Installatiehandleiding

versie 3.3.0

TPM (Trusted Platform Module)

computers.toshiba-europe.com

TOSHIBA

Leading Innovation

Inhoudsopgave

Copyright

Handelsmerken

Microsoft, Windows en Windows Vista zijn gedeponeerde handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen.

Alle andere merk- en productnamen zijn handelsmerken of gedeponeerde handelsmerken van hun respectievelijke bedrijven.

1 Inleiding

Uw computer bevat een ingebouwde Trusted Platform Module (TPM). U activeert TPM door deze in te schakelen of door de software Infineon Security Platform Tools te installeren. In deze installatiehandleiding wordt beschreven hoe u TPM installeert en configureert. Lees deze installatiehandleiding voordat u TPM gaat gebruiken.

1.1 Conventies

In deze handleiding worden de volgende notatieconventies gebruikt voor het beschrijven, identificeren en markeren van termen en bedieningsprocedures.

Veiligheidspictogrammen

Deze handleiding bevat veiligheidsinstructies die moeten worden opgevolgd ter voorkoming van mogelijke risico's die kunnen leiden tot lichamelijk letsel, beschadiging van de apparatuur of gegevensverlies. Deze veiligheidsinstructies zijn geclassificeerd overeenkomstig de ernst van het risico en worden aangeduid door de volgende pictogrammen:

Duidt op een mogelijk gevaarlijke situatie die bij veronachtzaming van de instructies materiële schade kan veroorzaken.

Duidt op belangrijke informatie.

1.2 TPM: een overzicht

De ingebouwde veiligheidscontroller TPM is gebaseerd op de specificaties van de Trusted Computing Group. TPM biedt gegevensbeveiliging door middel van geheime coderingssleutels in plaats van geheime coderingsformules (algoritmen). Bij codering die uitsluitend is gebaseerd op software, bestaat het gevaar dat de coderingssleutel die in het bestand of in het geheugen van de pc is opgeslagen, wordt gelezen en ontcijferd. Als de coderingssleutel daarentegen wordt opgeslagen in TPM, zijn de gegevens beter beveiligd.

Aangezien TPM openbare en gestandaardiseerde specificaties gebruikt, kan een veiliger pc-omgeving worden gebouwd door de bijbehorende beveiligingsoplossing te gebruiken.

Voor meer informatie over de TCG-specificatie gaat u naar de website op http://www.trustedcomputinggroup.org/

Codering, certificaten en wachtwoorden

- *TPM biedt een functie waarmee meerdere coderingssleutels, certificaten en wachtwoorden kunnen worden gemaakt en ingesteld. Nadat u ze hebt ingesteld, dient u wachtwoorden op een veilige plek te bewaren en een backup te maken van bestanden met coderingssleutels. Als u deze instellingen kwijtraakt of vergeet, kunnen bestanden die zijn gecodeerd met TPM, niet worden gedecodeerd en hebt u geen toegang tot de gecodeerde bestanden.*

TPM

- *Hoewel TPM de nieuwste beveiligingsfuncties biedt, kan dit geen volledige gegevens- en hardwarebeveiliging garanderen. Houd er daarom rekening mee dat Toshiba niet aansprakelijk is voor defecten of schade die mogelijk zijn veroorzaakt door het gebruik van deze functie.*

Als meerdere gebruikers zijn geregistreerd in Microsoft® Windows® en deze gebruikers TPM moeten gebruiken, moet elke gebruiker zich bij Windows® aanmelden en zich afzonderlijk registreren.

2 TPM voor het eerst gebruiken

Deze handleiding bevat alleen algemene richtlijnen. Raadpleeg de Help van TPM nadat u TPM Professional Package hebt geïnstalleerd.

Wanneer u TPM voor het eerst gebruikt, moet u dit als volgt configureren. (De instellingen 1 - 3 kunnen worden aangebracht door een gebruiker die is aangemeld als *Windows*®-beheerder.)

1. Schakel TPM in.
2. Installeer **Infineon TPM Professional Package**.
3. Registreer de eigenaar en de gebruikers in TPM.

2.1 TPM inschakelen

Breng de volgende BIOS-instellingen aan om TPM in te schakelen:

1. Houd de **Esc**-toets ingedrukt terwijl u de computer aanzet.
2. Er wordt een bericht weergegeven. Druk op **F1**.
3. Het scherm BIOS Setup verschijnt.
4. Druk op **Page Down** om het volgende scherm weer te geven.
5. Stel **TPM** bij **SECURITY CONTROLLER** in op **Enabled** (Ingeschakeld).

Bij sommige modellen bevat het scherm BIOS Setup de optie **Hide TPM** *(TPM verbergen). Als uw systeem de optie* **Hide TPM** heeft, *moet u dit instellen op* **No** *voordat u* **TPM** *instelt op* **Enabled**. *Doet u dat niet, dan kunt u* **TPM** *niet wijzigen.*

6. Druk op **End**, sla de wijzigingen in de BIOS-instellingen op en druk op **Y**.

De interne gegevensconsistentie in TPM kan niet worden gegarandeerd wanneer u reparatie of onderhoud aan de computer laat uitvoeren. Maak daarom voordat u reparatie of onderhoud aan de computer laat uitvoeren, niet alleen een backup van de bestanden op de vaste schijf, maar ook van de TPM-gegevens. (Zie hoofdstuk 8, TPM herstellen*.) De beveiligingsfuncties die TPM gebruiken, werken mogelijk niet meer correct als de gegevens in TPM verloren zijn gegaan. (Bestanden die zijn gecodeerd met TPM, kunnen bijvoorbeeld niet meer worden geopend.) Als u dit niet doet, kan dit gegevensverlies tot gevolg hebben.*

- **Bij levering is TPM** *standaard ingesteld op* **Disabled** *(Uitgeschakeld). Er kunnen zich ook gevallen voordoen waarin* **TPM** *is ingesteld op* **Disabled** *nadat reparatie of onderhoud aan de computer is uitgevoerd. Schakel TPM in door het opnieuw te configureren.*
- *Als u wilt voorkomen dat anderen dan de beheerder en de gebruikers van de computer de BIOS-instellingen wijzigen, wordt het ten zeerste aanbevolen een BIOS-wachtwoord en een BIOS-supervisorwachtwoord in te stellen. In de handleiding van de computer leest u hoe u deze wachtwoorden instelt.*

2.2 Infineon TPM Professional Package installeren

Installeer **Infineon TPM Professional Package** vanaf `C:\TOSHIBA\Drivers\TPM Utility`.

Infineon TPM Professional Package omvat de volgende software en voorzieningen:

- Security Platform Help
- Security Platform Settings Tool
- Security Platform-initialisatiewizard
- Security Platform-wizard voor gebruikersinitialisatie
- Security Platform-migratiewizard
- Security Platform-backupwizard
- Security Platform-wizard voor wachtwoordherstel
- Security Platform PKCS #12-importwizard
- Security Platform-certificaatviewer en -certificaatselectie
- Security Platform-taakbalkpictogram
- Security Platform-integratieservices
  - Integratie met Microsoft® Outlook®
  - Netscape®-integratie
  - Integratie met Encrypted File System
  - Personal Secure Drive
  - Beleidsbeheer
- Security Platform-services
  - TSS-serviceprovider (TCG Software Stack)
  - TSS Core-service
  - Bibliotheek met TSS-apparaatstuurprogramma's

2.3 Eigenaren en gebruikers registreren in TPM

1. Klik op het pictogram **Security Platform** in het systeemvak en selecteer **Security Platform Initialization**.

2. TPM wordt gestart en het venster ervan verschijnt. Klik op de knop **Volgende**.
3. Selecteer Initialize a new Security Platform (Een nieuw beveiligingsplatform initialiseren) in het venster **Initialization**. Klik op de knop **Volgende**.

4. Typ in het venster **Create Security Platform Owner** (Eigenaar van beveiligd platform maken) het wachtwoord voor verificatie van de eigenaar in de tekstvakken **Password** (Wachtwoord) en **Confirm Password** (Wachtwoord bevestigen) en klik op **Volgende**.
5. Het venster **Features** (Functies) wordt weergegeven. Selecteer de Security Platform-functie die u wilt instellen en klik op **Volgende**. Raadpleeg de Help voor meer informatie over de functies van Security Platform.

Het wordt ten zeerste aanbevolen **Automatic Backup** *in te stellen. Als deze optie niet is ingesteld, kunnen gecodeerde gebruikersgegevens bij problemen verloren gaan.*

6. Geef in het venster **Backup** de locatie op waar u het backupbestand wilt maken en opslaan. Klik op de knop **Volgende**.
7. Selecteer in het venster **Emergency Recovery** (Noodherstel) de optie **Create a new Recovery Token** (Een nieuw hersteltoken maken) en geef de locatie op waar u het **noodhersteltoken** wilt opslaan.
8. In het venster **Emergency Recovery** typt u het wachtwoord voor verificatie van het **noodhersteltoken** in de vakken Password en Confirm Password en klikt u op **Volgende**.

Het wordt ten zeerste aanbevolen een noodhersteltoken te maken, zodat de informatie in TPM en de gebruikersgegevens die betrekking hebben op TPM veilig zijn in het geval van ernstige problemen met het systeem. Als u deze aanbeveling niet opvolgt, kan dit leiden tot gegevensverlies.

9. Selecteer in het venster **Password Reset** (Wachtwoordherstel) de optie **Create a new Token** (Een nieuw token maken) en geef de locatie op waar u het **token voor wachtwoordherstel** wilt opslaan.
10. In het venster **Password Reset** typt u het wachtwoord voor verificatie van het **token voor wachtwoordherstel** in de vakken Password en Confirm Password en klikt u op **Volgende**.

Het wordt ten zeerste aanbevolen het **token voor wachtwoordherstel** *op te slaan op een opslagmedium, zoals een diskette, dat ook toegankelijk is in het geval van computerproblemen. Berg de diskette op een veilige plaats op, zodat u deze in de toekomst zo nodig kunt gebruiken.*

- Als er meerdere computers met TPM zijn, verschilt het token voor elke computer en moet u deze afzonderlijk opslaan.
- Het hersteltoken voor de geregistreerde TPM-eigenaar* kan niet opnieuw worden gemaakt. Om verlies te voorkomen, dient u meerdere kopieën van het token te maken en op te slaan, zoals hierboven wordt aanbevolen.

  *U kunt dezelfde naam voor de TPM-eigenaar maken door TPM te initialiseren via het BIOS-menu en een nieuwe eigenaar te registreren. Aangezien de eigenaar in dit geval in werkelijkheid verschilt van de vorige geregistreerde eigenaar, kunnen bestanden die eerder zijn gecodeerd, echter niet worden gedecodeerd.

- Als het token, samen met het wachtwoord, uitlekt naar of wordt gestolen door derden, hebben deze toegang tot de gecodeerde gegevens. Daarom wordt het ten zeerste aanbevolen tokens en wachtwoorden op te slaan op een veilige plaats.

  Zie hoofdstuk 8, *TPM herstellen*.

11. Er wordt een overzicht (**Summary**) weergegeven. Controleer het overzicht en klik op **Volgende**.
12. Het kan enkele minuten duren voordat het bericht **Wizard completed successfully** (Wizard voltooid) wordt weergegeven. Klik op het selectievakje **Start Security Platform User Initialization Wizard** en klik op de knop **Voltooien**.
13. Klik in het venster **User Initialization Wizard** op de knop **Volgende**.
14. Typ in het venster **Basic User Password** (Basisgebruikerswachtwoord) het wachtwoord voor gebruikersverificatie in de tekstvakken **Password** (Wachtwoord) en **Confirm Password** (Wachtwoord bevestigen) en klik op **Volgende**.
15. Zorg dat in het venster **Basic User Password Reset** (Basisgebruikerswachtwoord herstellen) de optie **Enable the resetting of my Basic User Password in case of an emergency** (Mijn basisgebruikerswachtwoord kan in noodgevallen worden hersteld) is geselecteerd. Geef de locatie op waar u het **Personal Secret File** (persoonlijke geheime bestand) wilt maken en opslaan.

Sla dit bestand op een veilige locatie op. In noodgevallen hebt u dit nodig om het basisgebruikerswachtwoord te herstellen.

16. Het venster **Password and Authentication** (Wachtwoord en verificatie) verschijnt. Controleer de weergegeven informatie en klik op **Volgende**.

Het kan enkele minuten duren voordat het venster Security Platform Features verschijnt.

17. Zorg dat de gewenste functies zijn geselecteed in het venster **Security Platform Features** en klik op **Volgende**.

- *Als u* **Secure E-mail** *(Beveiligde e-mail) wilt gebruiken, moet u de configuratie instellen via* **Mail Software***. Raadpleeg hoofdstuk 4,* Beveiligde e-mail*, voor meer informatie over beveiligde e-mail.*
- *De functie* **File and Folder encryption (EFS)** *(Bestands- en mapcodering (EFS)) is niet beschikbaar in Windows Vista® Home.*
- *De vaste schijf (HDD) moet zijn geformatteerd met NTFS als u de functie* **File and Folder encryption (EFS)** *wilt gebruiken.*

De configuraties die in dit gedeelte worden ingesteld, kunnen achteraf worden gewijzigd.

18. Als **Secure E-mail** is geselecteerd in het venster **Security Platform Features**, verschijnt het volgende venster. Klik op de knop **Volgende**.

Als u in dit venster klikt op een van de knoppen **Outlook®**, **Windows Mail/ Outlook Express** *of* **Netscape®**, *wordt de Help-informatie voor de instellingen voor* **Secure E-mail** *voor de desbetreffende* **mailsoftware** *weergegeven. (U kunt deze Help ook weergeven nadat de wizard is gesloten.)*

19. Een bericht over uitgifte van het **Encryption Certificate** (Coderingscertificaat) wordt weergegeven in het venster Security Platform Features. Selecteer het certificaat dat u wilt uitgeven en klik op **Volgende**. Gewoonlijk klikt u op de knop **Create** (Maken) om het certificaat te maken en te selecteren.

De standaardwaarde voor **Maximum Basic User Password age** *(Maximale gebruiksduur voor basisgebruikerswachtwoord) is ingesteld op* **[Disabled]** *(Uitgeschakeld). Als u de waarde voor Maximum Basic User Password age wilt wijzigen, kunt u dit opgeven via* **User** *in* **Security Policy**.

20. Als **Personal Secure Drive (PSD)** is geselecteerd in het venster **Security Platform Features**, verschijnt het volgende venster. In dit venster selecteert u het station dat u wilt toewijzen aan de PSD, waarna u de naam van het station invoert en op **Volgende** klikt. Raadpleeg hoofdstuk 3, *Personal Secure Drive*, voor meer informatie over de Personal Secure Drive (PSD).
21. Geef in het venster **Security Platform Features** op hoeveel opslagruimte u wilt toewijzen aan de PSD, selecteer het station en klik op **Volgende**.
22. De instelling Confirm wordt weergegeven. Klik **Volgende**.

- *Het wordt ten zeerste aanbevolen een ingebouwde vaste schijf (gewoonlijk station C) op te geven in de vervolgkeuzelijst* **My Personal Secure Drive will be saved on this drive** *(Mijn PSD wordt opgeslagen op dit station).*
- *De beschikbare ruimte op het hierboven opgegeven station moet meer zijn dan de ruimte die is opgegeven bij* **My Personal Secure Drive will have [XX] MB of storage space** *(Mijn PSD gebruikt [XX] MB opslagruimte).*

23. Na enige tijd verschijnt het bericht **Wizard completed** (Wizard voltooid). Klik op de knop **Voltooien**.

Als meerdere gebruikers zijn geregistreerd in Windows® en deze gebruikers TPM moeten gebruiken, moet elke gebruiker zich bij Windows® aanmelden en zich afzonderlijk registreren. Nadat u zich bij Windows® hebt aangemeld om de gebruikersregistratie uit te voeren, klikt u op het pictogram **Security Platform** *in het systeemvak en selecteert u* **Security Platform User initialization***.*

Als u de configuratie wilt wijzigen, klikt u op het pictogram **Security Platform Setting Tool** in het systeemvak en brengt u de wijzigingen aan in het configuratievenster.

- *Initialisatie*
  - *Als u Infineon TPM Professional Package gebruikt, hoeft u TPM niet vooraf te initialiseren in Windows Vista® via* **TPM-beheer op lokale computer***.*
  - *Als TPM is geïnitialiseerd in Infineon TPM Professional Package, hoeft u TPM niet te initialiseren in Windows Vista® via* **TPM-beheer op lokale computer***.*
- *Initialisatiemethode*

Als u Professional Package 3.0 gebruikt nadat TPM is geïnitialiseerd via de functie voor **TPM-instelling** *van Windows Vista®, wordt de normale platforminitialisatie als volgt uitgevoerd:*

1. *Nadat u Professional Package 3.0 hebt geïnitialiseerd, wordt het bericht* `Initialized other OS` *(Ander besturingssysteem geïnitialiseerd) weergegeven via het pictogram* **TPM** *op de taakbalk.*

   ** Dit betekent niet dat TPM niet correct werkt.*
2. *Als u* **Infineon Security Platform Setting Tool** *uitvoert in stap 1, wordt bij* **[Security Platform State:]**, **[Owner:]** *op het tabblad* **Info** *de staat weergegeven als '*`Initialized (Failure Mode 2)`*'.*

   ** Dit is geen fout. De platforminitialisatie is echter nog niet voltooid.*
3. *Wanneer u de wizard* **Security Platform User Initialization** *uitvoert, verschijnt het venster* **Initialization***. Hoewel* **Security Platform restoration from a Backup Archive** *(Security Platform herstellen vanaf een backuparchief) is geselecteerd, dient u* **Security Platform Initialization** *te selecteren.*
4. *In het volgende venster,* **Initialize Security Platform***, voert u het wachtwoord voor* **TPM-beheer op lokale computer** *in Windows Vista® in. U kunt nu het* **backupbestand met het wachtwoord van de TPM-eigenaar** *dat is opgeslagen via* **TPM-beheer op lokale computer** *niet gebruiken.*
5. *Als het gebruikerswachtwoord wordt gewijzigd door Infineon TPM Professional Package, kunt u het* **backupbestand met het wachtwoord van de TPM-eigenaar** *dat is gemaakt met* **TPM-beheer op lokale computer** *in Windows Vista® niet gebruiken.*

3 Personal Secure Drive

Een **Personal Secure Drive** is een opslagruimte waarin gegevens (bestanden) kunnen worden opgeslagen, waarbij de gegevensbestanden worden gecodeerd en opgeslagen op een virtueel station. De bestanden kunnen niet simpelweg worden gecodeerd en opgeslagen op de vaste schijf. Aangezien ze worden beveiligd door TPM, is de beveiliging veel hoger dan bij bestaande, softwarematige codering. De minimale grootte van de PSD is 10 MB. De maximale grootte van de PSD hangt af van het bestandssysteem waarin de PSD wordt gemaakt. Raadpleeg de Help voor meer informatie.

3.1 Voordelen van een Personal Secure Drive

- Codering van het virtuele station met behulp van de veilige AES-sleutel (Advanced Encryption Standard).
- RSA-algoritme voor het genereren van gecodeerde sleutels.
- Automatische codering en decodering van transparante beveiligingsgegevens.
- Bestanden kunnen gemakkelijk worden beveiligd.
- Eenvoudig in het gebruik: de Personal Secure Drive werkt op dezelfde manier als een standaard *Windows*®-station.
- Eenvoudige beheer- en configuratieprocedure met behulp van wizards.

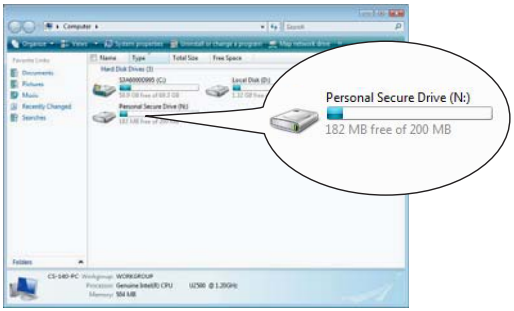
3.2 Personal Secure Drive (PSD): basisstappen

1. Als PSD is geselecteerd in het venster **Security Platform Features**, klikt u op het pictogram **Security Platform** in het systeemvak nadat u zich bij Windows hebt aangemeld en selecteert u [**Personal Secure Drive**] - [**Load**].

*Wanneer u klikt op het pictogram Security Platform in het systeemvak, kunt u kiezen tussen [**Personal Secure Drive**] - [**Load**] (Laden), [**Unload**] (Verwijderen) en [**Load at Logon**] (Laden bij aanmelden).*

2. Infineon Security Platform User Authentication (Gebruikersverificatie) wordt weergegeven. Voer het TPM-wachtwoord in. Het virtuele PSD-station wordt herkend nadat het wachtwoord is ingevoerd.

3. In het volgende voorbeeld is de PSD gedetecteerd in *Windows*® Verkenner.



Hoewel in dit venster de Personal Secure Drive is gedetecteerd als station **[N:]** met de stationsnaam **Personal Secure Drive**, kunt u deze instelling wijzigen via **User Settings** (Gebruikersinstellingen) van **Infineon Security Platform Settings Tool**.

- *Aangezien de functie* **Backup** van **Infineon Security Platform Settings Tool** *geen backup maakt van de bestanden op de PSD, dient u een algemene backupmethode te gebruiken om gegevensverlies te voorkomen. U kunt de bestanden op de PSD bijvoorbeeld via Verkenner kopiëren naar een extern, verwisselbaar medium.*
- *De gegevens voor het herstelpunt* van het systeem dat is gemaakt door de functie Systeemherstel van Windows®, worden verwijderd nadat het TPM-wachtwoord wordt ingevoerd tijdens het opstarten van Windows, de PSD is gekoppeld en het virtuele station is toegewezen. Het wordt ten zeerste aanbevolen om een van de volgende methoden te gebruiken om de gegevens in het herstelpunt van het systeem op te slaan.*
  - *Gebruik de PSD-functie niet, maar gebruik alleen de functie voor bestandscodering via het EFS.*
  - *Schakel de PSD-functie tijdelijk uit voordat u de Windows-omgeving wijzigt.*

  Schakel de PSD-functie uit -> stel het herstelpunt in -> wijzig het systeem -> controleer of Windows correct opstart -> herstel de vorige staat van de PSD-functie.

  ** Raadpleeg de Help van Windows® voor meer informatie over herstelpunten.*

- *De PSD moet worden ingesteld voor elke TPM-gebruiker. Als er bijvoorbeeld twee geregistreerde TPM-gebruikers, A en B zijn, kan B de inhoud van A niet zien.*
- *Aangezien de Personal Secure Drive (PSD) gebieden bevat die worden gebruikt door Windows NTFS (het bestandssysteem), is de werkelijke capaciteit van de PSD die kan worden gebruikt kleiner dan de beginwaarde tijdens de configuratie. Als het minimum van circa 10 MB wordt gebruikt en de PSD-capaciteit wordt verhoogd, neemt ook het gebied toe dat door NTFS wordt gebruikt.*

  Wanneer u de volledige vereiste capaciteit wilt gebruiken, moet u daarom tijdens de PSD-configuratie een hogere capaciteit opgeven. (Bijvoorbeeld: wanneer u circa 200 MB wilt gebruiken, moet u tijdens de configuratie een capaciteit van 220 MB opgeven voor de PSD.)

4 Beveiligde e-mail

Op dit beveiligingsplatform worden de digitale ID's die voor e-mail worden gebruikt, beveiligd door TPM en zo beschermd tegen verlies of diefstal.

Compatibele e-mailsoftware omvat Outlook®*, Windows Mail/Outlook Express* en Netscape®*.

* Houd er rekening mee dat deze functie mogelijk niet kan worden gebruikt, afhankelijk van de versie van de software.

4.1 Configuratie

1. Schaf een digitale ID voor gebruik met beveiligde e-mail aan bij een officiële certificeringsinstantie (CA of Certificate Authority). Raadpleeg de Help van TPM voor meer informatie over de CA.
2. Installeer de digitale ID op de computer volgens de gebruiks- en installatiemethoden van de CA. Zorg dat de digitale ID wordt gekoppeld aan TPM als een cryptografische serviceprovider (CSP).
3. Stel de configuratie voor beveiligde e-mail in de e-mailsoftware in. Raadpleeg de handleiding van de e-mailsoftware en de Help van Infineon Security Platform voor meer informatie.

Wanneer u de gebruikersregistratie bij TPM (stap 2.3) uitvoert, stelt u de optie **Secure E-mail** *in het venster Security Platform Features in alsof deze niet is toegewezen (*1, *2).*

*1 De Help raadplegen voor informatie over e-mail en TPM

1) Dubbelklik op het pictogram **TPM** in het systeemvak.
2) Selecteer de tab **Info**.
3) Klik op de knop **Help**.
4) Zoek met behulp van trefwoorden op het tabblad **Zoeken** naar onderwerpen waarover u meer wilt weten. (Voorbeeld: **E-mail**)

*2 De functie E-mail inschakelen via User Settings

1) Dubbelklik op het pictogram **TPM** in het systeemvak.
2) Klik op de tab **User Settings** (Gebruikersinstellingen).
3) Klik op de knop **Configure(ren)**.
4) Schakel de optie **Secure E-mail** in en klik op **Volgende**.

5 EFS-uitbreiding (Encrypting File System)

Als de optie File and Folder **encryption** (Bestands- en mapcodering) is ingeschakeld in stap 2.3, wordt de functie EFS van het besturingssysteem uitgebreid en wordt het systeem veiliger gemaakt, aangezien de gecodeerde sleutel voor bestanden die worden gecodeerd door EFS, wordt beveiligd door TPM.

De stappen voor het coderen/decoderen van bestanden zijn zeer vergelijkbaar.

Het verschil is dat wanneer u voor eerst toegang hebt tot bestanden die zijn gecodeerd met EFS nadat u zich hebt aangemeld bij *Windows*®, het TPM-wachtwoord van de momenteel aangemelde gebruiker moet worden ingevoerd.

- *In de volgende omstandigheden, indien bestanden die zijn gemaakt in* **[Basic User Key and Other Folders]** *(Basismappen met gebruikerssleutels en andere mappen) met EFS worden gecodeerd, start de TPM-software niet normaal op en kunnen de gecodeerde gegevens niet worden gedecodeerd.*
  - *TPM is geïnstalleerd*
  - *De initialisatie van het platform is voltooid*
  - *De EFS-functie is geselecteerd tijdens de gebruikersinitialisatie*

  Tijdens de initialisatiefase worden voor bestanden in **[Basic User Key and Other Folders]** *systeemkenmerken ingesteld die voorkomen dat ze worden gecodeerd. Wijzig de bestandskenmerken in de desbetreffende mappen niet.*

  ** Bij de oorspronkelijke configuratie van Windows zijn de volgende mappen verborgen.*

  [Basic User Key and Other Folders]

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

- *Wanneer archieven, backups en tokenbestanden zijn gecodeerd, kunnen ze in noodgevallen niet worden gedecodeerd.*

  Wanneer het token voor wachtwoordherstel en geheime bestanden zijn gecodeerd, kan het wachtwoord niet opnieuw worden ingesteld.

  Codeer de volgende bestanden en mappen niet.

  [Automatic Backup File] (Automatisch backupbestand)

  Standaardbestandsnaam: SPSystemBackup.xml

  Standaardwachtwoord: niet opgegeven (*)

  [Automatic Backup Data Storage Folder] (Map voor gegevensopslag voor automatische backup)

  Mapnaam (vast): SPSystemBackup (het bestand SPSystemBackup.xml wordt gemaakt als submap van de map die wordt gemaakt)

  [Emergency Recovery Token] (Noodhersteltoken)

  Standaardbestandsnaam: SPEmRecToken.xml

  Standaardwachtwoord: verwisselbaar medium (diskette, USB-geheugen etc.)

  [Password Reset Token] (Token voor wachtwoordherstel)

  Standaardbestandsnaam: SPPwdResetToken.xml

  Standaardwachtwoord: verwisselbaar medium (diskette, USB-geheugen etc.)

  [Basic User Password Reset] (Basisgebruikerswachtwoord herstellen)

  Standaardbestandsnaam: SPPwdResetSecret.xml

  Standaardwachtwoord: verwisselbaar medium (diskette, USB-geheugen etc.)

  [Backup Archive] (Backuparchief)

  Standaardbestandsnaam: SpBackupArchive.xml

  Standaardwachtwoord: niet opgegeven (*)

  [PSD Backup Archive] (PSD-backuparchief]

  Standaardbestandsnaam: SpPSDBackup.fsb

  Standaardwachtwoord: niet opgegeven (*)

  (*) Als u op **Reference** *kilkt, wordt 'User folder\Documents\Security Platform' geopend.*

- *Als bestandscodering door EFS wordt gebruikt, wordt het ten zeerste aanbevolen dat de gebruiker vertrouwd raakt met de EFS-informatie in Windows® Help. Zo kan worden voorkomen dat bestanden niet kunnen worden gedecodeerd doordat de coderingssleutel in EFS onbewust wordt gewijzigd of doordat de sleutel wordt kwijtgeraakt.*

6 TOSHIBA-wachtwoordhulpprogramma

Met behulp van het TOSHIBA-wachtwoordhulpprogramma kan de configuratie zodanig worden ingesteld dat wordt voorkomen dat gebruikers zonder supervisorrechten TPM-gerelateerde instellingen wijzigen in BIOS Setup.

Nadat deze configuratie is ingesteld, kunnen gebruikers zonder supervisorrechten TPM-gerelateerde instellingen in BIOS Setup (items in het vak **Security Controller**) niet wijzigen.

1. Voer het volgende bestand uit om het TOSHIBA-wachtwoordhulpprogramma te starten.

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

2. Registreer het supervisorwachtwoord op het tabblad **Supervisorwachtwoord**.
3. Open het venster Gebruikersbeleid via het tabblad **Supervisorwachtwoord**.
4. Schakel in het vak **TPM** de items uit waartoe gebruikers zonder supervisorrechten geen toegang hebben en die ze niet mogen wijzigen.
5. Klik op de knop **Instellen** en sla het gewijzigde gebruikersbeleid op nadat u de supervisorverificatie hebt voltooid.
6. Sluit het TOSHIBA-wachtwoordhulpprogramma.

7 Migratie van de TPM-omgeving en de pc wegdoen

7.1 Migratie

Klik op het pictogram **Security Platform** in het systeemvak en selecteer **Manage Security Platform** (Security Platform beheren). Klik in het venster **Infineon Security Platform Settings Tool** op de tab **Migration**. Als u op de tab **Migration** op de knop **Learn more...** (Meer informatie) klikt, wordt meer informatie over de migratiebewerking weergegeven. (Deze bewerking moet worden uitgevoerd op het bronplatform en op het doelplatform.) Voer de bewerking uit volgens de instructies op het scherm.

Tijdens dit proces worden alleen de TPM-gegevens gemigreerd. Voer de migratie van de gegevens binnen de Personal Security Drive en de bestanden die zijn gecodeerd met EFS daarom uit met behulp van de gebruikelijke bestandsbewerkingen.

- *Onthoud dat u* **Infineon TPM Professional Package** *ook moet installeren op het doelplatform.*
- *Als Windows® Firewall is ingeschakeld, is migratie tussen pc's in een netwerk niet mogelijk. De instelling van Windows® Firewall kan worden gewijzigd via het* **Beveiligingscentrum** *in het* **Configuratiescherm**.

7.2 De pc wegdoen

Als u de pc weggooit, volgt u de volgende twee procedures om te voorkomen dat vertrouwelijke gegevens worden onderschept.
Doe hetzelfde wanneer u de pc aan een ander overdoet.

1. Verwijder **Infineon TPM Professional Package** en verwijder het herstelarchief en het **token voor het noodherstelarchief**. Verwijder daarnaast alle gegevens van de vaste schijf.
2. Stap 1: Geef het scherm **BIOS Setup** weer.
   (Zie hoofdstuk 2, *TPM voor het eerst gebruiken*.)

   Stap 2: Verplaats de aanwijzer naar de optie **Clear TPM Owner** (TPM-eigenaar wissen) in het gedeelte **SECURITY CONTROLLER** en druk op de spatiebalk of Backspace. Hiermee worden alle gegevens in TPM vernietigd en wordt daarna TPM uitgeschakeld.

   Stap 3: Er wordt een bericht weergegeven. Druk op de toetsen **Y**, **E**, **S**, gevolgd door de **Enter**-toets.

Aangezien de interne TPM-gegevens worden verwijderd, kunnen de bestanden niet meer worden gelezen.

8 TPM herstellen

8.1 Noodherstelproces: een overzicht

U gebruikt het noodherstelproces:

- als u TPM wijzigt vanwege TPM-problemen
- als het moederbord met de ingebouwde TPM defect is en u het moederbord hetbt vervangen
- als TPM per ongeluk of om een andere reden is gewist

Raadpleeg het gedeelte *Restore Emergency Recovery Data Step by Step* in de Help voor meer informatie.

- *Het wordt aanbevolen vooraf een afdruk te maken van de stappen voor het herstellen van de noodherstelgegevens in de Help.*
- *De hier vermelde toelichtingen zijn bedoeld om de TPM-inhoud te herstellen en niet om TPM-gerelateerde gegevens, zoals met EFS gecodeerde bestanden of bestanden op de PSD, te herstellen. Voor bestanden op de ingebouwde vaste schijf wordt het ten zeerste aanbevolen afzonderlijke backups te maken en deze veilig op te slaan.*

8.2 Het gebruikerswachtwoord opnieuw instellen

Deze functie kan worden gebruikt als de Infineon Security Platform-gebruiker het basisgebruikerswachtwoord vergeet of als er een probleem is met de verificatiemethode van de gebruiker. Als het wachtwoord niet opnieuw kan worden ingesteld, kan de gebruiker de functies van Security Platform niet gebruiken. Hierdoor kunnen gegevens verloren gaan.

Raadpleeg *Basic User Password Reset* in de Help voor meer informatie.

8.3 PSD-herstel

PSD-gegevens kunnen worden hersteld als het PSD-certificaat is kwijtgeraakt, met behulp van Personal Secure Drive-herstel.

Raadpleeg *Personal Secure Drive Recovery* voor informatie.

Index

O

P

S

T

V

W

Memo

Zorg dat de gebruikte wachtwoorden of trefwoorden veilig worden opgeslagen (voor het geval een wachtwoord wordt vergeten) waar derden er geen toegang toe hebben (om te voorkomen dat geheime gegevens uitlekken). Bewaar ze niet op locaties die toegankelijk zijn voor onbevoegden (zoals op het bureaublad).

Eigenaarwachtwoord:

Basisgebruikerswachtwoord:

Opslaglocatie van noodhersteltoken:

Wachtwoord voor noodhersteltoken:

Opslaglocatie van backupbestand:

Opslaglocatie van token voor wachtwoordherstel:

Wachtwoord voor token voor wachtwoordherstel:

Opslaglocatie van het persoonlijke geheime bestand:

TPM-gebruikerswachtwoord

Windows®-gebruikersnaam:

TPM-gebruikerswachtwoord:

Windows®-gebruikersnaam:

TPM-gebruikerswachtwoord:

Windows®-gebruikersnaam:

TPM-gebruikerswachtwoord: