Guide d’installation V3.3.0

TPM (Trusted Platform Module)

computers.toshiba-europe.com

TOSHIBA

Leading Innovation

Table des matières

Copyright

Marques commerciales

Microsoft, Windows et Windows Vista sont des marques déposées de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays.

Toutes les autres marques et noms de produits sont des marques ou des marques déposées de la société de production.

1 Introduction

Votre ordinateur dispose d'un composant TPM (Trusted Platform Module) intégré. Pour l'exploiter, vous devez l'activer ou installer le logiciel Infineon Security Platform Tools. Le présent guide d'installation indique comment installer et configurer le composant TPM. Avant de l'utiliser, lisez attentivement le présent manuel d'installation.

1.1 Conventions

Le présent manuel applique les formats suivants pour décrire, identifier et mettre en évidence les termes et les procédures.

Icônes de sécurité

Ce manuel contient des consignes de sécurité que vous devez observer pour éviter tout risque de blessure, de dommages matériels ou de perte de données. Ces consignes ont été répertoriées en fonction de la gravité des risques encourus. Les icônes suivantes ont pour objectif d'attirer votre attention sur ces consignes :

Indique une situation de danger potentiel qui, si elle n'est pas évitée, peut provoquer un dommage matériel.

Fournit des informations importantes.

1.2 Vue d'ensemble du composant TPM

Le contrôleur de sécurité intégré TPM repose sur les spécifications du groupe TCG (Trusted Computing Group). TPM protège les données grâce à des clés de cryptage secrètes et non pas des formules de cryptage (algorithmes). En effet, lorsque le chiffrement dépend uniquement du logiciel, la clé de chiffrement risque d'être enregistrée dans le fichier ou d'être stockée dans la mémoire de l'ordinateur où elle peut être lue et déchiffrée. En stockant la clé de cryptage dans le composant TPM, les données sont protégées de façon plus sécurisée.

Dans la mesure où TPM utilise des spécifications de cryptage publiques et standardisées, vous pouvez mettre en place un environnement plus sécurisé en appliquant la solution de sécurité correspondante.

Pour plus de détails sur les spécifications du TCG, consultez leur site Web : http://www.trustedcomputinggroup.org/

Chiffrement, certificats et mots de passe

- *Le module TPM permet de créer et définir plusieurs clés de cryptage, certificats et mots de passe. Assurez-vous que les mots de passe ainsi définis sont stockés à un endroit approprié et que vous disposez d'une sauvegarde des clés de cryptage. Si ces paramètres sont perdus ou oubliés, les fichiers cryptés avec TPM ne peuvent plus être décryptés.*

TPM

- *Bien que TPM offre les fonctions de sécurité les plus récentes, il ne garantit pas une protection complète des données et du matériel. Veuillez tenir compte du fait que Toshiba n'est pas responsable en cas de panne ou de dommages pouvant résulter de l'utilisation de cette fonction.*

Si Microsoft® Windows® gère plusieurs utilisateurs, et si ces utilisateurs exécutent également TPM, ils doivent se connecter et s'inscrire individuellement sous Windows®.

2 Première utilisation de TPM

Le présent manuel contient uniquement des directives générales. Veuillez consulter l'aide de TPM après avoir installé Infineon TPM Professional Package.

Lorsque vous utilisez TPM pour la première fois, vous devez le configurer de la façon suivante. (Les paramètres 1 à 3 nécessitent d'ouvrir une session *Windows*® en tant qu'administrateur.)

1. Activez TPM.
2. Installez **Infineon TPM Professional Package**.
3. Inscrivez le propriétaire et les utilisateurs dans TPM.

2.1 Activation de TPM

Pour activer TPM, procédez comme suit au niveau du BIOS :

1. Mettez votre ordinateur sous tension en appuyant sur la touche **Esc**.
2. Un message s'affiche. Appuyez sur la touche **F1.**
3. La fenêtre de configuration du BIOS s'affiche.
4. Appuyez sur **Page vers le bas** pour passer à l'écran suivant.
5. Définissez le paramètre **TPM** de la section **SECURITY CONTROLLER** (Contrôleur de sécurité) sur **Enabled** (Activer).

Certains modèles peuvent présenter **Hide TPM** *en tant qu'option dans l'écran de configuration du BIOS. Si votre système présente cette option, elle doit être définie sur* **No** *avant de définir* **TPM** *sur* **Enabled***. Sinon, vous ne pourrez pas modifier* **TPM***.*

6. Appuyez sur la touche **End**, enregistrez les modifications des paramètres du BIOS et appuyez sur la touche **Y**.

La cohérence interne des données dans TPM n'est pas garantie lorsque l'ordinateur est en réparation ou maintenance. Avant de procéder à ce type d'opération, sauvegardez les fichiers du disque dur et les données TPM avec la fonction de sauvegarde. (Reportez-vous au chapitre8 - Restauration de TPM*.) Les fonctions de sécurité qui ont recours à TPM ne peuvent plus fonctionner correctement si les données TPM sont perdues. (Exemple : les fichiers cryptés avec TPM ne peuvent plus être ouverts.) Sinon, vous risquez de perdre des données.*

- *TPM est* **désactivé** *par défaut. En outre,* **TPM** *peut parfois être* **désactivé** *lorsque l'ordinateur doit être réparé par un technicien ou suite à une opération de maintenance. Vous devez activer TPM en le configurant de nouveau.*
- *Pour empêcher toute autre personne que l'administrateur ou les utilisateurs de l'ordinateur de modifier les paramètres du BIOS, il est fortement recommandé d'utiliser un mot de passe d'accès au BIOS, ainsi qu'un mot de passe de niveau Supervisor (administrateur). Veuillez vous reporter au manuel de l'utilisateur de l'ordinateur pour plus de détails sur ce type de mot de passe.*

2.2 Installation de Infineon TPM Professional Package

Installez **Infineon TPM Professional Package** à partir du dossier **`C:\TOSHIBA\Drivers\TPM Utility`**.

Le progiciel **Infineon TPM Professional Package** inclut les logiciels et les fonctions suivantes :

- Aide de la plate-forme de sécurité
- Security Platform Settings Tool
- Assistant d'initialisation de la plate-forme de sécurité
- Assistant d'initialisation utilisateur de la plate-forme de sécurité
- Assistant de migration de la plate-forme de sécurité
- Assistant de sauvegarde de la plate-forme de sécurité
- Assistant de réinitialisation du mot de passe de la plate-forme de sécurité
- Assistant d'importation PKCS #12 de la plate-forme de sécurité
- Lecteur de certificat de la plate-forme de sécurité et sélection de certificat
- Icône de notification dans la barre des tâches de la plate-forme de sécurité
- Services d'intégration de la plate-forme de sécurité
  - Intégration avec ® Outlook®
  - Intégration de Netscape®
  - Intégration de système de fichiers cryptés (EFS)
  - PSD (Personal Secure Drive)
  - Administration de stratégies
- Services de la plate-forme de sécurité
  - Fournisseur de service TCG TSS (pile logicielle TPM)
  - Service principal TSS
  - Bibliothèque de pilotes de périphérique TSS

2.3 Inscription des propriétaires et des utilisateurs dans TPM

1. Cliquez sur l'icône **Security Platform** (Plate-forme de sécurité) dans la barre d'état système et sélectionnez **Security Platform Initialization**.

2. TPM démarre et son écran s'affiche. Cliquez sur le bouton **Suivant**.
3. Dans l'écran **Initialization** (Initialisation), sélectionnez Initialize a new Security Platform (Initialiser une nouvelle plate-forme de sécurité). Cliquez sur le bouton **Suivant**.
4. Dans l'écran d'identification du propriétaire de la plate-forme, entrez le mot de passe dans les zones **Password** (Mot de passe) et **Confirm Password** (Confirmer), puis cliquez sur le bouton **Suivant**.
5. L'écran **Features** (Fonctionnalités) s'affiche. Sélectionnez la fonction Security Platform (Plate-forme de sécurité), puis cliquez sur le bouton **Suivant**. Consultez l'aide en ligne pour plus de détails sur les fonctions de la plate-forme de sécurité.

Il est fortement recommandé de sélectionner **Automatic Backup** *(Sauvegarde automatique). Sinon, les données utilisateur cryptées risquent d'être perdues en cas d'anomalie.*

6. Dans l'écran **Backup** (Sauvegarde), spécifiez l'emplacement de création et d'enregistrement du fichier de sauvegarde. Cliquez sur le bouton **Suivant**.
7. Dans l'écran **Emergency Recovery** (Restauration d'urgence), sélectionnez **Create a new Recovery Token** (Créer une nouvelle clé de restauration) puis spécifiez l'emplacement de création et d'enregistrement de la **clé de restauration d'urgence**.
8. Dans l'écran **Emergency Recovery** (Restauration d'urgence) dans la section d'**authentification de la clé de restauration d'urgence**, entrez le mot de passe dans les zones de saisie et de confirmation, puis cliquez sur le bouton **Suivant**.

Il est fortement recommandé de créer une clé de restauration d'urgence, de façon à ce que les informations de TPM et les données utilisateur se rapportant à TPM restent en sécurité en cas de problèmes système graves. Sinon, vous risquez de perdre des données.

9. Dans l'écran **Password Reset** (Mot de passe de réinitialisation), sélectionnez **Create a new Recovery Token** (Créer une nouvelle clé de restauration) puis spécifiez l'emplacement de création et d'**enregistrement de la clé de réinitialisation du mot de passe**.

10. Dans l'écran **Password Reset** (Réinitialisation du mot de passe) dans la section d'**authentification de la clé de réinitialisation du mot de passe**, entrez le mot de passe dans les zones de saisie et de confirmation, puis cliquez sur le bouton **Suivant**.

Il est fortement recommandé de créer et d'enregistrer la **clé de réinitialisation du mot de passe** *sur un support externe, tel qu'une disquette, disponible en cas de panne d'ordinateur. Vous devez stocker ce disque à un emplacement sûr en vue de son utilisation ultérieure.*

- Lorsque plusieurs ordinateurs utilisent TPM, ces derniers utilisent des jetons différents qui doivent être stockés séparément.
- Le jeton de restauration d'un propriétaire TPM inscrit* ne peut pas être recréé. De façon à prévenir les pertes, il est fortement recommandé de créer plusieurs copies du jeton, comme indiqué dans la remarque ci-dessus.

  *Il est possible de dupliquer le nom du propriétaire TPM en initialisant TPM à partir du menu du BIOS et en enregistrant un nouveau propriétaire. Cependant, dans la mesure où le cryptage dépend d'un jeton unique, les fichiers cryptés sous l'ancien nom ne sont pas accessibles.
- Si le jeton tombe aux mains d'une personne malveillante, cette dernière peut accéder aux données cryptées. Il est par conséquent fortement recommandé de choisir soigneusement un emplacement de stockage pour les jetons et les mots de passe.

  Reportez-vous au chapitre8 - *Restauration de TPM*.

11. Le récapitulatif s'affiche. Consultez-le et cliquez sur le bouton **Suivant**.
12. L'affichage du message **Wizard completed successfully** (L'Assistant s'est terminé avec succès) peut prendre plusieurs minutes. Ensuite, cliquez sur la case à cocher **Start Security Platform User Initialization Wizard** (Lancer l'Assistant d'initialisation de la plate-forme de sécurité de l'utilisateur), puis cliquez sur le bouton **Terminer**.
13. Dans l'écran **User Initialization Wizard** (Assistant d'initialisation utilisateur), cliquez sur le bouton **Suivant**.
14. Dans l'écran d'authentification de l'utilisateur, **Basic User Password** (Mot de passe de la clé utilisateur de bas), tapez le mot de passe dans les zones **Password** (Mot de passe) et **Confirm Password** (Confirmer), puis cliquez sur le bouton **Suivant**.
15. Dans l'écran **Basic User Password Reset** (Réinitialisation du mot utilisateur de base), assurez-vous que l'option **Enable the resetting of my Basic User Password in case of an emergency** (Rénitialiser mon mot utilisateur de base en cas d'urgence) est activée. Spécifiez l'emplacement de création et d'enregistrement du fichier **Personal Secret**.

Veillez à enregistrer ce fichier à un emplacement sûr. Il est indispensable pour réinitialiser le mot de passe utilisateur de base.

16. L'écran **Password and Authentication** (Mot de passe et authentification) s'affiche. Confirmez le contenu affiché et cliquez sur le bouton **Suivant**.

L'écran des fonctionnalités de la plate-forme de sécurité peut ne pas s'afficher immédiatement.

17. Assurez-vous que les fonctions voulues sont sélectionnées dans l'écran **Security Platform Features** (Fonctions de la plate-forme de sécurité) et cliquez sur le bouton **Suivant**.

- *Pour utiliser la fonction* **Secure E-mail** *(Messagerie sécurisée), il est nécessaire de configurer la section* **Mail Software** *(Logiciel de messagerie). Reportez-vous au chapitre 4,* Adresse e-mail sécurisée*, pour plus de détails sur la sécurisation de la messagerie.*
- *La fonction* **File and Folder encryption (EFS)** *(Chiffrement de dossiers et de fichiers) n'est pas disponible sous Windows® Vista Edition familiale.*
- *Le disque dur doit être au format NTFS pour bénéficier de la fonction* **EFS***.*

Les configurations définies dans cette section peuvent également être modifiées après la configuration.

18. Si l'option **Secure E-mail** est sélectionnée dans l'écran **Security Platform Features** (Fonctions de la plate-forme de sécurité), l'écran suivant s'affiche. Cliquez sur le bouton **Suivant**.

Cliquez sur le bouton **Outlook®***,* **Windows Mail/Outlook Express** *ou* **Netscape®** *de cet écran pour afficher l'aide relative aux paramètres de* **messagerie sécurisée** *pour les différents* **logiciels de messagerie***. (Cette aide reste accessible après la fermeture de l'Assistant.)*

19. Le message de publication du **certificat de cryptage** s'affiche dans l'écran des fonctionnalités de la plate-forme de sécurité. Sélectionnez le certificat à émettre et cliquez sur le bouton **Suivant**. Normalement, il suffit de cliquer sur le bouton **Create** (Créer) pour créer et sélectionner le certificat.

La valeur par défaut de **Maximum Basic User Password age** *(Age maximum du mot de passe utilisateur de base) est défini sur* **Disabled** *(Désactivé). Pour modifier cette option, sélectionnez* **User** *(Utilisateur) dans la section* **Security Policy** *(Stratégie de sécurité).*

20. Si l'option **Personal Secure Drive (PSD)** (Lecteur personnel sécurisé) est sélectionnée dans l'écran **Security Platform Features** (Fonctions de la plate-forme de sécurité), l'écran suivant s'affiche. Dans cet écran, sélectionnez le lecteur à associer au PSD, puis entrez le nom de ce lecteur et cliquez sur le bouton **Suivant**. Reportez-vous au chapitre 3, *PSD (Personal Secure Drive)*, pour plus de détails sur les lecteurs PSD.

21. Dans l'écran **Security Platform Features** (Fonctions de la plate-forme de sécurité), entrez le volume de l'espace de stockage à associer au lecteur PSD, puis sélectionner le lecteur et cliquez sur le bouton **Suivant**.
22. Le paramètre de confirmation s'affiche, cliquez sur le bouton **Suivant**.

- *Il est fortement recommandé de spécifier le disque dur intégré (normalement le lecteur C) comme lecteur PSD.*
- *L'espace disponible sur le lecteur spécifié ci-dessus ne doit pas dépasser l'espace spécifié avec l'option* **My Personal Secure Drive will have [XX] MB of storage space** *(Mon lecteur PSD dispose de xx Mo d'espace de stockage).*

23. Au bout d'un certain temps, le message **Wizard completed** (Assistant terminé) s'affiche. Cliquez sur **Terminer**.

Si Windows® gère plusieurs utilisateurs, et si ces utilisateurs exécutent également TPM, ces utilisateurs doivent se connecter et s'inscrire individuellement sous Windows®. Après vous être connecté à Windows® pour procéder à l'inscription d'un utilisateur, cliquez sur l'icône **Plate-forme de sécurité** *dans la barre d'état système et sélectionnez* **Security Platform User initialization** *(Initialisation de la plate-forme de sécurité utilisateur).*

Lorsque vous modifiez la configuration, cliquez sur l'icône **Security Platform Setting Tool** dans la barre d'état système et apportez les modifications voulues dans l'écran de configuration.

- *initialisation*
  - *Lorsque vous utilisez le progiciel TPM Professional, il n'est pas nécessaire d'initialiser TPM au préalable dans la section* **Gestion TPM sur l'ordinateur local** *de Windows Vista®.*
  - *Lorsque vous initialisez la fonctionnalité TPM avec le progiciel TPM Professional, il n'est pas nécessaire d'initialiser TPM au préalable dans la section* **Gestion TPM sur l'ordinateur local** *de Windows Vista®.*
- *Méthode d'initialisation*

Lorsque vous utilisez le progiciel professionnel V3.0 après avoir initialisé TPM avec la fonctionnalité **Configuration TPM** *de Windows Vista®, l'initialisation de la plate-forme se produit de la façon suivante :*

1. *Lorsque vous avez installé le progiciel V3.0, le message* **`Initialized other OS`** *(Autre SE initialisé) d'affiche près de l'icône* **TPM** *dans la barre des tâches.*

   ** Il ne s'agit pas d'un dysfonctionnement de TPM.*
2. *Si vous avez exécuté l'***outil de configuration de la plate-forme de sécurité Infineon** *au cours de l'étape 1, la section* **Security Platform State** (Etat de la plate-forme de sécurité), **Owner:** *(Propriétaire) de l'onglet* **Info** *affiche* **`Initialized (Failure Mode 2)`** *(Initialisé - mode d'échec 2).*

   ** Il ne s'agit pas d'une erreur. Ceci signifie que l'initialisation de la plate-forme ne s'est pas terminée.*
3. *Lorsque vous exécutez l'***Assistant d'initialisation utilisateur** *de la plate-forme de sécurité, l'écran* **Initialization** *(Initialisation) s'affiche. Même si l'option* **Security Platform restoration form a Backup Archive** *(Restauration de la plate-forme de sécurité à partir d'une archive de sauvegarde) a été activée, sélectionnez* **Security Platform Initialization** *(Initialisation de la plate-forme de sécurité).*
4. *Dans l'écran suivant, dans la section* **Initialize Security Platform** *(Initialiser la plate-forme de sécurité), entrez le mot de passe dans la section* **Gestion TPM sur l'ordinateur local** *de Windows Vista®. Pendant ce temps, vous ne pouvez pas utiliser le fichier de sauvegarde du mot de passe propriétaire TPM enregistré dans la section* **Gestion TPM sur l'ordinateur local**.
5. *Lorsque le mot de passe est modifié à l'aide du progiciel Infineon TPM Professional, vous ne pouvez pas utiliser le* **fichier de sauvegarde du mot de passe propriétaire TPM** *créé dans la section* **Gestion TPM sur l'ordinateur local** *de Windows Vista®.*

3 PSD (Personal Secure Drive)

L'option **Personal Secure Drive** crée un espace pour le stockage des informations (fichiers) et des fichiers de données cryptés dans le lecteur virtuel. Les fichiers ne sont pas simplement cryptés et stockés sur le disque dur. En effet, ils sont protégés par TPM, dont le niveau de sécurité est supérieur à celui qui est offert par les chiffrements purement logiciels. La taille minimum du PSD est de 10 Mo. Sa taille maximum dépend du système de fichier d'origine. Reportez-vous à l'aide en ligne pour plus de détails.

3.1 Avantages du lecteur PSD

- Chiffrement du lecteur virtuel avec la clé AES (Advanced Encryption Standard) sûre et sécurisée.
- Algorithme de RSA de génération de clé cryptée.
- Chiffrement et déchiffrement automatique et transparent des données de sécurité
- Les fichiers peuvent être protégés facilement.
- Opération unique : le lecteur PSD fonctionne de la même façon qu'un lecteur *Windows*® standard.
- Procédure simple de gestion et de configuration avec des Assistants.

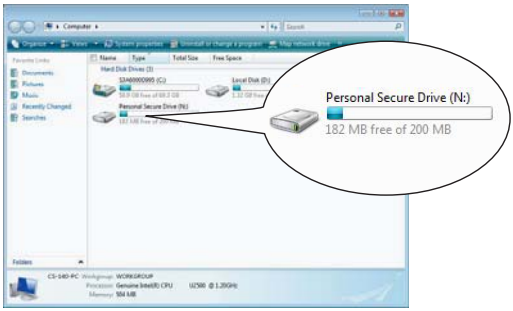
3.2 Lecteur PSD (Personal Secure Drive) - Opérations de base

1. Lorsque PSD est sélectionné dans la section **Security Platform Features** (Fonctionnalités de la plate-forme de sécurité), cliquez sur l'icône **Plate-forme de sécurité** dans la barre des tâches après vous être connecté à Windows et sélectionnez **Personal Secure Drive** - **Load**.

*Cliquez sur l'icône **Plate-forme de sécurité** dans la barre d'état système pour sélectionner **Personal Secure Drive - Load, Unload (PSD - Charger/Décharger)** ou **Load at Logon (Charger à l'ouverture de session).***

2. L'authentification utilisateur de la plate-forme de sécurité Infineon s'affiche. Entrez le mot de passe TPM. Le lecteur virtuel PSD est détecté si le mot de passe entré est correct.

3. Vous trouverez ci-dessous un exemple d'écran présentant le PSD détecté dans l'Explorateur *Windows*®.



Dans cet écran, bien que le lecteur PSD ait été détecté en tant que lecteur **[N:]**, sous le nom **Personal Secure Drive**, il est possible de modifier ces paramètres dans la section **User Settings** (Paramètres utilisateur) de l'outil de configuration des paramètres de la **plate-forme de sécurité Infineon**.

- *Dans la mesure où les fichiers du PSD ne sont pas sauvegardés avec la fonction* **Backup** (Sauvegarder) de l'**outil de configuration de la plate-forme de sécurité Infineon**, *vous devez copier manuellement les fichiers du PSD sur un support externe avec l'Explorateur pour vous prémunir contre les risques de pertes de données.*
- *Les données du point de restauration du système* définis par la fonction de restauration de Windows® sont supprimés après que le mot de passe TPM est entré pendant le démarrage de Windows, le PSD est monté et le lecteur virtuel attribué. Il est fortement recommandé d'utiliser l'une des méthodes suivantes pour enregistrer les données du point de restauration.*
  - *N'utilisez pas la fonction PSD et utilisez uniquement la fonction de cryptage des fichiers via EFS.*
  - *Désactivez temporairement la fonction PSD avant de modifier l'environnement de Windows.*

  Désactivez la fonction PSD -> Définissez le point de restauration -> Modifiez le système -> Assurez-vous que Windows démarre correctement -> Rétablissez l'état précédent de la fonction PSD.

  ** Veuillez consulter l'aide de Windows® pour plus de détails sur le point de restauration.*

- *Le PSD doit être défini pour chaque utilisateur TPM. Par exemple, si vous disposez de deux utilisateurs TPM inscrits, 'A' et 'B', B ne peut pas voir le contenu PSD de A.*
- *Dans la mesure où certaines sections du PSD sont exploitées par le système de fichiers de Windows, la capacité disponible du PSD est inférieure à la valeur initiale lors de la configuration. Lorsqu'une valeur minimale d'environ 10 Mo est consommée et que la capacité du PSD est accrue, les zones utilisées par le système de fichiers NTFS augmentent également.*

  Lorsque vous devez utiliser toute la capacité requise, vous devez spécifier une capacité supérieure pendant la configuration PSD.

  (lorsque vous devez utiliser environ 200 Mo, vous devez spécifier 220 Mo en tant que capacité du PSD pendant la configuration.)

4 Adresse e-mail sécurisée

Dans cette plate-forme de sécurité, l'ID numérique utilisée pour les e-mails est protégée par TPM contre les pertes et les vols.

Les logiciels de messagerie compatibles incluent Outlook®*, messagerie Windows/Outlook Express* et Netscape®*.

* La disponibilité de cette fonction dépend de la version du logiciel.

4.1 Configuration

1. Vous devez acquérir un ID numérique pour les messages sécurisés auprès de la CA (Commercial Certificate Authority). Consultez l'aide de TPM pour plus de détails sur CA.
2. Installez l'ID numérique sur l'ordinateur conformément aux méthodes d'installation et d'utilisation spécifiées par la CA. A ce stade, assurez-vous que l'ID numérique est reliée à TPM par un CSP (Cryptographic Service Provider - Fournisseur de services de cryptage).
3. Configurez la messagerie sécurisée à partir de votre logiciel de messagerie. Consultez le manuel pour prendre connaissance des procédures à suivre en fonction du logiciel utilisé et à l'aide de Infineon Security Platform pour plus de détails.

Définissez le paramètre **Secure E-mail** *(Messagerie sécurisée) dans la section Security Platform Features lorsque vous inscrivez un utilisateur dans TPM (étape 2.3) s'il n'a pas déjà été attribué (*1, *2).*

*1 Consultez l'aide pour plus de détails sur la messagerie et TPM

1) Double-cliquez sur l'icône **TPM** dans la barre d'état système.
2) Sélectionnez l'onglet **Info**.
3) Cliquez sur le bouton « **Aide** ».
4) Tapez les mots clés à rechercher dans l'onglet **Search**. (Exemple : **E-Mail**)

*2 Activation de la fonction E-mail dans la section User Settings (Paramètres utilisateur)

1) Double-cliquez sur l'icône **TPM** dans la barre d'état système.
2) Sélectionnez l'onglet **User Settings** (Paramètres utilisateur).
3) Cliquez sur le bouton **Configure**.
4) Sélectionnez l'option **Secure E-mail** (Messagerie sécurisée) et cliquez sur le bouton **Suivant**.

5 EFS (Encrypting File System) Extension

Lorsque l'option File and Folder **encryption** (Chiffrement des fichiers et dossiers) est sélectionnée à l'étape 2.3, la fonction EFS du système d'exploitation est étendue et le système devient plus sûr, car la clé de cryptage du fichier traité par EFS est protégée par TPM.

Les opérations requises pour le cryptage/déchiffrement des fichiers sont très similaires.

La seule différence étant que lorsque les fichiers cryptés par EFS sont accessibles après la connexion à Windows®, le mot de passe TPM de l'utilisateur connecté doit être entré.

- *Dans l'environnement suivant, lorsque les fichiers créés dans la section* **Basic User Key and Other Folders (Clé utilisateur de base et autres dossiers)** *sont cryptés avec EFS, le logiciel TPM ne se démarre pas normalement et les données cryptées ne peuvent pas être décryptées.*
  - *TPM est installé*
  - *La plate-forme a terminé sa procédure d'initialisation*
  - *La fonction EFS est sélectionnée pendant l'initialisation utilisateur*

  Pendant le statut d'initialisation, les fichiers figurant dans la section **Basic User Key and Other Folders** *(Clé utilisateur de base et autres dossiers) disposent d'attributs système pour empêcher leur cryptage. Ne changez pas les attributs de fichier dans les dossiers correspondants.*

  ** Lors de la configuration initiale de Windows, les dossiers suivants sont masqués.*

  Basic User Key and Other Folders (Clé utilisateur de base et autres dossiers)

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

- *Les archives, sauvegardes et clés cryptées ne peuvent pas être décryptées en cas d'urgence.*

  Lorsque des clés de réinitialisation du mot de passe et des fichiers masqués sont cryptés, le mot de passe ne peut pas être réinitialisé.

  Ne cryptez pas les fichiers et les dossiers suivants.

  Fichier de sauvegarde automatique

  nom de fichier par défaut: SPSystemBackup.xml

  mot de passe par défaut: non spécifié (*)

  Dossier de stockage automatique des sauvegardes

  Nom de dossier (fixe) : le fichier SPSystemBackup.xml est créé en tant que sous-dossier du dossier en cours de création)

  [clé de restauration d'urgence]

  Nom de fichier par défaut : SPEmRecToken.xml

  Mot de passe par défaut : Removable Media (FD, mémoire USB, etc.)

  Clé de réinitialisation du mot de passe

  Nom de fichier par défaut : SPPwdResetToken.xml

  Mot de passe par défaut : Removable Media (FD, mémoire USB, etc.)

  Réinitialisation du mot de passe utilisateur de base

  Nom de fichier par défaut : SPPwdResetSecret.xml

  Mot de passe par défaut : Removable Media (FD, mémoire USB, etc.)

  [Archive de sauvegarde]

  Nom de fichier par défaut : SpBackupArchive.xml

  Mot de passe par défaut : non spécifié (*)

  [Archive de sauvegarde PSD]

  Nom de fichier par défaut: SpPSDBackup.fsb

  Mot de passe par défaut : non spécifié (*)

  (*) Lorsque vous cliquez sur **Reference** *(Référence), le dossier « User folder\Documents\Security Platform » s'ouvre.*

- *Lorsque vous utilisez le cryptage EFS, il est fortement recommandé de se familiariser avec les informations relatives à EFS dans l'aide de Windows®. Ceci permet d'éviter les problèmes de déchiffrement des fichiers suite à une modification non voulue de la clé de cryptage EFS ou à la perte de cette dernière.*

6 Utilitaire Mot de passe TOSHIBA

Avec l'utilitaire Mot de passe TOSHIBA, vous pouvez configurer l'ordinateur de façon à ce que seules les personnes disposant d'autorisations de niveau Supervisor puissent accéder aux paramètres relatifs à TPM dans le programme de configuration du BIOS.

Une fois cette configuration définie, les utilisateurs ne disposant pas d'un accès Supervisor ne peuvent plus modifier les paramètres TPM au niveau du BIOS (options de la zone **Security Controller** - Contrôleur de sécurité).

1. Procédez comme suit pour démarrer l'utilitaire Mot de passe TOSHIBA.

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

2. Enregistrez le mot de passe Supervisor dans l'onglet Supervisor Password (Mot de passe responsable).
3. Ouvrez l'écran User Policy (Stratégie utilisateur) à partir de l'onglet **Responsable Password**.
4. Dans la zone **TPM**, désactivez les éléments qui sont réservés exclusivement aux détenteurs d'un mot de passe Supervisor.
5. Appuyez sur le bouton **Set** (Définir) et après avoir procédé à l'authentification, enregistrez la stratégie utilisateur ainsi modifiée.
6. Quittez l'utilitaire Mot de passe TOSHIBA

7 Migration de l'environnement TPM et mise au rebut de l'ordinateur

7.1 Migration

Cliquez sur l'icône **Security Platform** (Plate-forme de sécurité) dans la barre des tâches et sélectionnez **Manage Security Platform** (Gérer la plate-forme de sécurité). Dans la fenêtre de l'**outil de configuration de la plate-forme de sécurité Infineon**, cliquez sur l'onglet **Migration**. Dans l'onglet **Migration**, cliquez sur le bouton **Learn more...** (Plus de détails) pour afficher les détails de l'opération de migration. (Cette opération doit s'appliquer à la plate-forme source et à la plate-forme de destination.) Veuillez suivre les instructions qui s'affichent à l'écran.

Seules les données TPM sont migrées au cours de ce processus. Vous pouvez utiliser les opérations standard de déplacement de fichiers pour les données du lecteur PSD et les fichiers cryptés avec EFS.

- *Vous devez également installer* **Infineon TPM Professional Package** *sur la plate-forme de destination.*
- *Lorsque le pare-feu de Windows® est activé, il n'est pas possible de procéder à la migration par l'intermédiaire d'une connexion réseau. Vous pouvez désactiver le pare-feu Windows® dans la section* **Centre de sécurité** *du* **Panneau de configuration**.

7.2 Mise au rebut de l'ordinateur

Lorsque vous mettez l'ordinateur au rebut, veuillez exécuter les deux processus suivants pour prévenir toute perte d'informations confidentielles. Procédez de la même façon lorsque l'ordinateur change de propriétaire.

1. Désinstallez **Infineon TPM Professional Package**, supprimez l'archive de restauration et le **jeton de restauration d'urgence de l'archive**. En outre, veuillez supprimer toutes les données du disque dur.
2. Etape 1: Ouvrez l'écran de configuration **BIOS Setup**. (Reportez-vous au chapitre2 - *Première utilisation de TPM*.)

   Etape 2: Etape : Placez le curseur sur l'option **Clear TPM Owner** (Supprimer le propriétaire TPM) dans la section **SECURITY CONTROLLER** (Contrôleur de sécurité) et appuyez sur la barre d'espacement ou de retour arrière. Au cours de cette opération, toutes les données TPM sont détruites et la fonction TPM est désactivée.

   Etape 3: Un message s'affiche. Appuyez sur les touches **Y**, **E**, **S**, puis sur **Enter**.

Une fois les données TPM internes détruites, les fichiers ne peuvent plus être lus.

8 Restauration de TPM

8.1 Processus de restauration d'urgence - Vue d'ensemble

Le processus de restauration d'urgence s'applique :

- lors de la modification de TPM suite à des problèmes TPM ;
- lorsque la carte mère portant le composant TPM présente un défaut et lorsque la carte mère a été changée ;
- lorsque TPM a été effacé accidentellement ou pour toute autre raison.

Consultez la section *Restore Emergency Recovery Data Step by Step* (Restauration d'urgence étape par étape) de l'aide en ligne pour plus de détails.

- *Il est conseillé d'imprimer cette section de l'aide avant de commencer.*
- *Cette section porte sur la restauration du contenu TPM et non pas sur la restauration des données relatives à TPM, telles que les fichiers cryptés avec EFS ou les fichiers présents sur le lecteur PSD. Concernant les fichiers du disque dur intégré, il est fortement recommandé d'effectuer des sauvegardes distinctes, stockées à un endroit sûr.*

8.2 Réinitialisation du mot de passe utilisateur

Cette fonction peut être utilisée lorsque l'utilisateur de la plate-forme de sécurité Infineon oublie son mot de passe de base ou en cas de problème au niveau du dispositif d'authentification de l'utilisateur. Si le mot de passe ne peut pas être réinitialisé, l'utilisateur ne peut pas exécuter les fonctions de la plate-forme de sécurité. Cette opération peut entraîner la perte de données secrètes.

Consultez la section *Basic User Password Reset* (Réinitialisation du mot de passe utilisateur de base) de l'aide pour plus de détails.

8.3 Restauration du lecteur PSD

Les données PSD peuvent être restaurées en cas de perte du certificat, à l'aide de la fonctionnalité de restauration PSD.

Consultez la section *Personal Secure Drive Recovery* (Restauration du lecteur PSD) de l'aide en ligne pour plus de détails.

Index

R

S

U

Mémo

Assurez-vous que les mots de passe ou les mots clés sont stockés avec précautions (au cas où ces mots de passe seraient oubliés) à un endroit inaccessible à des tiers mal intentionnés (pour prévenir tout risque de fuite d'informations importantes). Ne stockez pas ces données à des emplacements d'accès facile(par exemple : collé sur un dessus de table).

Mot de passe du propriétaire:

Mot de passe utilisateur de base:

Emplacement de stockage de la clé de restauration d'urgence:

Mot de passe du jeton de restauration d'urgence:

Enmplacement de stockage du fichier de restauration :

Emplacement de stockage de la clé de réinitialisation du mot de passe :

Mot de passe de la clé de réinitialisation du mot de passe :

Emplacement de stockage du fichier de secret personnel :

Mot de passe utilisateur TPM

Nom d'utilisateur Windows® :

Mot de passe utilisateur TPM

Nom d'utilisateur Windows® :

Mot de passe utilisateur TPM

Nom d'utilisateur Windows® :

Mot de passe utilisateur TPM