Installationshandbuch V3.3.0

TPM (Trusted Platform Module)

computers.toshiba-europe.com

TOSHIBA

Leading Innovation

Inhaltsverzeichnis

Copyright

Marken

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

Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken der jeweiligen Eigentümer.

1 Einführung

Ihr Computer ist mit einem integrierten Trusted Platform Module (TPM) ausgestattet. Um das TPM nutzen zu können, müssen Sie es entweder aktivieren oder die Software „Infineon Security Platform Tools“ installieren. In diesem Installationshandbuch wird beschrieben, wie Sie das TPM installieren und konfigurieren. Lesen Sie dieses Handbuch bitte sorgfältig durch, bevor Sie das TPM verwenden.

1.1 Konventionen

In diesem Handbuch werden die folgenden Formate zum Beschreiben, Kennzeichnen und Hervorheben von Begriffen und Bedienverfahren verwendet.

Sicherheitshinweise

Dieses Handbuch enthält Sicherheitshinweise, die befolgt werden müssen, um potenzielle Risiken zu vermeiden, die zu Verletzungen, Sachschäden oder Datenverlust führen können. Die Sicherheitshinweise wurden nach Schweregrad des Risikos unterteilt und entsprechend mit Symbolen gekennzeichnet:

Weist auf eine möglicherweise gefährliche Situation hin, die zu Sachschäden führen kann.

Gibt wichtige Informationen an.

1.2 TPM - Überblick

Die integrierte Sicherheitssteuerung TPM basiert auf den Spezifikationen der Trusted Computing Group. Das TPM ermöglicht den Datenschutz mithilfe von geheimen Verschlüsselungsschlüsseln anstelle von geheimen Verschlüsselungsformeln (Algorithmen). Bei der Verschlüsselung ausschließlich auf Softwarebasis besteht das Risiko, dass der in der Datei gespeicherte oder in den Speicher des PCs gelesene Verschlüsselungsschlüssel abgefangen und entschlüsselt wird. Wird der Verschlüsselungsschlüssel dagegen im TPM gespeichert, werden die Daten besser geschützt.

Da das TPM öffentliche und standardisierte Spezifikationen verwendet, kann durch Nutzung der entsprechenden Sicherheitslösung eine sicherere PC-Umgebung aufgebaut werden.

Ausführliche Informationen zur TCG-Spezifikation finden Sie auf der TCG-Website unter http://www.trustedcomputinggroup.org/

Verschlüsselung, Zertifikate und Kennwörter

- *Das TPM beinhaltet eine Funktion, mit der sich mehrere Verschlüsselungsschlüssel, Zertifikate und Kennwörter erstellen und einrichten lassen. Nachdem Sie diese festgelegt haben, bewahren Sie die Kennwörter an einem sicheren Platz auf und erstellen Sie Sicherungskopien der Dateien mit den Verschlüsselungsschlüsseln. Wenn Sie diese Einstellungen verlieren oder vergessen, können Sie Dateien, die mit diesem TPM verschlüsselt wurden, nicht mehr entschlüsseln; die entsprechenden Daten sind dann nicht mehr aufrufbar.*

TPM

- *Das TPM verfügt über die neuesten Sicherheitsfunktionen, dennoch kann kein vollständiger Daten- und Hardwareschutz garantiert werden. Beachten Sie bitte, dass Toshiba für Fehlfunktionen, Datenverluste oder Schäden, die aus der Verwendung dieser Funktion resultieren, nicht haftbar ist.*

Falls mehrere Benutzer für Microsoft® Windows® registriert wurden und das TPM verwenden möchten, muss sich jeder Benutzer separat bei Windows® anmelden und sich registrieren.

2 Erstes Verwenden des TPM

In diesem Handbuch sind lediglich allgemeine Richtlinien enthalten. Lesen Sie nach der Installation des TPM Professional Package bitte die TPM-Hilfe.

Wenn Sie das TPM zum ersten Mal verwenden, müssen Sie es wie nachstehend beschrieben konfigurieren. (Für die Einstellungen 1 - 3 müssen Sie sich als *Windows*®-Administrator anmelden.)

1. Aktivieren Sie das TPM.
2. Installieren Sie das **Infineon TPM Professional Package**.
3. Registrieren Sie den Eigentümer und die Benutzer im TPM.

2.1 Aktivieren des TPM

Nehmen Sie die folgenden BIOS-Einstellungen vor, um das TPM zu aktivieren:

1. Halten Sie die Taste **Esc** gedrückt und schalten Sie den Computer ein.
2. Es wird eine Meldung angezeigt. Drücken Sie die Taste **F1**.
3. Der BIOS-Setup-Bildschirm wird angezeigt.
4. Drücken Sie die Taste **Page Down** (Bild ab), um den nächsten Bildschirm aufzurufen.
5. Setzen Sie den Eintrag **TPM** unter **SECURITY CONTROLLER** (Sicherheitssteuerung) auf **Enabled** (Aktivieren).

Bei einigen Modellen wird möglicherweise **TPM ausblenden** *als Option auf dem BIOS-Setup-Bildschirm angezeigt. Wenn bei Ihrem System* **TPM ausblenden** angezeigt wird, *sollte die Option auf* **Nein** *eingestellt sein, bevor Sie* **TPM** *auf* **Aktiviert** *einstellen. Andernfalls können Sie* **TPM** *nicht ändern.*

6. Drücken Sie die Taste **End**, speichern Sie die Änderungen an den BIOS-Einstellungen und drücken Sie die Taste **J**.

Die Konsistenz interner Daten im TPM kann nicht garantiert werden, wenn der Computer zu Reparatur- oder Wartungszwecken eingesandt wird. Bevor Sie den Computer zur Reparatur oder Wartung abgeben, sollten Sie deshalb nicht nur von den auf der Festplatte gespeicherten Dateien, sondern auch von den TPM-Daten eine Sicherungskopie erstellen, indem Sie die Backup-Funktion verwenden. (Lesen Sie dazu Kapitel 8 - TPM-Wiederherstellung*.) Die Sicherheitsfunktionen, die das TPM verwenden, arbeiten nicht mehr ordnungsgemäß, wenn die Daten im TPM verloren gehen. (Beispiel: Dateien, die mit dem TPM verschlüsselt wurden, können nicht mehr geöffnet werden.) Wenn Sie keine Sicherungskopien erstellen, könnten Sie Daten verlieren.*

- **TPM** *ist werkseitig bei Lieferung auf* **Deaktiviert** *eingestellt. Unter Umständen ist die* **TPM-***Einstellung auch auf* **Deaktiviert** *eingestellt, nachdem der Computer zur Wartung oder Reparatur eingeschickt wurde. Aktivieren Sie das TPM in diesem Fall, indem Sie es erneut konfigurieren.*
- *Damit außer dem Administrator und den Benutzern dieses Computers keine andere Person die BIOS-Einstellungen ändern kann, wird dringend empfohlen, ein BIOS-Passwort und ein BIOS-Supervisorpasswort einzurichten. Informationen zum Einrichten dieser Passwörter finden Sie im Benutzerhandbuch des Computers.*

2.2 Installieren des Infineon TPM Professional Package

Installieren Sie das **Infineon TPM Professional Package** aus `C:\TOSHIBA\Drivers\TPM Utility`.

Das **Infineon TPM Professional Package** enthält die folgenden Programme und Funktionen:

- Security Platform-Hilfe
- Security Platform Settings Tool (Tool für die Einstellungen)
- Security Platform Initialization Wizard (Initialisierungs-Assistent)
- Security Platform User Initialization Wizard (Assistent für die Benutzerinitialisierung)
- Security Platform Migration Wizard (Migrations-Assistent)
- Security Platform Backup Wizard (Backup-Assistent)
- Security Platform Password Reset Wizard (Assistent zum Zurücksetzen des Kennworts)
- Security Platform PKCS #12 Import Wizard (Assistent für den PKCS #12-Import)
- Security Platform Certificate viewer and Certificate Selection (Zertifikatsanzeige und -auswahl)
- Security Platform Taskbar Notification Icon (Benachrichtigungssymbol für die Taskleiste)
- Security Platform Integration Services (Integrationsdienste)
  - Microsoft® Outlook®-Integration
  - Netscape®-Integration
  - Encrypted File System Integration
  - Personal Secure Drive
  - Policy Administration (Richtlinienverwaltung)
- Security Platform Services
  - TSS (TCG Software Stack) Service Provider
  - TSS Core Service
  - TSS Device Driver Library (Gerätetreiberbibliothek)

2.3 Registrieren von Eigentümern und Benutzern im TPM

1. Klicken Sie im Infobereich der Taskleiste auf das Symbol **Security Platform** und wählen Sie **Security Platform Initialization** (Initialisierung der Security Platform).

2. Das TPM wird gestartet und der erste Bildschirm wird angezeigt. Klicken Sie auf **Weiter**.
3. Wählen Sie im Bildschirm **Initialization** die Option „Initialize a new Security Platform“ (Neue Security Platform initialisieren). Klicken Sie auf **Next** (Weiter).
4. Geben Sie im Bildschirm **Create Security Platform Owner** (Security Platform-Eigentümer erstellen) für die Eigentümerauthentifizierung das Kennwort in die Felder **Password** (Kennwort) und **Confirm Password** (Kennwort bestätigen) ein und klicken Sie auf **Next** (Weiter).
5. Es wird der Bildschirm **Features** (Funktionen) angezeigt. Wählen Sie die einzurichtende Security Platform-Funktion und klicken Sie auf **Next** (Weiter). Nähere Informationen zur den Security Platform-Funktionen finden Sie in der Hilfe.

Es wird dringend empfohlen, **Automatic Backup** *(Automatisches Backup) einzurichten. Wenn Sie diese Funktion nicht aktivieren, können verschlüsselte Benutzerdaten verloren gehen, falls es zu Fehlern kommt.*

6. Geben Sie im Bildschirm **Backup** den Speicherort für das Erstellen und Speichern der Backup-Datei an. Klicken Sie auf **Weiter**.
7. Wählen Sie im Bildschirm **Emergency Recovery** (Wiederherstellung im Notfall) die Option **Create a new Recovery Token** (Neues Wiederherstellungs-Token erstellen) und geben Sie den Speicherort für das Erstellen und Speichern des **Emergency Recovery Token** an.
8. Geben Sie im Bildschirm **Emergency Recovery** für die Authentifizierung des **Wiederherstellungs-Tokens** das Kennwort in die Felder „Password“ (Kennwort) und „Confirm Password“ (Kennwort bestätigen) ein und klicken Sie auf **Next** (Weiter).

Es wird dringend empfohlen, ein Wiederherstellungs-Token für den Notfall zu erstellen, damit die Informationen im TPM und die für das TPM relevanten Benutzerdaten auch im Fall schwerwiegender Probleme mit dem System geschützt sind. Wenn Sie diese Empfehlung nicht befolgen, könnten Daten verloren gehen.

9. Wählen Sie im Bildschirm **Password Reset** (Kennwort zurücksetzen) die Option **Create a new Token** (Neues Token erstellen) und geben Sie den Speicherort für das Erstellen und Speichern des **Password Reset Token** an.

10. Geben Sie im Bildschirm **Password Reset** für die Authentifizierung des Tokens zum Zurücksetzen des Kennworts das Kennwort in die Felder Password (Kennwort) und Confirm Password (Kennwort bestätigen) ein und klicken Sie auf **Next** (Weiter).

*Es wird dringend empfohlen, das Token zum Zurücksetzen des Kennworts (**Password Reset Token**) auf einem Speichermedium zu erstellen und zu speichern, auf das Sie auch bei einem Systemausfall Zugriff haben, zum Beispiel auf einer Diskette. Bewahren Sie diese Diskette dann an einem sicheren Ort auf, sodass Sie im Notfall darauf zugreifen können.*

- Wenn Sie mehrere Computer mit einem TPM verwenden, unterscheiden sich die Token der einzelnen Computer und sollten separat aufbewahrt werden.
- Das Wiederherstellungs-Token für den registrierten TPM-Eigentümer* kann nicht neu erstellt werden. Deshalb sollten Sie mehrere Kopien des Tokens erstellen und sicher aufbewahren, wie oben empfohlen.

  * Derselbe TPM-Eigentümername kann erstellt werden, indem das TPM im BIOS-Menü initialisiert und ein neuer Eigentümer registriert wird; der Eigentümer ist in diesem Fall jedoch nicht identisch mit dem zuvor registrierten Eigentümer. Zuvor verschlüsselte Dateien können nicht entschlüsselt werden.
- Wenn das Token von unbefugten Dritten zusammen mit dem Kennwort kopiert oder gestohlen wird, könnten diese auf die verschlüsselten Daten zugreifen. Deshalb müssen die Token und Kennwörter unbedingt sicher aufbewahrt werden.

  Lesen Sie dazu Kapitel 8 - *TPM-Wiederherstellung*.

11. Der Bildschirm **Summary** mit einer Zusammenfassung wird angezeigt. Überprüfen Sie die Angaben und klicken Sie auf **Next** (Weiter).
12. Es kann einige Minuten dauern, bis die Meldung **Wizard completed successfully** (Assistent erfolgreich abgeschlossen) angezeigt wird. Aktivieren Sie dann das Kontrollkästchen **Start Security Platform User Initialization Wizard** (Assistent für die Security Platform-Benutzerinitialisierung starten) und klicken Sie auf **Finish** (Fertig stellen).
13. Klicken Sie im Bildschirm **User Initialization Wizard** (Assistent für die Benutzerinitialisierung) auf **Next** (Weiter).
14. Geben Sie im Bildschirm **Basic User Password** (Basis-Benutzerschlüsselkennwort) für die Benutzerauthentifizierung das Kennwort in die Felder **Password** (Kennwort) und **Confirm Password** (Kennwort bestätigen) ein und klicken Sie auf **Next** (Weiter).

15. Vergewissern Sie sich, dass im Bildschirm **Basic User Password Reset** (Standardbenutzerkennwort zurücksetzen) die Option **Enable the resetting of my Basic User Password in case of an emergency** (Zurücksetzen meines Standardbenutzerkennworts im Notfall aktivieren) aktiviert ist. Geben Sie den Speicherort zum Erstellen und Speichern der persönlichen Geheimdatei (**Personal Secret**) an.

Bewahren Sie diese Datei an einem sicheren Ort auf. Im Notfall ist sie erforderlich, um das Standardbenutzerkennwort zurückzusetzen.

16. Es wird der Bildschirm **Password and Authentication** (Kennwort und Authentifizierung) angezeigt. Bestätigen Sie den angezeigten Inhalt und klicken Sie auf **Next** (Weiter).

Es kann einige Minuten dauern, bis der Bildschirm „Security Platform Features“ (Funktionen) angezeigt wird.

17. Vergewissern Sie sich, dass im Bildschirm **Security Platform Features** (Security Platform-Funktionen) die gewünschten Funktionen ausgewählt wurden und klicken Sie auf **Next** (Weiter).

- *Wenn Sie* **Secure E-mail** *(Sichere E-Mail) verwenden möchten, müssen Sie die Konfiguration in der* **Mail-Software** *einrichten. Nähere Informationen zur sicheren E-Mail finden Sie in Kapitel 4,* Sichere E-Mail*.*
- *Die Funktion* **File and Folder encryption** *(EFS) ist unter Windows Vista® Home nicht verfügbar.*
- *Die Festplatte muss im NTFS-Format formatiert sein, damit die Funktion* **File and Folder encryption (EFS)** *verwendet werden kann.*

Die in diesem Abschnitt vorgenommenen Einstellungen lassen sich auch nach der Konfiguration noch ändern.

18. Wenn Sie im Bildschirm **Security Platform Features** (Security Platform-Funktionen) die Funktion **Secure E-mail** (Sichere E-Mail) ausgewählt haben, wird der folgende Bildschirm angezeigt. Klicken Sie auf **Weiter**.

Wenn Sie in diesem Bildschirm auf eine der Schaltflächen **Outlook®**, **Windows Mail/Outlook Express** *oder* **Netscape®** *klicken, wird die Hilfe für die sicheren Einstellungen für die jeweilige Mail-Software angezeigt. (Die Hilfe können Sie auch aufrufen, wenn der Assistent beendet wurde.)*

19. Die Meldung **Encryption Certificate** (Verschlüsselungszertifikat) wird im Bildschirm „Security Platform Features“ angezeigt. Wählen Sie das auszugebende Zertifikat und klicken Sie auf **Next** (Weiter). Klicken Sie auf **Create** (Erstellen), um das Zertifikat zu erstellen und auszuwählen.

Die Standardeinstellung für **Maximum Basic User Password age** *(Max. Verwendungsdauer des Basis-Benutzerkennworts) lautet* **[Disabled]** *(Deaktiviert). Sie können die maximale Verwendungsdauer des Basis-Benutzerkennworts über den Eintrag* **User** *(Benutzer) unter* **Security Policy** *(Sicherheitsrichtlinien) ändern.*

20. Wenn Sie im Bildschirm **Security Platform Features** (Security Platform-Funktionen) die Funktion **Personal Secure Drive (PSD)** (Eigenes sicheres Laufwerk) ausgewählt haben, wird der folgende Bildschirm angezeigt. Wählen Sie in diesem Bildschirm das Laufwerk, das Sie als PSD verwenden möchten, geben Sie die Bezeichnung dieses Laufwerks ein und klicken Sie auf **Next** (Weiter). Nähere Informationen zum Personal Secure Drive (PSD) finden Sie in Kapitel 3, *Personal Secure Drive*.
21. Geben Sie im Bildschirm **Security Platform Features** (Security Platform-Funktionen) die Speichermenge an, die Sie dem PSD zuweisen möchten, wählen Sie das Laufwerk aus und klicken Sie auf **Next** (Weiter).
22. Bestätigen Sie den angezeigten Inhalt und klicken Sie auf **Next** (Weiter).

- *Es wird dringend empfohlen, im Pulldownmenü* **My Personal Secure Drive will be saved on this drive (Mein PSD wird auf diesem Laufwerk gespeichert) ein eingebautes Festplattenlaufwerk (normalerweise Laufwerk C:) anzugeben.**
- *Auf diesem Laufwerk sollte mehr Speicherplatz zur Verfügung stehen als der unter* **My Personal Secure Drive will have [XX] MB of storage space** *(Mein PSD soll über [XX] MB Speicherplatz verfügen) angegebene Speicherplatz.*

23. Nach einiger Zeit wird die Meldung **Wizard completed** (Assistent abgeschlossen) angezeigt. Klicken Sie auf **Finish** (Fertig stellen).

Falls mehrere Benutzer für Windows® registriert wurden und das TPM verwenden möchten, muss sich jeder Benutzer separat bei Windows® anmelden und sich registrieren. Nachdem Sie sich bei Windows® angemeldet haben, um die Benutzerregistrierung vorzunehmen, klicken Sie im Infobereich der Taskleiste auf das Symbol **Security Platform** *und wählen Sie* **Security Platform User initialization** *(Security Platform-Benutzerinitialisierung).*

Wenn Sie Änderungen an der Konfiguration vornehmen möchten, klicken Sie im Infobereich der Taskleiste auf das Symbol **Security Platform Setting Tool** (Tool für die Security Platform-Einstellungen) und ändern Sie die Einstellungen im Konfigurationsbildschirm.

- *Initialization (Initialisierung)*
  - *Wenn Sie Infineon TPM Professional Package verwenden, brauchen Sie TPM nicht unter* **TPM-Verwaltung auf lokalem Computer** *in Windows Vista® zu initialisieren.*
  - *Wenn TPM im Infineon TPM Professional Package initialisiert ist, brauchen Sie TPM nicht unter* **TPM-Verwaltung auf lokalem Computer** *in Windows Vista® zu initialisieren.*
- *Initialisierungsmethode*

Wenn Sie das Professional Package V3.0 verwenden, nachdem TPM mithilfe der Windows Vista®-Funktion **TPM-Einstellung** *initialisiert wurde, wird die normale Plattforminitialisierung wie folgt ausgeführt:*

1. *Nach der Installation von Professional Package V3.0 wird die Meldung* **`Initialized other OS`** *(Initialisiert, anderes Betriebssystem) über dem* **TPM-***Symbol in der Taskleiste angezeigt.*

   ** Dies bedeutet nicht, dass TPM nicht normal funktioniert.*
2. *Wenn Sie in* **Infineon Security Platform Setting Tool** *im Status von Schritt 1 ausführen, wird für* **[Security Platform State:]**, **[Owner:]** *(Security Platform-Status, Eigentümer) auf der Registerkarte* **Info** *als* **`Initialized (Failure Mode 2)`** *(Intialisiert / Ausfallmodus 2) angezeigt.*

   ** Dies ist kein Fehler. Die Initialisierung der Platform wurde jedoch nicht abgeschlossen.*
3. *Wenn Sie den* **Security Platform User Initialization Wizard** *(Assistent für die Security Platform-Benutzerinitialisierung) ausführen, wird ein Initialisierungsbildschirm angezeigt. Obwohl* **Security Platform restoration form a Backup Archive** *(Wiederherstellung aus Backup-Archiv) als Auswahl vorgegeben ist, wählen Sie* **Security Platform Initialization** *(Initialisierung) aus.*
4. *Geben Sie im nächsten Bildschirm von* **Initialize Security Platform** *das Kennwort ein, dass unter* **TPM-Verwaltung auf lokalem Computer** *von Windows Vista® eingerichtet wurde. Zu diesem Zeitpunkt können Sie die TPM-Eigentümerkennwort-Sicherungsdatei, die unter* **TPM-Verwaltung auf lokalem Computer** *gespeichert wurde, nicht verwenden.*
5. *Wenn das Benutzerkennwort im Infineon TPM Professional Package geändert wird, können Sie die TPM-Eigentümerkennwort-Sicherungsdatei, die in der* **TPM-Verwaltung auf lokalem Computer** *von Windows Vista® erstellt wurde, nicht verwenden.*

3 Personal Secure Drive

Das **Personal Secure Drive** erstellt einen Datenspeicher für die Informationen (Dateien). Datendateien können verschlüsselt und auf dem virtuellen Laufwerk gespeichert werden. Die Dateien werden nicht einfach nur verschlüsselt und auf der Festplatte gespeichert. Durch den Schutz mit dem TPM erreichen Sie eine höhere Sicherheit als mit vorhandener softwaregestützter Verschlüsselung. Die Mindestgröße des PSD kann auf 10 MB festgelegt werden. Die Höchstgröße des PSD ist vom Dateisystem, mit dem das PSD erstellt wird, abhängig. Weitere Informationen hierzu finden Sie in der Hilfe.

3.1 Vorteile des Personal Secure Drive

- Verschlüsselung des virtuellen Laufwerks mit dem sicheren AES-Schlüssel (AES = Advanced Encryption Standard).
- RSA-Algorithmus zum Erstellen verschlüsselter Schlüssel.
- Automatische Verschlüsselung und Entschlüsselung transparenter Sicherheitsdaten.
- Dateien lassen sich unkompliziert schützen.
- Einfache Verwendung: das PSD wird auf die gleiche Weise verwendet wie ein herkömmliches *Windows*®-Laufwerk.
- Unkomplizierte Verwaltung und Einrichtung mit Assistenten.

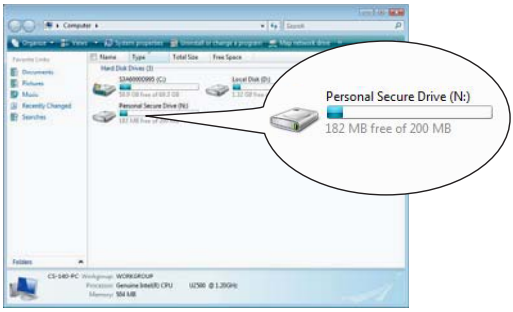
3.2 Personal Secure Drive (PSD) - Grundlagen der Verwendung

1. Wenn im Bildschirm **Security Platform Features** das PSD ausgewählt ist, klicken Sie auf das Symbol **Security Platform** in der Taskleiste, nachdem Sie sich bei Windows angemeldet haben, und wählen Sie [**Personal Secure Drive**] - [**Load**].

*Wenn Sie in der Taskleiste auf das Symbol Security Platform klicken, können Sie zwischen [**Personal Secure Drive**] - [**Load**] (Laden), [**Unload**] (Aus dem Speicher entfernen) oder [**Load at Logon**] (Beim Anmelden laden) wählen.*

2. „Infineon Security Platform User Authentication“ (Benutzerauthentifizierung) wird angezeigt. Geben Sie das TPM-Kennwort ein. Das virtuelle PSD-Laufwerk wird erkannt, nachdem Sie das korrekte Kennwort eingegeben haben.

3. Unten sehen Sie einen Beispielbildschirm von *Windows*® Explorer mit dem erkannten PSD.



Auch wenn das PSD als Laufwerk **[N:]** mit der Bezeichnung **Personal Secure Drive** erkannt wurde, können Sie diese Angaben in den Benutzereinstellungen (**User Settings**) im **Infineon Security Platform Settings Tool** ändern.

- *Da die Dateien auf dem PSD nicht mit der* **Backup**-Funktion des **Infineon Security Platform Settings** *Tools gesichert werden, sollten Sie möglichen Datenverlusten vorbeugen, indem Sie die Dateien vom PSD auf externe, austauschbare Datenträger kopieren.*
- *Die Daten für den Systemwiederherstellungspunkt*, der von der Windows®-Wiederherstellungsfunktion erstellt wird, werden gelöscht, nachdem das TPM-Kennwort beim Windows-Start eingegeben, das PSD bereitgestellt und das virtuelle Laufwerk zugewiesen wurde. Es wird dringend empfohlen, die Daten des Symstemwiederherstellungspunkts mit einer der beiden folgenden Methoden zu speichern.*
  - *Verwenden Sie die PSD-Funktion nicht, verwenden Sie nur die Dateiverschlüsselungsfunktion über EFS.*
  - *Deaktivieren Sie die PSD-Funktion kurzzeitig, bevor Sie Windows-Umgebung ändern.*

  Deaktivieren Sie die PSD-Funktion > Legen Sie den Wiederherstellungspunkt fest -> Modifizieren Sie das System -> Überprüfen Sie, ob Windows korrekt gestartet werden kann -> Aktivieren Sie die PSD-Funktion wieder.

  ** Nähere Informationen zum Wiederherstellungspunkt entnehmen Sie bitte der Windows®-Hilfe.*

- *Das PSD muss für jeden TPM-Benutzer eingerichtet werden. Wenn zum Beispiel die TPM-Benutzer A und B registriert wurden, kann B nicht den PSD-Inhalt von A sehen.*
- *Da einige Bereiche des PSD vom Windows-Dateisystem (NTFS) verwendet werden, ist die tatsächlich verwendbare Kapazität des PSD kleiner als der ursprüngliche Wert bei der Konfiguration. Wenn die Mindestgröße von etwa 10 MB belegt ist und die PSD-Kapazität erhöht wird, nehmen auch die vom NTFS belegten Bereiche mehr Speicher ein.*

  Wenn die Kapazität nicht ausreichend ist, legen Sie bei der PSD-Konfiguration eine höhere Kapazität fest.

  (Beispiel: Wenn Sie ca. 200 MB verwenden möchten, müssen Sie während der PSD-Konfiguration eine Kapazität von 220 MB festlegen.)

4 Sichere E-Mail

Bei dieser Sicherheitsplattform werden die digitalen Kennungen (IDs), die für E-Mail verwendet werden, durch das TPM vor Verlust oder Diebstahl geschützt.

Diese Funktion ist mit der E-Mail-Software Outlook®*, Windows Mail/ Outlook Express* und Netscape®* kompatibel.

* Je nach Softwareversion kann diese Funktion unter Umständen nicht verwendet werden.

4.1 Konfiguration

1. Erwerben Sie eine digitale ID für die Verwendung mit sicherer E-Mail von der kommerziellen Zertifizierungsstelle (Commercial Certificate Authority, CA). Nähere Informationen zur CA finden Sie in der TPM-Hilfe.
2. Installieren Sie die digitale ID gemäß den von der CA spezifizierten Verwendungs- und Installationsmethoden auf dem Computer. Stellen Sie zu diesem Zeitpunkt sichern, dass die digitale ID als ein Cryptographic Service Provider (CSP) mit dem TPM verknüpft ist.
3. Konfigurieren Sie die sichere E-Mail in der Mail-Software. Lesen Sie dazu das Handbuch der jeweiligen Mail-Software und die Hilfe zu Infineon Security Platform.

Aktivieren Sie die Funktion **Secure E-mail** *(Sichere E-Mail) in den Security Platform-Funktionen, wenn Sie die Benutzerregistrierung im TPM ausführen (Schritt 2.3), falls sie nicht zugewiesen wurde (*1, *2).*

*1 Nachschlagen von Informationen zu E-Mail und TPM in der Hilfe

1) Doppelklicken Sie im Infobereich der Taskleiste auf das Symbol **TPM**.
2) Wählen Sie die Registerkarte **Info**.
3) Klicken Sie auf **Help** (Hilfe).
4) Suchen Sie auf der Registerkarte **Search** (Suchen) mithilfe von Stichwörtern nach den gewünschten Themen. (Beispiel: **E-Mail**)

*2 Aktiveren der E-Mail-Funktion in den Benutzereinstellungen

1) Doppelklicken Sie im Infobereich der Taskleiste auf das Symbol **TPM**.
2) Klicken Sie auf die Registerkarte **User Settings** (Benutzereinstellungen).
3) Klicken Sie auf **Configure** (Konfigurieren).
4) Aktivieren Sie die Option **Secure E-mail** (Sichere E-Mail) und klicken Sie auf **Next** (Weiter).

5 EFS (Encrypting File System)-Erweiterung

Wenn Sie in Schritt 2.3 die Option **File and Folder encryption** (Datei- und Ordnerverschlüsselung) aktiviert haben, wird die EFS-Funktion des Betriebssystems erweitert. Das System wird damit sicherer, da der verschlüsselte Schlüssel für die durch EFS verschlüsselte Datei durch das TPM geschützt wird.

Die erforderlichen Schritte zum Verschlüsseln bzw. Entschlüsseln der Dateien sind sehr ähnlich.

Der Unterschied liegt darin, dass beim Zugriff auf ursprünglich mit EFS verschlüsselte Dateien nach dem Anmelden bei *Windows*® das TPM-Kennwort des aktuellen Benutzers eingegeben werden muss.

- *Unter den folgenden Bedingungen wird die TPM-Software nicht normal gestartet und die verschlüsselten Daten können nicht entschlüsselt werden, wenn Dateien unter* **[Basic User Key and Other Folders]** *(Basis-Benutzerschlüssel- und andere Ordner) mit EFS verschlüsselt wurden:*
  - *TPM ist installiert*
  - *Platform hat die Initialisierung abgeschlossen*
  - *bei der Benutzerinitialisierung wurde die EFS-Funktion ausgewählt*

  Während der Initialisierung verhindern Systemattribute dieser Dateien die Verschlüsselung. Ändern Sie die Dateiattribute in den folgenden Ordnern nicht.

  ** In der ursprünglichen Windows-Konfiguration sind die folgenden Ordner versteckt.*

  Basis-Benutzerschlüssel- und andere Ordner

  `C:\ProgramData\Infineon\TPM Software`

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

  `C:\Users\All Users\Infineon`

- *Wenn Archive, Backups und Token-Dateien verschlüsselt werden, können sie im Notfall nicht entschlüsselt werden.*

  Wenn das Token zum Zurücksetzen des Kennworts und Geheimdateien verschlüsselt werden, kann das Kennwort nicht zurückgesetzt werden.

  Verschlüsseln Sie die folgenden Dateien und Ordner nicht.

  [Automatische Backup-Datei]

  Standarddateiname: SPSystemBackup.xml

  Standardkennwort: Nicht festgelegt (*)

  [Ordner für automatisch erstellte Backup-Daten]

  Ordnername (festgelegt): SPSystemBackup (die Datei SPSystemBackup.xml wird in diesem Ordner erstellt)

  [Token für die Wiederherstellung im Notfall]

  Standarddateiname: SPEmRecToken.xml

  Standardkennwort: Austauschbares Medium (Diskette, USB-Speicher usw.)

  [Token zum Zurücksetzen des Kennworts]

  Standarddateiname: SPPwdResetToken.xml

  Standardkennwort: Austauschbares Medium (Diskette, USB-Speicher usw.)

  [Basis-Benutzerkennwort zurücksetzen]

  Standarddateiname: SPPwdResetSecret.xml

  Standardkennwort: Austauschbares Medium (Diskette, USB-Speicher usw.)

  [Backup-Archiv]

  Standarddateiname: SpBackupArchive.xml

  Standardkennwort: Nicht festgelegt (*)

  [PSD-Backup-Archiv]

  Standarddateiname: SpPSDBackup.fsb

  Standardkennwort: Nicht festgelegt (*)

  (*) Wenn Sie auf **Reference** *(Verweis) klicken, wird "User folder\Documents\Security Platform" geöffnet.*

- *Wenn die Dateiverschlüsselung mittels EFS verwendet wird, sollten sich alle Benutzer mit den Informationen über EFS in der Windows®-Hilfe vertraut machen. So kann leichter verhindert werden, dass Dateien nicht mehr entschlüsselt werden können, weil der in EFS verwendete Verschlüsselungsschlüssel unabsichtlich geändert wurde oder verloren ging.*

6 TOSHIBA Passwort-Dienstprogramm

Wenn Sie die TOSHIBA Passwort-Utility verwenden, kann die Konfiguration so eingerichtet werden, dass Benutzer ohne Supervisorberechtigung die TPM-bezogenen Einstellungen im BIOS-Setup nicht ändern können.

Nachdem Sie diese Konfiguration vorgenommen haben, können Benutzer ohne Supervisorberechtigung die TPM-bezogenen Einstellungen im BIOS-Setup (die Einträge im Feld **Security Controller** (Sicherheitssteuerung)) nicht ändern.

1. Führen Sie die folgenden Datei aus, um das TOSHIBA Passwort-Dienstprogramm aufzurufen.

   C:\Programme\TOSHIBA\PasswordUtility\TOSPU.exe

2. Richten Sie das Supervisorpasswort auf der Registerkarte **Supervisorpasswort** ein.
3. Öffnen Sie von der Registerkarte **Supervisorpasswort** aus den Bildschirm Benutzerrichtlinie.
4. Entfernen Sie im Feld **TPM** die Markierung von den Funktionen/Einrichtungen, die Benutzer ohne Supervisorberechtigung nicht aufrufen und ändern sollen.
5. Klicken Sie auf **Festlegen**, führen Sie die Supervisorauthentifizierung aus und speichern Sie die geänderte Benutzerrichtlinie.
6. Beenden Sie das TOSHIBA Passwort-Dienstprogramm.

7 Migration der TPM-Umgebung und Entsorgung

7.1 Migration

Klicken Sie im Infobereich der Taskleiste auf das Symbol **Security Platform** und wählen Sie **Manage Security Platform** (Security Platform verwalten). Klicken Sie im Fenster **Infineon Security Platform Settings Tool** (Tool für die Security Platform-Einstellungen) auf die Registerkarte **Migration**. Klicken Sie auf der Registerkarte **Migration** auf die Schaltfläche **Learn more...** (Weitere Informationen), um Details des Migrationsvorgangs anzuzeigen. (Der Vorgang muss sowohl für die Quellplattform als auch für die Zielplattform ausgeführt werden.) Befolgen Sie bitte die Anweisungen auf dem Bildschirm.

Bei diesem Prozess werden nur die TPM-Daten migriert, deshalb müssen Sie die Migration der Daten auf dem Personal Security Drive und der mit RFS verschlüsselten Dateien auf dem üblichen Wege vornehmen.

- *Vergessen Sie nicht, dass Sie das* **Infineon TPM Professional Package** *auch auf der Zielplattform installieren müssen.*
- *Wenn die Windows®-Firewall aktiviert ist, kann die Migration zwischen PCs über das Netzwerk nicht verwendet werden. Die Einstellungen für die Windows®-Firewall können im* **Sicherheits-Center** *in der* **Systemsteuerung** *geändert werden.*

7.2 PC-Entsorgung

Wenn Sie Ihren PC nicht mehr benötigen und entsorgen möchten, führen Sie bitte die nachstehend beschriebenen Schritte aus, um zu verhindern, dass auf vertrauliche Informationen zugegriffen werden kann. Gehen Sie ebenfalls auf diese Weise vor, wenn Sie den PC an einen anderen Eigentümer weitergeben bzw. verkaufen.

1. Deinstallieren Sie das **Infineon TPM Professional Package** und löschen Sie das Wiederherstellungsarchiv sowie den Token für das Wiederherstellungsarchiv. Außerdem löschen Sie alle Daten auf dem Festplattenlaufwerk.
2. Schritt 1: Zeigen Sie den Bildschirm **BIOS-Setup** an. (Lesen Sie dazu Kapitel 2 - *Erstes Verwenden des TPM*.)

   Schritt 2: Bewegen Sie den Cursor auf die Option **Clear TPM Owner** (TPM-Eigentümer löschen) unter dem Eintrag **SECURITY CONTROLLER** (Sicherheitssteuerung) und drücken Sie auf die Leertaste oder Rücktaste (Backspace). Bei diesem Vorgang werden alle Daten im TPM gelöscht und das TPM wird deaktiviert.

   Schritt 3: Es wird eine Meldung angezeigt. Drücken Sie **Y**, **E**, **S** und dann **Enter**.

Da die internen TPM-Daten gelöscht werden, können die Dateien nicht mehr gelesen werden.

8 TPM-Wiederherstellung

8.1 Wiederherstellung im Notfall - Überblick

Der Vorgang zur Wiederherstellung im Notfall wird verwendet,

- wenn das TPM aufgrund von TPM-Problemen geändert wurde
- wenn die Hauptplatine mit dem TPM beschädigt ist und ausgetauscht wurde
- wenn das TPM versehentlich oder aus anderen Gründen gelöscht wurde

Nähere Informationen finden Sie in der Hilfe unter *Restore Emergency Recovery Data Step by Step*.

- *Es wird empfohlen, vor der Wiederherstellung den Abschnitt „Restore Emergency Recovery Data Step by Step“ auszudrucken.*
- *Mit den beschriebenen Schritten wird der TPM-Inhalt wiederhergestellt, nicht jedoch die TPM-bezogenen Dateien wie zum Beispiel mit EFS verschlüsselte Dateien oder die Dateien auf dem PSD. Von den auf der eingebauten Festplatte gespeicherten Dateien sollten Sie unbedingt separate Sicherungskopien erstellen und an einem sicheren Ort aufbewahren.*

8.2 Benutzerkennwort zurücksetzen

Diese Funktion kann verwendet werden, wenn der Benutzer von Infineon Security Platform das Standardbenutzerkennwort vergisst oder wenn es ein Problem mit dem Authentifizierungsgerät gibt. Falls das Kennwort nicht zurückgesetzt werden kann, hat der Benutzer keinen Zugriff auf die Funktionen von Security Platform. Dies kann zu einem Verlust (vertraulicher) Daten führen.

Nähere Informationen finden Sie in der Hilfe unter *Basic User Password Reset*.

8.3 PSD-Wiederherstellung

Die PSD-Daten können mithilfe der Personal Secure Drive Recovery wiederhergestellt werden, wenn das PSD-Zertifikat nicht mehr verfügbar ist.

Nähere Informationen finden Sie in der Hilfe unter *Personal Secure Drive Recovery*.

Stichwortverzeichnis

Memo

Bewahren Sie Passwörter und Schlüsselwörter, die Sie verwenden, unbedingt an einem sicheren Ort auf, wo sie vor unbefugtem Zugriff geschützt sind (damit vertrauliche Informationen nicht an Außenstehende weitergegeben werden können). Legen Sie die Liste der Passwörter nicht an einem frei zugänglichen Ort ab (auf dem Schreibtisch, an der Pinnwand usw.).

Eigentümerkennwort:

Basis-Benutzerkennwort:

Speicherort des Tokens für die Wiederherstellung im Notfall:

Wiederherstellungs-Token-Kennwort:

Speicherort für Backupdateien:

Speicherort des Tokens zum Zurücksetzen des Kennworts:

Kennwort für das Token zum Zurücksetzen des Kennworts:

Speicherort der persönlichen Geheimdatei:

TPM-Benutzerkennwort

Windows®-Benutzername:

TPM-Benutzerkennwort:

Windows® -Benutzername:

TPM-Benutzerkennwort:

Windows®-Benutzername:

TPM-Benutzerkennwort: