Installationsvejledning v3.3.0

TPM (Trusted Platform Module)

computers.toshiba-europe.com

TOSHIBA
Leading Innovation

Indholdsfortegnelse

1 Indledning 4
1.1 Konvention 4
1.2 TPM - En oversigt 5

2 Første gang TPM bruges 6
2.1 Aktivering af TPM 6
2.2 Installation af Infineon TPM Professional Package 7
2.3 Registrering af ejere og brugere i TPM 7

3 Personal Secure Drive 13
3.1 Fordele ved Personal Secure Drive (Personligt sikkerhedsdrev) 13
3.2 Personal Secure Drive (PSD) (Personligt sikkerhedsdrev (PSD)) - Basisoperation 13

4 Secure E-Mail (Sikker e-mail) 16
4.1 Configuration 16

5 EFS (Encrypting File System) Extension 17

6 TOSHIBA Hjælpeprogram til adgangskode 19

7 Overflytning af TPM-miljø og bortskaffelse 20
7.1 Overflytning 20
7.2 Bortskaffelse af pc 20

8 Gendannelse til TPM 21
8.1 Nødgendannelsesproces - En oversigt 21
8.2 Nulstilling af brugeradgangskode 21
8.3 PSD-gendannelse 21

Indeks

Copyright

Varemærker

Microsoft, Windows og Windows Vista er registrerede varemærker, der tilhører Microsoft Corporation i USA og/eller andre lande.

Alle andre mærke- og produktnavne er registrerede varemærker tilhørende deres respektive ejere.

1 Indledning

Din computer har en integreret TPM (Trusted Platform Module). For at aktivere TPM skal du enten aktivere den eller installere Infineon Security Platform Tools-softwaren. Denne installationsvejledning beskriver, hvordan man installerer og konfigurerer TPM. Læs omhyggeligt denne installationsvejledning inden brug af TPM.

1.1 Konvention

Denne vejledning anvender nedenstående formater til at beskrive, identificere og fremhæve termer og betjeningsprocedurer.

Sikkerhedssymboler

Denne vejledning indeholder sikkerhedsanvisninger, som skal følges for at undgå potentielle farer, der kan medføre personskade, beskadigelse af udstyret eller tab af data. Sikkerhedsforskrifterne er grupperet efter risikograd, og symbolerne angiver disse anvisninger på følgende måde:

Angiver en potentiel overhængende fare, der kan medføre tingskade.

Angiver vigtige oplysninger.

1.2 TPM - En oversigt

Den indbyggede sikkerhedscontroller (TPM) er baseret på specifikationer fra Trusted Computing Group. TPM tilbyder databeskyttelse ved hjælp af sikkerhedskrypteringsnøgler i stedet for sikkerhedskrypteringsformler (algoritmer). Ved kryptering, der udelukkende er baseret på software, er der en fare for, at krypteringsnøglen, der er gemt i filen eller læses i computerens hukommelse, kan læses og dechifreres. Ved at lagre krypteringsnøglen i TPM i stedet for er data mere sikkert beskyttet.

Da TPM bruger offentlige og standardiserede specifikationer, kan der etableres et mere sikkert pc-miljø ved hjælp af den tilhørende sikkerhedsløsning.

Der findes flere oplysninger om TCG-specifikation på deres websted på http://www.trustedcomputinggroup.org/

Kryptering, certifkater og adgangskoder

- *TPM indeholder en funktion til at oprette og konfigurere flere krypteringsnøgler, certifikater og adgangskoder. Når det først er konfigureret, skal du sørge for, at adgangskoder bliver opbevaret forsigtigt, og at der er taget sikkerhedskopier af krypteringsnøglefiler. Hvis du mister eller glemmer disse indstillinger, kan filer, der er krypteret med denne TPM, ikke dekrypteres, og der er ikke adgang til krypterede data.*

TPM

- *Selvom TPM tilbyder de nyeste sikkerhedsfunktioner, garanterer de ikke komplet beskyttelse af data og hardware. Bemærk, at Toshiba ikke er ansvarlig for fejl eller skader, der kan være forårsaget på grund af brug af denne funktion.*

Hvis der er registreret flere brugere i Microsoft® Windows®, og hvis disse brugere skal bruge TPM, skal hver bruger logge på Windows® og blive registreret individuelt.

2 Første gang TPM bruges

Denne vejledning indeholder kun generelle retningslinjer. Se og læs HJÆLPEN til TPM, når du har installeret TPM Professional Package.

Når du bruger TPM for første gang, skal det konfigureres på følgende måde. (Indstillingerne 1 - 3 kan udføres ved at logge på som *Windows*®-administrator.)

1. Aktiver TPM.
2. Installer **Infineon TPM Professional Package**.
3. Registrer ejeren og brugere i TPM.

2.1 Aktivering af TPM

For at aktivere TPM skal du udføre følgende BIOS-indstillinger:

1. Tænd for din computer, mens du trykker på **Esc**-tasten.
2. Der vises en meddelelse. Tryk på **F1**-tasten.
3. Skærmbilledet med BIOS-konfigurationen vises.
4. Tryk på **Page Down** for at se det næste skærmbillede.
5. Indstil **TPM** i **SECURITY CONTROLLER** til **Enabled**.

Nogle modeller har **Hide TPM** *som en mulighed på skærmbilledet BIOS setup. Hvis dit system viser* **Hide TPM**,*, skal det indstilles til* **No***, inden du indstiller* **TPM** *til* **Enabled***. Ellers vil du ikke længere være i stand til at ændre* **TPM***.*

6. Tryk på **End**-tasten, gem ændringerne til BIOS-indstillingerne, og tryk på **Y** -tasten.

Intern dataensartethed i TPM garanteres ikke, når computeren er sendt til reparation eller vedligeholdelse. Inden du sender computeren til reparation eller vedligeholdelse, skal du både tage en sikkerhedskopi af filerne på HHD (Harddiskdrev og TPM-data ved hjælp af sikkerhedskopieringsfunktionen. (Se kapitel 8 - Gendannelse til TPM*.) Sikkerhedsfunktionerne, der bruger TPM, fungerer ikke længere korrekt, hvis data i TPM går tabt. (Eksempel: Filer, der blev krypteret ved hjælp af TPM, kan ikke længere åbnes). Hvis det mislykkes, kan det resultere i eventuelle tab af data.*

- **Når TPM** *leveres, er indstillingen* **Disabled (Deaktiveret)** *som standard Also (Også), men der kan være tilfælde, hvor* **TPM** *er indstillet til* **Disabled***, efter at computeren er sendt til reparation eller vedligeholdelse. Aktiver TPM ved at omkonfigurere den igen.*
- *For at forhindre at andre end administrator og brugere af denne computere ændrer BIOS-indstillingerne, anbefales det meget, at du indstiller en BIOS-adgangskode og en BIOS-adgangskode for systemansvarlig. Se brugervejledningen til computeren for at få oplysninger, hvordan man ændrer disse adgangskoder.*

2.2 Installation af Infineon TPM Professional Package

Installer **Infineon TPM Professional Package** fra `C:\TOSHIBA\Drivers\TPM Utility`.

Infineon TPM Professional Package indeholder følgende software og funktioner:

- Hjælp til Security Platform
- Security Platform Settings Tool
- Security Platform Initialization Wizard
- Security Platform User Initialization Wizard
- Security Platform Migration Wizard
- Security Platform Backup Wizard
- Security Platform Password Reset Wizard
- Security Platform PKCS #12 Import Wizard
- Security Platform Certificate viewer and Certificate Selection
- Meddelelsesikon på proceslinjen til Security Platform
- Security Platform Integration Services
  - Microsoft® Outlook® Integration
  - Netscape® Integration
  - Encrypted File System Integration
  - Personal Secure Drive
  - Policy Administration
- Security Platform Services
  - TSS (TCG Software Stack) Service Provider
  - TSS Core Service
  - TSS Device Driver Library

2.3 Registrering af ejere og brugere i TPM

1. Klik på ikonet **Security Platform** i proceslinjen, og vælg **Security Platform Initialization**.

2. TPM starter, og dets skærmbillede vises. Klik på knappen **Next** (Næste).
3. I skærmbilledet **Initialization** skal du vælge Initialize a new Security Platform (Initialiser en ny sikkerhedsplatform). Klik på knappen **Next** (Næste).

4. I skærmbilledet **Create Security Platform Owner (Opret ejer til sikkerhedsplatform)** til ejergodkendelse skal du indtaste adgangskoden i feltet **Password**(Adgangskode) og **Confirm Password** (Bekræft adgangskode) og klikke på knappen **Next** (Næste).
5. Skærmbilledet **Features (Funktioner)** vises. Vælg funktionen Security Platform (Sikkerhedsplatform) for at konfigurere funktionen, og klik på knappen **Next** (Næste). Se hjælpen til sikkerhedsplatformen for at få flere oplysninger.

Setting **Automatic Backup** *anbefales meget. Hvis den ikke er indstillet, kan de krypterede brugerdata gå tabt, hvis det ikke fungerer.*

6. I skærmbilledet **Backup (Sikkerhedskopiering)** skal du angive placeringen til oprettelse og lagring af filen med sikkerhedskopiering. Klik på knappen **Next** (Næste).
7. I skærmbilledet **Emergency Recovery** (Nødgendannelse) skal du vælge **Create a new Recovery Token (Opret et nyt nødgendannelsestoken)** du angive placeringen til oprettelse og lagring af **Emergency Recovery Archive Token** (Token til nødgendannelsesarkiv).
8. I skærmbilledet **Emergency Recovery (Nødgendannelse)** til godkendelse af **Emergency Recovery Token (Token til nødgendannelse)** skal du indtaste adgangskoden i feltet Password (Adgangskode) og Confirm Password (Bekræft adgangskode) og klikke på knappen **Next** (Næste).

Det anbefales meget, at du opretter et nødgendannelsestoken, så oplysninger i TPM og brugerdata relateret til TPM er sikre i tilfælde af alvorlige systemproblemer. Hvis du ikke følger denne anbefaling, kan det resultere i eventuelle tab af data.

9. I skærmbilledet **Password Reset (Nulstil adgangskode)** skal du vælge **Create a new Token (Opret et nyt token)**du angive placeringen til oprettelse og lagring af **Password Reset Token** (Token til nulstilling af adgangskode).
10. I skærmbilledet **Password Reset (Nulstilling af adgangskode)** til godkendelse af **Password Reset Token (Token til nulstilling af adgangskode)** skal du indtaste adgangskoden i feltet Password (Adgangskode) og Confirm Password (Bekræft adgangskode) og klikke på knappen **Next** (Næste).

Det anbefales meget, at du opretter og gemmer **Password Reset Token (Token til nulstilling af adgangskode)** *på et lagringsmedie, f.eks. en diskette, som der er adgang til selv i forbindelse med en computerfejl. Opbevar disketten et sikkert sted til fremtidig brug.*

- Hvis der er flere computere med TPM, findes der forskellige tokens for hver computer, og de skal gemmes separat.

- Gendannelsestoken, der er registreret for TPM-ejeren*, kan ikke oprettes igen. For at forhindre tab skal der oprettes og gemmes flere kopier af tokenen, som det anbefales herover.

  *Det samme TPM-ejernavn kan oprettes ved at initialisere TPM i BIOS-menuen og registrere en ny ejer. Men da ejeren er en anden end den tidligere registrerede ejer i dette tilfælde, kan tidligere krypterede filer ikke dekrypteres.

- Hvis token afsløres eller stjæles af tredjeparter sammen med adgangskoden, er de i stand til at få adgang til de krypterede data. Derfor anbefales det meget, at tokens og adgangskoder gemmes omhyggeligt.

  Se kapitel 8 - *Gendannelse til TPM*.

11. **Summary** (Oversigt) vises. Gennemgå oversigten, og klik på knappen **Next** (Næste).
12. Det tager et par minutter, inden meddelelsen **Wizard completed successfully** (Guide er udført) vises. Marker derefter afkrydsningsfeltet **Start Security Platform User Initialization Wizard** (Start guiden til brugerintialisering af sikkerhedsplatform, og klik på knappen **Finish** (Udfør).
13. I skærmbilledet **User Initialization Wizard** (Guiden Brugerinitialisering) skal du klikke på knappen **Next** (Næste).
14. I skærmbilledet **Basic User Key Password** (Grundlæggende adgangskode til brugernøgle) til brugergodkendelse skal du indtaste adgangskoden i feltet **Password** (Adgangskode) og **Confirm Password** (Bekræft adgangskode) og klikke på knappen **Next** (Næste).
15. I skærmbilledet **Basic User Password Reset (Nulstilling af basisadgangskode til bruger)** skal du kontrollere, at **Enable the resetting of my Basic User Password in case of an emergency (Aktiver nulstilling af min basisadgangskode til bruger i nødstilfælde)** er valgt. Angiv placeringen til oprettelse og lagring af filen **Personal Secret (Personlig sikkerhed)**.

Gem denne fil et sikkert sted. Det kan nogle gange kræves, at du nulstiller basisadgangskoden til brugeren.

16. Skærmbilledet **Password and Authentication (Adgangskode og godkendelse)** vises. Bekræft det viste indhold, og klik på knappen **Next** (Næste).

Det kan tage flere minutter før at skærmbilledet Security Platform Features (Funktioner til sikkerhedsplatform) vises.

17. Kontroller, at de ønskede funktioner er valgt i skærmbilledet **Security Platform Features** (Funktioner til sikkerhedsplatform), og klik på knappen **Next** (Næste).

- *For at bruge* **Secure E-mail** *(Sikker e-mail) er det nødvendigt at indstille konfigurationen i* **Mail Software** *(Mail software). Se kapitel 4 - Secure E-Mail (Sikker e-mail) for at få flere oplysninger om Secure E-mail (Sikker e-mail).*
- *Funktionen* **File and Folder encryption (EFS)** *(Fil- og mappekryptering (EFS)) er ikke tilgængelig i Windows Vista® Home.*
- *HDD (Hard Disk Drive) skal formateres i NTFS-format for at bruge funktionen* **File and Folder encryption (EFS)** *(Fil- og mappekryptering (EFS)).*

Konfigurationerne, der er indstillet i dette afsnit, kan også ændres efter konfiguration.

18. Hvis **Secure E-mail**(Sikker e-mail) er valgt i skærmbilledet **Security Platform Features** (Funktioner til sikkerhedsplatform), vises følgende skærmbillede. Klik på knappen **Next** (Næste).

Hvis der klikkes på knapperne **Outlook®**, **Windows Mail/Outlook Express** *eller* **Netscape®** *i skærmbilledet, vises hjælpen til indstillingerne* **Secure E-mail** *for den respektive* **Mail Software** *(mailsoftware). (Det er muligt at se denne hjælp, efter at guiden er lukket).*

19. Meddelelsen **Encryption Certificate (Krypteringscertifikat)** vises i skærmbilledet Security Platform Features (Funktioner til sikkerhedsplatform). Vælg det certifikat, som skal udstedes, og klik på knappen **Next** (Næste). Normalt skal du klikke på knappen **Create** (Opret) for at oprette og vælge certifikatet.

Standardværdien til **Maximum Basic User Password age (Maks. grundlæggende adgangskode til bruger (alder)** *er indstillet til* **[Disabled] (Deaktiveret)**. *Hvis du vil ændre Maximum Basic User Password age (Maks. grundlæggende adgangskode til bruger (alder)), kan du gøre dette under* **User (Bruger)** *i* **Security Policy (Sikkerhedspolitik)**.

20. Hvis **Personal Secure Drive (PSD)** (Personligt sikkerhedsdrev (PSD)) er valgt i skærmbilledet **Security Platform Features** (Funktioner til sikkerhedsplatform), vises følgende skærmbillede. I dette skærmbillede kan du vælge det ønskede drev til at allokere til PSD. Indtast derefter labelnavnet på dette drev, og klik på knappen **Next** (Næste).
    Se kapitel 3 - *Personal Secure Drive* for at få flere oplysninger om Personal Secure Drive (PSD) (Personligt sikkerhedsdrev (PSD)).
21. I skærmbilledet **Security Platform Features** (Funktioner til sikkerhedsplatform) skal du angive volumen på den lagerplads, som du vil allokere til PSD. Vælg derefter drevet, og klik på knappen **Next** (Næste).

22. Indstillingen Confirm (Bekræft) vises. Klik på knappen **Next** (Næste).

- *Det anbefales meget, at du angivet en indbygget HDD (Hard Disk Drive) (normalt C-drev) i rullemenuen* **My Personal Secure Drive will be saved on this drive** *(Mit personlige sikkerhedsdrev er gemt på dette drev).*
- *Den tilgængelige plads på drevet, der er angivet herover, skal være mere end den plads, der er angivet i* **My Personal Secure Drive will have [XX] MB of storage space** *(Mit personlige sikkerhedsdrev vil have [XX] MB lagerplads).*

23. Efter et stykke tid vises meddelelsen **Wizard completed** (Guide er udført). Klik på knappen **Finish** (Udfør).

Hvis der er registreret flere brugere i Windows®, og hvis disse brugere skal bruge TPM, skal hver bruger logge på Windows® og blive registreret individuelt. Når du har logget på Windows® for at udføre brugerregistrering, skal du klikke på ikonet **Security Platform** *(Sikkerhedsplatform) i proceslinjen og vælge* **Security Platform User initialization** *(Brugerinitialisering af sikkerhedsplatform).*

Ved ændring af konfigurationen skal du klikke på ikonet **Security Platform Setting Tool** (Indstillingsværktøj til sikkerhedsplatform) i proceslinjen og foretage ændringerne i konfigurationsskærmbilledet.

- *Initialization (Initialisering)*
  - *Ved brug af Infineon TPM Professional Package er der ikke brug for at initialisere TPM inden i Windows Vista™* **TPM Management på lokal computer***.*
  - *Når TPM initialiseres i Infineon TPM Professional Package er der ikke brug for at initialisere TPM inden i Windows Vista®* **TPM Management on Local Computer***.*
- *Initialiseringsmetode*

Ved brug af Professional Package V3.0 efter at TPM er initialiseret ved hjælp af funktionen Windows Vista® **TPM Setting***, kan normal platforminitialisering udføres på følgende måde:*

1. *Efter installation af Professional Package V3.0 vises "*`Initialized other OS`*" (Initialiseret af andet operativsystem) som en meddelelse fra* **TPM-ikonet** *på proceslinjen.*

   ** Dette betyder ikke, at TPM er unormal.*
2. *Når du kører* **Infineon Security Platform Setting Tool** *i trin 1, vises* **[Security Platform State:]**, **[Owner:]** *på fanen* **Info** *som "*`Initialized (Failure Mode 2)`*".*

   ** Dette er ikke en fejl. Men initialiseringen af platformen er ikke afsluttet.*

3. *Når du kører* **Security Platform User Initialization Wizard (Guiden til brugerinitialisering af sikkerhedsplatform)**, *vises skærmbilledet* **Initialization** *(Initialisering). Selvom* **Security Platform restoration form a Backup Archive (Gendannelse af sikkerhedsplatform fra et sikkerhedskopieringsarkiv)** *er valgt, skal du vælge* **Security Platform Initialization (Initialisering af sikkerhedsplatform)**.
4. *I det næste skærmbillede i* **Initialize Security Platform (Initialiser sikkerhedsplatform)** *skal du indtaste adgangskoden i Windows Vistas*® **TPM Management on Local Computer (TPM-styring på lokal computer)**. *I dette tidsrum kan du ikke bruge* **sikkerhedskopieringsfilen med TPM-ejerens adgangskode**, *der er gemt i* **TPM Management on Local Computer**.
5. *Hvis brugerens adgangskode ændres af Infineon TPM Professional Package, kan du ikke bruge den* **sikkerhedskopieringsfil med TPM-ejerens adgangskode**, *der blev oprettet i Windows Vistas*® **TPM Management on Local Computer**.

3 Personal Secure Drive

Personal Secure Drive (Personligt sikkerhedsdrev) opretter datalager til lagring af oplysninger (filer), og datafiler krypteres og gemmes i det virtuelle drev. Filerne er ikke simpelt krypteret og gemt i HDD. Da de er beskyttet af TPM, er sikkerhedsniveauet højere end eksisterende softwarebaseret kryptering. Den minimale størrelse på PSD kan angives til 10 MB.
Den maksimale størrelse på PSD varierer afhængigt af det filsystem, der opretter PSD. Se hjælpen for at få flere oplysninger.

3.1 Fordele ved Personal Secure Drive (Personligt sikkerhedsdrev)

- Kryptering af virtuelt drev vha. den sikre AES-nøgle (Advanced Encryption Standard).
- RSA-algoritme til krypteret nøglegenerering.
- Automatisk kryptering og dekryptering af transparente sikkerhedsdata.
- Filer kan let beskyttes.
- Simpel operation: Personal Secure Drive (Personligt sikkerhedsdrev) fungerer på samme måde som et *Windows*®-standarddrev.
- Let administration og konfigurationsprocedure vha. guiderne.

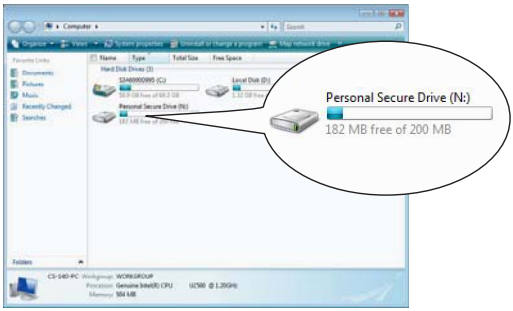
3.2 Personal Secure Drive (PSD) (Personligt sikkerhedsdrev (PSD)) - Basisoperation

1. Hvis PSD er valgt i **Security Platform Futures (Fremtidige sikkerhedsplatforme)**, skal du klikke på ikonet **Security Platform (Sikkerhedsplatform)** i proceslinjen, efter at du har logget på Windows og vælge **[Personal Secure Drive] (Personligt sikkerhedsdrev)**] - [**Load (Indlæs)**].

*Klik på ikonet Security Platform (Sikkerhedsplatform) i proceclinjen tillader valg af [**Personal Secure Drive (Personligt sikkerhedsdrev)**] - [**Load (Indlæs)**], [**Unload (Fjern)**] eller [**Load at Logon (Indlæs ved logon)**].*

2. Infineon Security Platform User Authentication vises. Indtast TPM-adgangskoden. Det virtuelle PSD-drev registreres først, når den korrekte adgangskode er indtastet.

3. Følgende er et skærmbillede med et eksempel, der viser PSD'en, som er registreret i *Windows*® Explorer.



Selvom det personlige sikkerhedsdrev i dette skærmbillede er registreret som Drev**[N:]** med et drevnavn på det **personlige sikkerhedsdrev**, er det muligt at ændre denne indstilling under **User Settings** (Brugerindstillinger) i **Infineon Security Platform Settings Tool** (Infineon - Indstillingsværktøj til sikkerhedsplatform).

- *Da filer i PSD'en ikke sikkerhedskopieres ved hjælp af funktionen* **Backup** (Sikkerhedskopi) i **Infineon Security Platform Settings** *Tool (Infineon - Indstillingsværktøj til sikkerhedsplatform), skal almindelige sikkerhedskopieringsmetoder, f.eks. kopiering af filer i PSD'en til et eksternt, flytbart medie, bruges for at undgå eventuelle tab af data.*
- *Dataene til systemgendannelsespunktet*, der er indstillet af Windows® -funktionen Systemgendannelse, slettes, efter at TPM-adgangskoden er indtastet under start af Windows. PSD'en tilsluttes, og det virtuelle drev tildeles. Det anbefales meget at bruge en af følgende metoder til at gemme data i system gendannelsespunktet.*
  - *Brug ikke PSD-funktionen, og brug kun filkrypteringsfunktionen via EFS'en.*
  - *Deaktiver midlertidigt PSD-funktionen, lige inden du ændrer Windows-miljøet.*

  Deaktiver PSD-funktionen -> Indstil gendannelsespunktet -> Ret systemet -> Kontroller, at Windows starter korrekt -> Indstil PSD-funktionen tilbage til den tidligere tilstand.

  ** Se Windows® Hjælp for at få flere oplysninger om gendannelsespunktet.*

- *PSD'en skal indstilles til hver TPM-bruger. F.eks. hvis der er registreret to TPM-brugere 'A' og 'B', kan B ikke se PSD-indholdet i A.*
- *Da der er området i Personal Secure Drive (PSD), som Windows' NTFS (filsystem) bruger, er den faktiske PSD-kapacitet, der kan anvendes, mindre end den oprindelige værdi under konfiguration. Når der som minimum er brugt ca. 10 MB, og PSD-kapaciteten er øget, bliver de områder, som NTFS bruger, også øget.*

  Hvis du ønsker al den krævede kapacitet, kan du angive højere kapacitet under PSD-konfiguration.

  *(eksempel: Hvis du vil bruge ca. 200 MB, kan du angive 220 MB som PS*D-kapacitet under konfiguration).

4 Secure E-Mail (Sikker e-mail)

I denne sikkerhedsplatform bliver digitale ID'er, der bruges til e-mail, beskyttet af TPM, som sikrer dem imod tab eller tyveri.

Kompatibel e-mail-software inkluderer Outlook®*, Windows Mail/Outlook Express* og Netscape®*.

* Bemærk, at det afhænger af softwareversionen, om denne funktion kan bruges.

4.1 Configuration

1. Hent et digitalt ID, som kan bruges med Secure E-Mail (Sikker e-mail) fra Commercial Certificate Authority (CA) (Kommercielle nøglecentre). Se hjælpen til TPM for at få flere oplysninger om CA.
2. Installer det digitale ID på computeren baseret på de brugs- og installationsmetoder, der er angivet af CA. På dette trin skal du kontrollere, at det digitale ID er knyttet til TPM som Cryptographic Service Provider (CSP) (Program til kryptografiske tjenester).
3. Indstil konfigurationen til Secure E-Mail (Sikker e-mail) i e-mail-softwaren. Se vejledningen til hver e-mail-software og hjælpen til sikkerhedsplatformen i Infineon for at få flere oplysninger.

Indstil **Secure E-mail** *(Sikker e-mail) under funktionerne til sikkerhedsplatformen, når du udfører brugerregistrering til TPM (trin 2.3), hvis den ikke blev tildelt (*1, *2).*

*1 Brug Hjælp til at finde oplysninger, der er relateret til e-mail og TPM

1) Dobbeltklik på ikonet **TPM**, der vises i proceslinjen.
2) Vælg fanen **Info** (Info).
3) Klik på knappen **Help (Hjælp)**.
4) Søg ved hjælp af nøgleord under fanen **Search** (Søg) efter elementer, som du vil have mere at vide om. (Eksempel: **E-Mail**)

*2 Aktivering af e-mail-funktionen i User Settings (Brugerindstillinger)

1) Dobbeltklik på ikonet **TPM**, der vises i proceslinjen.
2) Vælg fanen **User Settings** (Brugerindstillinger).
3) Klik på knappen **Configure** (Konfigurer).
4) Marker indstillingen **Secure E-mail** (Sikker e-mail), og klik på knappen **Next** (Næste).

5 EFS (Encrypting File System) Extension

Hvis funktionen File and Folder **encryption** (Fil- og mappekryptering) er markeret i trin 2.3, udvides EFS-funktionen i operativsystemet, og systemet gøres mere sikkert, idet krypteringsnøglen til filen, der er krypteret af EFS, beskyttes af TPM.

Handlingerne, der kræves til kryptering/dekryptering af filerne, ligner hinanden meget.

Forskellen i handlingen er, at der først forsøges at få adgang til filer, som er krypteret af EFS, efter at du er logget på *Windows*®, og TPM-adgangskoden til den aktuelle logonbruger skal indtastes.

- *Når filer, der er oprettet i* **[Basic User Key and Other Folders]***, er EFS-krypteret, starter TPM-softwaren ikke normalt op, og de krypterede data kan ikke dekrypteres.*
  - *TPM er installeret*
  - *Platform har udført initialisering*
  - *EFS-funktion vælges under brugerinitialisering*

  Under initialiseringsstatus har filer i **[Basic User Key and Other Folders]** *systemattributter, der forhindrer dem i at blive krypteret. Skift ikke filattributter for de tilhørende mapper.*

  ** I den første konfiguration i Windows er følgende mapper skjult.*

  [Basic User Key and Other Folders]

  `C:\ProgramData\Infineon\TPM Software`

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

  `C:\Users\All Users\Infineon`

- *Når arkiver, sikkerhedskopier og tokenfiler er krypteret, kan de ikke dekrypteres i nødstilfælde.*

  Når adgangskodens nulstillingstoken og sikre filer er krypterede, kan adgangskoden ikke nulstilles.

  Krypter ikke følgende filer og mapper.

  [Automatic Backup File] (Automatisk sikkerhedskopieringsfil)

  Standardfilnavn: SPSystemBackup.xml

  Standardadgangskode: Ikke angivet (*)

  [Automatic Backup Data Storage Folder] (Mappe med datalager til automatisk sikkerhedskopiering)

  Mappenavn (fast): SPSystemBackup (SPSystemBackup.xml-filen oprettes som en undermappe i den mappe, der oprettes)

  [Emergency Recovery Token] (Token til nødgendannelse)

  Standardfilnavn: SPEmRecToken.xml

  Standardadgangskode: Flytbart medie (FD, USB-hukommelse osv.)

  [Password Reset Token] (Token til nulstilling af adgangskode)

  Standardfilnavn: SPPwdResetToken.xml

  Standardadgangskode: Flytbart medie (FD, USB-hukommelse osv.)

  [Basic User Password Reset] (Nulstilling af grundlæggende adgangskode til bruger)

  Standardfilnavn: SPPwdResetSecret.xml

  Standardadgangskode: Flytbart medie (FD, USB-hukommelse osv.)

  [Backup Archive] (Sikkerhedskopieringsarkiv)

  Standardfilnavn: SpBackupArchive.xml

  Standardadgangskode: Ikke angivet (*)

  [PSD Backup Archive] (Sikkerhedskopieringsarkiv til PSD)

  Standardfilnavn: SpPSDBackup.fsb

  Standardadgang: Ikke angivet (*)

  (*) Når der klikkes på **Reference***, åbnes "User folder\Documents\Security Platform".*

- *Når du bruger filkryptering af EFS, anbefales det meget, at brugeren bliver bekendt med EFS-relaterede oplysninger i Windows® Hjælp. Dette vil være med til at forhindre, at filer ikke er i stand til at blive dekrypteret på grund af ukendte ændringer i krypteringsnøglen, som er brugt i EFS eller på grund af tabet af nøglen.*

6 TOSHIBA Hjælpeprogram til adgangskode

Ved at bruge TOSHIBA Hjælpeprogram til adgangskode kan konfigurationen indstilles til at forhindre brugere uden systemansvarligrettigheder i at ændre TPM-relaterede indstillinger i BIOS-konfigurationen.

Når denne konfiguration er indstillet, er brugere uden systemansvarligrettigheder ikke i stand til at ændre TPM-relaterede indstillinger i BIOS-konfigurationen (elementer i feltet **Security Controller** (Sikkerhedscontroller)).

1. Kør følgende fil for at starte TOSHIBA Hjælpeprogram til adgangskode.

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

2. Registrer adgangskoden for den systemansvarlige under fanen **Supervisor Password** (Adgangskode for systemansvarlig)
3. Åbn skærmbilledet User Policy setup (Konfiguration af brugerpolitik) fra fanen **Supervisor Password** (Adgangskode for systemansvarlig).
4. I feltet **TPM** skal du fjerne markeringen af de elementer, som du ikke vil have, at brugere uden systemansvarligrettigheder skal have adgang til og ændre.
5. Tryk på knappen **Set** (Indstil), og efter at du har udført bekræftelse af systemansvarligrettigheder. Gem den ændrede brugerpolitik.
6. Afslut TOSHIBA Hjælpeprogram til adgangskode.

7 Overflytning af TPM-miljø og bortskaffelse

7.1 Overflytning

Klik på ikonet **Security Platform** (Sikkerhedsplatform) i proceslinjen, og vælg **Manage Security Platform** (Administrer sikkerhedsplatform). I vinduet **Infineon Security Platform Settings Tool** (Infineon - Indstillingsværktøj til sikkerhedsplatform) skal du klikke på fanen **Migration** (Overflytning). På fanen **Migration** (Overflytning) skal du klikke på knappen **Learn more...** (Lær mere...) for at få flere oplysninger om overflytningen. (Handlingen skal udføres for både kildeplatform og destinationsplatform). Udfør handlingen i henhold til instruktionerne på skærmen.

Det er kun TPM-data, der overflyttes i denne proces, så udfør overflytningen af data inde i det personlige sikkerhedsdrev, og filerne krypteres med EFS ved hjælp af de almindelige filhandlinger

- *Husk, at det er nødvendigt også at installere* **Infineon TPM Professional Package** *i destinationsplatformen.*
- *Når Windows® Firewall er aktiveret, kan migrering mellem pc'er via et netværk ikke anvendes. Windows® Firewall-indstillingen kan ændres under* **Security Center** *i* **Kontrolpanel***.*

7.2 Bortskaffelse af pc

Ved bortskaffelse af pc'en skal du udføre følgende to processer for at undgå læk af fortrolige oplysninger. Gør det også, hvis der kommer en ny ejer af pc'en.

1. Afinstaller **Infineon TPM Professional Package**, og slet gendannelsesarkivet og **Emergency Recovery Archive Token** (Token til nødgendannelsesarkiv). Slet derudover alle data i HDD (Hard Disk Drive).
2. Trin 1: Få vist skærmbilledet **BIOS Setup**. (Se kapitel 2 - *Første gang TPM bruges*.)

   Trin 2: Flyt markøren til funktionen **Clear TPM Owner** (Ryd TPM-ejer) i indstillingen **SECURITY CONTROLLER** (SIKKERHEDSCONTROLLER), og tryk på mellemrumstasten. Med denne handling bliver alle data inde i TPM ødelagt, og derefter deaktiveres TPM.

   Trin 3: Der vises en meddelelse. Tryk på tasterne **Y**, **E**, **S** efterfulgt af **Enter**-tasten.

Nu hvor de interne TPM-data er slettet, kan filerne ikke længere læses.

8 Gendannelse til TPM

8.1 Nødgendannelsesproces - En oversigt

Nødgendannelsesprocessen bruges:

- ved ændring af TPM på grund af TPM-problemer.
- når motherboard med onboard TPM har en defekt, og motherboardet blev udskiftet.
- når TPM blev ryddet enten ved et uheld eller af andre årsager.

Se *Restore Emergency Recovery Data Step by Step* i hjælpen for at få flere oplysninger.

- *Det anbefales at udskrive Restore Emergency Recovery Data Step by Step i hjælpen.*
- *Forklaringerne, der er angivet her, er til gendannelse af TPM-indhold og ikke til gendannelse af TPM-relaterede data, f.eks. EFS-krypterede filer eller filer i PSD'en. For filer i den indbyggede HDD anbefales det meget, at sikkerhedskopier oprettes separat og gemmes et sikkert sted.*

8.2 Nulstilling af brugeradgangskode

Denne funktion kan bruges, hvis brugeren af Infineon Security Platform glemmer basisadgangskoden til brugeren, eller hvis der er et problem med brugerens godkendelsesenhed. Hvis adgangskoden ikke kan nulstilles, kan brugeren ikke bruge funktionerne i sikkerhedsplatformen. Dette kan resultere i mistede sikkerhedsdata.

Se *Basic User Password Reset (Nulstilling af basisadgangskode til bruger)* i hjælpen for at få flere oplysninger.

8.3 PSD-gendannelse

PSD-data kan gendannes, hvis PSD-certifikatet mistet ved hjælp af Personal Secure Drive Recovery.

Se *Personal Secure Drive Recovery* for at få flere oplysninger.

Indeks

A

Adgangskode 5
  ejer 8
  Emergency Recovery Token 8
Automatic Backup 8
  Data Storage Folder (Mappe med datalager til automatisk sikkerhedskopiering) 18
  File 18

B

Backup Archive (Sikkerhedskopieringsarkiv) 18
Basic User Password
  Reset 9, 18
  skærmbillede 9
BIOS
  indstillinger 6
  konfiguration 19
  konfigurationsskærmbillede 20
  skærmbillede 6
BIOS Setup
  skærmbillede 6

C

certifikater 5
CLEAR OWNER (RYD EJER) 20
Commercial Certificate Authority (CA) (Kommercielle nøglecentre) 16
Cryptographic Service Provider (CSP) (Program til kryptografiske tjenester) 16

D

Digitalt ID 16

E

Emergency Recovery
  Archive Token 20
  Create a new Token 8
  skærmbillede 8
  Token 8, 18
Encrypting File System 17

F

File and Folder encryption (EFS) (Fil- og mappekryptering (EFS)) 10

G

gendannelsespunkt 14

I

Infineon Security Platform Settings Tool 14
Infineon Security Platform Settings Tool 14
Initialize Security Platform
  skærmbillede 12

K

kryptering 5

M

Manage Security Platform (Administrer sikkerhedsplatform) 20
Maximum Basic User Password age (Maks. grundlæggende adgangskode til bruger (alder)) 10

N

Nødgendannelse
  proces 21

P

Password
Basic user 9
Password Reset
Create a new Token 8
skærmbillede 8
Token 8, 18
Personal Secret-fil (Personlig sikkerhed) 9
Personal Secure Drive 10, 14
PSD Backup Archive 18

S

Secure E-mail
Netscape 7, 10, 16
Outlook 7, 10, 16
Windows Mail/Outlook Express 10, 16
Secure E-mail (Sikker e-mail) 10, 16
SECURITY CONTROLLER (SIKKERHEDSCONTROLLER) 6, 20
Security Platform
Create Owner 8
Features-skærmbillede 10
gendannelse af sikkerhedsplatform fra et sikkerhedskopieringsarkiv 12
ikon 7, 11, 20
Initialization 7, 12
Setting Tool-ikon 11
User initialization 11
User Initialization Wizard 12
Sikkerhedskopieringsfil med TPM-ejerens adgangskode 12
sikkerhedskryptering
formler 5
nøgler 5
skærmbillede
Backup 8
Initialization 7
Password and Authentication 9
Security Platform Features 10
User Initialization Wizard 9
Supervisor Password (Adgangskode for systemansvarlig) 19

T

TOSHIBA Hjælpeprogram til adgangskode 19
TPM Management on Local Computer (TPM-styring på lokal computer) 11, 12
TPM-ejer 9

U

User Password
Reset 21
User Policy
konfigurationsskærmbillede 19
User Policy (Brugerpolitik) 19

W

Windows Firewall 20

Memo

Kontroller, at adgangskoder eller nøgleord opbevares omhyggeligt (hvis du glemmer adgangskoderne) et sted, hvor andre ikke har adgang til dem (for at forhindre læk af fortrolige oplysninger). Opbevar dem ikke på steder, hvor uautoriseret personale har adgang (eks.: indsat på skriveborde).

Ejerens adgangskode:

Grundlæggende adgangskode til bruger:

Opbevaringssted til Emergency Recovery Token:

Adgangskode til nødgendannelsestoken:

Opbevaringssted til sikkerhedskopieringsfil:

Opbevaringssted til Password Reset Token:

Adgangskode til Reset Token Password:

Opbevaringssted til Personal Secret-fil:

Adgangskode til TPM-bruger

Windows®-brugernavn:

Adgangskode til TPM-bruger:

Windows® -brugernavn:

Adgangskode til TPM-bruger:

Windows®-brugernavn:

Adgangskode til TPM-bruger: