



Trusted Platform Module (TPM)

Activation Guide

Guide d'activation

Aktivierungshandbuch

Windows XP Tablet PC Edition 2005

© 2007 Motion Computing, Inc. All rights reserved.

This document contains information protected by copyright. No part of this document may be reproduced in any form without written consent from Motion.

The information in this document is provided "as is" and is subject to change without notice. Motion is not liable for errors or omissions in this document.

Motion, Motion Computing, Speak Anywhere, and View Anywhere are trademarks or registered trademarks of Motion Computing, Inc. in the U.S.A. and other countries.

Acrobat is a registered trademark of Adobe Systems Incorporated.

Atheros, the Atheros logo, Super G, Super A/G, Wake-on-Wireless, and Wake-on-Theft are registered trademarks of Atheros Communications, Inc.

AuthenTec is a registered trademark of AuthenTec, Inc.

BLUETOOTH is a registered trademark owned by the Bluetooth SIG, Inc., U.S.A. and licensed to Motion Computing, Inc.

Intel, Intel Inside, the Intel Inside logo, Pentium, Centrino, and PROSet are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Knowles and IntelliSonic are trademarks or registered trademarks of Knowles Acoustics, Inc.

Microsoft Windows, Windows XP, Windows XP Tablet PC Edition, and Windows Journal are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

OmniPass is a trademark of Softex, Inc.

Realtek is a trademark of Realtek Semiconductor Corporation.

SigmaTel is a registered trademark and Universal Jacks is a trademark of SigmaTel Corporation.

Wi-Fi is a registered trademark of the Wi-Fi Alliance.

Motion Computing, Inc. has made every effort to identify trademarked properties and owners on this page. All brands and product names used in this document are for identification purposes only and may be trademarks or registered trademarks of their respective companies.

The warranties for Motion products are set forth in the express limited warranty statements accompanying such products. Nothing in this document constitutes an additional warranty.

The Motion Computing products and services may be covered by one or more patent-protected inventions. Additional patents may also be pending. For more information, see

www.motioncomputing.com/info/patents.asp.

Introduction

With the Infineon® Security Platform Tools and the built-in Trusted Computing Group compliant TPM (Trusted Platform Module), you can create and manage digital certificates for user and platform authentication. These features are most commonly used by enterprises and must be set up by an administrator before the security features can be used.

You can also use TPM as an authentication device within Motion™ OmniPass™. For example, you can use file and folder encryption, password replacement, and user management functions.

If you use the TPM and OmniPass security features, you should create a backup archive. A backup archive is the only way to recover your data if you have a hardware failure or if TPM is cleared. Back up your security data routinely, and store it in a secure location, such as on removable media that is stored in a secure environment.

You cannot recover any TPM-protected data if you do not have a backup archive. For more information, see the Infineon Security Platform Help after you have installed the TPM package.

Activation overview


The TPM activation process consists of the following:

- Enabling the TPM hardware
- Installing the Infineon Security Package
- Initializing the Security Platform
- Initializing a user
- Enrolling TPM in Motion OmniPass
- Setting up the authentication rules

Enabling the TPM hardware

Before you can use TPM, you must use the BIOS to enable the TPM hardware.

To enable the TPM hardware

1. Start the Tablet PC.
2. When the Motion Computing splash screen appears, quickly press the Rotate button (). If you miss the splash screen, restart the computer and try again.
3. In the PhoenixBIOS Set Up Utility, tap **Security** on the menu bar.
4. For TPM, tap the word **Disabled** to change it to **Enabled**.

To prevent unauthorized users from tampering with TPM settings and possibly deleting sensitive data, you should set a supervisor password in the BIOS. For more information, see the Tablet PC User Guide.

5. Tap **F10 Save and Exit**.

Installing the Infineon Security Package

The Infineon Security Package Software is required to use the TPM features on your Tablet PC. The setup program is preloaded on the hard disk drive of your Tablet PC. To install the Infineon Security Package Software, you must have Administrator privileges.

To install the Infineon Security Package

1. Go to C:\WINDOWS\Motion\Infineon_TPM.
2. Run setup.exe.
3. Follow the instructions in the setup program.


You must restart your computer after you install the TPM package.

Initializing the Security Platform

After you install the Infineon Security Package Software, you must initialize the Security Platform. You must have Administrator privileges to initialize the Security Platform.

Tap the **Help** button on any screen for more information about that screen.

To initialize the Security Platform

1. In the notification area, double-tap the TPM icon ()
2. In the Infineon Security Platform Initialization Wizard, tap **Next**. If the wizard does not appear, the platform may already be initialized.
3. Select **Security Platform initialization**. For information about restoring a Security Platform from a Backup Archive, see the Infineon Security Platform Help.
4. Enter the Security Platform Owner password.

The platform owner password is similar to the administrator password for a computer; however, the Security Platform can have only one owner.

5. Select the features you want to configure.


We strongly recommend that you use Automatic Backup. If you create a Backup Archive, you should keep it in a secure location, such as on removable media that you can detach and store in a secure environment.

6. Follow the instructions in the setup program according to the options you selected.
7. After you have confirmed the Security Platform settings, tap **Next**. On the Summary page, click **Finish**.

Initializing a user

To use TPM on a Tablet PC, you must be designated as a user. You can use the Infineon Security Platform User Initialization Wizard to initialize your user account.

To initialize a user

1. In the notification area, double-tap the TPM icon ()
2. In the Infineon Security Platform User Initialization Wizard, tap **Next**. If the wizard does not appear, the current user may already be initialized.
3. Create the Basic User Password.
4. Confirm the settings and tap **Next**.
5. Select the Security Platform features that you want to configure.
 - **Secure email**. Uses digital certificates to secure your email.
 - **File and folder encryption with Encrypting File System (EFS)**. Uses TPM-protected encryption keys to secure files and folders.
 - **File and folder encryption with Personal Secure Drive (PSD)**. Uses an encrypted partition on your hard disk drive to secure files and folders.
6. Follow the instructions in the setup program according to the options you selected.
7. On the Summary page, click **Finish**.

To learn more about the Infineon Security Platform features, see the Infineon Security Platform Help.

Enrolling TPM in Motion OmniPass

To use TPM as an authentication device, you must enroll the TPM device in OmniPass. If you are not already enrolled as an OmniPass user, you can use this procedure to add yourself as a new user.

To enroll TPM in Motion OmniPass

1. Open Motion Dashboard to the Security panel and tap **Motion OmniPass**.
2. In the Motion OmniPass window, tap **Run Enrollment Wizard**.

If you are already enrolled as an OmniPass user and want to enroll TPM in OmniPass, select **Modify a User's Device Enrollment**.
3. Enter your Windows account information and then tap **Next**.
4. For Select Authentication Device, select **TPM** and then tap **Next**.
5. In the Infineon Security Platform User Authentication window, enter the Basic User Password and select **Remember password for all applications**.
6. If you are finished enrolling devices, select **I am done enrolling security authentication devices** and tap **Next**.
7. Select your notification preferences and tap **Next**.
8. On the Backup User Profile screen, tap **Next** and select a location in which to save the user profile. Enter a password for the user profile.
9. On the Congratulations screen, tap **Done**.

If you are prompted to log on as the new OmniPass user, tap **Yes**.

Setting up the authentication rules

The TPM can be configured as a required authentication device within OmniPass.

To set up authentication rules

1. Open Motion Dashboard to the Security panel and tap **Motion OmniPass**.
2. In the Motion OmniPass window, tap **Change Your OmniPass Settings**.
3. Tap **Set user authentication rules and policies**.
4. If prompted, enter your authentication information.
5. On the Set Authentication Rules page, select the functions which you want TPM authentication to be required.

For example, if you selected File and Folder Encryption and Decryption, TPM is required to decrypt any file that was encrypted on that Tablet PC.

For more information, tap the **More Info** button.



Trusted Platform Module (TPM)

Guide d'activation

Windows XP Tablet PC Edition 2005

© 2007 Motion Computing, Inc. Tous droits réservés.

Les informations du présent document sont protégées par des droits d'auteur. Aucun élément du présent document ne peut être copié ou reproduit sous quelque forme que ce soit sans l'accord écrit de Motion

Les informations dans ce document sont fournies « en l'état » et peuvent faire l'objet de modifications sans préavis. Motion ne peut être tenu responsable des erreurs ou omissions dans ce document.

Motion, Motion Computing, Speak Anywhere et View Anywhere sont des marques commerciales ou des marques déposées de la société Motion Computing, Inc. aux Etats-Unis et dans d'autres pays.

Acrobat est une marque déposée de la société Adobe Systems Incorporated.

Atheros, le logo Atheros, Super G, Super A/G, Wake-on-Wireless et Wake-on-Theft sont des marques déposées de la société Atheros Communications, Inc.

AuthenTec est une marque déposée de la société AuthenTec, Inc.

BLUETOOTH est une marque déposée du groupe Bluetooth SIG, Inc., Etats-Unis, et utilisée sous licence par Motion Computing, Inc.

Intel, Intel Inside, le logo Intel Inside, Pentium, Centrino et PROSet sont des marques commerciales ou des marques déposés de la société Intel Corporation ou de ses filiales aux Etats-Unis et dans les autres pays.

Knowles et IntelliSonic sont des marques commerciales ou des marques déposées de la société Knowles Acoustics, Inc.

Microsoft Windows, Windows XP, Windows XP Tablet PC Edition et Windows Journal sont des marques commerciales ou des marques déposées de la société Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays.

OmniPass est une marque commerciale de la société Softex, Inc.

Realtek est une marque commerciale de la société Realtek Semiconductor Corporation.

SigmaTel est une marque déposée et Universal Jacks est une marque commerciale de la société SigmaTel Corporation.

Wi-Fi est une marque déposée de la société Wi-Fi Alliance.

Motion Computing, Inc. a fait en sorte d'identifier les appartenances et les propriétaires des marques déposées et commerciales. Les marques et les noms de produits mentionnés dans le présent document sont désignés exclusivement à des fins d'identification et peuvent être des marques commerciales ou déposées appartenant à leurs propriétaires respectifs.

Les garanties relatives aux produits, consenties par Motion, sont spécifiées dans les clauses de garantie limitée accompagnant les produits concernés. Aucun élément du présent document ne constitue une garantie complémentaire.

Les produits et services de Motion Computing peuvent être protégés par une ou plusieurs inventions brevetées. D'autres brevets peuvent être en cours de certification. Pour plus d'informations, consultez le site www.motioncomputing.com/info/patents.asp.

Introduction

Avec les outils de plate-forme de sécurité Infineon® et le module TPM (Trusted Platform Module) intégré agréé Trusted Computing Group, vous pouvez créer et gérer des certificats numériques pour l'authentification des utilisateurs et des plates-formes. Ces fonctions sont le plus souvent utilisées par des entreprises et, dans le cas des fonctions de sécurité, doivent être configurées par un administrateur avant d'être utilisées.

Le module TPM peut également faire office de périphérique d'authentification au sein de Motion™ OmniPass™. Vous pouvez, par exemple, utiliser le cryptage de fichiers et de dossiers, la modification de mot de passe et les fonctions de gestion d'utilisateur.

Si vous utilisez le module TPM et les fonctions de sécurité OmniPass, vous devriez créer une archive de sauvegarde. Il s'agit de la seule façon de récupérer vos données si vous rencontrez une panne matérielle ou si le module TPM est supprimé. Sauvegardez vos données de sécurité de façon régulière et stockez-les dans un emplacement sûr, tel qu'un support amovible stocké dans un environnement sécurisé.

Vous ne pouvez pas récupérer des données protégées par le module TPM si vous ne disposez pas d'une archive de sauvegarde. Pour plus d'informations, reportez-vous à l'Aide de la plate-forme de sécurité Infineon après avoir installé le package TPM.

Présentation d'activation


Le processus d'activation du module TPM est composé des étapes suivantes :

- Activation du matériel TPM
- Installation de Infineon Security Package
- Initialisation de la plate-forme de sécurité
- Initialisation d'un utilisateur
- Enregistrement de TPM dans Motion OmniPass
- Configuration des règles d'authentification

Activation du matériel TPM

Avant de pouvoir utiliser le module TPM, vous devez utiliser le BIOS pour activer le matériel TPM.

Pour activer le matériel TPM

1. Démarrez la tablette PC.
2. A partir de l'écran d'accueil Motion Computing, appuyez rapidement sur le bouton Rotation (). Si l'écran d'accueil ne s'affiche pas, redémarrez l'ordinateur et réessayez.
3. Dans l'utilitaire de configuration PhoenixBIOS, appuyez sur **Sécurité** dans la barre de menu.
4. Pour le module TPM, appuyez sur le mot **Désactivé** pour le modifier en **Activé**.

Pour empêcher des utilisateurs non autorisés de modifier les paramètres du module TPM et d'éventuellement supprimer des données confidentielles, vous devriez définir un mot de passe de responsable dans le BIOS. Pour plus d'informations, reportez-vous au Guide d'utilisateur de la tablette PC.

5. Appuyez sur **F10 Enregistrer et quitter**.

Installation de Infineon Security Package

Le logiciel Infineon Security Package est nécessaire pour utiliser les fonctions TPM sur votre tablette PC. Le programme d'installation est chargé sur le disque dur de votre tablette PC. Pour installer le logiciel Infineon Security Package, vous devez disposer des privilèges d'administrateur.

Pour installer Infineon Security Package

1. Sélectionnez C:\WINDOWS\Motion\Infineon_TPM.
2. Lancez « setup.exe ».
3. Suivez les instructions du programme d'installation.


Vous devez redémarrer votre ordinateur après avoir installé le package TPM.

Initialisation de la plate-forme de sécurité

Après avoir installé le logiciel Infineon Security Package, vous devez initialiser la plate-forme de sécurité. Vous devez disposer des privilèges d'administrateur pour initialiser la plate-forme de sécurité.

Appuyez sur le bouton **Aide** sur n'importe quel écran pour obtenir des informations sur cet écran.

Pour initialiser la plate-forme de sécurité

1. Dans la zone de notification, appuyez deux fois sur l'icône TPM ().
2. Dans l'Assistant d'initialisation de la plate-forme de sécurité Infineon, appuyez sur **Suivant**. Si l'assistant ne s'affiche pas, il se peut que la plate-forme soit déjà initialisée.
3. Sélectionnez **Initialisation de la plate-forme de sécurité**. Pour des informations sur la restauration d'une plate-forme de sécurité à partir d'une archive de sauvegarde, reportez-vous à l'Aide de la plate-forme de sécurité Infineon.
4. Entrez le mot de passe du détenteur de la plate-forme de sécurité.

Le mot de passe du détenteur de plate-forme est identique au mot de passe de l'administrateur pour un ordinateur, mais la plate-forme de sécurité ne peut avoir qu'un seul détenteur.

5. Sélectionnez les fonctions à configurer.


Nous vous recommandons fortement d'utiliser la sauvegarde automatique. Si vous créer une archive de sauvegarde, conservez-la dans un emplacement sûr, tel qu'un support amovible stocké dans un environnement sécurisé.

6. Suivez les instructions du programme de configuration en fonction des options sélectionnées.
7. Après avoir confirmé les paramètres de la plate-forme de sécurité, appuyez sur **Suivant**. A la page Récapitulatif, cliquez sur **Terminer**.

Initialisation d'un utilisateur

Pour utiliser TPM sur une tablette PC, vous devez être désigné en tant qu'utilisateur. Vous pouvez utiliser l'Assistant d'initialisation d'utilisateur de plate-forme de sécurité Infineon pour initialiser votre compte d'utilisateur.

Pour initialiser un utilisateur

1. Dans la zone de notification, appuyez deux fois sur l'icône TPM ()
2. Dans l'Assistant d'initialisation d'utilisateur de plate-forme de sécurité Infineon, appuyez sur **Suivant**. Si l'assistant ne s'affiche pas, il se peut que l'utilisateur actuel soit déjà initialisé.
3. Créez le mot de passe d'utilisateur basique.
4. Confirmez les paramètres et appuyez sur **Suivant**.
5. Sélectionnez les fonctions de plate-forme de sécurité à configurer.
 - **Courrier électronique sécurisé.** Utilise des certificats numériques pour sécuriser votre courrier électronique.
 - **Cryptage de fichiers et de dossiers à l'aide d'EFS (Encrypting File System).** Utilise les clés de cryptage protégées par TPM pour sécuriser les dossiers et fichiers.
 - **Cryptage de fichiers et de dossiers à l'aide de PSD (Personal Secure Drive).** Utilise une partition cryptée sur votre disque dur pour sécuriser les dossiers et fichiers.
6. Suivez les instructions du programme de configuration en fonction des options sélectionnées.
7. A la page Récapitulatif, cliquez sur **Terminer**.

Pour en savoir plus sur les fonctions de la plate-forme de sécurité Infineon, reportez-vous à l'Aide de la plate-forme de sécurité Infineon.

Enregistrement de TPM dans Motion OmniPass

Pour utiliser TPM en tant que périphérique d'authentification, vous devez enregistrer le périphérique TPM dans OmniPass. Si vous n'êtes pas encore enregistré en tant qu'utilisateur OmniPass, vous pouvez utiliser cette procédure pour vous ajouter en tant que nouvel utilisateur.

Enregistrement de TPM dans Motion OmniPass

1. Ouvrez Motion Dashboard jusqu'au panneau de sécurité et appuyez sur **Motion OmniPass**.
2. Dans la fenêtre Motion OmniPass, appuyez sur **Exécutez l'Assistant d'enregistrement**.

Si vous êtes déjà enregistré en tant qu'utilisateur OmniPass et que vous voulez enregistrer TPM dans OmniPass, sélectionnez **Modifier l'enregistrement de périphérique d'un utilisateur**.
3. Entrez vos informations de compte Windows puis appuyez sur **Suivant**.
4. Pour sélectionner un périphérique d'authentification, sélectionnez **TPM** puis appuyez sur **Suivant**.
5. Dans la fenêtre d'authentification d'utilisateur de la plate-forme de sécurité Infineon, entrez le mot de passe d'utilisateur basique et sélectionnez **Mémoriser mon mot de passe pour toutes les applications**.
6. Si vous avez terminé d'enregistrer les périphériques, sélectionnez **J'ai terminé d'enregistrer les périphériques d'authentification de sécurité** et appuyez sur **Suivant**.
7. Sélectionnez vos préférences de notification et appuyez sur **Suivant**.
8. A l'écran Profil d'utilisateur de sauvegarde, appuyez sur **Suivant** et sélectionnez un emplacement dans lequel enregistrer le profil d'utilisateur. Entrez un mot de passe pour le profil d'utilisateur.
9. A l'écran Félicitations, appuyez sur **Terminé**.

Si vous êtes invité à vous connecter en tant que nouvelle utilisateur OmniPass, appuyez sur **Oui**.

Configuration des règles d'authentification

Le TPM peut être configuré comme périphérique d'authentification requis dans OmniPass.

Pour configurer les règles d'authentification

1. Ouvrez Motion Dashboard jusqu'au panneau de sécurité et appuyez sur **Motion OmniPass**.
2. Dans la fenêtre Motion OmniPass, appuyez sur **Modifier vos paramètres OmniPass**.
3. Appuyez sur **Définir les stratégies et règles d'authentification**.
4. Si vous y êtes invité, entrez vos informations d'authentification.
5. A la page Définir les règles d'authentification, sélectionnez les fonctions pour lesquelles vous voulez que l'authentification TPM soit obligatoire.

Par exemple, si vous avez sélectionné Cryptage et décryptage des fichiers et dossiers, le TPM est nécessaire pour décrypter tout fichier crypté sur une tablette PC.

Pour plus d'informations, appuyez sur le bouton **Plus d'infos**.



Trusted Platform Module (TPM)

Aktivierungshandbuch

Windows XP Tablet PC Edition 2005

© 2007 Motion Computing, Inc. Alle Rechte vorbehalten.

Dieses Dokument enthält urheberrechtlich geschützte Informationen. Kein Teil dieses Dokuments darf ohne schriftliche Genehmigung von Motion reproduziert werden.

Die Informationen in diesem Dokument werden in ihrem derzeitigen Zustand zur Verfügung gestellt und unterliegen unangekündigten Änderungen. Motion haftet nicht für Fehler oder Auslassungen in diesem Dokument.

Motion, Motion Computing, Speak Anywhere und View Anywhere sind Marken oder eingetragene Marken von Motion Computing, Inc. in den USA und anderen Ländern.

Acrobat ist eine eingetragene Marke von Adobe Systems Incorporated.

Atheros, das Atheros-Logo, Super G, Super A/G, Wake-on-Wireless und Wake-on-Theft sind eingetragene Marken von Atheros Communications, Inc.

AuthenTec ist eine eingetragene Marke von AuthenTec, Inc.

BLUETOOTH ist eine eingetragene Marke im Besitz der Bluetooth SIG, Inc., U.S.A. und wurde für Motion Computing, Inc. lizenziert.

Intel, Intel Inside, das Intel Inside-Logo, Pentium, Centrino und PROSet sind Marken oder eingetragene Marken von Intel Corporation oder deren Niederlassungen in den Vereinigten Staaten und anderen Ländern.

Knowles und IntelliSonic sind Marken oder eingetragene Marken von Knowles Acoustics, Inc.

Microsoft Windows, Windows XP, Windows XP Tablet PC Edition und Windows Journal sind Marken oder eingetragene Marken von Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern.

OmniPass ist eine Marke von Softex, Inc.

Realtek ist eine Marke von Realtek Semiconductor Corporation.

SigmaTel ist eine eingetragene Marke und Universal Jacks ist eine Marke von SigmaTel Corporation.

Wi-Fi ist eine eingetragene Marke der Wi-Fi Alliance.

Motion Computing, Inc. war bestrebt, sämtliches Markeneigentum und deren Inhaber auf dieser Seite zu erwähnen. Alle Marken und Produktnamen in diesem Dokument dienen ausschließlich Identifizierungszwecken und können Marken oder eingetragene Marken ihrer jeweiligen Unternehmen sein.

Die Garantien für Motion-Produkte sind in den Erklärungen zur eingeschränkten Garantie ausgeführt, die den Produkten beiliegen. Keine Informationen in diesem Dokument stellen eine zusätzliche Garantie dar.

Die Motion Computing-Produkte und -Dienstleistungen können einer oder mehreren der folgenden durch Patente geschützten Erfindungen unterliegen. Weitere Patente sind angemeldet. Weitere Informationen erhalten Sie unter www.motioncomputing.com/info/patents.asp.

Einführung

Mit den Infineon® Security Platform-Tools und dem integrierten Trusted Computing Group-kompatiblen TPM (Trusted Platform Module) können Sie digitale Zertifikate für die Benutzer- und Plattform-Authentifikation erstellen und verwalten. Diese Funktionen werden überwiegend in Unternehmen eingesetzt und müssen von einem Administrator eingerichtet werden, bevor die Sicherheitsfunktionen verwendet werden können.

TPM kann auch als Authentifizierungsgerät innerhalb von Motion™ OmniPass™ verwendet werden. Sie können beispielsweise Datei- und Ordnerschlüsselung, Kennwortersetzung und Benutzerverwaltungsfunktionen verwenden.

Bei Verwendung der Sicherheitsfunktionen von TPM und OmniPass sollten Sie ein Sicherungsarchiv erstellen. Ein Sicherungsarchiv stellt die einzige Möglichkeit dar, Daten wiederherzustellen, wenn ein Hardware-Ausfall auftritt oder TPM gelöscht wird. Sichern Sie Ihre Sicherheitsdaten regelmäßig und speichern Sie sie an einem sicheren Speicherort, beispielsweise einem Wechselmedium, das an einem sicheren Ort aufbewahrt wird.

TPM-geschützte Daten können nicht wiederhergestellt werden, wenn kein Sicherungsarchiv zur Verfügung steht. Weitere Informationen finden Sie nach der Installation des TPM-Pakets in der Infineon Security Platform-Hilfe.

Übersicht über die Aktivierung

Der TPM-Aktivierungsvorgang besteht aus den folgenden Schritten:

- Aktivieren der TPM-Hardware
- Installieren des Infineon Security Package
- Initialisieren der Security Platform
- Initialisieren eines Benutzers
- Anmelden von TPM in Motion OmniPass
- Einrichten der Authentifizierungsregeln

Aktivieren der TPM-Hardware

Vor der Verwendung von TPM müssen Sie die TPM-Hardware in BIOS aktivieren.

So aktivieren Sie die TPM-Hardware

1. Starten Sie den Tablet PC.
2. Wenn der Motion Computing-Willkommensbildschirm angezeigt wird, drücken Sie rasch die Taste Drehen (⌚). Starten Sie den Computer neu und versuchen Sie es erneut, wenn Sie den Willkommensbildschirm verpassen.
3. Tippen Sie in der Menüleiste des PhoenixBIOS-Setup-Dienstprogramms auf **Security**.
4. Tippen Sie unter TPM auf das Wort **Disabled**, um es in **Enabled** zu ändern.

Um zu verhindern, dass unbefugte Benutzer Änderungen in den TPM-Einstellungen vornehmen und möglicherweise wichtige Daten löschen, sollten Sie im BIOS ein Supervisor-Kennwort einrichten. Weitere Informationen finden Sie im Tablet PC-Benutzerhandbuch.

5. Tippen Sie auf **F10 Save and Exit**.

Installieren des Infineon Security Package

Die Infineon Security Package-Software ist zur Verwendung der TPM-Funktionen auf dem Tablet PC erforderlich. Das Setup-Programm ist auf der Festplatte des Tablet PC vorinstalliert. Zum Installieren der Infineon Security Package-Software benötigen Sie Administratorberechtigungen.

So installieren Sie das Infineon Security Package

1. Wechseln Sie in das Verzeichnis C:\WINDOWS\Motion\Infineon_TPM.
2. Führen Sie die Datei setup.exe aus.
3. Befolgen Sie die Anweisungen des Setup-Programms.

Nach der Installation des TPM-Pakets müssen Sie den Computer neu starten.

Initialisieren der Security Platform

Nach der Installation der Infineon Security Package-Software müssen Sie die Security Platform initialisieren. Zum Initialisieren der Security Platform benötigen Sie Administratorberechtigungen.

Tippen Sie auf einem beliebigen Bildschirm auf die Schaltfläche **Hilfe**, um weitere Informationen zu diesem Bildschirm anzuzeigen.

So initialisieren Sie die Security Platform

1. Doppeltippen Sie im Benachrichtigungsbereich auf das TPM-Symbol ().
2. Tippen Sie im Assistenten zum Initialisieren von Infineon Security Platform auf **Weiter**. Falls der Assistent nicht angezeigt wird, ist die Plattform möglicherweise bereits initialisiert.
3. Wählen Sie die Option **Security Platform-Initialisierung** aus. Informationen zum Wiederherstellen einer Security Platform aus einem Sicherungsarchiv finden Sie in der Infineon Security Platform-Hilfe.
4. Geben Sie das Security Platform-Besitzerkennwort ein.

Das Plattformbesitzerkennwort ähnelt in seiner Funktion dem Administratorkennwort für einen Computer. Bei der Security Platform kann es allerdings nur einen Besitzer geben.

5. Wählen Sie die Funktionen aus, die Sie konfigurieren möchten.


Wir empfehlen dringend, die automatische Sicherung zu verwenden. Falls Sie ein Sicherungsarchiv erstellen, sollten Sie es an einem sicheren Speicherort speichern, beispielsweise einem Wechselmedium, das entnommen und an einem sicheren Ort aufbewahrt werden kann.

6. Befolgen Sie die Anweisungen des Setup-Programms gemäß der ausgewählten Optionen.
7. Tippen Sie nach dem Bestätigen der Security Platform-Einstellungen auf **Weiter**. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertig stellen**.

Initialisieren eines Benutzers

Um TPM auf einem Tablet PC verwenden zu können, müssen Sie als Benutzer eingerichtet sein. Sie können den Assistenten zum Initialisieren von Benutzern der Infineon Security Platform verwenden, um Ihr Benutzerkonto zu initialisieren.

So initialisieren Sie einen Benutzer

1. Doppeltippen Sie im Benachrichtigungsbereich auf das TPM-Symbol ()
2. Tippen Sie im Assistenten zum Initialisieren von Benutzern der Infineon Security Platform auf **Weiter**. Falls der Assistent nicht angezeigt wird, ist der aktuelle Benutzer möglicherweise bereits initialisiert.
3. Erstellen Sie das grundlegende Benutzerkennwort.
4. Bestätigen Sie die Einstellungen und tippen Sie auf **Weiter**.
5. Wählen Sie die Security Platform-Funktionen aus, die Sie konfigurieren möchten.
 - **Sichere E-Mail**. Zum Sichern von E-Mails werden digitale Zertifikate verwendet.
 - **Datei- und Ordnerschlüsselung mit Encrypting File System (EFS)**. Zum Sichern von Dateien und Ordnern werden TPM-geschützte Verschlüsselungsschlüssel verwendet.
 - **Datei- und Ordnerschlüsselung Personal Secure Drive (PSD)**. Zum Sichern von Dateien und Ordnern wird eine verschlüsselte Partition auf der Festplatte verwendet.
6. Befolgen Sie die Anweisungen des Setup-Programms gemäß der ausgewählten Optionen.
7. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertig stellen**.

Weitere Informationen zu den Infineon Security Platform-Funktionen finden Sie in der Infineon Security Platform-Hilfe.

Anmelden von TPM in Motion OmniPass

Um TPM als Authentifizierungsmedium zu verwenden, müssen Sie TPM in OmniPass erfassen. Falls Sie nicht bereits als OmniPass-Benutzer angemeldet sind, können Sie dieses Verfahren verwenden, um sich als neuer Benutzer hinzuzufügen.

So melden Sie TPM in Motion OmniPass an

1. Starten Sie das Motion Dashboard im Bereich **Sicherheit** und tippen Sie auf **Motion OmniPass**.
2. Tippen Sie im Motion OmniPass-Fenster auf **Anmeldeassistenten ausführen**.

Falls Sie bereits als OmniPass-Benutzer angemeldet sind und TPM in OmniPass anmelden möchten, wählen Sie die Option **Geräteanmeldung eines Benutzers ändern** aus.
3. Geben Sie Ihre Windows-Kontoinformationen ein und tippen Sie dann auf **Weiter**.
4. Wählen Sie unter **Authentifizierungsgerät auswählen** die Option **TPM** aus und tippen Sie dann auf **Weiter**.
5. Geben Sie im Fenster zur Plattform-Authentifikation der Infineon Security Platform das grundlegende Benutzerkennwort ein und wählen Sie **Kennwort für alle Anwendungen speichern** aus.
6. Wenn Sie das Anmelden von Geräten abgeschlossen haben, wählen Sie **Ich habe die Anmeldung von Geräten zur Sicherheitsauthentifizierung abgeschlossen** aus und tippen Sie dann auf **Weiter**.
7. Wählen Sie Ihre Benachrichtigungseinstellungen aus und tippen Sie auf **Weiter**.
8. Tippen Sie im Bildschirm **Ersatzbenutzerprofil** auf **Weiter** und wählen Sie einen Speicherort aus, an dem das Benutzerprofil gespeichert werden soll. Geben Sie ein Kennwort für das Benutzerprofil ein.
9. Tippen Sie im Bildschirm **Herzlichen Glückwunsch** auf **Fertig**.

Tippen Sie auf **Ja**, wenn Sie zum Anmelden als neuer OmniPass-Benutzer aufgefordert werden.

Einrichten der Authentifizierungsregeln

TPM kann als erforderliches Authentifizierungsmedium in OmniPass konfiguriert werden.

So richten Sie die Authentifizierungsregeln ein

1. Starten Sie das Motion Dashboard im Bereich **Sicherheit** und tippen Sie auf **Motion OmniPass**.
2. Tippen Sie im Motion OmniPass-Fenster auf **Eigene OmniPass-Einstellungen ändern**.
3. Tippen Sie auf **Benutzerauthentifizierungsregeln und Richtlinien festlegen**.
4. Geben Sie ggf. Ihre Authentifizierungsinformationen ein.
5. Wählen Sie auf der Seite zum Festlegen der Authentifizierungsregeln die Funktionen aus, für die die TPM-Authentifizierung erforderlich sein soll.

Falls Sie beispielsweise die Option zum Ver- und Entschlüsseln von Dateien und Ordnern aktivieren, ist TPM erforderlich, um alle Dateien zu entschlüsseln, die auf diesem Tablet PC verschlüsselt wurden.

Weitere Informationen erhalten Sie, indem Sie auf **Weitere Informationen** tippen.