Guida HP ProtectTools Embedded Security

HP Business Desktops
modello dx5150

Numero di parte del documento: 376352-061

Dicembre 2004

La presente guida contiene istruzioni per l'uso del software di configurazione dei parametri del chip HP ProtectTools Embedded Security.

AVVERTENZA: Il testo presentato in questo modo indica che la mancata osservanza delle istruzioni potrebbe comportare lesioni fisiche o addirittura la perdita della vita.

ATTENZIONE: Il testo presentato in questo modo indica che la mancata osservanza delle relative istruzioni può causare danni alle apparecchiature o perdite di informazioni.

Guida HP ProtectTools Embedded Security

Prima edizione (Dicembre 2004)

Numero di parte del documento: 376352-061

Sommario

HP ProtectTools Embedded Security

HP ProtectTools Embedded Security

HP ProtectTools Security Manager è il software che consente di configurare i parametri per HP ProtectTools Embedded Security. Manager è un'interfaccia (shell) che punta alle varie opzioni disponibili del software Embedded Security. HP ProtectTools Embedded Security è un gruppo di software che comprende Personal Secure Drive (PSD), interfaccia codifica/chip TPM, migrazione sicurezza, creazione di archivi e controllo tramite password.

Requisiti

Per poter utilizzare le funzioni di sicurezza sono necessari gli strumenti seguenti:

- software HP ProtectTools Embedded Security
- software HP ProtectTools Embedded Security Manager
- chip HP ProtectTools Embedded Security installato nel computer

Per informazioni sulla configurazione della soluzione Embedded Security vedere "Procedure di configurazione" a pagina 8.

Concetti base di ProtectTools Embedded Security

Questa seziona contiene informazioni specialistiche su concetti fondamentali per poter utilizzare HP ProtectTools Embedded Security e HP ProtectTools Security Manager.

Chip HP ProtectTools Embedded Security

Il chip Embedded Security è un componente hardware con funzioni di sicurezza e crittografia, che mette a disposizione un'area di memorizzazione "tamper-proof" (a prova di manomissione) per la protezione di chiavi pubbliche e private. Solo i tecnici dell'assistenza HP autorizzati possono accedere al chip, installato di fabbrica, o eliminarlo.

Personal Secure Drive (PSD)

Una delle funzioni di Embedded Security è il Personal Secure Drive (PSD). Il PSD è un disco virtuale che viene creato sul disco fisso durante il processo di inizializzazione utente di HP ProtectTools Embedded Security. In questo disco possono essere memorizzati i dati sensibili. Il PSD consente la creazione e l'accesso a file e cartelle come con qualsiasi altra unità.

Per accedere al PSD sono necessari l'accesso fisico al computer su cui risiede il PSD e la password PSD. Una volta immessa la password, il PSD viene visualizzato e i file sono resi disponibili. I file restano disponibili fino al log off, dopodiché il PSD viene automaticamente nascosto. Non è possibile accedere ai PSD in rete.

I dati crittografati vengono memorizzati sul PSD. Sul PSD vengono memorizzate le chiavi utilizzate per crittografare i file sul chip HP ProtectTools Embedded Security, impedendo l'accesso ai dati agli utenti non autorizzati e vincolando i dati stessi al computer specifico. In tal modo i dati protetti sono accessibili solo da quest'ultimo.

Posta elettronica

La posta elettronica sicura è un'altra delle funzioni di Embedded Security. Grazie ad essa è possibile condividere le informazioni riservate, con la certezza che l'autenticità delle stesse non venga meno durante il trasferimento. La posta elettronica sicura consente di:

- Selezionare un certificato di chiave pubblica emesso da una Certification Authority (CA).
- Firmare i messaggi digitalmente.
- Crittografare i messaggi.

HP ProtectTools Embedded Security ed HP ProtectTools Security Manager migliorano anche la funzionalità della posta elettronica fornendo una protezione aggiuntiva della chiave utilizzata per crittografare, decrittare e firmare digitalmente i messaggi. Queste funzioni di potenziamento della posta elettronica sono disponibili con i seguenti client:

- Microsoft Outlook Express (versione 4 e successive)
- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Netscape Messenger 4,79
- Netscape Messenger 7.0

Per le istruzioni per l'uso dei client di posta elettronica consultare l'HP ProtectTools Embedded Security Email Integration Help.

EFS (Encrypted File System) avanzato

EFS è il servizio di crittografia di Microsoft Windows 2000 e Windows XP Professional. EFS garantisce la riservatezza dei dati con le seguenti funzioni:

- crittografia dei file da parte degli utenti quando sono memorizzati su disco
- accesso semplice e rapido a file crittografati
- crittografia dei dati automatica (e trasparente)
- possibilità per l'amministratore di sistema di recuperare i dati crittografati dagli utenti

HP ProtectTools Embedded Security ed HP ProtectTools Security Manager migliorano anche l'EFS fornendo una protezione aggiuntiva della chiave utilizzata per crittografare e decrittare i dati.

Per ulteriori informazioni sull'EFS, consultare la guida in linea del sistema operativo.

Utenti ed amministratori

Utenti

Gli utenti dispongono dell'accesso base ad Embedded Security, che consente loro di:

- inviare e ricevere messaggi di posta elettronica crittografati
- crittografare file e cartelle
- inizializzare la chiave personale Basic User (Utente base)
- creare, eliminare e modificare account personali utente nell'ambito della sicurezza integrata
- configurare, creare, utilizzare ed eliminare PSD individuali

Amministratori

Gli amministratori inizializzano la soluzione Embedded Security sui computer e possono:

- configurare la macchina locale e le politiche utente di Embedded Security
- preparare le chiavi ed i certificati utente per la migrazione
- cambiare la password del titolare di Embedded Security
- disabilitare ed abilitare Embedded Security
- autorizzare i computer di destinazione per la migrazione delle chiavi e dei certificati utente
- recuperare dati memorizzati e crittografati tramite Embedded Security

Per ulteriori informazioni sugli utenti e gli amministratori di Embedded Security, consultare la guida in linea del sistema operativo. Per ulteriori informazioni sui titolari di Embedded Security, consultare l'HP ProtectTools Embedded Security Email Integration Help.

Certificati digitali

I certificati digitali sono una sorta di "chiave" elettronica che conferma l'identità di una persona fisica o di una società. Le chiavi sono costituite da numeri o stringhe di caratteri noti solamente al mittente e/o al destinatario. I certificati digitali ne autenticano il titolare mediante firma digitale allegata ai messaggi di posta elettronica da questi inviati.

I certificati digitali vengono emessi dalle Certification Authority (CA) e contengono i seguenti dati:

- chiave pubblica del titolare
- nome del titolare
- data di scadenza del certificato digitale
- numero di serie del certificato digitale
- nome della CA che ha emesso il certificato digitale
- firma digitale della CA che ha emesso il certificato digitale

Firma digitale

La firma digitale visualizza il nome della CA che ha emesso il certificato digitale se serve per:

- verificare l'identità del mittente del documento digitale
- e certificare che il contenuto non è stato modificato successivamente all'invio.

Per ulteriori informazioni sulla firma digitale, consultare la guida in linea del sistema operativo.

Chiavi pubbliche e private

La crittografia asimmetrica, ovverosia il metodo utilizzato da Embedded Security per crittografare le informazioni, richiede l'uso di due chiavi: una pubblica ed una privata.

Le chiavi pubbliche possono essere liberamente distribuite a diversi utenti, mentre quelle private sono detenute dai singoli utenti individualmente.

Ad esempio, per inviare un messaggio di posta elettronica crittografato, l'utente A utilizzerà una chiave pubblica (liberamente disponibile) dell'utente B per crittografare il contenuto del messaggio inviato a quest'ultimo. Dato che l'utente B è l'unico a possedere la sua chiave privata, è anche il solo in grado di decrittare il contenuto del messaggio inviato dall'utente A.

La tecnologia compatibile con le chiavi pubbliche consente di trasmettere informazioni riservate su reti pubbliche, servirsi della firma digitale per garantire l'autenticità del messaggio e fornire l'autenticazione tra server e client.

Recupero d'emergenza

L'archivio di recupero d'emergenza (Emergency Recovery Archive) creato dall'amministratore durante la configurazione di Embedded Security, è un file in cui vengono memorizzate le informazioni sensibili relative al computer, ai suoi utenti ed alle chiavi private utilizzate per proteggere i dati crittografati o riservati. In caso di guasto al computer queste informazioni sensibili devono essere recuperate per avere accesso ai dati protetti.

L'Emergency Recovery Token, anch'esso creato dall'amministratore in fase di configurazione di Embedded Security, è un file in cui vengono memorizzate le chiavi utilizzate per proteggere i dati nell'Emergency Recovery Archive. Il token è necessario per accedere all'archivio. L'accesso all'Emergency Recovery Token è protetto mediante password. La password è necessaria per ripristinare il sistema Embedded Security.

Politiche

Le politiche sono regole che disciplinano il comportamento del computer o del software. L'amministratore di sistema in genere specifica le politiche di sicurezza per garantire l'uso coerente di Embedded Security all'interno di un'organizzazione. Esistono due tipi di politiche di sicurezza: politiche macchina e politiche utente.

Politiche macchina

Le politiche macchina sono regole che disciplinano il comportamento generale di Embedded Security rispetto ad un determinato computer.

Politiche utente

Le politiche utente sono regole che disciplinano i diritti dell'utente di Embedded Security.

Per ulteriori informazioni sulle politiche macchina e sulle politiche utente, consultare HP ProtectTools Embedded Security Help.

Procedure di configurazione

Procedere come segue per abilitare ed inizializzare il chip di Embedded Security con l'utility Computer Setup del BIOS:

ATTENZIONE: Per evitare rischi di sicurezza, HP consiglia di affidare l'inizializzazione del chip Embedded Security ad una persona autorizzata (vedere punto 4). In caso di mancata inizializzazione del chip Embedded Security potrebbero prendere possesso del sistema un utente non autorizzato, un computer worm, o un virus.

La password del supervisore deve essere impostata nel BIOS in Computer Setup per poter accedere alle configurazioni dei chip. Per ulteriori informazioni vedere la *Guida dell'utility Computer Setup (F10)* sul *CD della documentazione* in dotazione al computer.

Abilitazione del chip

1. Accendere o riavviare il computer. In Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena il computer è acceso, premere e tenere premuto il tasto **F10** finché non si accede a Computer Setup.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Servirsi dei tasti freccia per selezionare **Set Supervisor Password** e premere **Invio**.
4. Immettere la password del supervisore e premere **Invio**.
5. Riavviare il computer. In Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
6. Al prompt dei comandi **Press any key to enter TPM Configuration** premere un tasto.
7. Immettere la password del supervisore e premere **Invio**.
8. Premere **E** per abilitare il chip TPM.

   A questo punto il chip è abilitato.

Inizializzazione del chip Embedded Security

Nella maggior parte dei casi, l'inizializzazione compete all'amministratore del sistema informatico.

1. Fare clic destro sull'icona **HP ProtectTools** nel system tray, seguito da clic sinistro su **Embedded Security Initialization (Inizializzazione Embedded Security)**.

   Viene visualizzata la schermata della procedura guidata d'inizializzazione (**HP ProtectTools Embedded Security Initialization Wizard**).

2. Fare clic su **Avanti**.
3. Immettere e confermare la password Take Ownership (Assunzione di controllo) e fare clic su **Avanti**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

4. Fare clic su **Avanti** per accettare la posizione dell'archivio di recupero predefinita.
5. Immettere e confermare la password Emergency Recovery Token (Token recupero d'emergenza) e fare clic su **Avanti**.
6. Fare clic su **Sfoglia** e selezionare la destinazione.

ATTENZIONE: La chiave Emergency Recovery Token serve per recuperare i dati crittografati in caso di guasto al computer o al chip Embedded Security. Senza la chiave non è possibile recuperare i dati. I dati non sono accessibili senza la password Basic User (Utente base). Conservare la chiave in un luogo sicuro.

7. Fare clic su **Salva** per accettare posizione e nome file predefiniti e fare clic su **Avanti**.
8. Fare clic su **Avanti** per confermare le impostazioni prima che venga inizializzata la Security Platform.

ATTENZIONE: Può darsi che venga visualizzato un messaggio che avverte che le funzioni di Embedded Security non sono state inizializzate. Non fare clic sul messaggio: si chiuderà da solo dopo pochi secondi e se ne terrà conto nel prosieguo della procedura.

9. Se a questo punto è necessario impostare un account utente, verificare che sia selezionata la casella di controllo **Start Embedded Security User Initialization Wizard (Avvia inizializzazione guidata utente Embedded Security)**. Fare clic su **Fine**.

Impostazione di un account utente

Impostazione di un account utente:

- originare una chiave Basic User (Utente base) per la protezione dei dati crittografati
- impostare un PSD per memorizzare file e cartelle crittografati

ATTENZIONE: Conservare la password Basic User (Utente base). Senza di essa non è possibile accedere ai dati crittografati.

Per impostare un account Basic User ed abilitare il relativo utente all'utilizzo delle funzioni di sicurezza:

1. Se la procedura guidata di inizializzazione utente **Embedded Security** non si è avviata, fare clic destro sull'icona **HP ProtectTools** nel system tray, quindi clic sinistro su **Embedded Security User Initialization (Inizializzazione utente Embedded Security)**.

   Viene visualizzata la procedura guidata **Embedded Security User Initialization Wizard**.
2. Fare clic su **Avanti**.
3. Immettere e confermare la password Basic User Key (Chiave utente base) e fare clic su **Avanti**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

4. Fare clic su **Avanti** per confermare.
5. Selezionare le funzioni di sicurezza appropriate e fare clic su **Avanti**.
6. Fare clic su **Avanti** per tralasciare i file della guida.
7. Se esistono diversi certificati di crittografia, fare clic su quello appropriato.

   Fare clic su **Avanti** per applicare il certificato di crittografia.
8. Configurare il PSD con le impostazioni appropriate e fare clic su **Avanti**.
9. Configurare nuovamente il PSD con le impostazioni appropriate e fare su **Avanti**.

La dimensione minima del PSD è 50 MB, quella massima 2.000 MB.

10. Fare clic su **Avanti** per confermare.

A seconda delle dimensioni del PSD, il computer può impiegare diversi minuti per elaborare la conferma.

11. Fare clic su **Fine**.
12. Fare clic su **Sì** per riavviare il computer.

Operazioni d'uso comune

In questa sezione vengono esaminate le operazioni base più frequentemente eseguite da utenti e titolari.

Operazioni utente

Le operazioni base riservate agli utenti sono la configurazione del PSD, la crittografia di file e cartelle e l'invio/ricezione di messaggi di posta elettronica mediante crittografia e/o firma digitale.

Uso del PSD

Per utilizzare il PSD immettere la password PSD personale. Il PSD viene visualizzato e file vengono decrittati. Il PSD si usa come tutte le altre unità.

Una volta finito di utilizzare il PSD, effettuare il log off. La presenza del PSD viene nascosta automaticamente.

Crittografia di file e cartelle

Per utilizzare EFS in Windows 2000 e Windows XP Professional occorre tenere presente quanto segue:

- È possibile crittografare solamente file e cartelle su partizioni NTFS. Non è invece possibile crittografare file e cartelle su partizioni FAT.
- Non è possibile crittografare file di sistema e file compressi, ed a loro volta i file crittografati non possono essere compressi.
- Le cartelle temporanee dovrebbero essere crittografate, dato che i file ivi contenuti sono potenzialmente interessanti per chi intende violare i dati.
- Quando l'utente crittografa un file o una cartella per la prima volta viene definita automaticamente una politica di recupero. Ciò consente agli utenti che dovessero perdere i certificati personali e le chiavi private di utilizzare un agente di recupero per decrittare i dati.

Per crittografare file e cartelle:

1. Selezionare il file o la cartella da crittografare.
2. Fare clic destro col mouse o il Touchpad.
3. Fare clic su **Encrypt (Crittografia)**.
4. Fare clic su **Apply changes to this folder only (Applica modifica solo a questa cartella) Apply changes to this folder, subfolder and files (Applica modifiche a questa cartella, sottocartella e file)**.
5. Fare clic su **OK**.

Invio e ricezione di messaggi di posta elettronica con crittografia e/o firma digitale

Per le istruzioni su queste operazioni, consultare la guida in linea del programma di posta elettronica.

Per utilizzare messaggi sicuri, occorre configurare il client di posta elettronica per l'uso di un certificato digitale generato da Embedded Security. Se non è disponibile un certificato digitale richiederlo ad un'Autorità di Certificazione. Per le istruzioni sulla configurazione della posta elettronica e sull'ottenimento del certificato digitale, consultare la guida in linea del programma di posta elettronica.

Per inviare un messaggio di posta elettronica crittografato, sono necessari una copia della chiave pubblica o un certificato di crittografia del destinatario, il quale contiene una copia della chiave.

Microsoft Outlook utilizza la chiave pubblica del destinatario per crittografare il messaggio di posta elettronica; non è pertanto necessario immettere la chiave privata. Tuttavia, è necessaria la chiave privata per leggere un messaggio crittografato, perché la decrittazione richiede la chiave privata corrispondente a quella pubblica utilizzata per crittografare il messaggio.

Operazioni dell'amministratore

L'amministratore può eseguire numerose operazioni, alcune delle quali descritte qui di seguito. Per ulteriori informazioni, consultare la guida di HP ProtectTools Embedded Security.

Migrazione di chiavi tramite la procedura guidata di migrazione sicurezza computer

La migrazione è un'attività avanzata dell'amministratore che consente la gestione, il ripristino e il trasferimento di chiavi e certificati.

La prima fase della migrazione prevede l'autorizzazione, la configurazione e la gestione del processo di migrazione. Una volta completata la fase di autorizzazione, l'utente esporta ed importa chiavi e certificati dal computer di origine al computer di destinazione.

Per ulteriori informazioni sulla migrazione, consultare la guida di HP ProtectTools Embedded Security.

Recupero delle informazioni

Nel caso di guasto del chip o reset:

- È possibile utilizzare la procedura guidata di ripristino d'emergenza (Emergency Restore Wizard) per recuperare dati dal PSD.
- Il PSD supporta inoltre il recupero tramite agente di recupero, cioè un meccanismo simile all'EFS (Encryption File Systems).

  Per determinare se sul computer è presente un agente di recupero registrato fare clic su **Start > Tutti i programmi > Strumenti di amministrazione > Criteri di protezione locali > Criteri chiave pubblica > Agenti di recupero dati crittografati**.

Per ulteriori informazioni, consultare la guida in linea del sistema operativo.

Windows XP Professional non crea automaticamente un agente di recupero registrato. Per la configurazione di agenti di recupero registrati, procedere come di seguito indicato.

Per recuperare i dati, l'agente di recupero registrato deve disporre di certificato digitale e chiavi. La chiave privata e il certificato di recupero dati devono essere esportati su disco e conservati in luogo sicuro. La chiave privata di recupero dati va cancellata dal computer. Per poter recuperare i dati è necessario avere l'accesso fisico alla chiave privata di recupero dati.

Ripristino del chip Embedded Security alle impostazioni originali tramite Computer Setup

ATTENZIONE: Questa attività annulla il controllo personale sul chip Embedded Security, dopodiché, chiunque può inizializzarlo di nuovo.

In presenza di file crittografati, il ripristino del chip Embedded Security alle impostazioni originali potrebbe comportare perdita di dati.

Per riportare il chip Embedded Security alle impostazioni originali:

1. Accendere o riavviare il computer. In Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Al prompt dei comandi **Press any key to enter TPM Configuration** premere un tasto.
3. Immettere la password del supervisore e premere **Invio**.
4. Premere **C** per cancellare il chip TPM.
5. Premere **S** per confermare.

   A questo punto il chip è stato cancellato.

Suggerimenti per un funzionamento ottimale

HP suggerisce i seguenti accorgimenti per l'uso di Embedded Security.

- Un amministratore di sicurezza informatica dovrebbe configurare la password del supervisore nel BIOS in Computer Setup ed inizializzare il chip Embedded Security prima di consegnare il computer agli utenti.
- Un amministratore di sicurezza informatica dovrebbe configurare l'archivio di recupero d'emergenza in fase di configurazione della soluzione Embedded Security, invitando gli utenti a salvare i dati ed eseguire i backup su base regolare. In caso di guasto al sistema, è l'unico modo per poter recuperare i dati crittografati. L'Emergency Recovery Archive e l'Emergency Recovery Token dovrebbero essere memorizzati separatamente.
- Crittografare le cartelle anziché i singoli file in modo da crittografare anche i corrispondenti file temporanei.

- Crittografare i dati sensibili su computer appartenenti a un dominio. In tal modo ci si tutela contro la compromissione dei dati a seguito di attacchi crittografici offline.
- Effettuare su base regolare il backup di tutto il server in cui sono memorizzati dati server crittografati. Ciò garantisce che in caso di recupero dati, vengano ripristinati anche i profili che contengono le chiavi descrittive.
- Se si crittografano tipi di file monitorati da System Restore, memorizzare i file in un volume non monitorato.
- Il sistema non supporta livelli di crittografia multipli. Ad esempio, un utente non deve memorizzare un file crittografato EFS nel PSD, né cercare di crittografare un file già ivi memorizzato.

Quesiti ricorrenti (FAQ)

Come si fa a sapere se sul computer è installato il chip HP ProtectTools Embedded Security?

Trattandosi di un componente di sistema, viene elencato in Gestione periferiche.

Dove si può reperire il software HP ProtectTools Embedded Security?

Software, driver e guida online sono reperibili sul sito HP http://www.hp.com/products/security.

È possibile disinstallare il software HP ProtectTools Embedded Security? e come?

Sì. Il software viene disinstallato con la procedura standard di Windows. Prima della disinstallazione, è necessario salvare i dati protetti propri dell'utente, altrimenti gli stessi andranno perduti. La fase finale della disinstallazione consiste nel disabilitare il chip.

1. Accendere o riavviare il computer. In Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Al prompt dei comandi **Press any key to enter TPM Configuration** premere un tasto.
3. Immettere la password del supervisore e premere **Invio**.
4. Premere **D** per disabilitare il chip TPM.

   A questo punto il chip è disabilitato.

Risoluzione dei problemi

Embedded Security non funziona. Che cosa si deve fare?

1. Fare clic destro sull'icona **HP ProtectTools** nel system tray, seguito da clic sinistro su **Manage Embedded Security (Gestione Embedded Security)**.
2. Fare clic su **Embedded Security > Info > Self Test (Autotest)**.

Selezionare inoltre **Embedded Security State, Chip, Owner (Stato, Chip, Proprietario Embedded Security)** e **User (Utente)**.

Dopo un ripristino del sistema a seguito di un guasto che cosa si deve fare?

ATTENZIONE: Nella maggior parte dei casi l'amministratore di sistema esegue la procedura sotto indicata. Se la procedura non viene eseguita correttamente, potrebbe verificarsi perdita di dati permanente.

Per poter recuperare i dati dopo la sostituzione del chip ProtectTools è necessario quanto segue:

- SPEmRecToken.xml: chiave Emergency Recovery Token
- SPEmRecArchive.xml: cartella nascosta, posizione predefinita: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Password ProtectTools
  - Supervisore
  - Take Ownership
  - Emergency Recovery Token
  - Basic User

1. Accendere o riavviare il computer. In Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
2. Al prompt dei comandi **Press any key to enter TPM Configuration** premere un tasto.
3. Immettere la password del supervisore e premere **Invio**.
4. Premere **C** per cancellare il chip TPM.

5. Premere **S** per confermare.
6. Riavviare il computer. In Windows fare clic su **Start > Chiudi sessione > Riavvia il sistema**.
7. Al prompt dei comandi **Press any key to enter TPM Configuration** premere un tasto.
8. Immettere la password del supervisore e premere **Invio**.
9. Premere **E** per abilitare il chip TPM.

   A questo punto il chip è abilitato.
10. Quando Windows si è avviato, fare clic destro sull'icona **HP ProtectTools Embedded Security** nel system tray, seguito da clic sinistro su **Manage Embedded Security (Gestione Embedded Security)**.
11. Selezionare la casella di controllo: **I want to restore the existing Embedded Security (Voglio ripristinare l'Embedded Security esistente)** e fare clic su **Avanti**.
12. Digitare e confermare la password Take Ownership originale. Fare clic su **Avanti**.
13. Fare clic su **Do not create a recovery archive (Non creare un archivio di recupero)**, quindi su **Avanti**.

ATTENZIONE: La creazione di un nuovo archivio comporta la perdita totale dei dati a seguito di sovrascrittura dell'archivio necessario per il recupero.

14. Fare clic su **Sì** per procedere senza creare un archivio di recupero.
15. Fare clic su **Avanti** per confermare.
16. Fare clic su **Sfoglia** e individuare l'archivio d'emergenza, la cui posizione predefinita è: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
17. Fare clic su **Apri** e su **Avanti**.
18. Fare clic su **Sfoglia** e individuare il token di recupero creato durante la fase di inizializzazione **HP ProtectTools Embedded Security**, fare clic sul token, quindi su **Apri**.
19. Immettere la password Token e fare clic su **Avanti**.

20. Selezionare il nome della macchina e fare clic su **Avanti**.
21. Fare clic su **Avanti** per confermare.

    Se appare un messaggio che indica che il ripristino non è stato eseguito, ritornare al punto 1. Controllare attentamente password, posizione e nome del token, posizione e nome dell'archivio.
22. Se a questo punto è necessario impostare un account utente, verificare che sia selezionata la casella di controllo **Start Embedded Security User Initialization Wizard (Avvia inizializzazione guidata utente Embedded Security)**. Fare clic su **Fine**.

Le operazioni di cui ai punti 23–35 ripristinano le chiavi Basic User e devono essere ripetute per tutti gli utenti.

---

23. Se la procedura guidata di inizializzazione utente **Embedded Security** non si è avviata fare clic destro sull'icona **HP ProtectTools Embedded Security** nel system tray, quindi clic sinistro su **Restore Embedded Security Features (Ripristina funzioni Embedded Security)**.

    Viene visualizzata la procedura di inizializzazione guidata utente **Embedded Security**.
24. Fare clic su **Avanti**.
25. Fare clic su **Recover your basic user key (Recupera chiave utente base)** e fare clic su **Avanti**.
26. Selezionare un utente, immettere la relativa password Basic User Key e fare clic su **Avanti**.
27. Fare clic su **Avanti** per confermare le impostazioni ed accettare la posizione dei dati di recupero predefinita.
28. Selezionare le funzioni di sicurezza appropriate e fare clic su **Avanti**.
29. Fare clic su **Avanti** per tralasciare i file della guida.
30. Se esistono diversi certificati di crittografia, fare clic su quello appropriato.

    Fare clic su **Avanti** per applicare il certificato di crittografia.

31. Selezionare **I want to change my Personal Secure Drive settings (Voglio cambiare le impostazioni Personal Secure Drive)** se del caso e fare clic su **Avanti**.
32. Confermare le funzioni di sicurezza e fare clic su **Avanti**.
33. Confermare le impostazioni e fare clic su **Avanti**.
34. Immettere la password PSD e fare clic su **OK**.
35. Fare clic su **Fine** e su **Sì** per riavviare.

ATTENZIONE: Conservare la password Basic User (Utente base). Senza di essa non è possibile accedere ai dati crittografati.

Glossario

Archivio di recupero d'emergenza: si tratta di un'area di memorizzazione protetta che consente la ri-crittografia di chiavi utente base da una chiave proprietaria di piattaforma ad un'altra.

Autorità di Certificazione (Certification Authority, CA): servizio che emette i certificati richiesti per gestire un'infrastruttura di chiavi pubbliche.

Certificati digitali: credenziali elettroniche che confermano l'identità di una persona o di una società vincolando l'identità del titolare del certificato digitale ad una coppia di chiavi elettroniche utilizzate per firmare le informazioni digitali.

Criptazione: vedi algoritmo, crittografia; qualsiasi procedura utilizzata in crittografia per convertire testo normale in testo cifrato ed evitare così che i dati vengano letti da persone non autorizzate. Esistono diversi tipi di criptazione dei dati che costituiscono la base della sicurezza di rete. I più comuni sono Data Encryption Standard e criptazione di chiavi pubbliche.

Crittografia: teoria e pratica di crittografia e decrittazione; codifica dei dati in modo tale che possano essere decodificati solo da determinate persone. Un sistema di crittografia e decrittazione dei dati viene denominato sistema crittografico (cryptosystem). Normalmente questi sistemi comportano un algoritmo per la combinazione dei dati originali ("testo normale", plaintext) con una o più "chiavi" numeriche o stringhe di caratteri note solo al mittente o al destinatario. L'output risultante viene denominato "testo cifrato" (cipher text).

CSP (Cryptographic Service Provider): fornitore o libreria di algoritmi crittografici utilizzabili in un'interfaccia prestabilita per eseguire determinate funzioni crittografiche.

Decrittazione: qualsiasi procedura utilizzata in crittografia per convertire il testo cifrato (dati crittografati) in testo normale.

EFS (Encryption File System): sistema di crittografia di tutti i file e sottocartelle della cartella selezionata.

Firma digitale: funzione utilizzata per verificare l'identità del mittente di un documento digitale e certificare che il contenuto non sia stato modificato dopo che il mittente lo ha firmato.

Migrazione: attività che consente la gestione, il ripristino e il trasferimento di chiavi e certificati.

Personal Secure Drive (PSD): unità che mette a disposizione un'area di memorizzazione protetta per dati sensibili.

PKI (Public Key Infrastructure): standard che definisce le interfacce per la creazione, l'uso e l'amministrazione di certificati e chiavi crittografiche.

TPM (Trusted Platform Module): livello hardware di sicurezza dei dati. Integrato nel sistema, il chip Embedded Security è in grado di controllare l'integrità del sistema e autenticare utenti terzi ad accedere alla piattaforma, restando sempre e completamente sotto il controllo dell'utente principale.