (Carica).

*Se si fa clic sull'icona Security Platform nella barra delle applicazioni, è possibile selezionare[**Personal Secure Drive**] - [**Load**] (Carica), [**Unload**] (Scarica) o [**Load at Logon**] (Carica all'accesso).*

2. Viene visualizzata la schermata di autenticazione utente Infineon Security Platform User Authentication. Inserire la password di TPM. L'unità virtuale PSD verrà riconosciuta all'inserimento della password corretta.

3. La schermata di esempio della figura seguente mostra l'unità PSD rilevata in Esplora risorse di *Windows*®.



In questa schermata l'unità PSD è indicata come unità **[N:]** e con il nome **Personal Secure Drive**, ma è possibile modificare tale impostazione nella sezione **User Settings** (Impostazioni utente) di **Infineon Security Platform Settings Tool** (Strumento di impostazione di Infineon Security Platform).

- *Poiché la funzione* **Backup** di **Infineon Security Platform Setting** *Tool (Strumento di impostazione di Infineon Security Platform) non consente di effettuare il backup dei file dell'unità PSD, è necessario utilizzare un metodo di backup standard per evitare possibili perdite di dati, ad esempio la copiatura dei file PSD su un supporto esterno rimovibile.*
- *I dati del punto di ripristino del sistema* impostato dalla funzione Ripristino configurazione di sistema di Windows® vengono cancellati dopo l'inserimento della password TPM all'avvio di Windows, il caricamento di PSD e l'assegnazione dell'unità virtuale. Si consiglia vivamente di utilizzare uno dei seguenti metodi per salvare i dati del punto di ripristino del sistema.*
  - *Non utilizzare la funzione PSD ma solo la funzione di crittografia dei file di EFS.*
  - *Disabilitare temporaneamente la funzione PSD prima di modificare l'ambiente Windows.*

  Disabilitare la funzione PSD -> Impostare il punto di ripristino -> Modificare il sistema -> Controllare che l'avvio di Windows venga eseguito correttamente -> Ripristinare lo stato precedente della funzione PSD.

  ** Per informazioni dettagliate sull'impostazione di un punto di ripristino, consultare la Guida in linea di Windows®.*

- *La funzione PSD deve essere impostata per ogni utente TPM. Ad esempio, se sono presenti i due utenti TPM registrati "A" e "B", B non può visualizzare il contenuto dell'unità PSD di A.*
- *Poiché nella PSD (Personal Secure Drive) vi sono aree utilizzate dal file system NTFS di Windows, la capacità effettiva della PSD utilizzabile è inferiore al valore iniziale durante la configurazione. Quando viene utilizzato un minimo di circa 10 MB e viene incrementata la capacità della PSD, aumentano anche le aree utilizzate da NTFS.*

  Se si desidera utilizzare tutta la capacità richiesta, è necessario specificare una maggiore capacità durante la configurazione della PSD.

  *Ad esempio, se si desidera utilizzare circa 200 MB, è necessario specificare una capacità di P*SD pari a 220 MB durante la configurazione.

4 Secure E-Mail

In questa piattaforma di sicurezza, gli ID digitali utilizzati per l'e-mail vengono protetti da TPM per impedirne la perdita o il furto.

I software e-mail supportati sono Outlook®*, Windows Mail/Outlook Express* e Netscape®*.

* La disponibilità della funzione dipende anche dalla versione del software.

4.1 Configurazione

1. Ottenere da un'autorità di certificazione commerciale (CA) un ID digitale da utilizzare in Secure E-Mail. Per informazioni sull'autorità di certificazione, consultare la Guida in linea di TPM.
2. Installare l'ID digitale sul computer seguendo i metodi di utilizzo e installazione indicati dall'autorità di certificazione. A questo punto, verificare che l'ID digitale sia collegato a TPM come CSP (Cryptographic Service Provider, fornitore di servizi di crittografia).
3. Effettuare le impostazioni relative a Secure E-Mail nel software e-mail. Per informazioni dettagliate, consultare il manuale del software e-mail e la Guida in linea di Infineon Security Platform.

Impostare l'opzione **Secure E-mail** *nella schermata Security Platform Features (Funzioni piattaforma di sicurezza) quando si esegue la registrazione utente in TPM (punto 2.3), se non è già stata assegnata (*1, *2).*

*1 Uso della Guida in linea per cercare informazioni relative a e-mail e TPM

1) Fare doppio clic sull'icona **TPM** nella barra delle applicazioni.
2) Selezionare la scheda **Info** (Informazioni).
3) Fare clic sul pulsante della **Guida in linea**.
4) Effettuare una ricerca specificando le parole chiave appropriate nella scheda **Search** (Ricerca) per trovare gli argomenti desiderati. (Ad esempio: **e-mail**)

*2 Abilitazione della funzione E-mail in User Settings (Impostazioni utente)

1) Fare doppio clic sull'icona **TPM** nella barra delle applicazioni.
2) Selezionare la scheda **User Settings** (Impostazioni utente).
3) Fare clic sul pulsante **Configure** (Configura).
4) Selezionare l'opzione **Secure E-mail** e fare clic sul pulsante **Next** (Avanti).

5 Estensione EFS (Encrypting File System)

Se l'opzione **File and Folder Encryption** (Crittografia file e cartelle) è stata selezionata al punto 2.3, la funzione EFS del sistema operativo viene estesa e il sistema diventa più sicuro poiché la chiave cifrata del file cifrato da EFS è protetta da TPM.

Le operazioni necessarie per cifrare e decifrare i file sono molto simili.

La differenza consiste nel fatto che quando si accede inizialmente ai file cifrati da EFS dopo il login in *Windows*®, è necessario inserire la password TPM dell'utente corrente.

- *Nell'ambiente descritto di seguito, quando i file creati in* **[Basic User Key and Other Folders]** *(Chiave utente base e altre cartelle) sono cifrati con EFS, il software TPM non si avvia normalmente e i dati cifrati non possono essere decifrati.*
  - *Il software TPM è installato.*
  - *L'installazione della piattaforma è stata completata.*
  - *La funzione EFS è stata selezionata durante l'inizializzazione utente.*

  Nello stato di inizializzazione, i file in **[Basic User Key and Other Folders]** *(Chiave utente base e altre cartelle) hanno attributi di sistema che ne impediscono la cifratura. Non modificare gli attributi dei file nelle cartelle corrispondenti.*

  ** Nella configurazione iniziale di Windows, le seguenti cartelle sono nascoste.*

  [Basic User Key and Other Folders] (Chiave utente base e altre cartelle)

  ```
  C:\ProgramData\Infineon\TPM Software
  C:\ProgramData\Infineon\TPM Software 2.0
  C:\Users\All Users\Infineon
  ```

- *Se gli archivi, i backup e i file di chiave sono cifrati, non possono essere decifrati durante un'emergenza.*

  Se la chiave di ripristino password e i file segreti sono cifrati, la password non può essere ripristinata.

  Non cifrare i seguenti file e cartelle.

  [Automatic Backup File] (File di backup automatico)

  Default Filename (Nome file predefinito): SPSystemBackup.xml

  Default Password (Password predefinita): non specificata (*)

  [Automatic Backup Data Storage Folder] (Cartella di archiviazione dati backup automatico)

  Folder Name (Fixed): SPSystemBackup (il file SPSystemBackup.xml viene creato come sottocartella della cartella creata)

  [Emergency Recovery Token] (Chiave per il ripristino di emergenza)

  Default Filename (Nome file predefinito): SPEmRecToken.xml

  Default Password (Password predefinita): Removable Media (FD, memoria USB, ecc.)

  [Password Reset Token] (Chiave di ripristino password)

  Default Filename (Nome file predefinito): SPPwdResetToken.xml

  Default Password (Password predefinita): Removable Media (FD, memoria USB, ecc.)

  [Basic User Password Reset (Ripristino password utente base)

  Default Filename (Nome file predefinito): SPPwdResetSecret.xml

  Default Password (Password predefinita): Removable Media (FD, memoria USB, ecc.)

  [Backup Archive] (Archivio di backup)

  Default Filename (Nome file predefinito): SpBackupArchive.xml

  Default Password (Password predefinita): non specificata (*)

  [PSD Backup Archive] (Archivio di backup PSD)

  Default Filename (Nome file predefinito): SpPSDBackup.fsb

  Default Password (Password predefinita): non specificata (*)

  (*) Quando si fa clic su **Reference** *(Riferimento), si apre la cartella "Cartella utente\Documenti\Security Platform".*

- *Quando si utilizza la crittografia file EFS, si consiglia vivamente di consultare le informazioni relative a tale funzione nella Guida in linea di Windows®. In questo modo si potrà evitare il rischio di non riuscire a decifrare i file per avere inavvertitamente modificato la chiave di crittografia utilizzata in EFS o per aver perso la chiave stessa.*

6 Utilità password TOSHIBA

Utilizzando l'Utilità password TOSHIBA, è possibile impostare la configurazione in modo da impedire agli utenti sprovvisti dei privilegi di supervisore di modificare le impostazioni relative a TPM nella configurazione del BIOS.

Una volta effettuata questa impostazione, gli utenti sprovvisti dei privilegi di supervisore non saranno in grado di modificare le impostazioni relative a TPM nella configurazione del BIOS (le opzioni della casella **Security Controller** (Controller di sicurezza)).

1. Eseguire il seguente file per avviare l'Utilità password TOSHIBA.

   `C:\Program Files\TOSHIBA\PasswordUtility\TOSPU.exe`

2. Registrare la password del supervisore nella scheda **Password supervisore**.
3. Aprire la schermata di configurazione Criterio utente dalla scheda **Password supervisore**.
4. Nella scheda **TPM**, deselezionare le opzioni che non dovranno essere accessibili dagli utenti sprovvisti dei privilegi di supervisore.
5. Fare clic sul pulsante **Imposta**, quindi, dopo aver eseguito l'autenticazione come supervisore, salvare il criterio utente modificato.
6. Uscire dall'Utilità password TOSHIBA.

7 Trasferimento dell'ambiente TPM e smaltimento del computer

7.1 Trasferimento

Fare clic sull'icona **Security Platform** nella barra delle applicazioni e selezionare **Manage Security Platform** (Gestione piattaforma di sicurezza). Nella finestra **Infineon Security Platform Setting Tool** (Strumento di impostazione di Infineon Security Platform), fare clic sulla scheda **Migration** (Trasferimento). Nella scheda **Migration**, è possibile fare clic sul pulsante **Learn more...** (Per saperne di più...) per visualizzare informazioni sull'operazione di trasferimento. (L'operazione deve essere eseguita sia per la piattaforma di origine che per quella di destinazione.) Eseguire l'operazione seguendo le istruzioni visualizzate sullo schermo.

Solo i dati di TPM vengono trasferiti durante il processo; per trasferire i dati di Personal Security Drive e i file cifrati con EFS, utilizzare le normali operazioni di gestione dei file.

- *È necessario installare* **Infineon TPM Professional Package** *anche sulla piattaforma di destinazione.*
- *Il trasferimento tra computer attraverso una rete non è possibile se si utilizza Windows® Firewall. È possibile modificare l'impostazione di Windows® Firewall in* **Security Center** *(Centro sicurezza) a cui si accede dal* **Pannello di controllo***.*

7.2 Smaltimento del computer

Quando si elimina il computer, eseguire i due processi seguenti per fare in modo che nessuno possa entrare in possesso di informazioni riservate. Prendere le stesse precauzioni anche in caso di passaggio del computer a un altro proprietario.

1. Disinstallare **Infineon TPM Professional Package** ed eliminare l'archivio di ripristino e la chiave dell'archivio di ripristino di emergenza (**Emergency Recovery Archive Token**). Eliminare tutti i dati presenti nell'unità disco rigido.
2. Punto 1: Visualizzare la schermata di **configurazione del BIOS**. (Per ulteriori informazioni, consultare il capitolo 2 - *Uso di TPM per la prima volta*.)

   Punto 2: Spostare il cursore sull'opzione **Clear TPM Owner** (Cancella proprietario TPM) della voce **SECURITY CONTROLLER** (Controller di sicurezza) e premere la barra spaziatrice o il tasto Backspace. Mediante questa operazione, tutti i dati di TPM vengono distrutti e TPM viene disabilitato.

   Punto 3: Viene visualizzato un messaggio. Premere i tasti **Y**, **E** e **S** seguiti dal tasto **Invio**.

Dopo l'eliminazione dei dati interni di TPM, non è più possibile leggere i file.

8 Ripristino di TPM

8.1 Processo di ripristino di emergenza - Panoramica

Il processo di ripristino di emergenza viene utilizzato nei seguenti casi:

- Quando si verificano problemi in TPM che richiedono delle modifiche al software.
- Quando si sostituisce la scheda madre con TPM incorporato in conseguenza di un difetto.
- Quando TPM viene cancellato accidentalmente o per altri motivi.

Per ulteriori informazioni, consultare la sezione della Guida in linea relativa al *ripristino di emergenza dei dati*.

- *Si consiglia di stampare preventivamente una copia della sezione della Guida in linea relativa al ripristino di emergenza dei dati.*
- *Le informazioni riportate di seguito si riferiscono al ripristino di TPM e non dei dati ad esso relativi, come i file cifrati con EFS o i file nell'unità PSD. Per i file presenti nel disco rigido incorporato, si consiglia vivamente di creare copie di backup separate e di archiviarle in modo sicuro.*

8.2 Ripristino della password utente

Questa funzione può essere utilizzata se l'utente di Infineon Security Platform dimentica la password utente di base oppure se si verifica un problema con il dispositivo di autenticazione dell'utente. Se non è possibile ripristinare la password, l'utente non può utilizzare le funzioni di Security Platform. Questo potrebbe causare la perdita dei dati riservati.

Per informazioni dettagliate, consultare la sezione della Guida in linea relativa al ripristino della password utente di base.

8.3 Ripristino di PSD

Se il certificato PSD viene perso, è possibile recuperare i dati PSD utilizzando la funzione Personal Secure Drive Recovery.

Per ulteriori informazioni, consultare la relativa sezione.

Indice analitico

R

S

T

U

W

Promemoria

Assicurarsi che le password o le chiavi utilizzate siano conservate in modo sicuro (qualora dovessero essere dimenticate) e in un luogo non accessibile da altre persone, per proteggere le proprie informazioni riservate. Non conservare tali dati in luoghi dove siano facilmente visibili da altre persone (ad esempio, annotati su foglietti adesivi applicati alla propria scrivania).

Password del proprietario:

Password utente base:

Luogo in cui è conservata la chiave per il ripristino di emergenza:

Password chiave per il ripristino di emergenza:

Posizione di salvataggio del file di archivio:

Posizione di salvataggio della chiave di ripristino password:

Password della chiave di ripristino password:

Posizione di salvataggio del file Personal Secret:

Password utente TPM

Nome utente di Windows®:

Password utente TPM:

Nome utente di Windows®:

Password utente TPM:

Nome utente di Windows®:

Password utente TPM: