Installationsguide V3.3.0

TPM (Trusted Platform Module)

computers.toshiba-europe.com

TOSHIBA

Leading Innovation

Innehållsförteckning

Copyright

Varumärken

Microsoft, Windows och Windows Vista är registrerade varumärken som tillhör Microsoft Corporation i USA och/eller i andra länder.

Övriga märken och produktnamn är varumärken eller registrerade varumärken för respektive företag.

1 Inledning

Datorn innehåller en TPM-modul (Trusted Platform Module). Du aktiverar TPM-modulen genom att aktivera eller installera programmet Infineon Security Platform Tools (verktyg för Infineon-säkerhetsplattformen). I den här handboken beskrivs hur du installerar och ställer in TPM. Innan du börjar använda TPM ska du läsa igenom vad som står i den här installationshandboken.

1.1 Konventioner

I handboken används följande konventioner för att beskriva, markera och framhäva termer och anvisningar.

Säkerhetssymboler

Den här handboken innehåller säkerhetsanvisningar som du måste följa för att undvika skador på din person, skador på utrustningen eller förlust av data. Säkerhetsvarningarna har klassificerats enligt hur allvarliga de kan vara, och följande symboler används för att göra dig uppmärksam på instruktionerna:

Anger en potentiell fara som, om anvisningarna inte följs, kan resultera i egendomsskador.

Innehåller viktig information.

1.2 TPM – en översikt

Den inbyggda TPM-modulen för säkerhetskontroll baseras på specifikationer från Trusted Computing Group. Med TPM-modulen skyddar du dina data med hemliga krypteringsnycklar i stället för hemliga krypteringsformler (algoritmer). Med en kryptering, som bara baseras på program, finns det en risk att krypteringsnyckeln sparas i en fil eller läses in i datorns minne så att den kan hittas av andra och dechiffreras. Dina data blir mer skyddade när du förvarar krypteringsnyckeln i TPM-modulen.

Eftersom offentliga och standardiserade specifikationer används för TPM, kan du bygga upp en säkrare datormiljö med hjälp av den här säkerhetslösningen.

Mer information om TCG-specifikationerna finns på webbplatsen http://www.trustedcomputinggroup.org/.

Kryptering, certifikat och lösenord

- *I TPM-modulen finns en funktion för att skapa och ställa in flera krypteringsnycklar, certifikat och lösenord. När inställningarna är gjorda ska du förvara lösenorden på ett säkert ställe och säkerhetskopiera filerna med krypteringsnycklar. Om du tappar bort inställningarna eller glömmer bort dem, kan filer som krypterats med den här TPM-modulen inte dekrypteras och krypterade data kan inte öppnas.*

TPM

- *Trots att de senaste säkerhetsfunktionerna finns i TPM-modulen, går det inte att garantera fullständigt skydd av data och maskinvara. Observera att Toshiba inte är ansvarig för fel eller skador som kan orsakas av att du använder den här funktionen.*

Om flera användare har registrerats i Microsoft® Windows®, och om dessa användare ska använda TPM, måste varje användare logga in i Windows® och registrera sig.

2 Använda TPM-modulen första gången

I den här handboken finns bara anvisningar av generell natur. Mer information finns i TPM HELP, som du får tillgång till när du har installerat TPM Professional Package.

Du måste göra följande inställningar innan du använder TPM-modulen första gången: (Inställningarna i punkt 1 - 3 gör du sedan du loggat in som *Windows*®-administratör.)

1. Aktivera TPM.
2. **Installera Infineon TPM Professional Package**.
3. Registrera ägaren och användarna i TPM.

2.1 Aktivera TPM-modulen

Gör följande BIOS-inställningar när du vill aktivera TPM-modulen.

1. **Starta datorn och håll ned Esc-tangenten.**
2. Ett meddelande visas. Tryck på **F1.**
3. I fönstret visas nu BIOS-inställningarna.
4. Tryck på tangenten **Page Down** för att öppna nästa fönster.
5. Välj **Enabled** (Aktivera) för TPM i **SECURITY CONTROLLER** (Säkerhetskontroller).

I vissa modeller kan **Hide TPM** *(Dölj TPM) var ett BIOS-alternativ. Om du ser* **Hide TPM**, *ska du välja alternativet* **No** *(Nej) innan du väljer* **Enabled** *(Aktiverad) för* **TPM**. *I annat fall kan du inte ändra* **TPM**.

6. Tryck på **End**-tangenten, spara BIOS-inställningarna och tryck sedan på **Y**-tangenten.

Intern datakonsistens i TPM går inte att garantera när datorn repareras eller underhålls. Innan du skickar iväg datorn ska du göra en säkerhetskopia, inte bara av filerna på hårddisken utan också av de data som finns i TPM-modulen. Du använder då säkerhetskopieringsfunktionen. (Mer information finns i kapitel 8 - TPM-återställning*.) De säkerhetsfunktioner som använder TPM fungerar inte längre tillfredsställande om de data som finns i TPM-modulen försvinner. (Exempel: De filer som krypterades med TPM går inte längre att öppna.) Om du inte utför säkerhetskopieringen riskerar du att data kan försvinna.*

- **Vid leveransen är** *TPM-modulen som standard* **inaktiverad** *(Disabled). Det kan också inträffa att* **TPM-modulen** *är* **inaktiverad** *(Disabled) när datorn kommer tillbaka från reparation eller underhåll. Du ska då aktivera TPM och ställa in funktionen på nytt.*
- *Du bör förhindra att andra än administratören och datoranvändarna ändrar BIOS-inställningarna. Vi rekommenderar därför att du ställer in ett BIOS-lösenord och ett annat BIOS-lösenord för den klassificeringsansvarige. I datorns användarhandbok beskrivs hur du ställer in dessa lösenord.*

2.2 Installera Infineon TPM Professional Package

Installera **Infineon TPM Professional Package** från `C:\TOSHIBA\Drivers\TPM Utility`

I **Infineon TPM Professional Package** finns följande program och funktioner:

- Hjälp för Security Platform
- Security Platform Settings Tool (inställningsverktyg)
- Security Platform Initialization Wizard (installationsguide)
- Security Platform User Initialization Wizard (användarinitieringsguide)
- Security Platform Migration Wizard (överflyttningsguide)
- Security Platform Backup Wizard (säkerhetskopieringsguide)
- Security Platform Password Reset Wizard (guide för lösenordsåterställning)
- Security Platform PKCS #12 Import Wizard (importguide för PKCS #12)
- Certifikatvisning och certifikatval för Security Platform (säkerhetsplattformen)
- Security Platform-ikon för meddelandefältet
- Security Platform Integration Services (integrationstjänster)
  - Integrering med Microsoft® Outlook®
  - Netscape©-integrering
  - Integrering för krypterade filer
  - PSD-enheten
  - Principadministration
- Tjänster för Security Platform (säkerhetsplattformen)
  - TSS (TCG Software Stack) – serviceleverantör
  - TSS – kärntjänster
  - TSS – bibliotek för enhetsdrivrutiner

2.3 Registrering av ägare och användare i TPM

1. Klicka på ikonen **Security Platform** i meddelandefältet och välj **Security Platform Initialization** (Security Platform-initiering).

2. TPM startar och fönstret öppnas. Klicka på **Next** (Nästa).
3. I fönstret **Initialization** (Initiering) väljer du Initialize a new Security Platform (Initiera en ny Security Platform). **Klicka på Nästa.**
4. I fönstret **Create Security Platform Owner** (Skapa ägare för säkerhetsplattformen) för ägarautentisering anger du lösenordet i **Password** och bekräftar det sedan i **Confirm Password**. Klicka därefter på **Nästa**.
5. Fönstret **Features** (Funktioner) öppnas. Välj vilken Security Platform-funktion du vill ställa in och klicka sedan på **Nästa**. Mer information finns i hjälpen för säkerhetsplattformsfunktionen.

Du bör ställa in **Automatic Backup** *(Automatisk säkerhetskopiering). Om du inte gör det kan du förlora avvikande krypterade data.*

6. I fönstret **Backup (Säkerhetskopiering)** anger du platsen där du skapar och sparar säkerhetskopian. Klicka på **Next** (Nästa).
7. I fönstret **Emergency Recovery (Återställning)** väljer du **Create a new Recovery Token (Skapa en ny token-nyckel för återställning)** och anger platsen där du vill skapa och spara **Emergency Recovery Archive Token(Token-nyckel för återställningsarkivet).**
8. I fönstret **Emergency Recovery** (Återställning) för autentisering av token-nyckeln anger du lösenordet (Password) och bekräftar det sedan i **Confirm Password**. Klicka därefter på **Nästa**.

Vi rekommenderar att du skapar en token-nyckel för återställningsarkivet så att informationen i TPM, och de användardata som hör till TPM, sparas om något allvarligt systemfel skulle inträffa. Om du inte följer våra rekommendationer riskerar du att förlora data.

9. I fönstret **Password Reset** (Lösenordsåterställning) väljer du **Create a new Token** (Skapa en ny token-nyckel) och anger platsen där du vill skapa och spara **lösenordsåterställningsnyckeln**.

10. I fönstret **Password Reset** (Lösenordsåterställning) för autentisering av lösenordsåterställningsnyckeln anger du lösenordet och bekräftar det sedan i **Confirm Password**. Klicka därefter på **Next** (Nästa).

Vi rekommenderar att du skapar och sparar lösenordsåterställningsnyckeln på ett lagringsmedium, exempelvis en diskett, som går att använda även när datorn inte fungerar. Förvara disketten på en säkert ställe så att du hittar den när den kan komma att behövas.

- Om det finns flera datorer med TPM, är token-nyckeln för varje dator olika och de bör därför förvaras på skilda ställen.
- Återställningstoken-nyckeln för en registrerad TPM-ägare* går inte att skapa om på nytt. Du bör skapa och spara flera kopior av token-nyckeln enligt rekommendationen ovan.

  *Samma TPM-ägarnamn kan skapas med TPM i BIOS-menyn och en ny ägare kan registreras. Den nye ägaren är emellertid skild från den tidigare registrerade ägaren i det här fallet så tidigare krypterade filer kan inte dekrypteras.
- Om token-nyckeln tillsammans med lösenordet stjäls eller på annat sätt snappas upp av obehöriga, kommer dessa att få tillgång dina till krypterade data. Du ska därför förvara token-nyckeln och lösenordet på olika ställen.

  Mer information finns i kapitel 8 - *TPM-återställning*.

11. **Summary (Sammanställning) visas.** Kontrollera sammanställningen och klicka på **Next**.
12. Det kan ta någon minut innan meddelandet **Wizard completed successfully** (Guiden har slutförts) visas. Markera därefter kryssrutan **Start Security Platform User Initialization Wizard** (Starta användarinitieringsguiden för Security Platform) och klicka på **Finish** (Slutför).
13. I **User Initialization Wizard** (Användarinitieringsguiden) klickar du på **Next**.
14. I fönstret **Basic User Password** (Användarlösenord) för användarautentisering anger du lösenordet i **Password** och bekräftar det sedan i **Confirm Password**. Klicka sedan på **Next**.
15. I fönstret **Basic User Password Reset** (Återställning av användarlösenord) kontrollerar du att **Enable the resetting of my Basic User Password in case of an emergency** (Aktivera återställning av användarlösenord vid nödläge) har markerats. Ange var du vill skapa och spara filen **Personal Secret** (Personlig hemlighet).

Se till att du förvarar filen på ett säkert ställe. Du kan i framtiden behöva återställa användarlösenordet (Basic User Password).

16. Fönstret **Password and Authentication** (Lösenord och autentisering) öppnas. Kontrollera att det som visas stämmer och klicka sedan på knappen **Next**.

Det kan flera minuter innan fönstret med säkerhetsplattformsfunktioner öppnas.

17. Kontrollera att nödvändiga alternativ är markerade i **Security Platform Features** (Security Platform-funktioner) och klicka på **Next**.

- *Om du vill använda* **Secure E-mail** *(Säker e-posthantering) måste du göra nödvändiga inställningar i* **Mail Software** *(E-postprogram). Mer information om säker e-posthantering finns i kapitel 4,* Säker e-posthantering.
- *Funktionen* **File and Folder encryption (EFS)** *(Fil- och mappkryptering) är inte aktiverad i Windows® Vista Home.*
- *Hårddisken måste vara NTFS-formaterad för att det ska gå att använda funktionen för fil- och mappkryptering (EFS-kryptering).*

Inställningar i det här avsnittet går också att ändra senare.

18. Om du markerar **Secure E-mail** (Säker e-posthantering) i **Security Platform Features** (Security Platform-funktioner) öppnas nästa fönster. Klicka på **Next** (Nästa).

Om du klickar på någon av knapparna Outlook, Windows Mail/Outlook Express eller Netscape här, öppnas hjälpavsnittet för Secure E-mail-inställningarna för respektive e-postprogram. (Det går också att se den här hjälpen när du stängt guiden.)

19. Krypteringscertifikatsmeddelandet ska visas i fönstret **Security Platform Features** (Security Platform-funktioner). Markera certifikatet som ska utfärdas och klicka sedan på **Next**. I vanliga fall kan du klicka på knappen **Create** (Skapa) för att skapa och välja certifikatet.

Standardvärdet för **Maximum Basic User Password age** *(Maximal ålder för användarlösenord) är* **Disabled** *(Inaktiverad). Du kan ändra maximal ålder för användarlösenordet i* **User** *(Användare) i* **Security Policy** *(Säkerhetsprinciper).*

20. Om du markerar **Personal Secure Drive (PSD)** (Säker personlig enhet) i **Security Platform Features** öppnas nästa fönster. I det här fönstret markerar du enheten som du vill tilldela för PSD. Skriv sedan enhetens etikettnamn och klicka på **Next**. Mer information om PSD-enheter finns i kapitel 3, *PSD-enheten*.
21. I **Security Platform Features** (Security Platform-funktioner) anger du hur mycket förvaringsutrymme du vill tilldela för PSD-enheten. Markera därefter enheten och klickar på **Next**.
22. **Confirm setting** (Bekräfta inställning) visas. Klicka på knappen Next.

- *Vi rekommenderar att du väljer den inbyggda hårddisken (vanligtvis C-enheten) för* **My Personal Secure Drive (Min säkerhetsenhet) i den nedrullningsbara menyn.**
- *Det tillgängliga utrymmet, för enheten angiven ovan, ska vara större än det utrymme som anges i* **My Personal Secure Drive will have [XX] MB of storage space** *(Min säkerhetsenhet kommer att ha [XX] MB i lagringsutrymme).*

23. Efter en stund kommer meddelandet **Wizard completed** (Guiden har slutförts) att visas. Klicka på knappen **Finish** (Slutför).

Om flera användare har registrerats i Windows®, och om dessa användare ska använda TPM-modulen, måste varje användare logga in i Windows® och registrera sig. Sedan användaren loggat in i Windows® och registrerat sig, ska han/hon klicka på ikonen **Security Platform** *i meddelandefältet och välja* **Security Platform User initialization** *(Användarinitiering av Security Platform).*

Om du vill ändra inställningarna klickar du på ikonen **Security Platform Setting Tool** (Verktyg för Security Platform-inställningar) i meddelandefältet och gör ändringarna i fönstret.

- *Initiering*
  - *När du använder Infineon TPM Professional Package behöver du inte börja med att initiera TPM-modulen i TPM Management on Local Computer (TPM-hantering på lokal dator) i Windows Vista®.*
  - *När du initierat TPM-modulen i Infineon TPM Professional Package behöver du inte initiera den i TPM Management on Local Computer (TPM-hantering på lokal dator) i Windows Vista®.*
- *Initieringsmetod*

När du använder Professional Package V3.0 sedan TPM-modulen har initierats i funktionen för TPM-inställningarna i Windows Vista®, utförs den normala plattformsinitieringen enligt följande:

1. *Sedan du installerat Professional Package V3.0 visas meddelandet "*`Initialized other OS`*" (Initiering av annat OS) vid ikonen* **TPM** *i Aktivitetsfältet.*

   ** Detta betyder inte att det finns något TPM-fel.*
2. *När du använder verktyget för* **Infineon Security Platform-inställningar** *i Steg 1, visas "Initialized (Failure Mode 2)" (Initierad (felläge 2)) för [Security Platform State:] (Security Platform-läge) och [Owner:] (Ägare) på fliken Info.*

   ** Detta beror inte på något fel. Plattformsinitieringen är emellertid inte avslutad.*
3. *När du använder* **Security Platform User Initialization Wizard** *(Guide för Security Platform-användarinitiering) visas ett initieringsfönster. Trots att* **Security Platform restoration form a Backup Archive** *(Security Platform-återställning från en säkerhetskopia) är markerat ska du välja* **Security Platform Initialization** *(Security Platform-initiering).*
4. *I nästa fönster i* **Initialize Security Platform** *(Initiera Security Platform) anger du lösenordet som angetts i TPM Management on Local Computer (TPM-hantering på lokal dator) i Windows Vista®.*
   Under den här tiden kan du inte använda **TPM Owner Password Backup file** *(Säkerhetskopia för TPM-ägarlösenord) som sparats i* **TPM Management on Local Computer***.*
5. *När användarlösenordet ändras i Infineon TPM Professional Package, kan du inte använda* **TPM Owner Password Backup file** *som skapats i TPM Management on Local Computer i Windows Vista®.*

3 PSD-enheten

Med **Personal Secure Drive** (Säker personlig enhet) går det att skapa förvaringsutrymmen för filer som ska krypteras och sparas på den virtuella enheten. Filerna inte bara sparas och krypteras på hårddisken. Eftersom de skyddas av TPM ges de också högre säkerhet än befintlig programbaserad kryptering. PSD får inte vara mindre än 10 MB. Hur stor PSD kan vara beror på i vilket filsystem PSD skapas. I hjälpen finns mer information.

3.1 Fördelar med PSD-enheter

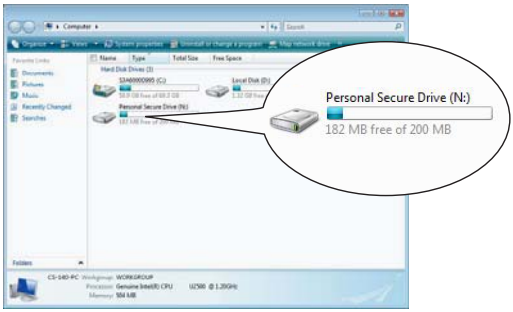
- Krypteringen av den virtuella enheten görs med säkra AES-nycklar (Advanced Encryption Standard).
- RSA-algoritm för krypterad nyckelgenerering.
- Automatisk kryptering och dekryptering av transparenta säkerhetsdata.
- Filer är lätta att skydda.
- Enkelt handhavande: PSD-funktionerna fungerar på samma sätt som för vanliga *Windows*®-enheter.
- Enkel hantering och enkla inställningar med hjälp av guider.

3.2 Grundläggande PSD-operationer

1. Om du valt PSD i **Security Platform Features** (Security Platform-funktioner) klickar du på ikonen för **Security Platform** i meddelandefältet sedan du loggat in i Windows och väljer [**Personal Secure Drive**] - [**Load**] (PSD – ladda).

*När du klickar på ikonen för Security Platform i meddelandefältet kan du välja [**Personal Secure Drive**] - [**Load**], [**Unload**] (PSD – ladda, ta bort) eller [**Load at Logon**] (ladda vid inloggning).*

2. Infineon Security Platform User Authentication (användarautentisering för Infineon Security Platform) öppnas. Skriv TPM-lösenordet. Den virtuella PSD-enheten accepteras när du angett rätt lösenord.
3. Här nedan visas ett exempel på hur PSD-enheten kan se ut i Windows® Utforskaren.



Trots att PSD-enheten har enhetsbokstaven **[N:]** och namnet **Personal Secure Drive**, går det i det här fönstret att ändra dessa inställningar med **User Settings** (Användarinställningar) i **Infineon Security Platform Settings Tool** (Verktyg för Security Platform-inställningar).

- *Eftersom filer i PSD-enheten inte säkerhetskopieras med* **säkerhetskopieringsfunktionen** i **Infineon Security Platform Settings Tool**, *ska du använda de vanliga kopieringsfunktionerna i Utforskaren för att kopiera PSD-filerna till ett externt och utbytbart medium så att du förhindrar dataförluster.*
- *Data för systemåterställningspunkten*, en inställning som görs med funktionen Systemåterställning i Windows®, tas bort när TPM-lösenordet anges då datorn startas, PSD-enheten monteras och den virtuella enheten tilldelas. Du bör använda en av följande metoder för att spara data för systemåterställningspunkten:*
  - *Använd inte PSD-funktionen och använd endast filkrypteringsfunktionen via EFS.*
  - *Inaktivera temporärt PDS-funktionen precis innan du ändrar inställningarna för Windows-miljön.*

  Inaktivera PSD-funktion -> Set the Restore Point (Ställ in återställningspunkten) -> Modify the system (Ändra datorinställningar) -> Check that Windows starts up properly (Kontrollera att Windows startar korrekt) -> Set the PSD function back to its previous state (Återställ PSD-funktionen till tidigare läge).

  ** Mer information om återställningspunkten finns i Windows® Hjälp.*

- *PSD-inställningarna måste göras för varje TPM-användare. Om det exempelvis finns två registrerade TPM-användare ”A” och ”B”, kan ”B” inte se PSD-innehållet för ”A”.*
- *Eftersom det finns områden i Personal Secure Drive (PSD) som används av NTFS-filsystemet i Windows, är det område som går att använda mindre än initialvärdet under konfigurationen. När minst cirka 10 MB har använts och PSD-kapaciteten har ökat, ökas också området som används av NTFS.*

  När du vill använda all nödvändig kapacitet måste du ange högre kapacitet under PSD-konfigureringen.

  (Exempel: Om du vill använda cirka 200 MB måste du ange 220 MB som PSD-kapacitet under konfigurationen.)

4 Säker e-posthantering

Med den här säkerhetsplattformen skyddas de ID-nummer som används för e-posthanteringen av TPM-modulen så att de inte försvinner eller stjäls.

Kompatibla e-postprogram är bl.a. Outlook*, Windows Mail/Outlook Express* och Netscape*.

* Observera att funktionen kanske inte går att använda i vissa versioner av programmen.

4.1 Inställningar

1. Hämta från Commercial Certificate Authority (CA) ett ID-nummer som ska användas i Secure E-Mail (Säker e-posthantering). I hjälpen för TPM finns mer information om CA.
2. Installera ID-numret i datorn enligt de anvisningar som du får från CA. Se till att ID-numret länkas till TPM-modulen som ett CSP (Cryptographic Service Provider).
3. Gör inställningarna för Secure E-Mail i e-postprogrammet. I användarhandboken till respektive e-postprogram och i hjälpen för Infineon Security Platform finns mer information.

Ställ in **Secure E-mail** *i Security Platform-funktionen vid TPM-registreringen (steg 2.3) om det inte har tilldelats (*1, *2).*

*1 Använd Help (hjälp) för att leta efter information om e-post och TPM

1) Dubbelklicka på ikonen **TPM** i meddelandefältet.
2) Välj fliken **Info**.
3) Klicka på knappen **Help** (Hjälp).
4) Sök med hjälp av nyckelord, under fliken **Search**, efter det du vill veta mer om. (Exempel: **E-Mail**)

*2 Aktiverar e-postfunktionen i User Settings (användarinställningar)

1) Dubbelklicka på ikonen **TPM** i meddelandefältet.
2) Välj fliken **User Settings** (Användarinställningar).
3) Klicka på knappen **Konfigurera**.
4) Markera alternativet **Secure E-mail** och klicka på **Next**.

5 EFS-tillägg (Encrypting File System)

Om alternativet för fil- och mappkryptering markeras i steg 2.3, utökas EFS-funktionen för operativsystemet och datoranvändningen blir säkrare eftersom EFS-krypterade nycklar för filer skyddas av TPM-modulen.

Du krypterar/dekrypterar filer på ungefär samma sätt.

Skillnaden är att när filer som krypteras med EFS öppnas efter *Windows*®-inloggningen, måste TPM-lösenordet för den aktuella användaren anges.

- *I följande miljöer när filer som skapas i* **[Basic User Key and Other Folders]** *(Användarnyckel och andra mappar) EFS-krypteras, kommer TPM-programmet inte att startas normalt och krypterade data kan inte dekrypteras.*
  - *TPM är installerat*
  - *Initieringen är avslutad för Platform*
  - *En EFS-funktion väljs under användarinitiering*

  Under initieringen har filer i **[Basic User Key and Other Folders]** *attribut som förhindrar att de dekrypteras. Ändra inte filattributen i motsvarande mappar.*

  ** Under initialkonfigurationen av Windows är följande mappar dolda.*

  [Basic User Key and Other Folders]

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

- *När arkiv, säkerhetskopior och token-filer krypteras kan de inte dekrypteras vid en nödsituation.*

  När lösenordsåterställningsnyckeln och hemliga filer krypteras kan lösenordet inte återställas.

  Kryptera inte följande filer och mappar:

  [Automatic Backup File]

  standardfilnamn: SPSystemBackup.xml

  standardlösenord: inte specificerad (*)

  [Automatic Backup Data Storage Folder]

  Mappnamn (fast): SPSystemBackup (SPSystemBackup.xml-filen skapas i en undermapp till den mapp som skapas)

  [Återställningsnyckel]

  standardfilnamn: SPEmRecToken.xml

  standardlösenord: utbytbara media (diskett, USB osv.)

  [Password Reset Token]

  standardfilnamn: SPPwdResetToken.xml

  standardlösenord: utbytbara media (diskett, USB osv.)

  [Basic User Password Reset]

  standardfilnamn: SPPwdResetSecret.xml

  standardlösenord: utbytbara media (diskett, USB osv.)

  [Säkerhetskopieringsarkiv]

  standardfilnamn: SpBackupArchive.xml

  standardlösenord: inte specificerad (*)

  [PSD-säkerhetskopieringsarkiv]

  standardfilnamn: SpPSDBackup.fsb

  standarlösenord: Inte specificerad (*)

  (*) När du klickar på **Reference** *(Referens) öppnas "User folder\Documents\Security Platform".*

- *Innan du krypterar filen med EFS bör du först läsa den EFS-relaterade informationen i Windows® Hjälp. Det blir då lättare att undvika att filer kommer att kunna dekrypteras på grund av ofrivilliga ändringar av krypteringsnyckeln, som används i EFS, eller på grund av att du tappat bort nyckeln.*

6 Verktyget TOSHIBA Password

Om du använder verktyget för TOSHIBA-lösenord kan du göra inställningar som förhindrar att användare, som saknar administratörsbehörighet, ändrar TPM-relaterade inställningar i BIOS.

När inställningen är gjord, kan användare som saknar administratörsbehörighet inte ändra TPM-inställningarna i BIOS (i rutan **Security Controller** (Säkerhetskontroller)).

1. Använd följande fil för att starta verktyget för TOSHIBA-lösenord.

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

2. Registrera administratörslösenordet på fliken **Supervisor Password** (Administratörslösenord).
3. Öppna fönstret för användarprinciper från fliken **Supervisor Password** (Administratörslösenord).
4. I rutan **TPM** tar du bort markeringen för det som du inte vill att användare, som saknar administratörsbehörighet, ska kunna ändra.
5. Klicka på knappen **Set** (Ange) sedan administratörsautentiseringen har utförts. Spara de nya användarprinciperna.
6. Stäng verktyget för TOSHIBA-lösenord.

7 Överflyttning av TPM-miljön och avyttring

7.1 Överflyttning

Klicka på ikonen för **Security Platform** i meddelandefältet och välj **Manage Security Platform** (Hantera Security Platform). I fönstret **Infineon Security Platform Settings tool** (Verktyg för Infineon Security Platform-inställningar) klickar du på fliken **Migration** (Överflyttning). På fliken **Migration** klickar du på knappen **Learn more...** (Lär dig mera) om du vill ha mer information om överflyttningar. (Operationen måste utföras både för källplattformen och målplattformen.) Utför operationerna enligt anvisningarna i fönstret.

Det är endast TPM-data som överförs under den här processen så du ska utföra överflyttningen av PSD-data, och filer krypterade med EFS, med hjälp av de vanliga filhanteringskommandona.

- *Kom ihåg att du måste installera* **Infineon TPM Professional Package** *också på målplattformen.*
- *När Windows®-brandväggen är aktiverad går det inte att göra överflyttningar mellan olika datorer i ett nätverk. Inställningarna för Windows®-brandväggen ändras i* **Säkerhetscenter** *i* **Kontrollpanelen**.

7.2 Avyttring av datorn

När du gör dig av med datorn ska du utföra följande två åtgärder för att förhindra att hemlig information kommer i orätta händer. Du ska göra samma sak även när datorn byter ägare.

1. Avinstallera **Infineon TPM Professional Package** samt ta bort återställningsarkivet och **Emergency Recovery Archive Token** (Token-nyckel för återställningsarkivet). Du ska dessutom ta bort alla relevanta data på hårddisken.
2. Steg 1: Öppna BIOS-inställningarna. (Mer information finns i kapitel 2 - *Använda TPM-modulen första gången*.)

   Steg 2: Flytta markören till alternativet **Clear TPM Owner** (Ta bort TPM-ägare) i inställningen **SECURITY CONTROLLER** (Säkerhetskontroller) och tryck sedan på blanksteg eller backsteg. Nu tas alla data i TPM bort och TPM inaktiveras.

   Steg 3: Ett meddelande visas. Tryck på tangenterna **Y, E, S** följt av **Retur**.

Eftersom interna TPM-data tagits bort går det inte längre att läsa filerna.

8 TPM-återställning

8.1 Återställningsprocessen – en översikt

Återställningsprocessen används när:

- TPM behöver ändras på grund av TPM-problem
- ett fel uppstått i moderkortet med TPM och när moderkortet förändrats
- TPM rensades antingen ofrivilligt eller av annan orsak.

Se även *Restore Emergency Recovery Data Step by Step* (Återställa data – steg för steg) i hjälpen om du vill ha mer information.

- *Du bör skriva ut Restore Emergency Recovery Data Step by Step (återställa data – steg för steg) i hjälpen och läsa vad som står där innan du börjar.*
- *Förklaringarna här gäller för återställning av TPM-innehållet och inte för återställning av TPM-relaterade data som EFS-krypterade filer eller filer i PSD. För filer på den inbyggda hårddisken rekommenderar vi att du gör separata säkerhetskopior och att du förvarar kopiorna på ett säkert ställe.*

8.2 Återställning av användarlösenordet

Den här funktionen kan användas om användaren av Infineon Security Platform glömmer lösenordet och om det är nåt problem med användarens autentiseringsenhet. Användaren måste kunna återställa lösenordet för att kunna använda säkerhetsplattformen. Detta kan leda till att det inte går att läsa hemliga data.

Mer information finns i *Basic User Password Reset* (Återställning av användarlösenord) i hjälpen.

8.3 PSD-återställning

PSD-data kan återställas om PSD-certifikatet tappas bort vid en PSD-återställning.

Mer information finns i *Personal Secure Drive Recovery* (PSD-återställning).

Register

M

P

S

T

V

W

Meddelande

Se till att de lösenord och nyckelord som används förvaras på ett säkert ställe så att du hittar dem om du skulle glömma dem och så att obehöriga inte kan komma åt dem och informationen. Förvara dem exempelvis inte fastsatta med klisterlappar på skrivbordet.

Ägarlösenord:

Användarlösenord:

Förvaringsplats för återställningsnyckeln:

Lösenord för återställningsnyckel:

Förvaringsplats för säkerhetskopieringsfil:

Förvaringsplats för lösenordsåterställningsnyckel:

Lösenord för lösenordsåterställningsnyckel:

Förvaringsplats för filen Personal Secret:

Lösenord för TPM-användare

Windows®-användarnamn:

Lösenord för TPM-användare:

Windows®-användarnamn:

Lösenord för TPM-användare:

Windows®-användarnamn:

Lösenord för TPM-användare: