HP ProtectTools Embedded Security Handbuch

HP Business Desktops
dx5150 Modell

Dokument-Teilenummer: 376352-041

Dezember 2004

In diesem Handbuch finden Sie Anleitungen zur Verwendung der Software, mit der Sie die Einstellungen für den HP ProtectTools Embedded Security-Chip konfigurieren können.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Hewlett-Packard („HP“) haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt. Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Informationen in dieser Veröffentlichung werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt. Insbesondere enthalten diese Informationen keinerlei zugesicherte Eigenschaften. Alle sich aus der Verwendung dieser Informationen ergebenden Risiken trägt der Benutzer. Die Garantien für HP Produkte werden ausschließlich in der entsprechenden, zum Produkt gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten.

VORSICHT: In dieser Form gekennzeichneter Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.

ACHTUNG: Kennzeichnet eine Anweisung, deren Nichtbeachtung zur Beschädigung von Komponenten oder zum Verlust von Daten führen kann.

HP ProtectTools Embedded Security Handbuch

Erste Ausgabe (Dezember 2004)

Dokument-Teilenummer: 376352-041

Inhalt

HP ProtectTools Embedded Security

HP ProtectTools Embedded Security

Der HP ProtectTools Security Manager ist die Software, mit der Sie die Einstellungen für HP ProtectTools Embedded Security konfigurieren können. Der Manager ist eine Schnittstelle (Shell), die auf die in der Embedded Security-Software verfügbaren Optionen verweist. HP ProtectTools Embedded Security ist eine Software-Suite, die Funktionen wie das HP PSD (Personal Secure Drive, persönliches sicheres Laufwerk), Verschlüsselung/ TPM-Chip-Schnittstelle, Sicherheitsmigration, Archiverstellung und Kennwortsteuerung umfasst.

Anforderungen

Zur Nutzung dieser Sicherheitsfunktionen sind folgende Tools erforderlich:

- HP ProtectTools Embedded Security-Software
- HP ProtectTools Security Manager-Software
- HP ProtectTools Embedded Security-Chip (im System installiert)

Informationen zum Einrichten der Embedded Security-Lösung finden Sie unter „Einrichtungsverfahren“ auf Seite 8.

Grundlegende Begriffe zu ProtectTools Embedded Security

Dieser Abschnitt enthält wichtige Informationen zu Begriffen, deren Verständnis wichtig ist, um HP ProtectTools Embedded Security sowie den HP ProtectTools Security Manager zu verwenden.

HP ProtectTools Embedded Security-Chip

Der Embedded Security-Chip ist eine Hardware-Komponente, die Sicherheits- und Verschlüsselungsfunktionen bietet sowie einen vor unbefugtem Zugriff sicheren Speicherbereich zum Schutz der öffentlichen und privaten Schlüssel bereitstellt. Der Chip wird werkseitig vorinstalliert. Der Zugriff auf den Chip oder seine Entfernung sollte ausschließlich durch einen Servicepartner erfolgen.

Das PSD (Personal Secure Drive)

Eine Embedded Security-Funktion ist das PSD (Personal Secure Drive, persönliches sicheres Laufwerk). Das PSD ist ein virtuelles Laufwerk, das bei der Benutzerinitialisierung von HP ProtectTools Embedded Security auf der Festplatte erstellt wird. Dieses Laufwerk bietet einen geschützten Speicherbereich für sensible Daten. Das PSD ermöglicht das Erstellen von Dateien und Ordnern und den Zugriff darauf, wie jedes andere Laufwerk auch.

Für den Zugriff auf das PSD benötigen Sie den physischen Zugang zu dem Computer, auf dem das PSD resident ist, sowie das PSD-Kennwort. Wenn Sie Ihr PSD-Kennwort eingeben, wird das PSD sichtbar, und Sie können auf die Dateien zugreifen. Die Dateien bleiben verfügbar, bis Sie sich wieder abmelden. Dann wird auch das PSD automatisch ausgeblendet. Der Zugriff auf PSD-Laufwerke über ein Netzwerk ist nicht möglich.

Auf dem PSD werden verschlüsselte Daten gespeichert. Die dafür verwendeten Schlüssel werden auf dem HP ProtectTools Embedded Security-Chip gespeichert, sodass die Daten vor unbefugtem Benutzerzugriff geschützt und an den Computer gebunden sind. Dies bedeutet, dass der Zugriff auf die geschützten Daten nur auf dem Ziel-Computer erfolgen kann.

E-Mail

Sichere E-Mail ist eine andere wichtige Funktion von Embedded Security. Diese Funktion ermöglicht den Austausch vertraulicher Informationen und stellt sicher, dass die Authentizität der Informationen bei der Übertragung erhalten bleibt. Sichere E-Mail ermöglicht Ihnen Folgendes:

- Wahl eines von einer Zertifizierungsbehörde ausgestellten Zertifikats auf der Basis eines öffentlichen Schlüssels
- Digitales Unterzeichnen von Mitteilungen
- Verschlüsselung von Mitteilungen

HP ProtectTools Embedded Security und der HP ProtectTools Security Manager erhöhen die E-Mail-Sicherheit, indem sie zusätzlichen Schutz für den Schlüssel bieten, der zum Verschlüsseln, Entschlüsseln und digitalen Unterzeichnen von Mitteilungen verwendet wird. Diese Software erhöht die E-Mail-Sicherheit bei Verwendung folgender E-Mail-Clients:

- Microsoft Outlook Express (Version 4 oder höher)
- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Netscape Messenger 4.79
- Netscape Messenger 7.0

Anleitungen zur Verwendung von E-Mail-Clients finden Sie in der Hilfe zur E-Mail-Integration von HP ProtectTools Embedded Security.

Verbessertes EFS (Encryption File System)

Das Dateisystem EFS (Encryption File System, Verschlüsselungsdateisystem) ist der unter Microsoft Windows 2000 und Windows XP Professional verfügbare Verschlüsselungsdienst. EFS ermöglicht den Schutz der Daten durch folgendes Funktionsangebot:

- Verschlüsselung von Dateien durch den Benutzer beim Speichern auf einen Datenträger
- Schneller und einfacher Zugriff auf verschlüsselte Dateien
- Automatische (und transparente) Verschlüsselung von Daten
- Befähigung des Systemadministrators zur Wiederherstellung von Daten, die von einem anderen Benutzer verschlüsselt wurden

HP ProtectTools Embedded Security und der HP ProtectTools Security Manager verbessern das Dateiverschlüsselungssystem (EFS), indem sie zusätzlichen Schutz für den Schlüssel bieten, der zum Verschlüsseln und Entschlüsseln von Daten verwendet wird.

Weitere Informationen zum EFS finden Sie in der Online-Hilfe zum Betriebssystem.

Benutzer und Administratoren

Benutzer

Benutzer verfügen über grundlegenden Zugriff auf Embedded Security und können folgende Aufgaben durchführen:

- Senden und Empfangen von verschlüsselter E-Mail
- Verschlüsseln von Dateien und Ordnern
- Initialisieren eines persönlichen Basic-User-Schlüssels (Standardbenutzerschlüssel)
- Erstellen, Löschen oder Ändern eines persönlichen Benutzerkontos in Embedded Security
- Konfigurieren, Erstellen, Verwenden und Löschen eines PSD-Laufwerks

Administratoren

Administratoren initialisieren die Embedded Security-Lösung auf einem Computer und können folgende Aufgaben durchführen:

- Konfigurieren des lokalen Computers und der Benutzerrichtlinien für Embedded Security
- Vorbereiten von Benutzerschlüsseln und Zertifikaten für die Migration
- Ändern des Embedded Security-Besitzerkennworts
- Deaktivieren und Aktivieren von Embedded Security
- Autorisieren des Zielcomputers für die Migration von Benutzerschlüsseln und Zertifikaten
- Wiederherstellen der mit Embedded Security gespeicherten und verschlüsselten Daten

Weitere Informationen zu Benutzern und Administratoren in Verbindung mit Embedded Security finden Sie in der Online-Hilfe zum Betriebssystem. Weitere Informationen zu Besitzern in Verbindung mit Embedded Security finden Sie in der Hilfe zu HP ProtectTools Embedded Security.

Digitale Zertifikate

Digitale Zertifikate sind eine Art elektronischer „Schlüssel“ zur Bestätigung der Identität einer Person oder eines Unternehmens. Die Schlüssel bestehen aus Zahlen oder Zeichenfolgen, die nur dem Absender und/oder dem Empfänger bekannt sind. Ein digitales Zertifikat authentifiziert den Zertifikatsbesitzer, indem es eine digitale Signatur bereitstellt, die seinen E-Mails hinzufügt wird.

Ein digitales Zertifikat wird von einer Zertifizierungsbehörde ausgestellt und enthält folgende Informationen:

- den öffentlichen Schlüssel des Besitzers
- den Namen des Besitzers
- das Ablaufdatum des digitalen Zertifikats
- die Seriennummer des digitalen Zertifikats
- den Namen der Zertifizierungsbehörde, die das digitale Zertifikat ausgestellt hat
- die digitale Signatur der Zertifizierungsbehörde, die das digitale Zertifikat ausgestellt hat

Digitale Signatur

Eine digitale Signatur gibt den Namen der Zertifizierungsbehörde an, die das digitale Zertifikat ausgestellt hat. Sie wird verwendet, um:

- die Identität des Absenders eines digitalen Dokuments sicherzustellen
- zu beglaubigen, dass der Inhalt nicht geändert wurde, nachdem der Absender das Dokument digital unterzeichnet hat

Weitere Informationen zu digitalen Signaturen finden Sie in der Online-Hilfe zum Betriebssystem.

Öffentlicher Schlüssel und privater Schlüssel

Die asymmetrische Verschlüsselung, das von Embedded Security verwendete Verfahren zur Verschlüsselung von Daten, erfordert die Verwendung von zwei Schlüsseln, einem öffentlichen und einem privaten Schlüssel.

Ein öffentlicher Schlüssel kann ohne Einschränkung an viele Benutzer verteilt werden. Ein privater Schlüssel dagegen wird nur von einem einzigen Benutzer verwendet.

Um beispielsweise eine verschlüsselte E-Mail zu senden, verwendet Benutzer A den (frei verfügbaren) öffentlichen Schlüssel von Benutzer B, um den Inhalt der für Benutzer B bestimmten E-Mail zu verschlüsseln. Da außer Benutzer B keine andere Person über dessen privaten Schlüssel verfügt, kann nur er den Inhalt der E-Mail entschlüsseln, die ihm Benutzer A gesandt hat.

Technologie auf der Grundlage öffentlicher Schlüssel (Public-Key-Technologie) ermöglicht es, vertrauliche Informationen über öffentliche Netzwerke zu übertragen, die Authentizität von E-Mails durch digitale Signaturen sicherzustellen und die Authentifizierung zwischen Server und Client zu erreichen.

Wiederherstellung im Notfall

Das vom Administrator beim Einrichten von Embedded Security erstellte Wiederherstellungsarchiv (Emergency Recovery Archive) ist eine Datei, in der sensible Informationen über den Computer und seine Benutzer gespeichert sind, sowie die privaten Schlüssel, mit denen verschlüsselte oder vertrauliche Daten geschützt werden. Bei einem Systemausfall werden diese Informationen benötigt, um den Zugriff auf geschützte Daten wiederherzustellen.

Das ebenfalls vom Administrator bei der Einrichtung von Embedded Security erstellte Wiederherstellungs-Token (Emergency Recovery Token) ist eine Datei, in der die Schlüssel gespeichert sind, die zum Schutz der Daten im Wiederherstellungsarchiv verwendet werden. Das Token ist für den Zugriff auf das Archiv erforderlich. Der Zugriff auf das Wiederherstellungs-Token ist durch ein Kennwort geschützt. Dieses Kennwort wird für den Fall benötigt, dass das Embedded Security-System wiederhergestellt werden muss.

Richtlinien

Richtlinien sind Regeln, die das Verhalten eines Computers oder eines Softwareprogramms bestimmen. Ein Systemadministrator definiert in der Regel Sicherheitsrichtlinien, um die einheitliche Verwendung von Embedded Security im gesamten Unternehmen sicherzustellen. Die zwei Arten von Sicherheitsrichtlinien sind Computerrichtlinien und Benutzerrichtlinien.

Computerrichtlinien

Computerrichtlinien sind Regeln, die das Gesamtverhalten von Embedded Security im Hinblick auf einen bestimmten Computer bestimmen.

Benutzerrichtlinien

Benutzerrichtlinien sind Regeln, die die Rechte eines Benutzers von Embedded Security bestimmen.

Weitere Informationen zu Computer- und Benutzersicherheitsrichtlinien finden Sie in der Hilfe zu HP ProtectTools Embedded Security.

Einrichtungsverfahren

Befolgen Sie die unten aufgeführten Schritte, um den Embedded Security-Chip mithilfe von Computer Setup (F10) im System-BIOS zu aktivieren und zu initialisieren.

ACHTUNG: Um ein Sicherheitsrisiko auszuschalten, empfiehlt HP die sofortige Initialisierung des Embedded Security-Chips durch eine von Ihrem Unternehmen autorisierte Person (siehe Schritt 4). Wenn der Embedded Security-Chip nicht initialisiert wird, besteht die Gefahr, dass ein unbefugter Benutzer, ein Computerwurm oder ein Computervirus sich des Systems bemächtigen kann.

Das BIOS-Supervisor-Kennwort muss in Computer Setup eingerichtet werden, bevor der Chip konfiguriert werden kann. Weitere Informationen finden Sie im *Computer Setup (F10) Utility Handbuch* auf der *Documentation CD*, die im Lieferumfang des Computers enthalten ist.

Aktivieren des Chips

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Microsoft Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

3. Wählen Sie mit den Pfeiltasten die Option **Set Supervisor Password** (Supervisor-Kennwort einrichten), und drücken Sie dann die **Eingabetaste**.
4. Geben Sie das gewünschte Kennwort ein, und drücken Sie die **Eingabetaste**.

5. Starten Sie den Computer neu. Klicken Sie unter Microsoft Windows auf **Start > Beenden > Neu starten**.
6. Sobald die Meldung **Press any key to enter TPM Configuration** (Beliebige Taste für die TPM-Konfiguration drücken) angezeigt wird, drücken Sie eine Taste.
7. Geben Sie das Supervisor-Kennwort ein, und drücken Sie die **Eingabetaste**.
8. Drücken Sie **E**, um den TPM-Chip zu aktivieren.

   Der Chip ist nun aktiviert.

Initialisieren des Embedded Security-Chips

In den meisten Fällen wird der Embedded Security-Chip vom Systemadministrator initialisiert.

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** in der Taskleiste und anschließend mit der linken Maustaste auf **Embedded Security Initialization** (Embedded Security initialisieren).

   Der **HP ProtectTools Embedded Security Initialization Wizard** (Assistent für die Initialisierung von HP ProtectTools Embedded Security) wird aufgerufen.
2. Klicken Sie auf **Next** (Weiter).
3. Geben Sie ein Besitzerkennwort ein, und bestätigen Sie es. Klicken Sie dann auf **Next** (Weiter).

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

4. Klicken Sie auf **Next** (Weiter), um das Standardverzeichnis für das Wiederherstellungsarchiv zu übernehmen.
5. Geben Sie ein Kennwort für das Wiederherstellungs-Token ein, und bestätigen Sie es. Klicken Sie dann auf **Next** (Weiter).

6. Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie den gewünschten Speicherort aus.

ACHTUNG: Der Schlüssel für das Wiederherstellungs-Token (Emergency Recovery Token Key) wird im Falle eines Computerschadens oder einer Beschädigung des Embedded Security-Chips für die Wiederherstellung der verschlüsselten Daten benötigt. Die Daten können ohne diesen Schlüssel nicht wiederhergestellt werden. (Für den Zugriff auf die Daten wird außerdem das Basic-User-Kennwort benötigt.) Bewahren Sie diesen Schlüssel an einem sicheren Ort auf.

7. Klicken Sie auf **Save** (Speichern), um das Verzeichnis und den Standarddateinamen zu übernehmen. Klicken Sie dann auf **Next** (Weiter).
8. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen, bevor die Sicherheitsplattform initialisiert wird.

ACHTUNG: Gegebenenfalls wird eine Meldung mit dem Hinweis angezeigt, dass die Embedded Security-Funktionen nicht initialisiert wurden. Klicken Sie nicht auf die Meldung, da darauf zu einem späteren Zeitpunkt eingegangen und die Meldung nach einigen Sekunden wieder ausgeblendet wird.

9. Wenn das Benutzerkonto jetzt eingerichtet werden soll, vergewissern Sie sich, dass das Kontrollkästchen **Start Embedded Security User Initialization Wizard** (Assistent für die Benutzerinitialisierung von Embedded Security starten) aktiviert ist. Klicken Sie auf **Finish** (Fertig stellen).

Einrichten eines Benutzerkontos

Beim Einrichten eines Benutzerkontos:

- wird ein Basic User-Schlüssel zum Schutz der verschlüsselten Daten erstellt
- wird ein PSD zum Speichern von verschlüsselten Dateien und Ordnern erstellt

ACHTUNG: Bewahren Sie das Basic-User-Kennwort sorgfältig auf. Der Zugriff auf verschlüsselte Daten oder ihre Wiederherstellung ist ohne dieses Kennwort nicht möglich.

So richten Sie ein Basic-User-Konto ein und aktivieren die Benutzersicherheitsfunktionen:

1. Wenn der **Embedded Security User Initialization Wizard** (Assistent für die Benutzerinitialisierung von Embedded Security) nicht geöffnet ist, klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** in der Taskleiste und anschließend mit der linken Maustaste auf **Embedded Security User Initialization** (Benutzerinitialisierung von Embedded Security).

   Der **Embedded Security User Initialization Wizard** (Assistent für die Benutzerinitialisierung von Embedded Security) wird aufgerufen.

2. Klicken Sie auf **Next** (Weiter).
3. Geben Sie ein Kennwort für den Basic-User-Schlüssel ein, und klicken Sie dann auf **Next** (Weiter).

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

4. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.
5. Wählen Sie die gewünschten Sicherheitsfunktionen aus, und klicken Sie auf **Next** (Weiter).
6. Klicken Sie auf **Next** (Weiter), um Hilfedateien zu übergehen.
7. Wenn mehr als ein Verschlüsselungszertifikat vorhanden ist, klicken Sie auf das gewünschte Zertifikat.

   Klicken Sie auf **Next** (Weiter), um das Verschlüsselungszertifikat anzuwenden.

8. Konfigurieren Sie das PSD mit den gewünschten Einstellungen, und klicken Sie auf **Next** (Weiter).
9. Konfigurieren Sie das PSD erneut mit den gewünschten Einstellungen, und klicken Sie auf **Next** (Weiter).

Die Mindestgröße für das PSD sind 50 MB, die maximale Größe beträgt 2.000 MB.

10. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.

Je nach Größe des PSD-Laufwerks kann es einige Minuten dauern, bis der Computer die Bestätigung verarbeitet hat.

11. Klicken Sie auf **Finish** (Fertig stellen).
12. Klicken Sie auf **Yes** (Ja), um den Computer neu zu starten.

Häufig durchgeführte Aufgaben

In diesem Abschnitt werden grundlegende Aufgaben erläutert, die von Benutzern und Besitzern am häufigsten durchgeführt werden.

Benutzeraufgaben

Zu den grundlegenden Benutzeraufgaben gehört das Einrichten des PSD-Laufwerks, das Verschlüsseln von Dateien und Ordnern sowie das Senden und Empfangen von E-Mail mit Verschlüsselung und/oder digitalen Signaturen.

Verwenden des PSD-Laufwerks

Um das PSD nutzen zu können, müssen Sie Ihr PSD-Kennwort eingeben. Daraufhin wird das PSD angezeigt, und die Dateien werden entschlüsselt. Das PSD kann wie jedes andere Laufwerk verwendet werden.

Melden Sie sich ordnungsgemäß ab, wenn Sie die Arbeit mit dem PSD beendet haben. Das PSD wird dann automatisch ausgeblendet.

Verschlüsseln von Dateien und Ordnern

Beachten Sie beim Arbeiten mit EFS unter Windows 2000 und Windows XP Professional Folgendes:

- Nur Dateien und Ordner auf NTFS-Partitionen können verschlüsselt werden. (Dateien und Ordner auf FAT-Partitionen können nicht verschlüsselt werden.)
- Systemdateien und komprimierte Dateien können nicht verschlüsselt werden, und umgekehrt können verschlüsselte Dateien nicht komprimiert werden.
- Temporäre Ordner sollten verschlüsselt werden, da temporäre Dateien von potenziellem Interesse für Unbefugte sind.
- Bei der ersten Verschlüsselung einer Datei oder eines Ordners wird automatisch eine Wiederherstellungsrichtlinie erstellt. Dadurch wird sichergestellt, dass Benutzer, die ihre Zertifikate und privaten Schlüssel verlieren, einen Wiederherstellungs-Agent verwenden können, um ihre Daten zu entschlüsseln.

So verschlüsseln Sie Dateien und Ordner:

1. Wählen Sie die Datei oder den Ordner aus, den Sie verschlüsseln möchten.
2. Klicken Sie mit der rechten Maustaste oder dem Touchpad.
3. Klicken Sie auf **Verschlüsseln**.
4. Klicken Sie entweder auf **Änderungen nur für diesen Ordner übernehmen** oder auf **Änderungen für diesen Ordner, Unterordner und Dateien übernehmen**.
5. Klicken Sie auf **OK**.

Senden und Empfangen von E-Mail mit Verschlüsselung und/oder digitalen Signaturen

Anleitungen zum digitalen Unterzeichnen und Verschlüsseln von E-Mail finden Sie in der Online-Hilfe zum E-Mail-Client.

Um sichere E-Mail zu nutzen, müssen Sie zuerst den E-Mail-Client für die Verwendung eines digitalen Zertifikats konfigurieren, das mithilfe von Embedded Security erstellt wird. Wenn kein digitales Zertifikat verfügbar ist, müssen Sie sich von einer Zertifizierungsbehörde ein Zertifikat ausstellen lassen. Anleitungen zum Konfigurieren von E-Mail und zum Erwerb eines digitalen Zertifikats finden Sie in der Online-Hilfe zum E-Mail-Client.

Zum Senden einer verschlüsselten E-Mail-Nachricht benötigen Sie eine Kopie des öffentlichen Schlüssels oder Verschlüsselungszertifikats des Empfängers. (Das Zertifikat enthält eine Kopie des öffentlichen Schlüssels des Empfängers.)

Microsoft Outlook verwendet den öffentlichen Schlüssel des Empfängers, um Ihre E-Mail zu verschlüsseln. Daher werden Sie nicht aufgefordert, Ihren privaten Schlüssel einzufügen. Sie benötigen Ihren privaten Schlüssel jedoch, um eine verschlüsselte E-Mail zu lesen. Denn zur Entschlüsselung wird der private Schlüssel benötigt, der dem öffentlichen Schlüssel entspricht, mit dem die E-Mail verschlüsselt wurde.

Administratoraufgaben

Der Administrator kann eine Reihe von Aufgaben ausführen, von denen einige nachstehend beschrieben werden. Weitere Informationen finden Sie in der Hilfe zu HP ProtectTools Embedded Security.

Migration von Schlüsseln mit dem Assistenten für Sicherheitsmigration

Die Migration ist eine fortgeschrittene Administratoraufgabe, die die Verwaltung, Wiederherstellung und Übertragung von Schlüsseln und Zertifikaten umfasst.

Der erste Schritt bei der Migration ist die Autorisierung, Einrichtung und Verwaltung des Migrationsprozesses. Sofort nach der Autorisierung kann der Benutzer Schlüssel und Zertifikate vom Quellcomputer zum Zielcomputer exportieren bzw. importieren.

Ausführliche Informationen zur Migration finden Sie in der Hilfe zu HP ProtectTools Embedded Security.

Wiederherstellen von Daten

Wenn der Embedded Security-Chip beschädigt oder zurückgesetzt wurde:

- Mithilfe des Wiederherstellungs-Assistenten können Daten aus dem PSD wiederhergestellt werden.
- Das PSD unterstützt außerdem die Wiederherstellung durch den Einsatz eines Wiederherstellungs-Agent, dessen Funktionsweise in hohem Maße dem EFS entspricht.

  Um festzustellen, ob sich ein registrierter Wiederherstellungs-Agent auf dem Computer befindet, klicken Sie auf **Start > Alle Programme > Administrator Tools > Local Security Policy (Lokale Sicherheitsrichtlinie) > Public Key Policies (Richtlinien für öffentliche Schlüssel) > Encrypted Data Recovery Agents (Wiederherstellungs-Agenten für verschlüsselte Daten)**.

Weitere Informationen finden Sie in der Online-Hilfe zum Betriebssystem.

Windows XP Professional erstellt nicht automatisch einen registrierten Wiederherstellungs-Agent. Folgen Sie den Anleitungen des Betriebssystems, um den registrierten Wiederherstellungs-Agent einzurichten.

Zum Wiederherstellen von Daten benötigt der registrierte Wiederherstellungs-Agent das digitale Zertifikat und die Schlüssel. Es empfiehlt sich, das für die Wiederherstellung benötigte Zertifikat und den privaten Schlüssel auf einen Datenträger zu exportieren, diesen an einem sicheren Ort aufzubewahren und den privaten Schlüssel aus dem Computer zu löschen. Die einzige Person, die Daten wiederherstellen kann, ist der Benutzer, der über den physischen Zugang zu dem privaten Schlüssel für die Datenwiederherstellung verfügt.

Wiederherstellen der Standardvoreinstellungen des Embedded Security-Chips über Computer Setup

ACHTUNG: Bei der Durchführung dieser Aufgabe wird der Besitz des Embedded Security-Chips wieder freigegeben. Dies bedeutet, dass dann jede beliebige Person den Embedded Security-Chip initialisieren kann.

Bei der Wiederherstellung der Standardvoreinstellungen des Embedded Security-Chips können Daten verloren gehen, wenn verschlüsselte Dateien vorhanden sind.

So setzen Sie den Embedded Security-Chip auf die Standardvoreinstellungen zurück:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Microsoft Windows auf **Start > Beenden > Neu starten**.
2. Sobald die Meldung **Press any key to enter TPM Configuration** (Beliebige Taste für die TPM-Konfiguration drücken) angezeigt wird, drücken Sie eine Taste.
3. Geben Sie das Supervisor-Kennwort ein, und drücken Sie die **Eingabetaste**.
4. Drücken Sie **C**, um die Daten auf dem TPM-Chip zu löschen.
5. Drücken Sie **Y**, um den Vorgang zu bestätigen.

   Die Daten auf dem Chip sind nun gelöscht.

Empfohlene Vorgehensweisen

HP empfiehlt bei der Verwendung von Embedded Security die Befolgung der nachstehenden Hinweise.

- Ein IT-Sicherheitsadministrator sollte das BIOS-Supervisor-Kennwort in Computer Setup einrichten und den Embedded Security-Chip initialisieren, bevor der Computer Benutzern zugewiesen wird.
- Ein IT-Sicherheitsadministrator sollte beim Einrichten der Embedded Security-Lösung das Wiederherstellungsarchiv erstellen und die Benutzer bitten, ihre Daten regelmäßig zu speichern und Sicherungskopien zu erstellen. Bei einem Systemausfall ist dies die einzige Möglichkeit zur Wiederherstellung von verschlüsselten Daten. Das Wiederherstellungsarchiv und das Wiederherstellungs-Token sollten jeweils separat gespeichert werden.

- Verschlüsseln Sie Ordner und nicht einzelne Dateien, damit die temporären Dateien, die bei der Bearbeitung erstellt werden, ebenfalls verschlüsselt werden.
- Verschlüsseln Sie sensible Daten auf Computern, die zu einer Domäne gehören. Dadurch sind die Daten gegen offline durchgeführte kryptographische Angriffe geschützt.
- Erstellen Sie regelmäßig Sicherungskopien des Servers, auf dem Server-basierte verschlüsselte Daten gespeichert sind. Dadurch wird sichergestellt, dass im Wiederherstellungsfall die Profile, die Schlüssel für die Entschlüsselung enthalten, ebenfalls wiederhergestellt werden können.
- Wenn Sie Dateitypen verschlüsseln, die von System Restore überwacht werden, stellen Sie die Dateien auf einen Datenträger, der nicht von System Restore überwacht wird.
- Das System unterstützt nicht mehrere Verschlüsselungsebenen Zum Beispiel sollte ein Benutzer keine EFS-verschlüsselte Datei im PSD speichern oder versuchen, eine Datei zu verschlüsseln, die sich bereits im PSD befindet.

Häufig gestellte Fragen

Woher weiß ich, ob mein Computer über einen HP ProtectTools Embedded Security-Chip verfügt?

Der Chip ist eine im System installierte Hardware-Komponente. Die Komponente wird im Geräte-Manager aufgelistet.

Wo erhalte ich die HP ProtectTools Embedded Security-Software?

Sie können die Software, die Treiber und die Online-Hilfe von der HP Website unter http://www.hp.com/products/security herunterladen.

Kann die HP ProtectTools Embedded Security-Software deinstalliert werden? Und falls ja, wie?

Ja Die Deinstallation wird mit dem Standardverfahren zum Deinstallieren von Windows Software durchgeführt. Sichern Sie benutzerspezifische, geschützte Daten, bevor Sie mit der Deinstallation beginnen. Sonst gehen diese Daten verloren. Der letzte Schritt bei der Deinstallation besteht darin, den Chip zu deaktivieren.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Microsoft Windows auf **Start > Beenden > Neu starten**.
2. Sobald die Meldung **Press any key to enter TPM Configuration** (Beliebige Taste für die TPM-Konfiguration drücken) angezeigt wird, drücken Sie eine Taste.
3. Geben Sie das Supervisor-Kennwort ein, und drücken Sie die **Eingabetaste**.
4. Drücken Sie **D**, um den TPM-Chip zu deaktivieren.

   Der Chip ist nun deaktiviert.

Fehlerbehebung

Bei mir funktioniert Embedded Security nicht. Was muss ich tun?

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** in der Taskleiste und anschließend mit der linken Maustaste auf **Manage Embedded Security** (Embedded Security verwalten).
2. Klicken Sie auf **Embedded Security > Info > Self Test** (Embedded Security > Info > Selbsttest).

Überprüfen Sie außerdem die Einstellungen unter **Embedded Security State, Chip, Owner** (Embedded Security-Status, Chip, Besitzer) und **User** (Benutzer).

Ich habe mein System nach einem Absturz wiederhergestellt. Was muss ich jetzt tun?

ACHTUNG: In den meisten Fällen führt der Systemadministrator diese Schritte durch. Bei nicht ordnungsgemäßer Durchführung können Daten unwiderruflich verloren gehen.

Zur Wiederherstellung von Daten nach dem Austauschen des ProtectTools-Chips benötigen Sie Folgendes:

- SPEmRecToken.xml – Schlüssel für das Wiederherstellungs-Token (Emergency Recovery Token Key)
- SPEmRecArchive.xml – Ausgeblendeter Ordner, Standardverzeichnis: C:\Documents and Settings\All Users\ Application Data\Infineon\TPM Software\Recovery Archive (C:\Dokumente und Einstellungen\Alle Benutzer\ Anwendungsdaten\ Infineon\TPM-Software\Wiederherstellungsarchiv)
- ProtectTools-Kennwörter
  - Supervisor
  - Besitzerkennwort
  - Kennwort für das Wiederherstellungs-Token (Emergency Recovery Token)
  - Basic-User-Kennwort

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Microsoft Windows auf **Start > Beenden > Neu starten**.
2. Sobald die Meldung **Press any key to enter TPM Configuration** (Beliebige Taste für die TPM-Konfiguration drücken) angezeigt wird, drücken Sie eine Taste.
3. Geben Sie das Supervisor-Kennwort ein, und drücken Sie die **Eingabetaste**.
4. Drücken Sie **C**, um die Daten auf dem TPM-Chip zu löschen.
5. Drücken Sie **Y**, um den Vorgang zu bestätigen.
6. Starten Sie den Computer neu. Klicken Sie unter Microsoft Windows auf **Start > Beenden > Neu starten**.
7. Sobald die Meldung **Press any key to enter TPM Configuration** (Beliebige Taste für die TPM-Konfiguration drücken) angezeigt wird, drücken Sie eine Taste.
8. Geben Sie das Supervisor-Kennwort ein, und drücken Sie die **Eingabetaste**.
9. Drücken Sie **E**, um den TPM-Chip zu aktivieren.

   Der Chip ist nun aktiviert.

10. Klicken Sie nach dem Öffnen von Windows mit der rechten Maustaste auf das Symbol **HP ProtectTools Embedded Security** in der Taskleiste und anschließend mit der linken Maustaste auf **Embedded Security Initialization** (Embedded Security initialisieren).
11. Aktivieren Sie das Kontrollkästchen: **I want to restore the existing Embedded Security** (Bestehende Embedded Security wiederherstellen), und klicken Sie dann auf **Next** (Weiter).
12. Geben Sie das ursprüngliche Besitzerkennwort ein, und bestätigen Sie es. Klicken Sie auf **Next** (Weiter).
13. Klicken Sie auf **Do not create a recovery archive** (Kein Wiederherstellungsarchiv erstellen) und anschließend auf **Next** (Weiter).

ACHTUNG: Wenn ein neues Archiv erstellt wird, gehen alle Daten verloren, da das für die Wiederherstellung erforderliche Archiv überschrieben wird.

14. Klicken Sie auf **Yes** (Ja), um fortzufahren, ohne ein Wiederherstellungsarchiv zu erstellen.
15. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.
16. Klicken Sie auf **Browse** (Durchsuchen), und suchen Sie das Wiederherstellungsarchiv im folgenden Standardverzeichnis: C:\Documents and Settings\ All Users\Application Data\Infineon\ TPM Software\RecoveryArchive\SPEmRecArchive.xml (C:\Dokumente und Einstellungen\ Alle Benutzer\ Anwendungsdaten\ Infineon\TPM-Software\Wiederherstellungsarchiv\ SPEmRecArchive.xml)
17. Klicken Sie auf **Open** (Öffnen) und auf **Next** (Weiter).
18. Klicken Sie auf **Browse** (Durchsuchen), und suchen Sie das Wiederherstellungs-Token, das bei der ersten **Initialisierung von HP ProtectTools Embedded Security** erstellt wurde. Klicken Sie auf das Token und auf **Open** (Öffnen).
19. Geben Sie das Token-Kennwort ein, und klicken Sie auf **Next** (Weiter).
20. Wählen Sie den Computernamen aus, und klicken Sie auf **Next** (Weiter).

21. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.

    Wenn über eine Meldung angezeigt wird, dass die Wiederherstellung fehlgeschlagen ist, gehen Sie zu Schritt 1 zurück. Überprüfen Sie sorgfältig die Kennwörter, den Speicherort und den Namen des Token sowie den Speicherort und den Namen des Archivs.

22. Wenn das Benutzerkonto jetzt eingerichtet werden soll, vergewissern Sie sich, dass das Kontrollkästchen **Start Embedded Security User Initialization Wizard** (Assistent für die Benutzerinitialisierung von Embedded Security starten) aktiviert ist. Klicken Sie auf **Finish** (Fertig stellen).

Mit den Schritten 23 bis 35 werden die Basic-User-Schlüssel wiederhergestellt. Diese Schritte müssen für jeden Benutzer separat durchgeführt werden.

---

23. Wenn der **Embedded Security User initialization Wizard** (Assistent für die Benutzerinitialisierung von Embedded Security) nicht geöffnet ist, klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools Embedded Security** in der Taskleiste und anschließend mit der linken Maustaste auf **Restore Embedded Security Features** (Embedded Security-Funktionen wiederherstellen).

    Der **Embedded Security User Initialization Wizard** (Assistent für die Benutzerinitialisierung von Embedded Security) wird aufgerufen.

24. Klicken Sie auf **Next** (Weiter).

25. Klicken Sie auf **Recover your basic user key** (Eigenen Basic-User-Schlüssel wiederherstellen) und dann auf **Next** (Weiter).

26. Wählen Sie einen Benutzer aus, geben Sie das ursprüngliche Kennwort für den Basic-User-Schlüssel für diesen Benutzer ein, und klicken Sie dann auf **Next** (Weiter).

27. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen und das Standardverzeichnis für die Wiederherstellungsdaten zu übernehmen.

28. Wählen Sie die gewünschten Sicherheitsfunktionen aus, und klicken Sie auf **Next** (Weiter).

29. Klicken Sie auf **Next** (Weiter), um Hilfedateien zu übergehen.

30. Wenn mehr als ein Verschlüsselungszertifikat vorhanden ist, klicken Sie auf das gewünschte Zertifikat.

    Klicken Sie auf **Next** (Weiter), um das Verschlüsselungszertifikat anzuwenden.

31. Klicken Sie auf **I want to change my Personal Secure Drive settings** (PSD-Einstellungen ändern) und dann auf **Next** (Weiter).

32. Bestätigen Sie die Sicherheitsfunktionen, und klicken Sie auf **Next** (Weiter).

33. Bestätigen Sie die Einstellungen, und klicken Sie auf **Next** (Weiter).

34. Geben Sie das PSD-Kennwort ein, und klicken Sie auf **OK**.

35. Klicken Sie auf **Finish** (Fertig stellen) und dann auf **Yes** (Ja), um einen Neustart durchzuführen.

ACHTUNG: Bewahren Sie das Basic-User-Kennwort sorgfältig auf. Der Zugriff auf verschlüsselte Daten oder ihre Wiederherstellung ist ohne dieses Kennwort nicht möglich.

Glossar

Digitale Signatur – Eine Funktion, die verwendet wird, um die Identität des Absenders eines digitalen Dokuments sicherzustellen und zu bestätigen, dass der Inhalt nicht geändert wurde, nachdem der Absender das Dokument unterzeichnet hat.

Digitale Zertifikate – Elektronische Beglaubigungen, die die Identität einer Person oder eines Unternehmens bestätigen, indem sie die Identität des Zertifikatsbesitzers mit zwei elektronischen Schlüsseln verknüpfen, die zum Unterzeichnen digitaler Informationen verwendet werden.

EFS (Encryption File System) – Verschlüsselungsdateisystem. Bei diesem System werden in einem ausgewählten Ordner alle Dateien und Unterordner verschlüsselt.

Entschlüsselung – Jedes in der Kryptographie verwendete Verfahren zum Umwandeln von Chiffretext (verschlüsselte Daten) in Klartext.

Kryptographie – Theorie und Praxis der Verschlüsselung und Entschlüsselung. Das Kodieren von Daten, sodass sie nur von bestimmten Personen dekodiert werden können. Ein System zum Verschlüsseln und Entschlüsseln von Daten wird als Kryptosystem bezeichnet. Dazu gehört in der Regel ein Algorithmus zum Kombinieren der ursprünglichen Daten („Klartext“) mit einem oder mehreren „Schlüsseln“ (Zahlen oder Zeichenfolgen, die nur dem Absender und/oder dem Empfänger bekannt sind). Das Ergebnis wird als „Chiffretext“ bezeichnet.

Kryptographischer Dienstanbieter (CSP) – Ein Anbieter oder eine Bibliothek von kryptographischen Algorithmen, die in einer angemessen definierten Schnittstelle zur Durchführung bestimmter kryptographischer Aufgaben verwendet werden können.

Migration – Eine Aufgabe, die die Verwaltung, Wiederherstellung und Übertragung von Schlüsseln und Zertifikaten umfasst.

PKI-Infrastruktur (Public Key Infrastructure) – Ein Standard zur Definition der Schnittstellen zum Erstellen, Verwenden und Verwalten von Zertifikaten und kryptographischen Schlüsseln.

PSD (Personal Secure Drive) – Persönliches sicheres Laufwerk. Das PSD bietet einen geschützten Speicherbereich für sensible Daten.

TPM-Modul (Trusted Platform Module) – Bietet Datensicherheit auf Hardware-Ebene. Der im System installierte Embedded Security-Chip kann die Systemintegrität überprüfen und Drittbenutzer, die auf die Plattform zugreifen, authentifizieren, und bleibt dabei unter vollständiger Kontrolle seines primären Benutzers.

Verschlüsselung – Algorithmus, Kryptographie. Jedes in der Kryptographie verwendete Verfahren zum Umwandeln von Klartext in Chiffretext, um zu verhindern, dass die Daten von Unbefugten gelesen werden. Es gibt viele Arten der Datenverschlüsselung, und sie bilden die Basis für die Netzwerksicherheit. Gängige Arten sind DES (Data Encryption Standard, Datenverschlüsselungsstandard) und Kryptographie auf der Basis öffentlicher Schlüssel (Public-Key-Kryptographie).

Wiederherstellungsarchiv – Ein geschützter Speicherbereich, der die erneute Verschlüsselung von Basic-User-Schlüsseln von einem Schlüssel des Plattformbesitzers zu einem anderen Schlüssel ermöglicht.

Zertifizierungsbehörde (CA) - Ein Dienst zur Ausstellung der Zertifikate, die für eine auf öffentlichen Schlüsseln basierende PKI-Infrastruktur (Public Key Infrastructure) erforderlich sind.