

Infineon Security Platform Solution



Bienvenue dans la solution Infineon Security Platform

La solution logicielle Infineon Security Platform utilise le Trusted Platform Module pour sécuriser vos données et applications.

Pour davantage de précisions, veuillez visiter notre site Web à l'adresse :

<http://www.infineon.com/tpm/software>



©Infineon Technologies AG

Infineon Security Platform Solution

Présentation

Le logiciel de la solution Infineon Security Platform est un ensemble complet d'outils qui met en œuvre les fonctions de le Trusted Platform Module incorporé dans votre système. Cette solution fournit des services permettant de créer facilement des certificats numériques à l'aide de l'Infineon Trusted Platform Module ainsi que de gérer ces certificats. Vous pouvez utiliser les certificats pour :

- Envoyer et recevoir des messages sécurisés depuis des clients de messagerie tels que Microsoft Windows Mail/Outlook Express, Microsoft Outlook ou Mozilla Thunderbird
- Installer le navigateur (par exemple Mozilla Firefox ou Internet Explorer) et le serveur web (par exemple Microsoft Internet Information Server) pour l'authentification de clients
- Signature de macros de Microsoft Word.
- Encrypter les fichiers et dossiers
- Sécuriser les connexions réseau

Les secrets d'utilisateur peuvent être migrés vers d'autres ordinateurs, assurant ainsi à l'utilisateur une complète sécurité sur les ordinateurs supplémentaires.

Le logiciel de la solution Infineon Security Platform inclut les composants suivants :

- Outil de paramétrage Security Platform
- Assistant d'Initialisation Rapide de Security Platform
- Assistant Initialisation de Security Platform
- Assistant Initialisation de l'utilisateur de Security Platform
- Assistant Migration de Security Platform
- Assistant Sauvegarde de Security Platform
- Assistant Réinitialisation du mot de passe de Security Platform
- Assistant d'Importation PKCS #12 de Security Platform
- Visualisateur du certificat et sélection du certificat de Security Platform

- Security Platform pictogramme Zone de notification barre de tâches
- Services d'intégration de Security Platform
- Services de Security Platform
- Server Integration Services
- Personal Secure Drive

En plus de fournir des informations sur l'[installation de la solution logicielle Infineon Security Platform](#), ce document vous permet d'utiliser de façon optimale votre Infineon Trusted Platform Module ainsi que la solution logicielle Infineon Security Platform pour exécuter des tâches telles que :

- [l'obtention de certificats numériques](#)
- [le cryptage de dossiers et de fichiers](#)
- [la configuration des clients de messagerie électronique pour envoyer du courrier électronique crypté et signé numériquement](#)

Par ailleurs, ce document permettra également aux administrateurs des systèmes d'entreprise d'exécuter des tâches telles que :

- [le mappage des certificats avec Internet Information Server et Active Directory](#)
- [l'authentification de clients avec Internet Explorer, l'authentification de clients avec Mozilla Firefox](#)
- [l'utilisation des certificats numériques pour la signature électronique de macros dans Microsoft Word](#)

L'administration de la fonctionnalité de [Sauvegarde et récupération d'urgence](#) constitue une tâche essentielle. Cette fonction est mise en place pendant l'initialisation de Security Platform et n'affecte pas les fonctionnalités générales de sécurité énumérées ci-dessus. Cette opération est importante pour éviter la perte de données en cas de panne de l'ordinateur.

Infineon Security Platform Solution

Les avantages de l'utilisation de le Trusted Platform Module

Le développement phénoménal d'Internet et la tendance qu'ont les réseaux d'entreprises d'étendre l'accès à leurs réseaux aux clients et fournisseurs situés à l'extérieur du pare-feu de la société, ont mis l'accent sur le problème de la sécurité. Même si les formes électroniques d'identification prennent actuellement le dessus sur l'identification papier ou visuelle, les questions de sécurité et de confidentialité sont devenues la principale source de préoccupation. Or, ces questions semblent avoir trouvé leur solution dans les applications à base de clés publiques. Parmi les types de services que la technologie de clé publique facilite, on trouve la transmission sécurisée de données sur les réseaux publics, la signature numérique garantissant l'authenticité d'un message électronique et l'authentification d'un client par le serveur et vice versa.

Le volume des communications par Internet est en constante augmentation. De nombreuses applications, telles que celles destinées au commerce électronique, sont basées sur la confiance dans le partenaire de communication et la fiabilité de la connexion. Vous devez offrir à la fois authenticité, intégrité ainsi que confidentialité des données professionnelles et privées. Avec le développement de **TCG (Trusted Computing Group)**, un projet commercial de grande envergure a été mis sur pied. Son but est d'accroître la confiance dans la sécurité des transactions sur Internet. TCG a défini un dispositif - appelé **Trusted Platform Module (TPM, Security Chip)** - qui prendra en charge un grand nombre de fonctions de sécurité.

Le circuit de sécurité est à la base de la confiance accordée à une plate-forme donnée (telle que sur les desktops ou les notebooks). S'il est intégré à un ordinateur doté d'un système d'exploitation qui prend en charge ce circuit, il pourra vérifier l'intégrité du système et authentifier les utilisateurs tiers désireux d'accéder aux fonctions de sécurité tout en restant sous le contrôle intégral de son utilisateur principal. Ainsi, la confidentialité des données privées et professionnelles sera assurée. Les plates-formes conçues autour du circuit de sécurité permettront, pour la première fois, de créer les bases pour une infrastructure mondiale utilisant les clés publiques (PKI). La sécurité de nombreuses applications destinées aux environnements privés et professionnels sera à son tour garantie, tout en rendant possible pour la première fois d'autres types d'applications.

Les activités de TCG et les normes de sécurité qui en résultent, mettent en lumière les besoins actuels de la technologie de sécurité. L'architecture de l'Infineon Trusted Platform Module a été conçue pour offrir à la fois les plus hautes normes de sécurité existantes, basées sur une technologie de sécurité éprouvée, et une intégration de système aisée en fournissant une solution de sécurité complète. L'Infineon Trusted Platform Module offre les mises en oeuvre cryptographiques de RSA et des algorithmes de hachage (SHA-1 et MD-5) pour une performance optimisée ainsi qu'un générateur de nombres vraiment aléatoires (TRNG). Il s'agit d'un dispositif protégé, offrant les niveaux de sécurité les plus élevés par rapport aux types d'analyse SPA (simple power analysis) et DPA (differential power analysis).

Jusqu'à présent, les utilisateurs de systèmes ont sauvegardé leurs certificats et clés privées sur les disques durs de leurs ordinateurs, laissant leurs données à la merci de prédateurs ou de personnes pouvant accéder physiquement à l'appareil. Par contraste, le Trusted Platform Module offre un support d'information inviolable pour sécuriser les données.



©Infineon

Technologies AG

Infineon Security Platform Solution

Microsoft Windows

Cette page contient des informations propres aux versions du système d'exploitation Microsoft Windows.

Contrôle des comptes utilisateurs

Le Contrôle des comptes utilisateurs est une fonction importante offerte par Windows Vista et supérieur. Avec le Contrôle des comptes utilisateurs, les administrateurs des systèmes informatiques peuvent lancer la plupart des applications, des composants et des processus avec des droits restreints, mais ils ont le « potentiel d'augmentation » pour des tâches administratives et des fonctions d'application spécifiques. Lorsque les utilisateurs normaux font appel à une tâche de système qui nécessite des droits d'administration, telles que la tentative d'installer une application, Windows va aviser l'utilisateur et il demande la permission de l'administrateur, c'est à dire le nom d'utilisateur et le mot de passe d'un compte avec des droits d'administration pour exécuter cette tâche. En plus, le Contrôle des comptes utilisateurs fait que même les comptes administrateur fonctionnent comme des comptes normaux pour la plupart du temps, et chaque fois qu'on essaie d'exécuter une tâche au niveau d'administration, l'administrateur va recevoir une invite à augmenter temporairement les droits pour effectuer cette seule tâche.

Windows utilise une icône bouclier  pour indiquer qu'une fonction particulière nécessite des droits d'administration pour effectuer la tâche (par exemple pour la restauration de Security Platform via l'[Assistant Initialisation Infineon Security Platform](#)).



- Dans Windows 7, l'icône bouclier n'est pas visible en permanence par défaut, mais uniquement après une configuration appropriée.
- L'icône bouclier peut être légèrement différente, selon la session Windows.

Microsoft BitLocker

Il est possible d'utiliser le [BitLocker](#), de Microsoft, inclus dans certaines éditions de Windows Vista pour chiffrer un entier disque dur, rendant plus difficile l'accès aux données de l'ordinateur en cas de perte ou de vol. Le Chiffrement de lecteur BitLocker, avec ou sans Trusted Platform Module, fournit un chiffrement complet du disque. Trusted Platform Module rend le chiffrement du lecteur encore plus sûr, car il utilise le microprocesseur pour générer des clés cryptographiques sur la base des balayages des fichiers core du système, en plus d'une clé pour le disque dur lui-même. Pour configurer cette fonction voir [Assistant Initialisation Infineon Security Platform](#) et [Outil de configuration Infineon Security Platform](#).

Gestion de module de plateforme sécurisée

L'application *Gestion TPM (Trusted Platform Module)* de Microsoft est une nouvelle fonctionnalité présente dans Windows Vista et supérieur. On peut utiliser cette application pour établir la possession d'un Trusted Platform Module et pour le gérer. Des informations plus détaillées sont disponibles dans Microsoft TechNet. Veuillez consulter Microsoft TechNet.

Erreurs

Si des erreurs TPM ou TSS inattendues se produisent sous Windows Vista ou sur les systèmes d'exploitation ultérieurs, veuillez vérifier si les commandes TPM sont bloquées à l'aide du paramétrage de la Stratégie de groupe Windows.



©Infineon

Technologies AG

Infineon Security Platform Solution - Modes d'opération

Modes d'opération

Mode Serveur

En mode serveur, les Server Integration Services intègrent Security Platform dans un Trust Domain à gestion centralisée.

 Informations plus détaillées sur le mode serveur sont disponibles dans le *Guide technique pour Trusted Computing Management Server*.

Conditions préliminaires pour Inscription plateformes et Inscription utilisateurs dans le mode serveur

	Explication
L'inscription des plateformes	<p>L'inscription des plateformes est effectuée automatiquement, sans l'intervention de l'utilisateur.</p> <p>Conditions préalables :</p> <ul style="list-style-type: none">• La plateforme Trust Domain doit être membre du Groupe d'inscription plateformes (pour plus de détails, consulter le <i>Guide technique pour Trusted Computing Management Server</i>).• Trusted Platform Module est activé.• Trusted Platform Module n'a pas été encore initialisé (ni par Infineon TPM Professional Package dans le mode autonome, ni par Trusted Domain Server dans le mode serveur, ni par un autre logiciel comme par exemple <i>Windows Trusted Platform Module (TPM) Management</i>).• La plateforme Trust Domain est en ligne, c'est-à-dire qu'il y a une connexion réseau vers le serveur Trust Domain.
L'inscription des utilisateurs	<p>L'inscription des utilisateurs est effectuée par interaction, comme pour le mode autonome, si les conditions préalables suivantes sont remplies :</p> <p>Conditions préalables :</p> <ul style="list-style-type: none">• L'utilisateur de Trust Domain doit être membre du Groupe d'inscription utilisateurs (pour plus de détails, consulter le <i>Guide technique pour Trusted Computing Management Server</i>).

- Le Trusted Platform Module sur la plateforme de l'utilisateur est activé.
- La plateforme Trust Domain est en ligne, c'est-à-dire qu'il y a une connexion réseau vers le serveur Trust Domain.
- L'utilisateur a ouvert une session dans le domaine.

Mode Autonome

En mode autonome, Security Platform n'est pas intégré dans un Trust Domain à gestion centralisée.

Différences entre les modes d'opération :

La table suivante liste le comportement des différentes composantes de l'interface utilisateur dans les modes d'opération:

Composante	Mode autonome	Mode Serveur
Outil de paramétrage	Cette composante est conçue comme un applet du Panneau de configuration. Les administrateurs et les utilisateurs peuvent exécuter l'initialisation et la configuration de Security Platform Fonctionnalités et gestion de toutes les fonctionnalités de Security Platform.	La configuration de tous paramètres de propriétaire et authentification de Security Platform est gérée automatiquement par le Trusted Computing management Server. Les pages Avancé et Migration ne sont pas disponibles.
Assistant d'Initialisation Rapide	Combinaison d'initialisation de plateforme et utilisateur avec paramètres par défaut (recommandé pour la plupart des utilisateurs).	Les tâches spécifiques à la plateforme sont ignorées, car le Trust Computing Management Server les prend en charge.
Assistant Initialisation	Initialisation, Activation et Restauration des fonctionnalités de Security Platform (étapes administratives). Cet assistant est complètement fonctionnel dans ce mode.	L'initialisation, l'activation et la restauration surviennent automatiquement une fois le système client est intégré dans un Trust Domain à gestion centralisée, c'est-à-dire l'administrateur ne doit pas exécuter cette tâche. L'assistant de Security Platform n'est pas fonctionnel si la plateforme est membre du groupe d'inscription plateformes.
Assistant	L'assistant Initialisation de	L'initialisation de l'utilisateur

Initialisation de l'utilisateur	<p>L'Utilisateur prend en charge l'initialisation des utilisateurs de Security Platform et la configuration des fonctionnalités de Security Platform. Cet assistant est complètement fonctionnel dans ce mode.</p>	<p>est possible seulement si l'utilisateur actuel est membre du groupe d'inscription utilisateurs spécifié sur Trusted Computing Management Server. Cet assistant est également complètement fonctionnel dans ce mode.</p>
Assistant Migration	<p>La migration des clés spécifiques et des certificats spécifiques pour l'utilisateur depuis une plateforme source vers une plateforme destination inclut des étapes utilisateur et des étapes administratives. Cet assistant est complètement fonctionnel dans ce mode.</p>	<p>Cet assistant n'est pas disponible, car la migration des clés spécifiques et des certificats spécifiques pour l'utilisateur est effectuée automatiquement par Trusted Computing Management Server, donc l'administrateur et l'utilisateur ne doivent pas effectuer cette activité.</p>
Assistant Sauvegarde	<p>Les Sauvegarde et Restauration automatique et manuelle incluent des étapes utilisateurs et administratives. Lorsque le Personal Secure Drive (PSD) a été configuré, la Sauvegarde et Restauration manuelle de cette unité peuvent être effectuées.</p>	<p>La Sauvegarde et la Restauration sont effectuées par les Server Integration Services. Lorsque le Personal Secure Drive (PSD) a été configuré, la Sauvegarde manuelle et la Restauration manuelle de cette unité peuvent être effectuées.</p>
Assistant de réinitialisation du mot de passe	<p>La réinitialisation du Mot de passe utilisateur de base inclut des étapes utilisateurs et des étapes administratives. L'administrateur prépare la réinitialisation du mot de passe pour un utilisateur et</p>	<p>Le Trusted Computing Management Server s'en occupe de la préparation et la fourniture du Code d'autorisation de la Réinitialisation du code du mot de passe pour un</p>

	fournit le Code d'autorisation de la réinitialisation du mot de passe. L'utilisateur réinitialise son Mot de passe utilisateur de base.	utilisateur spécifique et un administrateur spécifique. Une option supplémentaire existe pour la récupération du Code d'autorisation de la réinitialisation depuis le serveur.
Assistant d'Importation PKCS #12	Cet assistant est utilisé pour importer les fichiers Personal Information Exchange dans le Security Platform et il est complètement fonctionnel dans ce mode.	Aucun changement dans le comportement de cet assistant, également fonctionnel dans ce mode.
Icône Notification de la barre d'outils	Effectuer des tâches administratives de Security Platform et obtenir des informations sensibles concernant l'état. L'application est complètement fonctionnelle dans ce mode.	Dans ce mode, il n'y a pas des tâches dont le serveur s'en occupe sans l'intervention de l'utilisateur.



Infineon Security Platform Solution

Installation du logiciel de la solution Infineon Security Platform

Lorsqu'une version installée du logiciel de la solution Infineon Security Platform existe déjà sur votre système, la désinstallation du logiciel n'est pas nécessaire. Une installation existante peut être remplacée ou actualisée dans une opération dans une seule étape.



Mise à jour: La mise à jour des versions anciennes du produit est décrite dans *ReadmeUpgrade.txt*

1. Lancez le programme d'installation

Remarque : Lorsque le logiciel Infineon Security Platform est déjà installé sur votre système, ainsi on ouvre un dialogue dans lequel vous pouvez choisir la modification, la réparation ou la suppression de l'installation existante.

2. L'assistant InstallShield est lancé et la version du logiciel Infineon Security Platform est affichée avec quelques informations légales.
3. Cliquez sur le bouton **Suivant** pour continuer le processus d'installation. Le Contrat de Licence Utilisateur Final (CLUF) est affiché.
4. Lisez le contrat avec attention. Acceptez les termes du contrat de licence. Cliquez sur le bouton **Suivant** pour continuer le processus d'installation.
5. Ensuite quelques informations générales d'installation doivent être fournies. Entrez dans les boîtes appropriées les informations sur vous et votre organisation.
6. Cliquez sur le bouton **Suivant** pour continuer le processus d'installation.
7. Dans la fenêtre **Type d'Installation** sélectionnez le type d'installation souhaité :
 - Sélectionnez **Complet**, si vous souhaitez installer tous les composants dans le répertoire d'installation par défaut.
 - Sinon, sélectionnez **Personnaliser**.
8. Sélectionnez les composants à installer. Lisez la description de chaque composante dans le côté droit de l'écran et décidez lorsque vous désirez l'installer tout de suite sur votre système, l'installer ultérieurement ou ne pas

l'installer. Quelques composants sont obligatoires et ne peuvent pas être désélectionnés. Vous pouvez sélectionner également le répertoire dans lequel vous désirez installer le logiciel Infineon Security Platform.

9. Cliquez sur le bouton **Suivant** pour continuer le processus d'installation.
10. Cliquez sur **Installer** pour finaliser le processus d'installation.
11. L'assistant InstallShield installe le logiciel de la solution Infineon Security Platform.

Selon votre sélection, le programme d'installation installe les composants suivants sur votre système :

- Outil de paramétrage Security Platform
 - Assistant d'Initialisation Rapide de Security Platform
 - Assistant Initialisation de Security Platform
 - Assistant Initialisation de l'utilisateur de Security Platform
 - Assistant Migration de Security Platform
 - Assistant Sauvegarde de Security Platform
 - Assistant Réinitialisation du mot de passe de Security Platform
 - Assistant d'Importation PKCS #12 de Security Platform
 - Visualisateur du certificat et sélection du certificat de Security Platform
 - Security Platform pictogramme Zone de notification barre de tâches
 - Personal Secure Drive
 - Infineon TPM Cryptographic Service Providers
 - Pile du logiciel Security Platform
 - Logiciel pilote Trusted Platform Module
 - Server Integration Services
12. Le processus d'installation du logiciel Infineon Security Platform doit être finalisé.
 13. Sélectionnez **Préparer Inscription TPM** afin [d'activer](#) le Trusted Platform Module, si souhaité (seulement sur systèmes avec Trusted Platform Module désactivé et support d'Interface de Présence Physique). Cela vous permet d'initialiser votre plateforme ultérieurement, sans devoir redémarrer votre système.
 14. Sélectionnez l'option **Afficher le fichier readme**, si c'est le cas.
 15. Cliquez sur **Terminer** pour finaliser l'installation.



TPM

©Infineon Technologies AG

Infineon Security Platform Solution

Installation et administration d'Infineon Security Platform

Lors de la livraison du produit, l'état initial d'Infineon Security Platform est désactivé par défaut. Ainsi, aucune fuite d'informations confidentielles ne peut se produire dans cette phase entre l'Infineon Security Platform et le fabricant de plate-formes, puisqu'il n'existe aucun secret partagé sous aucune forme.

L'état courant d'un système Infineon Security Platform n'est jamais affecté par l'installation de la solution logicielle Infineon Security Platform.

Avant de pouvoir profiter de votre Infineon Security Platform, vous devez :

- Activer Infineon Security Platform en suivant la procédure indiquée dans la documentation correspondante:

- Installez votre Infineon Security Platform et l'Utilisateur en lançant l'Assistant d'Initialisation Rapide



Dans le [mode serveur](#), Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée, c'est-à-dire l'administrateur ne doit pas exécuter cette tâche.

Reportez-vous à [Outils de la solution Infineon Security Platform](#), pour obtenir une information détaillée sur les assistants et outils d'administration.

Si l'Infineon Security Platform ainsi qu'un utilisateur d'Infineon Security Platform sont installés, vous êtes prêt à [obtenir un certificat numérique pour le Trusted Platform Module](#).

Les opérations qui peuvent être exécutées sont contrôlées par l'état actuel d'Infineon Security Platform. La [Vue d'ensemble des états](#) donne la liste des valeurs d'état possibles.

Vous trouverez des réponses aux questions fréquentes sur la gestion de Security Platform dans le chapitre [Questions fréquentes](#).



©Infineon Technologies AG

Infineon Security Platform Solution

Rôles de l'utilisateur

La solution Security Platform implique quelques rôles de l'utilisateur :

- Tous les rôles d'utilisateur de Security Platform sont fondés sur les comptes utilisateurs Windows (utilisateurs locaux ou utilisateurs du domaine). Ces comptes utilisateurs ont été authentifiés par l'ouverture de session Windows.
- Chaque rôle utilisateur a un but prévu.
- Lorsque Security Platform est configurée, les membres des rôles utilisateur différents sont initialisés.
- L'activation comme un rôle utilisateur spécifique exige une authentification spécifique (par exemple en fournissant un mot de passe spécifique).
- Une personne peut avoir des rôles utilisateur multiples.

La table suivante présente tous les rôles utilisateur.

Rôles de l'utilisateur	Fondé sur...	But et tâches	Initialisation	Authentification
Propriétaire de Security Platform	Compte utilisateur Windows (local ou domaine), membre du groupe Administrateurs	Effectue les tâches administratives critiques, par ex. la restauration de Security Platform.	L'initialisation de Security Platform permet à un utilisateur Windows d'agir comme un propriétaire Security Platform.	Mot de passe propriétaire
Administrateur Security Platform (nommé également « Administrateur »)	Compte utilisateur Windows (local ou domaine), membre du groupe Administrateurs	Effectue des tâches administratives, exigeant des droits administratifs Windows.	Aucune initialisation spéciale nécessaire.	En plus de l'authentification comme administrateur Windows, quelques tâches administratives exigent l'authentification aux fichiers protégés par

				mots de p dédiés.
Utilisateur Security Platform (nommé également « Utilisateur »)	Compte utilisateur Windows (local ou domaine)	Utilise les fonctionnalités de Security Platform, par exemple le cryptage de fichiers et dossiers ou la messagerie électronique sécurisée. Configure les fonctionnalités et effectue des tâches de Security Platform spécifiques à l'utilisateur.	L'initialisation de l'utilisateur de Security Platform permet à un utilisateur Windows d'agir comme un propriétaire Security Platform.	Mot de pa utilisateur base
Agent de récupération EFS/PSD (nommé également « Utilisateur »)	Utilisation d'un certificat de récupération et d'une clé privée dédiés.	Récupération de données EFS ou PSD d'un utilisateur lorsque les informations d'identification EFS/PSD sont perdues.	La récupération EFS/PSD est activée par la registration des agents de récupération.	Clé privée l'agent de récupérati



Infineon Security Platform Solution

Authentification de l'utilisateur

Pour des raisons de sécurité, vous devez vous authentifier sur Infineon Security Platform pour utiliser les fonctions de sécurité. Par exemple le cryptage de fichiers exige la clé utilisateur de base, protégée avec votre mot de passe utilisateur de base. L'entrée de ce mot de passe signifie l'authentification sur Security Platform. Seulement après une authentification avec succès vous pouvez utiliser la clé utilisateur de base.

La solution Infineon Security Platform fournit deux niveaux d'authentification pour protéger la clé utilisateur de base :

Authentification du mot de passe

La clé utilisateur de base est protégée par le *Mot de passe utilisateur de base*. Ce mot de passe doit être entré manuellement.

Authentification étendue

La clé utilisateur de base est protégée par la *Phrase de passe utilisateur de base*. Cette phrase de passe est enregistrée en sûreté par un dispositif d'authentification, par exemple une carte à puce, une clé USB sécurisé, un lecteur d'empreintes digitales ou un autre dispositif biométrique d'authentification. La phrase de passe peut être accédée seulement par ce dispositif d'authentification, par exemple en insérant une carte à puce et en introduisant son numéro d'identification personnel ou en appuyant le doigt sur le lecteur d'empreintes digitales.

Mots et phrases de passe

Avec l'**Authentification du mot de passe**, un mot de passe « normal » sert comme Mot de passe utilisateur de base. Bien que l'utilisation des mots de passe longs et complexes soit techniquement possible, la plupart des mots de passe sont assez courts, car ils doivent être mémorisés.

Avec **Authentification étendue** vous ne devez plus mémoriser les mots de passe, car ils sont gérés par le dispositif d'authentification. Pour l'utilisateur, le mot de passe est remplacé par une authentification par le numéro d'identification personnel ou par l'authentification biométrique.

L'authentification étendue est ainsi plus conviviale. D'autre côté, le niveau de sécurité est élevé considérablement par les fonctions de sécurité du dispositif d'authentification. Par exemple, dans une carte à puce il y a un compteur de reprise qui bloque la carte après plusieurs entrées incorrectes d'un numéro d'identification personnel. Ainsi les attaques en force sont faites impossible et des numéros d'identification personnels assez simples peuvent être utilisés.

Pour accentuer la combinaison par l'authentification étendue des mots de passe longs et complexes avec la convivialité, on utilise un autre terme à la place du *Mot de passe* : la *Phrase de passe*. Une phrase de passe n'est pas en fait différente d'un mot de passe long et complexe.

La solution Security Platform fait la différence entre ces deux termes :

- Le **Mot de passe** est utilisé dans le mode Authentification du mot de passe et signifie *Mot de passe utilisateur de base*.
- La **Phrase de passe** est utilisée dans le mode Authentification étendue. Signifie également Mot de passe utilisateur de base. Dans ce contexte, le mot de passe utilisateur de base est appelé *Phrase de passe utilisateur de base*.

Installation et administration de l'authentification étendue

Les dispositifs d'authentification sont fournis comme plugiciels qui doivent être installés séparément. Le logiciel de la solution Security Platform détecte automatiquement les dispositifs d'authentification installés.

La configuration des dispositifs d'authentification est spécifique à l'utilisateur, c.à.d des utilisateurs différents de Security Platform, peuvent utiliser des dispositifs d'authentification différents. L'utilisation de l'authentification étendue peut être contrôlée par les [stratégies](#).

Configuration pas à pas de l'authentification étendue

Configuration de l'authentification étendue - Tâches d'administration	Composant logiciel à utiliser
1. Installation du dispositif d'authentification	Installation à part. Consultez le fournisseur du plugiciel d'authentification.
2. Activation de l'utilisation de certains dispositifs d'authentification pour tous les utilisateurs.	Lorsque Security Platform n'est pas encore initialisée : Assistant Initialisation Lorsque Security Platform est déjà initialisée : Outil de paramétrage - Avancé - Configuration...
Configuration de l'authentification étendue - Tâche utilisateur	Composant logiciel à utiliser
3. Sélection du niveau et dispositif d'authentification pour l'utilisateur actuel de Security Platform.	Lorsque l'utilisateur n'est pas encore initialisé : Assistant Initialisation de l'utilisateur Lorsque l'utilisateur est déjà initialisé : Outil de paramétrage - Paramètres utilisateur - Configuration...



Infineon Security Platform Solution

Jetons, fichiers de sauvegarde des données et autres fichiers de gestion de Security Platform

La solution Infineon Security Platform utilise quelques fichiers pour les tâches de gestion telles que la sauvegarde, la récupération d'urgence ou la réinitialisation du mot de passe (par exemple les jetons et les fichiers de sauvegarde des données). Quelques-uns sont pour les administrateurs de Security Platform, autres sont pour les utilisateurs de Security Platform. Ne faites pas une confusion entre ces types de fichiers.

La table suivante présente les fichiers de gestion de Security Platform.

Fichier	Utilisé par...	But/Explication
Fichier de Sauvegarde du Mot de Passe Propriétaire	Administrateur	Utilisé pour l'authentification du Mot de Passe Propriétaire (au lieu de taper le Mot de Passe Propriétaire). Ce fichier est compatible avec le Fichier de Sauvegarde de Mot de Passe Propriétaire généré par l'application Microsoft "Trusted Platform Module (TPM) Management".  Ce fichier n'est pas exigé en mode serveur étant donné que le Trusted Computing Management Server gère la tâche de préparation et de livraison de ce mot de passe.
Fichiers de sauvegarde des données utilisés pour la restauration, la récupération d'urgence et la	Administrateur/Utilisateur	Contient les informations d'identification et les paramètres de Security Platform et les sauvegardes de Personal Secure Drive. Créé par les sauvegardes automatiques et manuelles.

réinitialisation du mot de passe		<p>Exigé pour restauration lorsqu'un disque dur est brisé, des données sont perdues ou un Trusted Platform Module est brisé. Les données de réinitialisation du mot de passe dans un fichier de sauvegarde des données sont exigées pour réinitialiser les mots de passe utilisateur de base.</p> <p> Ces archives ne sont pas exigées dans le mode serveur, car la réinitialisation du mot de passe, la sauvegarde et la restauration de Security Platform sont gérées par Trusted Computing Management Server.</p>
Jeton de récupération d'urgence	Administrateur	<p>Créé au cours de la configuration des fonctionnalités de Security Platform (lorsque l'Assistant d'Initialisation de Security Platform est utilisé).</p> <p>Exigé pour restauration, lorsque la récupération d'urgence est exigée (Trusted Platform Module brisé).</p> <p> Ce fichier n'est pas exigé en mode serveur, car la restauration de Security Platform est gérée par Trusted Computing Management Server.</p>

<p>Jeton réinitialisation du mot de passe</p>	<p>Administrateur</p>	<p>Créé au cours de la configuration des fonctionnalités de Security Platform (lorsque l'Assistant d'Initialisation de Security Platform est utilisé). Exigé pour préparer la réinitialisation du mot de passe pour un certain utilisateur.</p> <p> Ce fichier n'est pas exigé en mode serveur, car la réinitialisation du mot de passe est gérée par Trusted Computing Management Server.</p>
<p>Récupération d'Urgence / Jeton de Réinitialisation de Mot de Passe</p>	<p>Administrateur</p>	<p>Créé pendant l'Initialisation de Security Platform (lorsque l'Assistant d'Initialisation Rapide de Security Platform est utilisé). Combinaison du Jeton de Récupération d'Urgence et du Jeton de Réinitialisation de Mot de Passe dans un fichier.</p>
<p>Sauvegarde des données de migration</p>	<p>Utilisateur</p>	<p>Contient les clés et les certificats utilisateurs à migrer vers une autre Security Platform. Créé au cours de l'étape <i>Exportation</i> de la migration. Exigé au cours de l'étape <i>Importation</i> de la migration.</p> <p> Ce fichier n'est pas exigé en mode serveur, car la migration est gérée par</p>

		Trusted Computing Management Server.
Secret personnel pour réinitialisation du mot de passe	Utilisateur	Créé au cours de la configuration des paramètres de l'utilisateur de Security Platform. Exigé pour réinitialiser le mot de passe d'un utilisateur de base.
Fichier de code d'autorisation pour réinitialisation	Administrateur/Utilisateur	<p>Contient le code d'autorisation de la réinitialisation, demandé pour la réinitialisation du mot de passe d'un utilisateur de base. Créé au cours des étapes administratives de la réinitialisation du mot de passe. Demandé au cours des étapes utilisateur de la réinitialisation du mot de passe.</p> <p> Dans le mode serveur, ce fichier est créé par Trusted Computing Management Server.</p>
Fichier PKCS #12 (fichier Personal Information Exchange)	Utilisateur	Contient la clé privée et le certificat d'un utilisateur. Exigé pour importer un certificat.



Infineon Security Platform Solution

Fonctionnement avancé de Security Platform

[Sauvegarde et restauration de données Security Platform](#)

[Récupération de Données EFS et PSD via Agent de Récupération](#)

[Migration de clés vers d'autres systèmes](#)

[Réinitialisation du mot de passe utilisateur de base](#)

[Défense contre les attaques de type dictionnaire](#)

Technologies AG



Infineon Security Platform Solution

Sauvegarde et restauration de données Security Platform

Sauvegarde Security Platform inclut toutes les données en cas d'urgence. Après une erreur matérielle, une erreur de support de stockage ou une erreur Trusted Platform Module, la restauration Security Platform rétablit l'accès aux fonctions de Security Platform pour tous les utilisateurs.

En outre, vous pouvez sauvegarder et restaurer vos données Personal Secure Drive. Les données des autres applications utilisant la solution Security Platform (par exemple le courriel Secure) ne sont pas incluses dans la sauvegarde Security Platform.



- En [mode serveur](#), Sauvegarde et Restauration de paramètres et titres d'utilisateurs sont gérés par Trusted Computing Management Server, à l'exception de Sauvegarde et Restauration des fichiers d'image de Personal Secure Drive (PSD).
- La mise à jour [d'informations d'identification et paramètres utilisateur](#) sera gérée par Trusted Computing Management Server, est aussi selon Sauvegarde et restauration.

Portée de la sauvegarde

La sauvegarde Security Platform inclut les données suivantes :

Les informations d'identification et paramètres Security Platform	
Contenu de la sauvegarde	Une copie des informations d'identification et paramètres spécifiques à l'utilisateur stockés sur Security Platform.
Objectif	La restauration des informations d'identification et paramètres spécifiques à l'utilisateur après une erreur matérielle ou une erreur de support de stockage. Sinon, les utilisateurs ne pourront plus accéder aux fonctions de Security Platform et les données utilisateur seront perdues.
Archives	<ul style="list-style-type: none">• Sauvegarde de récupération d'urgence écrite automatiquement (« Sauvegarde de récupération d'urgence système », par ex. un fichier SPSystemBackup.xml et un dossier SPSystemBackup) : Configurée par l'administrateur de Security Platform. Contient les informations d'identification et paramètres pour tous les utilisateurs de Security Platform (pour un ou plusieurs ordinateurs Security Platform). Contient également les informations d'identification de l'ordinateur et de l'utilisateur, utilisées pour faire la correspondance entre les ordinateurs et les utilisateurs au cours du processus de restauration.• Sauvegarde de récupération d'urgence écrite manuellement (par exemple SPBackupArchive.xml) : Créée par l'utilisateur de Security Platform. Contient les informations d'identification et paramètres d'un utilisateur de Security Platform (pour un ordinateur Security Platform). Contient également les informations d'identification de l'ordinateur et de l'utilisateur, utilisées pour faire la correspondance entre l'ordinateur et l'utilisateur au cours du processus de restauration.
Récupération d'urgence	
Contenu de la	Toutes les clés utilisateur de base Security Platform, cryptées spécialement pour la récupération d'urgence.

sauvegarde	
Objectif	<p>Le cryptage à nouveau de toutes les clés utilisateur de base après une erreur Trusted Platform Module. Dans ce cas, une nouvelle Security Platform doit être installée et un nouveau propriétaire est créé. La récupération d'urgence permet le cryptage à nouveau des clés utilisateur de base depuis la vieille clé propriétaire vers une nouvelle clé.</p> <p>Sinon, les utilisateurs ne pourront plus accéder aux fonctions de Security Platform et les données utilisateur seront perdues.</p>
Archives	<ul style="list-style-type: none"> • Les données de récupération d'urgence sont incluses dans les sauvegardes de récupération d'urgence écrites automatiquement. Elles sont également incluses pour l'utilisateur concerné dans les archives de sauvegarde écrites manuellement, si la sauvegarde automatique a déjà été configurée lors de la sauvegarde manuelle. • Jeton de Récupération d'Urgence (par ex. SPEmRecToken.xml) ou Jeton combiné de Récupération d'Urgence / Réinitialisation de Mot de Passe (par ex. SpToken_<PCName>.xml) : Créé par l'Administrateur de Security Platform. Cela est exigé pour une restauration de Données de Récupération d'Urgence.

Personal Secure Drive

Contenu de la sauvegarde	Une copie des titres PSD, paramètres de configuration et données chiffrées.
Objectif	<p>La restauration des données PSD cryptées et des paramètres de configuration après une erreur matérielle ou une erreur de support de stockage.</p> <p>Sinon, les utilisateurs ne pourront plus décrypter leurs données PSD.</p> <p>Remarques :</p> <ul style="list-style-type: none"> • Par contraste avec la sauvegarde PSD, les outils de sauvegarde standards du disque dur produisent des sauvegardes non cryptées. • Si les titres PSD sont perdus et aucune sauvegarde de titre n'est

disponible, mais le fichier d'image PSD ou le fichier d'image de sauvegarde est disponible, ces données peuvent être récupérées via [Récupération Personal Secure Drive](#).

Archives

- Les paramètres de configuration PSD sont inclus dans les **sauvegardes de récupération d'urgence écrites automatiquement** et également dans les **sauvegardes de récupération d'urgence écrites manuellement**.
- **Fichier de sauvegarde PSD** (par exemple SpPSDBackup.fsb) : Une copie de sauvegarde du fichier image PSD peut être créée au cours d'une sauvegarde manuelle de l'utilisateur de Security Platform.

Types de sauvegarde

Type	Explication
Sauvegarde de Système ("Sauvegarde Automatique")	<p>Comprend toujours titres et paramètres de l'ordinateur et de tous les utilisateurs qui sont initialisés au moment où la sauvegarde du système est effectuée (y compris Données de Récupération d'Urgence).</p> <p>Détails sur la manière d'exécuter une Sauvegarde de Système</p>
Sauvegarde Manuelle	<p>Comprend titres et paramètres de l'ordinateur et de l'utilisateur actuel.</p> <p>Comprend Données de Récupération d'Urgence pour l'utilisateur actuel, si la Sauvegarde Automatique a déjà été configurée au moment où la sauvegarde manuelle est effectuée.</p> <p>Vous pouvez facultativement sauvegarder des fichiers d'image Personal Secure Drive (PSD) actuellement configurés pour l'utilisateur actuel.</p> <p>Détails sur l'exécution d'une Sauvegarde Manuelle</p>

Scénarios de restauration

Fonction du type d'urgence, il y a des scénarios de restauration différents :

Scénario de restauration	Portée de restauration concernée
Disque dur brisé ou données perdues	Informations d'identification et paramètres Security Platform, Personal Secure Drive
Trusted Platform Module nouveau	Récupération d'urgence
Security Platform nouveau à initialiser	Récupération d'urgence, informations d'identification et paramètres Security Platform, Personal Secure Drive

Comment sauvegarder et restaurer

Comment configurer les sauvegardes automatiques (« Sauvegarde système »)	Composant logiciel à utiliser
<p>Tâche d'administration : Configurer les sauvegardes automatiques pour tous les utilisateurs (incluant les informations d'identification et paramètres Security Platform, les paramètres de configuration récupération d'urgence et PSD).</p>	<p>Lorsque Security Platform n'est pas encore initialisée :</p> <p>Configuration via Assistant Initialisation rapide</p> <p>Ici la Sauvegarde du Système est automatiquement configurée avec les paramètres par défaut.</p> <p>Configuration via Assistant Initialisation Security Platform</p> <p>Suivez les étapes mentionnées :</p> <ul style="list-style-type: none">• Lancez Infineon Security Platform Settings Tool. Sur la page d'Accueil de l'Assistant d'Initialisation Rapide, sélectionnez Initialisation Avancée.• Sélectionnez l'initialisation de Security Platform et cliquez sur Suivant.• Paramétrez le Mot de Passe Propriétaire et cliquez sur Suivant.• Dans l'Assistant Initialisation, cochez la case à cocher Sauvegarde automatique (inclut Récupération d'urgence) et cliquez sur Suivant.• Parcourez vers un emplacement

sur l'unité de disque dur pour enregistrer la sauvegarde de secours. Un Archive de sauvegarde est formée d'un fichier XML (par ex. SPSysSystemBackup.xml) et un dossier (par ex. SPSysSystemBackup) qui seront créés l'emplacement par défaut : *\%ALLUSERSPROFILE%\My Documents\Security Platform.*

- La sauvegarde quotidienne par défaut est planifiée pour 12H00. Pour modifier l'heure, cliquez sur **Planifier...**, sélectionnez une heure de début pour créer une sauvegarde planifiée et cliquez sur **Ok**, puis cliquez sur **Suivant**.
- Sélectionnez l'option **Créer un nouveau Jeton de Récupération**.
- Parcourez jusqu'à un emplacement de votre choix pour enregistrer le fichier de Jeton de Récupération d'Urgence (nom de fichier par défaut : SPEmRecToken.xml).
- Configurez un nouveau mot de passe pour jeton et cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Cochez la case à cocher **Exécuter sauvegarde automatique maintenant**. Cliquez sur **Terminer** sur la page Fin.
- Les informations d'identification et paramètres Security Platform

sont sauvegardés maintenant pour la première fois. Des sauvegardes régulières seront exécutées selon planification.

Lorsque Security Platform est déjà initialisée : [Outil de paramétrage - Sauvegarde - Configuration...](#)

Suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et sélectionnez **Sauvegarde**.
- Cliquez sur **Configurer...** et lancez l'Assistant Initialisation.
- Parcourez vers un emplacement sur l'unité de disque dur pour enregistrer la sauvegarde de secours. Un Archive de sauvegarde est formée d'un fichier XML (par ex. SPSsystemBackup.xml) et un dossier (par ex. SPSsystemBackup) qui seront créés l'emplacement par défaut : *\%ALLUSERSPROFILE%\My Documents\Security Platform*.
- La sauvegarde quotidienne par défaut est planifiée pour 12H00. Pour modifier l'heure, cliquez sur **Planifier...** , sélectionnez une heure de début pour créer une sauvegarde planifiée et cliquez sur **Ok**, puis cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Cochez la case à cocher **Exécuter sauvegarde automatique maintenant** et

cliquez sur **Terminer** sur la page Fin.

- Les informations d'identification et paramètres Security Platform sont sauvegardés maintenant pour la première fois. Des sauvegardes régulières seront exécutées selon planification.



Ce bouton est désactivé en [mode serveur](#), car la sauvegarde automatique est gérée par Trusted Computing Management Server, donc aucune configuration explicite n'est nécessaire de la part de l'utilisateur.

Comment sauvegarder (« Sauvegarde manuelle »)

Tâche utilisateur : Effectuer la sauvegarde manuelle pour l'utilisateur actuel.

Composant logiciel à utiliser

Suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et sélectionnez **Sauvegarde**. [Outil de paramétrage - Sauvegarde - Sauvegarde...](#)
- Cliquez sur **Sauvegarder...** et lancez l'Assistant Sauvegarde.
- Cliquez sur **Parcourir...** et sélectionnez un emplacement sur l'unité de disque dur pour enregistrer la sauvegarde de secours (Nom par défaut fichier : SPBackupArchive.xml). Cliquez sur **Suivant**.
- Configurez vos paramètres de sauvegarde de Personal Secure Drive (voir [Configurer Paramètres de Sauvegarde de](#)

[Personal Secure Drive](#)) et cliquez sur **Suivant**.

- Confirmez les paramètres et cliquez sur **Suivant**.
- Cliquez sur **Terminer** sur la page Fin.



En [mode serveur](#), vous pouvez seulement sauvegarder votre Personal Secure Drive (PSD). En mode serveur, Trusted Computing Management Server effectue la sauvegarde des titres et paramètres de l'utilisateur. En plus des conditions citées ci-dessus, ce bouton est désactivé si votre Personal Secure Drive (PSD) n'est pas configuré.

Comment restaurer

Tâche d'administration : Préparation de la restauration pour certains utilisateurs.

Tâche utilisateur : Exécuter une restauration manuelle pour l'utilisateur actuel. Lorsque la restauration a été préparée pour l'utilisateur actuel, alors effectuez la restauration.



Lorsqu'une sauvegarde de récupération d'urgence écrite manuellement est disponible et aucune donnée de récupération d'urgence ne doit pas être restaurée, alors un utilisateur peut effectuer la restauration sans être préparée par un administrateur.

Composant logiciel à utiliser

[Outil de paramétrage - Sauvegarder - Restaurer tous...](#)

Comment sauvegarder

Composant logiciel à utiliser

("Sauvegarde manuelle")

Tâche utilisateur : Exécuter une restauration manuelle pour l'utilisateur actuel.

Si les données de Récupération d'Urgence sont comprises dans la sauvegarde manuelle et l'utilisateur courant est l'administrateur, cette sauvegarde peut être utilisée également pour une restauration de Récupération d'Urgence d'un utilisateur courant.

Suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et sélectionnez **Sauvegarde**.
[Security Module - Sauvegarder - Restaurer...](#)
- Cliquez sur **Restaurer...** et lancez l'Assistant Sauvegarde.
- Si vous souhaitez restaurer vos paramètres et titres, vérifiez la case **Restaurer mes paramètres et titres**. Cliquez sur **Parcourir...** et naviguez vers l'Archive de Sauvegarde (nom de fichier par défaut : SPBackupArchive.xml).
- Cliquez sur **Suivant**.
- Authentifiez-vous et cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Si vous souhaitez restaurer un ou plusieurs Personal Secure Drives, configurez vos paramètres de restauration de Personal Secure Drive (voir [Configurer Paramètres Personnels de Restauration Personal Secure Drive](#)).
- Cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Par option, vous pouvez vérifier la case **Démarrer Assistant Initialisation Utilisateur Security Platform** si vous souhaitez configurer d'autres

caractéristiques de Security Platform.

- Cliquez sur **Terminer** sur la page Fin.
- Vos certificats sont maintenant restaurés. Vous pouvez visualiser vos certificats dans **Paramètres utilisateur - Certificats Security Platform**.
- Cliquez avec le bouton droit sur la pictogramme Zone de notification barre de tâches et chargez votre PSD. Authentifiez-vous.



En [mode serveur](#), vous pouvez seulement restaurer votre Personal Secure Drive (PSD). En mode serveur, Trusted Computing Management Server exécute la restauration des informations d'identifications et des paramètres.

Stratégies concernant la sauvegarde

- La configuration des sauvegardes automatiques peut être appliquée par la stratégie [*Application de la configuration de sauvegarde incluant la récupération d'urgence*](#).
- Le chemin de sauvegarde cible pour les sauvegardes automatiques peut être appliqué par la stratégie [*Location de la sauvegarde de secours*](#).
- La mise à jour de la sauvegarde système après des changements significatifs des données Security Platform peut être appliquée avec la stratégie [*Appliquer la sauvegarde système immédiate*](#).



Infineon Security Platform Solution

Gestion de la fonctionnalité de récupération d'urgence

Le logiciel de la solution Infineon Security Platform a été conçu pour offrir une prise en charge étendue, non seulement pour les flux de travaux quotidiens, mais également pour des opérations de récupération sur le système en cas de panne grave.

Le problème le plus grave pouvant survenir est l'endommagement de le Trusted Platform Module. Cette situation conduit à une perte du Propriétaire Infineon Security Platform qui est la racine physique pour secrets ainsi que la racine logique pour toutes les clés spécifiques des Utilisateurs d'Infineon Security Platform. Lorsque Trusted Platform Module doit être remplacé, un nouveau Propriétaire Infineon Security Platform est créé, car il n'y a pas de possibilité de transférer une clé existant d'un Trusted Platform Module à un autre.

Pour surmonter ce problème potentiel, un mécanisme de récupération d'urgence a été intégré dans le logiciel de la solution Infineon Security Platform. Ce mécanisme permet le nouveau chiffrement des Clés Utilisateurs de Base d'un Propriétaire Infineon Security Platform à un autre. A cet effet, une sauvegarde de récupération d'urgence (incluant la récupération d'urgence) doit être créée lors de l'installation d'Infineon Security Platform. L'administrateur le fait en utilisant l'[Assistant d'Initialisation Rapide de Security Platform](#) ou l'[Assistant d'Initialisation de Security Platform](#).

La restauration en cas d'urgence est effectuée en utilisant l'[Assistant Sauvegarde de Security Platform](#).



Trusted Computing Management Server gère la sauvegarde et restauration en [mode serveur](#), sauf pour la sauvegarde et restauration des fichiers image Personal Secure Drive (PSD).

Jeton de récupération d'urgence, mot de passe et archive

Le concept de récupération d'urgence est similaire à la [réinitialisation du mot de passe](#) concernant l'utilisation du jeton, mot de passe et archive.

La restauration des clés utilisateur en cas d'urgence exige quelques informations stockées dans une archive. Les données de récupération d'urgence dans cette archive peuvent être utilisées en combinaison avec un jeton de récupération protégé avec un mot de passe dédié.

L'archive contient des copies cryptées des clés utilisateur de base pour permettre la restauration en cas d'erreur Trusted Platform Module. Lorsque la récupération d'urgence n'est pas configurée, il est possible que les utilisateurs ne puissent pas restaurer leurs données cryptées en cas d'erreur Security Platform. La restauration d'urgence est configurée une seule fois et l'archive respective est accédée automatiquement ultérieurement par les composants de Security Platform. L'archive doit être accédée pour tous les utilisateurs de ce Security Platform.

Pour plusieurs renseignements généraux sur la gestion de la récupération d'urgence, consultez les [Questions répétitives](#).

[Guide pas à pas pour effectuer une récupération d'urgence](#)



Initialisation forcée de l'utilisateur lorsque la sauvegarde de récupération d'urgence n'est pas disponible :

Lorsque la clé utilisateur de base ne peut pas être chargée (par exemple suite à la liquidation de la propriété Trusted Platform Module et la reprise de la propriété), l'Assistant Initialisation de l'utilisateur de Security Platform ne permet pas la continuation de l'initialisation de l'utilisateur. La solution correcte dans cette situation est la restauration de données de récupération d'urgence.

Lorsque la sauvegarde de récupération d'urgence n'est pas disponible pour n'importe quelle raison (par exemple elle est perdue ou corrompue), la clé utilisateur de base ne peut pas être restaurée. Pour continuer la création d'une nouvelle clé utilisateur de base dans ce cas, l'Assistant Initialisation de l'utilisateur de Security Platform doit être lancé avec le [paramètre de commande](#) : `SpUserWz.exe /forceinit`.

Remarque :

- Une nouvelle clé utilisateur de base sera créée et donc toutes les données protégées précédemment seront perdues.
- Le paramètre *SpUserWz.exe /forceinit* de ligne de commande n'est pas supporté dans le [mode serveur](#).



Infineon Security Platform Solution

Guide pas à pas pour effectuer une récupération d'urgence

La procédure de récupération d'urgence permet de restaurer les fonctionnalités d'Infineon Security Platform en cas de tombée en panne et remplacement ultérieur d'un Trusted Platform Module. La procédure de restauration comporte deux étapes :

Ces opérations sont exécutées par un administrateur d'Infineon Security Platform :

- Cette étape comprend l'activation de le Trusted Platform Module, l'initialisation de Security Platform ainsi que la restauration du contenu de la sauvegarde de récupération d'urgence.



Dans le [mode serveur](#), Trusted Platform Module doit être activé avant la connexion du système au Trust Domain par l'administrateur. Aucune tâche administrative n'est disponible, car Trusted Computing Management Server gère ces tâches.

Ces opérations sont exécutées par les utilisateurs d'Infineon Security Platform :

- Restauration des clés utilisateur de base de façon à pouvoir accéder à nouveau aux données protégées, ou génération d'une nouvelle clé utilisateur de base, entraînant la perte de toutes les données existantes protégées.



Conditions préalables :

- **Fichier avec la Sauvegarde de récupération d'urgence :** Ce archive est créé lorsque la fonction de sauvegarde de Security Platform est configurée. La configuration de la fonction de sauvegarde pour inclure la récupération d'urgence est recommandée pour sauvegarder les données utilisateur en cas d'erreur grave du système. La sauvegarde de récupération d'urgence doit être accessible pour le processus de restauration. Celle-ci doit être stockée dans un emplacement à sécurité intégrée, tel qu'un dossier de réseau avec sauvegardes régulières. Lorsqu'elle se trouve sur un disque dur local, l'inclusion du archive dans une sauvegarde périodique est recommandée. Les [questions répétitives](#) contiennent des conseils supplémentaires concernant la configuration correct des

données de récupération d'urgence.

- **Jeton de récupération d'urgence** : Ce jeton protège la sauvegarde de récupération d'urgence de tout accès non autorisé et nécessite l'utilisation d'un mot de passe séparé. Ce fichier est créé lorsque la fonction de sauvegarde de Security Platform est configurée. Cela devrait être stocké en dehors de l'Archive de Sauvegarde sur un support amovible dans un environnement sécurisé. La procédure de récupération doit pouvoir accéder au jeton de récupération d'urgence.
- Trusted Computing Management Server gère la sauvegarde et restauration en [mode serveur](#), sauf pour la sauvegarde et restauration des fichiers image Personal Secure Drive (PSD).

Étapes administratives

Étape n°1 - Préparation de le Trusted Platform Module	Comment procéder :
<p>Une panne de le Trusted Platform Module est une raison qui justifie l'exécution d'une récupération d'urgence. Si c'est le cas, le circuit de remplacement doit d'abord être activé dans le BIOS système.</p> <p>Si la panne est due à un autre composant matériel (par ex. le disque dur), le système devra d'abord être correctement réinstallé (restauration du système d'exploitation, du profil de l'utilisateur ainsi que des données protégées) avant que la restauration de l'Infineon Security Platform puisse avoir lieu.</p>	<p>L'opération est exécutée par un administrateur de système. Une description de la méthode permettant d'activer ce circuit est fournie ici :</p>
Étape n°2 - Initialisation de Security Platform et restauration de données de récupération d'urgence	Comment procéder :
<p>Après avoir activé le Trusted Platform Module, vous devez initialiser Security Platform et restaurer la sauvegarde de récupération d'urgence. Pour pouvoir effectuer cette étape, les fichiers de la sauvegarde de récupération d'urgence ainsi que du jeton de récupération d'urgence doivent être accessibles.</p>	<p>Seul un administrateur d'Infineon Security Platform est en mesure de lancer une procédure de récupération d'urgence. Démarrez l'Assistant Initialisation d'Infineon Security Platform et sélectionnez Restaurer une sauvegarde de récupération d'urgence.</p>

Étape utilisateur

Récupération de l'utilisateur d'Infineon Security Platform	Comment procéder :
<p>Une fois les étapes administratives complétées, la restauration des utilisateurs d'Infineon Security Platform peut être effectuée. La récupération doit s'effectuer séparément pour chaque utilisateur individuel d'Infineon Security Platform dans une étape séparée.</p>	<p>Démarrez l'Assistant Initialisation de l'utilisateur de Security Platform. L'assistant détecte automatiquement l'état de récupération dès qu'il a été lancé. Il permet de choisir entre la création d'une nouvelle clé utilisateur de base ou la restauration d'une clé existante à partir d'une sauvegarde de récupération d'urgence. De manière générale, une clé existante doit être restaurée, sinon tout accès aux données précédemment cryptées sera interdit. Suivez les instructions sur l'écran pour terminer la procédure.</p>



Infineon Security Platform Solution

Mettre à jour les informations d'identification et configuration d'utilisateur (Mode Serveur)

Chaque fois une mise à jour de vos informations d'identification et configuration d'utilisateur est nécessaire, on vous informe par une bulle. Cette bulle est affichée dans la zone de notification de la barre des tâches lorsque vous avez ouvert une session Windows. Cliquez sur la bulle pour exécuter la mise à jour. Si vous n'observez pas ou ignorez cette bulle, vous pouvez lancer la mise à jour par l'intermédiaire d'un [élément du menu Notification de la barre des tâches](#).

Une mise à jour de vos informations d'identification et configuration d'utilisateur est nécessaire dans les situations suivantes :

- Vous n'avez pas encore informations d'identification et configuration d'utilisateur sur la plateforme actuelle (car vous venez de vous y inscrire), mais le Trusted Computing Management Server possède déjà les informations d'identification et configuration pour votre compte utilisateur (car vous avez déjà utilisé une autre plateforme).
- Vous avez déjà des informations d'identification et configuration d'utilisateur sur la plateforme actuelle, mais vos informations d'identification et configuration ont été modifiées depuis une autre plateforme.
- Vous avez eu auparavant des informations d'identification et configuration d'utilisateur sur la plateforme actuelle, mais elles sont perdues (par exemple à cause d'un disque dur cassé).
- Vos informations actuelles d'identification et configuration de l'utilisateur ne sont pas cohérentes (par exemple un changement antérieur a échoué). Dans ce cas vous devez obtenir depuis le serveur vos dernières informations d'identification et paramètres connus et valides.

Ainsi vos informations d'identification et configuration sont synchronisées sur plusieurs plateformes et restaurées sur les plateformes cassées.



- Vérifiez si un Personal Secure Drive n'est pas chargé, avant de mettre à jour vos informations d'identification et configuration.
- La mise à jour de vos informations d'identification et configuration exige votre [authentification de l'utilisateur](#).

Technologies AG



Solution Infineon Security Platform

Récupération de Données EFS et PSD via Agent de Récupération

Un agent de récupération vous permet d'accéder à vos données EFS ou PSD dans les cas suivants :

- Les titres de chiffrement de données sont perdus.
- Aucune sauvegarde de titre n'est disponible.
- Les données chiffrées sont disponibles (Fichiers EFS, fichier d'image PSD ou fichier d'image de sauvegarde).
- Un agent de récupération est disponible.

Plus d'informations relatives à la récupération EFS sont disponibles dans Microsoft TechNet.

Plus d'informations relatives à la récupération PSD sont disponibles ici : [Récupération de Personal Secure Drive](#).



©Infineon Technologies AG

Infineon Security Platform Solution

Migration de clés vers d'autres systèmes

Après avoir installé un utilisateur de système en tant qu'utilisateur d'Infineon Security Platform, il peut s'avérer nécessaire de pouvoir disposer de l'environnement de sécurité spécifique à l'utilisateur, non seulement sur l'ordinateur où l'installation a été effectuée, mais aussi sur d'autres ordinateurs auxquels l'utilisateur peut accéder. Des installations multiples sur différents ordinateurs n'offriront pas de solution puisque les éléments de sécurité ne seront pas compatibles - par exemple, un courrier électronique signé sur un ordinateur ne sera pas accepté par l'autre en raison de la présence de différentes clés de signature.

Concepts de base de la migration

Infineon Security Platform permet de maintenir et de gérer cette situation en offrant un chemin de migration pour le secret spécifique à un utilisateur. L'idée fondamentale de cette technologie est la stricte séparation entre le rôle administratif et le rôle opérationnel d'une migration. Cette séparation est nécessaire pour garantir la confidentialité des secrets transférés et pour empêcher en même temps toute possibilité de transférer ces secrets sans qu'une instance administrative n'en soit avertie.

Après la migration réussie d'un utilisateur, l'ordinateur de destination présente exactement le même environnement de sécurité que celui de l'ordinateur source. Du point de vue de l'utilisateur d'Infineon Security Platform, il n'existe aucune différence dans le comportement opérationnel des systèmes.

Toutefois, les deux ordinateurs restent toujours des systèmes Infineon Security Platform indépendants. La migration des clés utilisateurs n'a aucun impact sur la structure primaire de sécurité d'Infineon Security Platform. Et plus important encore, les secrets stockés dans le Trusted Platform Module ne sont pas affectés par cette opération.



En [mode serveur](#), la migration des informations d'identification et paramètres utilisateur est gérée par Trusted Computing Management Server. A l'ouverture de session, les utilisateurs obtiennent les mises à jour nécessaires chaque fois les informations d'identification et paramètres se sont modifié(e)s. Nommé également *itinération*. La mise à jour depuis la base de données du serveur remplace les informations d'identification locales et les paramètres locaux utilisateur. Dans le mode [autonome](#), les informations d'identification et les paramètres utilisateur sur la source de la migration et l'ordinateur cible sont fusionnées.

L'opération elle-même est exécutée à l'aide de l'[Assistant Migration d'Infineon Security Platform](#).



Migration vers un ordinateur sans les clés et certificats utilisateurs :
Le processus de migration installera des clés et certificats utilisateurs nouveaux sur l'ordinateur vers lequel vous effectuez la migration. Vous devez configurer les fonctionnalités de Security Platform à utiliser avec ces clés et certificats nouveaux.



Migration vers un ordinateur avec des clés et certificats utilisateurs (clé utilisateur de base différente) :

Le processus de migration invalidera les clés et certificats Security Platform existants installés sur l'ordinateur de destination. Vos données cryptées peuvent être perdues suite à cette opération. Décryptez vos données cryptées avant de continuer la migration ou contactez votre administrateur de système pour la procédure de récupération des données.



Migration vers un ordinateur avec clés et certificats utilisateurs (la même clé utilisateur de base) :

Lorsque l'ordinateur de destination utilise déjà la même clé utilisateur de base comme l'ordinateur source, le processus de migration fusionnera vos clés et certificats utilisateur. Après migration, les clés et certificats de la sauvegarde des données de migration seront actifs. Les clés et certificats anciens seront gardés. Ainsi vous ne manquerez pas les données cryptées. Par exemple, lorsque vous avez crypté vos données avec EFS ou PSD sur l'ordinateur source de la migration et sur l'ordinateur de destination, mais vous avez utilisé des certificats différents sur les deux ordinateurs, la migration activera le certificat depuis l'ordinateur source sur l'ordinateur de destination. Le certificat utilisé par l'ordinateur de destination auparavant sera gardé et peut être réactivé n'importe quand.



Migration et Personal Secure Drive :

- Si un utilisateur avait des Personal Secure Drives configurés sur l'ordinateur d'origine sur un support amovible (par ex. USB flash drive), ce support peut aussi être utilisé sur l'ordinateur de destination.
- Si un utilisateur avait des Personal Secure Drives configurés sur l'ordinateur d'origine sur un lecteur dur fixé, il est important de sauvegarder tous les fichiers d'image de Personal Secure Drive à migrer et de stocker les fichiers d'image de sauvegarde sur l'ordinateur d'origine dans un emplacement qui est accessible par tous les deux ordinateurs. Afin d'utiliser une copie d'un Personal Secure Drive d'origine sur l'ordinateur de destination, le fichier d'image de sauvegarde concerné de l'ordinateur d'origine doit être restauré. Notez qu'après la migration vous aurez deux Personal Secure Drives indépendants sur l'ordinateur d'origine et de destination. Les utilisateurs doivent reconfigurer les Personal Secure Drives sur l'ordinateur de destination (voir [Gérer vos Personal](#)

[Secure Drives](#)). Afin de reconfigurer un Personal Secure Drive, sélectionnez *Je souhaite changer mes paramètres de Personal Secure Drive* et suivez les instructions sur l'écran.

- Notez que les paramètres et titres existants de PSD sur l'ordinateur de destination seront supprimés, si les Clés Basiques Utilisateur sont différents sur l'ordinateur d'origine et de destination. Dans ce cas, il vous est recommandé de sauvegarder une copie déchiffrée de vos données PSD avant la migration. Vous pouvez le faire en supprimant le PSD avec l'option de sauvegarder une copie déchiffrée (voir [Gérer vos Personal Secure Drives](#)).



Infineon Security Platform Solution

Migration pas à pas

Le processus de migration des informations d'identification se divise en deux parties : les étapes administratives et les étapes utilisateur. La première partie comprend l'autorisation, l'installation et la gestion du processus de migration effectué par l'administrateur. Une fois les étapes d'administration terminées, les utilisateurs n'ont qu'à exporter et importer leurs clés et certificats de la source vers la cible.



En [mode serveur](#), la migration des clés et certificats utilisateur est gérée par Trusted Computing Management Server, donc vous ne devez pas exécuter les étapes de migration (avec l'exception des Etapes Utilisateur 3 et 4).

Étapes administratives

Étape 1 - Exportation de l'identité de l'ordinateur de destination

Pour effectuer la migration, il faut d'abord identifier un ordinateur de destination sur lequel les clés utilisateur et les certificats doivent être transférés. Pour que cela soit possible, une clé publique identifiant l'ordinateur de destination est rendue disponible (exportée) par un administrateur de l'ordinateur de destination. Cette clé sera utilisée ultérieurement pour assigner les clés utilisateur et les certificats à cet ordinateur (Remarque : Lorsque le contenu est protégé par la clé publique du système de destination, seule la clé privée de l'ordinateur qui est protégée par le Trusted Platform Module peut accéder aux clés et aux certificats transférés). Cette étape est nécessaire pour créer une base de confiance dans l'exécution de la migration - en garantissant que seuls les systèmes de destination choisis peuvent accéder aux informations d'identification secrètes de l'utilisateur.

Comment procéder :

L'administrateur d'Infineon Security Platform du système de destination doit exporter le certificat ordinateur (clé publique) vers un fichier. Suivez les étapes mentionnées :

- Sélectionnez **Migration** dans d'Infineon Security Platform Settings Tool.
- Sélectionnez **Ce système est la plate-forme de destination** et cliquez sur **Enregistrer...**
- Naviguez vers un emplacement de stockage fichier que vous choisissez ; ceci doit être accessible pour les deux ordinateurs. Le fichier est enregistré avec un nom par défaut fichier **SpPubKeyArchive.xml**.

Support de stockage acceptable : Supports amovibles ou unité réseau mappée.

Retenez l'emplacement et le nom fichier pour la clé exportée, car ces infos seront requises dans l'étape suivante.

Étape 2 - Autorisation par le propriétaire de l'ordinateur source

A l'étape suivante de la migration, le propriétaire du système source (l'ordinateur à migrer) doit autoriser la migration des clés utilisateur et des certificats vers un ordinateur de destination spécifique. A cet effet, le propriétaire doit avoir accès à la clé publique de l'ordinateur de destination. Il s'agit de la clé publique exportée antérieurement par un administrateur de l'ordinateur de destination (voir étape n° 1 ci-dessus). L'autorisation, par un propriétaire d'Infineon Security Platform, de l'ordinateur de destination force la pile du logiciel de sécurité à vérifier que les clés utilisateur et les certificats soient exclusivement assignés à l'ordinateur de destination spécifié. Comment procéder :

Comment procéder :

Le propriétaire d'Infineon Security Platform de l'ordinateur source (ordinateur à migrer) doit autoriser l'exportation d'informations d'identification utilisateur vers l'ordinateur de destination. Suivez les étapes mentionnées :

- Sélectionnez **Migration** dans d'Infineon Security Platform Settings Tool.
- Sélectionnez **Ce système est la plate-forme source** et cliquez sur **Autoriser...**
- Dans l'écran Autoriser migration, cliquez sur **Importer...**
- Naviguez vers l'emplacement du fichier clé publique **SpPubKeyArchive.xml** et cliquez sur **Ouvrir**.
- Saisissez le mot de passe du propriétaire de l'ordinateur source et cliquez sur **OK**.
- Vérifiez si le nom hôte de l'ordinateur de destination et l'ID unique plate-forme sont listés et ensuite cliquez sur **Fermer**.

Etape 1 et Etape 2 combinées - Exportation et autorisation automatiques

Il existe une autre manière de combiner et d'exécuter les deux étapes décrites ci-dessus : par l'auto-exportation et l'autorisation qui omet l'étape 1 et qui est très proche de l'étape 2. Le propriétaire d'Infineon Security Platform de l'ordinateur source autorise la migration des clés utilisateur et des certificats situés sur un ordinateur spécifique vers un ordinateur de destination spécifique. La différence est qu'au lieu d'identifier manuellement le fichier avec les références d'identification de l'ordinateur de destination, la plateforme cible est identifiée à l'aide du dialogue de navigation standard d'un ordinateur de réseau. Une fois un système identifié, Infineon Security Platform essaie d'établir un contact dynamique avec le système de destination (en utilisant le mécanisme DCOM) et il demande les clés et certificats de la plateforme. Si le système cible est équipé de l'Infineon Security Platform, l'information de migration sera automatiquement transférée entre les deux ordinateurs.

Conditions préalables :

- Ordinateur source : L'utilisateur actuel (le propriétaire d'Infineon Security Platform) doit être membre du groupe Administrateurs pour l'ordinateur de destination.
- Ordinateur de destination : Infineon Security Platform est installée et activée.
- Ordinateur de destination : La stratégie système *Permettre aux administrateurs de récupérer la clé publique SRK à distance*

Comment procéder :

Le propriétaire d'Infineon Security Platform de l'ordinateur source (ordinateur à migrer) doit autoriser l'exportation des clés et certificats utilisateur vers l'ordinateur de destination. Suivez les étapes mentionnées :

- Sélectionnez **Migration** dans d'Infineon Security Platform Settings Tool.
- Sélectionnez **Ce système est la plate-forme source** et cliquez sur **Autoriser...**
- Dans l'écran Autoriser migration, cliquez sur **Parcourir...** Le dialogue de navigation réseau s'ouvre.
- Naviguez et trouvez l'ordinateur de destination et sélectionnez **OK**.
- Le transfert automatique des informations de migration s'initialise depuis l'ordinateur source vers l'ordinateur de destination.

est activée.

- Ordinateur de destination : Aucun pare-feu ne bloque la demande entrée DCOM (par exemple un pare-feu intégré dans Microsoft Windows XP ou un autre pare-feu).
- Le réseau est configuré pour permettre les demandes DCOM.
- L'ordinateur source et l'ordinateur de destination doivent être membres des domaines autorisés à s'approuver.

Si l'autorisation automatique n'est pas possible, les étapes manuelles (1 et 2) décrites ci-dessus doit être suivies.

Étapes utilisateur



Si le Personal Secure Drive d'un utilisateur est configuré sur l'ordinateur source, c'est important de prendre la sauvegarde de Personal Secure Drive et de stocker le fichier de sauvegarde PSD (nom de fichier par défaut : **SpPSDBackup.fsb**) pour l'ordinateur source dans un emplacement pouvant être accédé depuis les deux ordinateurs. Afin d'utiliser une copie des fichiers d'image PSD de source sur le PC de destination, les fichiers d'image de sauvegarde du PC de source doivent être mis à disposition.

Étape 1 - Exportation des clés utilisateur et des certificats depuis l'ordinateur source

Après avoir finalisé les opérations d'administration, les différents utilisateurs d'Infineon Security Platform sont autorisés à exporter, de façon sécurisée, leurs clés et certificats (protégés par la clé publique du système de destination et, par conséquent, lisibles uniquement par la plateforme de destination).

Comment procéder :

Les utilisateurs d'Infineon Security Platform sur l'ordinateur source exporte leurs clés et certificats pour migration. Suivez les étapes mentionnées :

- Sélectionnez **Migration** dans d'Infineon Security Platform.
- Sélectionnez **Ce système est la plate-forme source** et cliquez sur **Exporter...**
- Choisissez l'ordinateur de destination dans la liste et cliquez sur **Suivant**.
- Naviguez vers un emplacement de stockage fichier que vous choisissiez ; ceci doit être accessible pour les deux ordinateurs. Le fichier est enregistré avec le nom par défaut de fichier

	<p>SpMigrationArchive.xml. Cliquez sur Suivant.</p> <ul style="list-style-type: none"> • Saisissez le mot de passe utilisateur de base pour l'ordinateur source et cliquez sur Suivant. • Confirmez les paramètres et cliquez sur Suivant. • Dans l'écran Dernière page, vérifiez si l'exportation des clés et certificats utilisateur est réussite et cliquez sur Terminer. <p>Retenez l'emplacement et le nom du fichier archive et fichier de sauvegarde PSD, car ces infos seront requises dans l'étape suivante.</p>
<p>Étape 2 - Importation des clés utilisateur et des certificats sur l'ordinateur de destination</p>	<p>Comment procéder :</p>
<p>Puis, les utilisateurs doivent également « importer » les clés et certificats vers les ordinateurs de destination, dans la mesure où ils sont détenteurs d'un compte utilisateur.</p>	<p>Sur un ordinateur de destination, les utilisateurs individuels d'Infineon Security Platform peuvent importer leurs clés et certificats pour migration. Suivez les étapes mentionnées :</p> <ul style="list-style-type: none"> • Sélectionnez Migration dans d'Infineon Security Platform. • Sélectionnez Ce système est la plate-forme de destination et cliquez sur

Importer....

- Naviguez vers l'emplacement du fichier archive **SpMigrationArchive.xml** et cliquez sur **Suivant**.
- Saisissez le mot de passe utilisateur de base configuré sur l'ordinateur source et cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Si les fonctions Security Platform ont été configurées auparavant sur la plateforme de destination, un avertissement s'affiche. Lisez attentivement le message et cliquez sur **Oui**.
- Dans l'écran Dernière page, vérifiez si la migration des clés et certificats utilisateur a été réussite et cliquez sur **Terminer**.
- Dans la fenêtre Terminer de l'assistant, vous avez la possibilité de passer automatiquement à l'étape suivante en sélectionnant l'option **Démarrer l'Assistant Initialisation de l'utilisateur de Security Platform**.

 Notez les conseils sur [Migration et Personal Secure Drives](#).

Étape 3 - Configuration des applications pour utiliser les clés et certificats transférés

Comment procéder :

Une fois la migration des clés et certificats terminée, il est important d'associer ces nouvelles informations d'identification aux différentes applications que l'utilisateur veut utiliser sur l'ordinateur de destination.

Puisque les informations d'identification peuvent être utilisées par des applications très diverses, chaque fournisseur de logiciel d'application proposera sa méthode particulière pour importer les clés et certificats transférés. Par exemple les utilisateurs peuvent configurer le système de fichiers de cryptage (EFS) pour utiliser le certificat migré. Suivez les étapes mentionnées :

- Allez dans **Paramètres utilisateur** dans d'Infineon Security Platform Settings Tool.
- Cliquez sur **Configurer...**
- Suivez les instructions affichées sur l'écran et cliquez sur **Modifier...** dans la page Fonctions Security Platform - Certificat de cryptage.
- Sélectionnez le certificat migré, cliquez sur **OK** et continuez avec la page suivante de l'assistant.

Étape 4 - Reconfiguration de fonctions utilisateur - Personal Secure Drive

Comment procéder :

Une fois que la migration des clés et certificats est complétée, l'utilisateur doit reconfigurer les paramètres de Personal Secure Drive sur l'ordinateur de destination.

Si un ou plus de Personal Secure Drives ont été configurés sur le PC de source, vous devez reconfigurer les Personal Secure Drives migrés sur le PC de destination (voir [Gérer vos Personal Secure Drives](#)). Afin de reconfigurer un Personal Secure Drive, sélectionnez *Je souhaite changer mes paramètres de Personal Secure Drive* et suivez les instructions sur écran. Afin d'utiliser une copie d'une source Personal Secure Drive sur l'ordinateur de destination, le fichier d'image de sauvegarde concerné (nom de fichier par défaut : **SpPSDBackup.fsb**) de l'ordinateur d'origine doit être restauré. Notez qu'après la restauration vous aurez deux Personal Secure Drives indépendants sur l'ordinateur d'origine et de destination.



Infineon Security Platform Solution

Réinitialisation du mot de passe utilisateur de base

La solution Infineon Security Platform permet la réinitialisation des mots de passe utilisateur de base.

Cette fonction peut être utilisée lorsqu'un utilisateur de Security Platform a oublié son mot de passe utilisateur de base ou a des problèmes avec le dispositif d'authentification. Sinon l'accès aux fonctions de Security Platform sera bloqué pour l'utilisateur. Dans ce cas, des données confidentielles seraient perdues.



En [mode serveur](#) le Trusted Computing Management Server gère la tâche de créer un Jeton Réinitialisation Mot de Passe pour tous les utilisateurs, préparer et fournir le Code d'Autorisation de Réinitialisation pour les utilisateurs spécifiques, c'est-à-dire vous n'avez pas besoin d'effectuer ces tâches. Par conséquent, toutes les touches sauf *Réinitialiser* et *Activer* sont désactivées.

Jeton réinitialisation du mot de passe, mot de passe et archive

Le concept de réinitialisation du mot de passe est similaire à la [récupération d'urgence](#) concernant l'utilisation du jeton, mot de passe et archive.

La réinitialisation du mot de passe d'un utilisateur de base exige quelques informations stockées dans une archive. Les données de réinitialisation du mot de passe dans cette archive peuvent être utilisées en combinaison avec un jeton de réinitialisation du mot de passe protégé avec un mot de passe dédié.

Cette archive contient quelques données cryptées pour chaque utilisateur pour permettre le changement du mot de passe d'un utilisateur de base sans connaître le mot de passe courant. Lorsque la réinitialisation du mot de passe n'est pas configurée, les utilisateurs ne pourront pas réinitialiser leurs mots de passe utilisateur de base. La réinitialisation du mot de passe est configurée une seule fois et l'archive respective est accédée automatiquement ultérieurement par les composants de Security Platform. Le fichier archive doit être accédé pour tous les utilisateurs de ce Security Platform.

Comment activer la fonction Réinitialisation du mot de passe

La fonction réinitialisation des mots de passe utilisateur de base peut être utilisée seulement lorsque l'administrateur de Security Platform a configuré cette fonction pour tous les utilisateurs.

Un utilisateur de Security Platform ne peut réinitialiser que son mot de passe, après l'activation de cette fonction pour son compte utilisateur. L'activation exige le mot de passe utilisateur de base ou l'authentification étendue. Un utilisateur ne peut pas donc activer et effectuer la réinitialisation du mot de passe utilisateur de base lorsque le mot de passe courant est déjà perdu.

Comment réinitialiser le mot de passe d'un utilisateur

Pour des raisons de sécurité, la réinitialisation du mot de passe contient deux tâches - une tâche d'administration et une tâche utilisateur. Lorsque votre compte utilisateur est utilisé comme administrateur Security Platform et également comme utilisateur Security Platform, alors vous pouvez réinitialiser votre mot de passe dans une seule étape.

Réinitialisation du mot de passe pas à pas

Comment activer la réinitialisation du mot de passe	Composant logiciel à utiliser
<p>1. Tâche d'administration : Configuration des données de réinitialisation du mot de passe pour tous les utilisateurs.</p> <p> Cette étape peut être appliquée par la stratégie Application de la configuration de réinitialisation mot de passe.</p>	<p>Lorsque Security Platform n'est pas encore initialisée :</p> <p>Configuration via Assistant Rapide Initialisation</p> <p>Ici la Réinitialisation du Mot de Passe est automatiquement configurée avec les paramètres par défaut.</p> <p>Configuration via Assistant Initialisation Security Platform</p> <p>Pour configurer Réinitialisation du mot de passe, suivez les étapes mentionnées :</p> <ul style="list-style-type: none">• Lancez Infineon Security Platform Settings Tool. Sur la page d'Accueil de l'Assistant d'Initialisation Rapide, sélectionnez Initialisation Avancée.• Dans l'Assistant Initialisation, cochez la case à cocher Réinitialisation du mot de passe et cliquez sur Suivant.• Sélectionnez l'option Créer nouveau jeton.• Naviguez vers un emplacement pour enregistrer le fichier jeton de Réinitialisation du mot de passe (nom par défaut de fichier : SPPwdResetToken.xml). Support de stockage acceptable : Support amovible ou unité

réseau mappée.

- Configurez un nouveau mot de passe pour jeton et cliquez sur **Suivant**
- Confirmez les paramètres et cliquez sur **Suivant**.
- Dans l'écran Dernière page, cliquez sur **Terminer**.

Lorsque Security Platform est déjà initialisée : [Outil de paramétrage - Réinitialisation mot de passe - Configuration...](#)

Pour configurer Réinitialisation du mot de passe, suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et sélectionnez **Réinitialisation du mot de passe**.
- Cliquez sur **Configurer...**
- Sélectionnez l'option **Créer nouveau jeton**.
- Naviguez vers un emplacement pour enregistrer le fichier jeton de Réinitialisation du mot de passe (nom par défaut de fichier : **SPPwdResetToken.xml**).
Support de stockage acceptable : Support amovible ou unité réseau mappée.
- Configurez un nouveau mot de passe pour jeton et cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Dans l'écran Dernière page, cliquez sur **Terminer**.

2. Tâche utilisateur : Activer la fonction réinitialisation pour l'utilisateur actuel.



Cette étape peut être appliquée par la stratégie [Application de l'activation de la réinitialisation mot de passe](#).

Lorsque l'utilisateur n'est pas encore initialisé : [Assistant Initialisation de l'utilisateur](#)

Pour activer Réinitialisation du mot de passe et créer un secret personnel pour l'utilisateur, suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool. Sur la page d'Accueil de l'Assistant d'Initialisation Rapide, sélectionnez **Initialisation Avancée**.
- Dans l'Assistant Initialisation de l'utilisateur, cochez la case à cocher **Activer la réinitialisation du mot de passe utilisateur de base en cas d'urgence**.
- Parcourez vers un emplacement sur l'unité de disque dur pour enregistrer le fichier secret personnel (nom par défaut de fichier : **SPPwdResetSecret.xml**). Cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Les fonctions Security Platform peuvent être configurées plus tard. Décochez toutes les options et cliquez sur **Suivant**.
- Dans l'écran Dernière page, cliquez sur **Terminer**.

Lorsque l'utilisateur est déjà initialisé : [Outil de paramétrage - Réinitialisation mot de passe -](#)

[Activation...](#)

Pour créer un nouveau secret personnel pour l'utilisateur courant, suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et sélectionnez **Réinitialisation du mot de passe**.
- Cliquez sur **Activer...** Un message d'information apparaît. Lisez attentivement le message et cliquez sur **OK**.
- Parcourez vers un emplacement sur l'unité de disque dur pour enregistrer le fichier secret personnel (nom par défaut de fichier : **SPPwdResetSecret.xml**).
- Lorsqu'on vous demande **Voulez-vous le remplacer**, cliquez sur **Oui**.
- Authentifiez-vous et cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Dans l'écran Dernière page, cliquez sur **Terminer**.

Comment réinitialiser le mot de passe d'un utilisateur

3. Tâche d'administration : Préparation de la réinitialisation du mot de passe pour un utilisateur ou préparation et réinitialisation pour le compte administrateur courant dans une seule étape.

Composant logiciel à utiliser

[Outil de paramétrage - Réinitialisation mot de passe - Préparation...](#) (démarrage de l'assistant Réinitialisation mot de passe)

Pour créer un code d'autorisation pour

réinitialisation du mot de passe pour un certain utilisateur, suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et sélectionnez **Réinitialisation du mot de passe**.
- Cliquez sur **Préparer...**
- Sélectionnez dans la liste un utilisateur spécifique dont le mot de passe doit être réinitialisé et cliquez sur **Suivant**.
- Parcourez vers l'emplacement du fichier jeton de réinitialisation du mot de passe (nom par défaut de fichier : **SPPwdResetToken.xml**) et saisissez le mot de passe qui protège ce fichier. Cliquez sur **Suivant**.
- Parcourez vers un emplacement (par exemple une unité réseau mappée sur le disque dur) pour enregistrer le code d'autorisation pour réinitialisation du mot de passe (nom par défaut de fichier : **SPPwdResetCode.xml**), pour que l'utilisateur puisse l'accéder. Cliquez sur **Suivant**.
- Dans l'écran Dernière page, cliquez sur **Terminer**.

Pour préparer et réinitialiser le mot de passe utilisateur de base pour l'administrateur courant, suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et

sélectionnez **Réinitialisation du mot de passe**.

- Cliquez sur **Préparer...**
- Sélectionnez l'administrateur dont le mot de passe doit être réinitialisé et cliquez sur **Suivant**.
- Parcourez vers l'emplacement du fichier jeton de réinitialisation du mot de passe (nom par défaut de fichier : **SPPwdResetToken.xml**) et saisissez le mot de passe qui protège ce fichier. Cliquez sur **Suivant**.
- Naviguez vers l'emplacement du fichier secret personnel (nom par défaut de fichier : **SPPwdResetSecret.xml**) et cliquez sur **Suivant**.
- Saisissez et confirmez un nouveau mot de passe utilisateur de base et cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Dans l'écran Dernière page, cliquez sur **Terminer**.

4. Tâche utilisateur : Réinitialiser le mot de passe pour l'utilisateur actuel (possible seulement lorsque la réinitialisation du mot de passe est déjà préparée pour cet utilisateur).

[Outil de paramétrage - Réinitialisation mot de passe - Réinitialisation...](#) (démarre l'assistant Réinitialisation mot de passe)

Pour réinitialiser le mot de passe utilisateur de base pour l'utilisateur courant, suivez les étapes mentionnées :

- Lancez Infineon Security Platform Settings Tool et

sélectionnez **Réinitialisation du mot de passe**.

- Cliquez sur **Réinitialiser...**
- Naviguez vers l'emplacement du fichier secret personnel (nom par défaut de fichier : **SPPwdResetSecret.xml**).
- Naviguez vers l'emplacement du fichier code d'autorisation pour réinitialisation du mot de passe (nom par défaut de fichier : **SPPwdResetCode.xml**) et cliquez sur **Suivant**.
- Saisissez et confirmez un nouveau mot de passe utilisateur de base et cliquez sur **Suivant**.
- Confirmez les paramètres et cliquez sur **Suivant**.
- Dans l'écran Dernière page, cliquez sur **Terminer**.



Infineon Security Platform Solution

Défense contre les attaques de type dictionnaire



Remarques :

- Ce sujet s'applique seulement aux Security Platforms avec un Trusted Platform Module 1.2. Les détails pour le mécanisme de défense contre les attaques de type dictionnaire Security Platform ne sont valides que pour les Security Platforms avec un Infineon Trusted Platform Module 1.2.
- Ce sujet s'adresse principalement au propriétaire de Infineon Security Platform.

Une **Attaque de type dictionnaire** est une méthode utilisée pour briser les systèmes de sécurité, surtout les systèmes de sécurité basés sur mots de passe, dans laquelle l'attaquant test systématiquement tous les mots de passe possibles en commençant par des mots ayant une possibilité élevée d'être utilisés, par exemple noms et places. Le mot "dictionnaire" signifie l'utilisation par un attaquant de tous les mots d'un dictionnaire en essayant de découvrir le mot de passe. Les attaques de type dictionnaire sont exécutées habituellement par un logiciel et non manuellement.

Une attaque de type dictionnaire contre la solution Infineon Security Platform peut essayer de briser le [mot de passe du propriétaire](#), le [mot de passe d'un utilisateur de base](#) ou des clés protégées par des mots de passe. Une attaque de type dictionnaire contre un mot de passe est nommée également un **attaque du mot de passe**. Dans la version TCG 1.2 standard, on a introduit un mécanisme de protection contre les attaques de type dictionnaire. La solution Infineon Security Platform utilise ce mécanisme. Les mesures de défense ne sont pas prises seulement dans le cas d'une attaque réelle, mais également lorsque plusieurs saisies erronées accidentelles des mots de passe sont effectuées.

Comment éviter les attaques de type dictionnaire

Recommandations pour éviter les attaques de type dictionnaire :

- Respectez les mesures générales de sécurité, comme présentées par les portails de sécurité.
- Configurez des valeurs assez basses pour le seuil pour les attaques de type dictionnaire (voir la stratégie [Configuration du seuil pour les attaques de type dictionnaire](#)).
- Utilisez des mots de passe complexes, pour empêcher leur brisure.

Comment réagir aux attaques de type dictionnaire

Lorsqu'une Infineon Security Platform rapporte une attaque de type dictionnaire, analysez les mesures suivantes :

- Pour commencer, laissez votre système désactivé temporairement.
- Déconnectez votre système du réseau.
- Vérifiez le Visualisateur d'événements Microsoft pour plusieurs renseignements.
- Visitez les portails de sécurité pour informations sur les dernières menaces contre la sécurité.
- Détectez et éliminez l'application ou le service attaquant. Analysez la possibilité de contacter un spécialiste pour vous aider.
- Prenez les mesures de sécurité pour bloquer autres attaques (par ex. en installant les mises à jour de sécurité, configurant les pare-feu et les stratégies de sécurité).

Connectez votre système au réseau. Redémarrez votre système pour activer à nouveau Infineon Security Platform.

[Mesures de défense contre les attaques de type dictionnaires](#)

[Interface utilisateur pour les attaques de type dictionnaire](#)



Technologies AG

Infineon Security Platform Solution

Mesures de défense contre les attaques de type dictionnaires



Remarques :

- Ce sujet s'applique seulement aux Security Platforms avec un Trusted Platform Module 1.2. Les détails pour le mécanisme de défense contre les attaques de type dictionnaire Security Platform ne sont valides que pour les Security Platforms avec un Infineon Trusted Platform Module 1.2.
- Ce sujet s'adresse principalement au propriétaire de Security Platform.

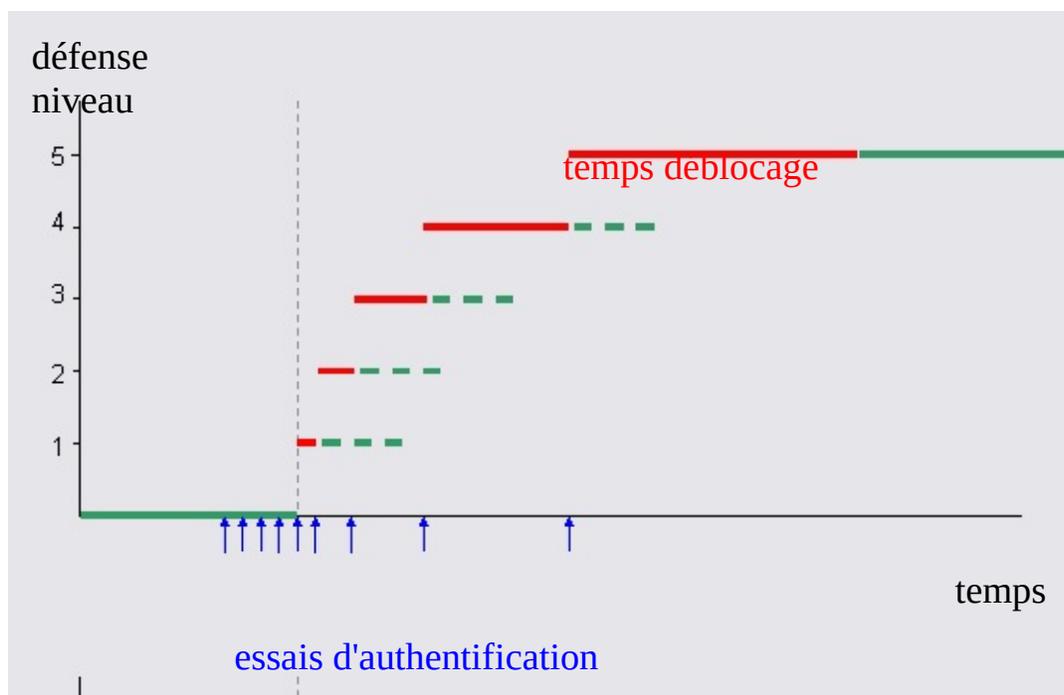
La solution Security Platform rejette les attaques de type dictionnaire en utilisant les mesures suivantes :

- S'il y a multiples essais d'authentification échoués, Security Platform est **temporairement désactivée** jusqu'au redémarrage prochain du système. Ainsi le propriétaire de Security Platform peut prendre des mesures supplémentaires contre les attaques avant de réactiver Security Platform.
- En plus un **temps de déblocage** est activé : Les essais supplémentaires d'authentification sont rejetés pour un certain intervalle. Chaque essai d'authentification échoué augmente le **niveau de défense**, en doublant le temps de déblocage.
- S'il n'y a plus d'essais d'authentification échoués pour un certain intervalle, le niveau de défense est réduit.
- Le propriétaire de Security Platform peut **réinitialiser** le niveau de défense.

Les illustrations suivantes décrivent ces mesures.

Le niveau de défense est augmenté suite aux essais d'authentification échoués répétés

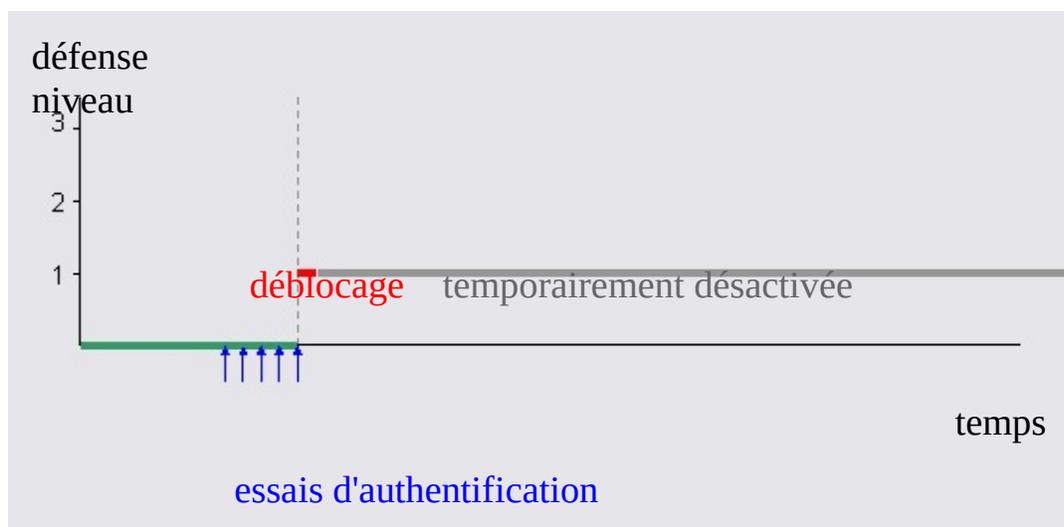
Cette illustration présente comment les essais d'authentification échoués déterminent l'augmentation du niveau de défense et du temps de déblochage, lorsque Security Platform n'est pas temporairement désactivée.



Dans cet exemple, le seuil de défense est le cinquième essai d'authentification. L'attaquant essaie de s'authentifier. Par suite, le niveau de défense est augmenté quand le temps de déblochage de l'état actuel est expiré.

Eviter l'augmentation du niveau de défense en désactivant temporairement Security Platform

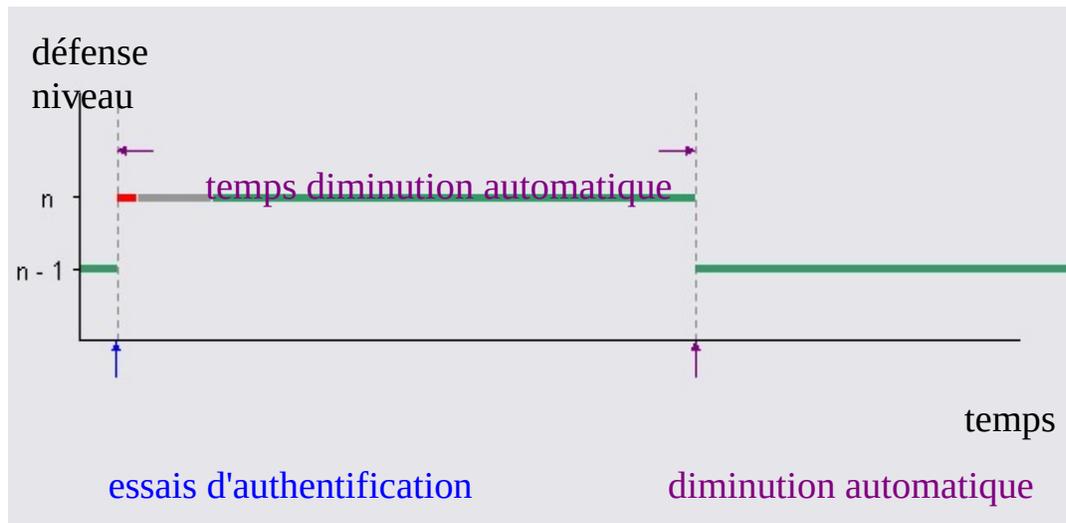
Pour bloquer autres attaques dans une première phase et pour éviter des temps de déblocage longues, Security Platform est temporairement désactivée quand le seuil de défense est dépassé.



Dans cet exemple Security Platform ne peut plus être attaquée, même après l'expiration du temps de déblocage. Security Platform sera activée une fois le système redémarré.

Diminution automatique du niveau de défense

Cette illustration présente comment le niveau de défense est diminué à nouveau après un certain intervalle, lorsqu'il n'y a plus d'essais d'authentification échoués.



Dans cet exemple un essai d'authentification échoué détermine une augmentation du niveau de défense et un temps de déblocage(rouge). On suppose que le système est redémarré après un intervalle court (gris). Lorsque le temps de diminution automatique est expiré, le niveau de défense est réduit en mode automatique. Pour les niveaux bas de défense, le temps de diminution automatique est beaucoup plus élevé que le temps de déblocage.

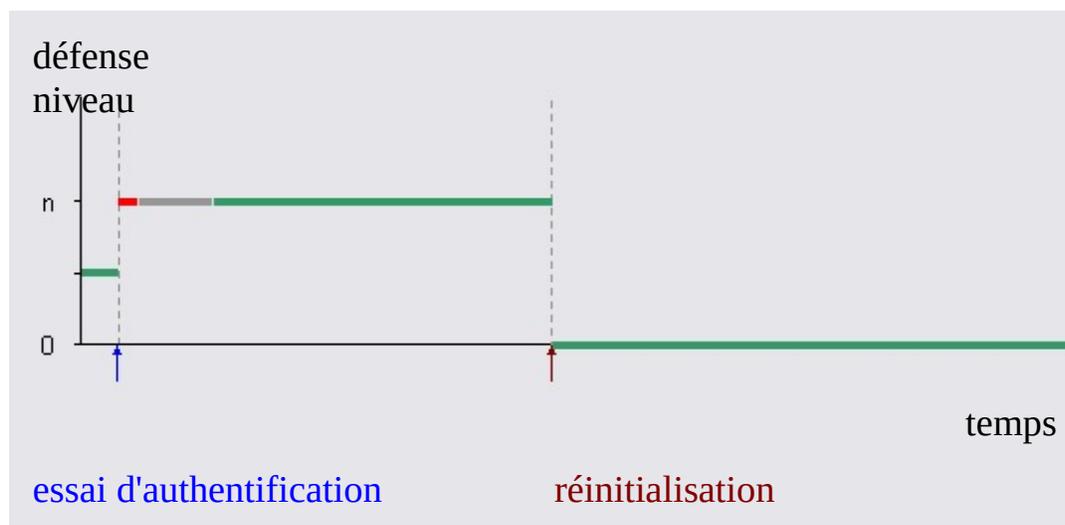


Remarques :

- Le temps de diminution automatique ne dépend pas du temps de déblocage et du redémarrage du système.
- La diminution automatique n'exige pas un redémarrage du système.
- Pour les niveaux bas de défense, le temps de diminution automatique est beaucoup plus élevé que le temps de déblocage.

Réinitialisation niveau défense

Cette illustration présente la réinitialisation du niveau de défense réalisée par le propriétaire de Security Platform.



Comme dans l'illustration précédente, vous pouvez remarquer l'augmentation du niveau de défense, le temps de déblocage (**rouge**) et le système désactiver temporairement jusqu'au prochain redémarrage du système (**gris**). Ici on suppose que le propriétaire de Security Platform réinitialise le niveau de défense, car il ne veut plus attendre l'augmentation automatique di niveau de défense.

Paramètres typiques pour la défense contre les attaques de type dictionnaire

La table suivante présente quelques paramètres typiques pour la défense contre les attaques de type dictionnaire pour les Infineon Trusted Platform Module. Les valeurs présentées peuvent être différentes pour votre Trusted Platform Module.

Essais autorisés pour l'authentification de Clé (par ex. utilisés pour l'authentification de l'Utilisateur de Security Platform)	5	Après 5 essais échoués dans une période de 6 heures, des mesures de défense contre les attaques de type dictionnaire sont prises (voir la stratégie Configuration du seuil pour les attaques de type dictionnaire et Configurer Paramètres de Défense d'Attaque par Dictionnaire).
Essais permis pour authentification du propriétaire de Security Platform	3	Après 3 essais échoués dans une période de 6 heures, des mesures de défense contre les attaques de type dictionnaire sont prises (voir la stratégie Configuration du seuil pour les attaques de type dictionnaire et Configurer Paramètres de Défense d'Attaque par Dictionnaire).
Essais autorisés pour l'authentification de Données (par ex. utilisés par Windows BitLocker en combinaison avec PIN)	10	Après 10 tentatives manquées pendant 6 heures, des mesures de défense d'attaque par dictionnaire sont prises (voir stratégie Configuration du seuil pour les attaques de type dictionnaire et Configurer Paramètres de Défense d'Attaque par Dictionnaire).
Temps de déblocage minimum	~10 s	Le temps de déblocage initial après le dépassement du seuil est de 10 secondes.
Temps de déblocage	~24	Le temps de déblocage maximal est de 24

maximal	h	heures. Cette limite est atteinte pour moins de 15 essais d'authentification échoués après le dépassement du seuil.
Temps de diminution automatique du niveau de défense	~6 h	Environ 6 heures après avoir atteint un certain niveau de défense, le niveau de défense est réduit en mode automatique par 1. Cette opération s'applique seulement s'il n'y a plus d'essais d'authentification échoués pendant les 6 heures. Un tel essai augmente le niveau de défense par 1.

Ces paramètres assurent un niveau de sécurité élevé dans le cas d'une attaque réelle de type dictionnaire. D'un autre côté, la saisie accidentelle d'un mot de passe erroné est gérée d'une manière amicale et flexible.



Le temps de déblocage et temps de diminution automatique du niveau de défense ne s'appliquent que pour les systèmes en fonction.



Infineon Security Platform Solution

Interface utilisateur pour les attaques de type dictionnaire



Remarques :

- Ce sujet s'applique seulement aux Security Platforms avec un Trusted Platform Module 1.2. Les détails pour le mécanisme de défense contre les attaques de type dictionnaire Security Platform ne sont valides que pour les Security Platforms avec un Infineon Trusted Platform Module 1.2.
- Ce sujet s'adresse principalement au propriétaire de Security Platform.

Le propriétaire et l'administrateur de Security Platform sont responsables pour les paramètres et les mesures de défense contre les attaques de type dictionnaire. En cas d'une saisie incorrecte répétée d'un mot de passe ou en cas d'une attaque réelle de type dictionnaire, l'utilisateur de Security Platform est informé.

La table suivante présente les composantes de l'interface utilisateur liées aux attaques de type dictionnaire :

Configure dictionary attack threshold	Le propriétaire de Security Platform ou un administrateur autorisé peut configurer le nombre d'essais échoués permis avant de prendre des mesures de défense contre les attaques de type dictionnaire. Cela peut être fait soit via la configuration des Paramètres de la Security Platform , ou via la stratégie Configuration du seuil pour les attaques de type dictionnaire .
Réinitialisation niveau défense	<p>Mode autonome :</p> <p>Le Propriétaire de Security Platform peut réinitialiser le niveau de défense via Outil de Paramétrage – Avancé – Réinitialiser.... L'Assistant d'Initialisation de Security Platform <i>SpTPMWz.exe</i> est alors lancé avec le paramètre de la ligne de commande <code>-resetattack</code>.</p> <p> Le mot de passe du propriétaire est exigé pour exécuter cette opération. Saisissez le mot de passe correcte. Après plusieurs saisies erronées du mot de passe du propriétaire, votre Security Platform sera bloquée temporairement. Pendant ce temps vous ne pourrez plus réinitialiser le niveau de défense contre les attaques de type dictionnaire.</p>

Mode serveur :

Trusted Computing Management Server représente une modalité efficace et sûre, contrôlée par le serveur, pour réinitialiser le niveau de défense contre les attaques de type dictionnaire :

- La fonction Réinitialisation du niveau de défense peut être configurée et gérée sans la présence locale d'administrateurs et sans connaître les mots de passe des propriétaires.
- La réinitialisation du niveau de défense peut être lancée depuis une plateforme Trust Domain à distance, depuis n'importe quel ordinateur ayant une connexion réseau vers le serveur Trust Domain.



Si l'administrateur connaît le mot de passe du propriétaire, le niveau de défense peut être réinitialisé également localement en lançant l'Assistant pour l'initialisation de Security Platform *SpTPMWz.exe* avec le paramètre de ligne de commande *-resetattack* ou */resetattack*. Ceci est la seule utilisation permise pour l'Assistant pour l'initialisation de Security Platform dans le mode serveur.

Notifications et avertissements

Des **messages** expliquant l'état actuel et les mesures de défense contre les attaques de type dictionnaire sont affichés dans les situations suivantes :

- Authentification échouée (pour le propriétaire de Security Platform et les utilisateurs de Security Platform)
- Dépassement du seuil pour les attaques de type dictionnaire
- Essai d'authentification au cours du temps de déblocage

En cas d'une attaque réelle de type dictionnaire (qui n'est pas déterminée par essais échoués accidentels d'authentification) un **message d'erreur alarme est affiché.**



Solution Infineon Security Platform

Configurer les Paramètres de Défense d'Attaque par Dictionnaire

Cette page vous permet de configurer le nombre d'essais d'authentification qui devraient être autorisés pour différents types d'authentification avant que des mesures de défense d'attaque par dictionnaire ne soient prises.



Notes :

- Ce sujet est seulement important pour Security Platforms avec un Trusted Platform Module 1.2. Les détails du mécanisme de défense d'attaque par dictionnaire de la Security Platform sont seulement valides pour les Security Platforms avec un Infineon Trusted Platform Module 1.2.
- Ce sujet est principalement orienté vers le Propriétaire de la Security Platform.



Disponibilité de la page :

- Cette page d'assistant est seulement disponible si la [stratégie Configurer seuil d'attaque par dictionnaire](#) n'est pas configurée.

Le tableau suivant indique des conseils comment utiliser cette page d'assistant.

Élément de Page de l'Assistant	Explication
<input type="radio"/> <i>Compteurs spécifiques d'authentification</i>	Sélectionnez cette option si vous souhaitez déterminer le nombre d'essais autorisés pour chaque type d'authentification individuellement.
<input checked="" type="checkbox"/> <i>Seuls compteurs concernant Security Platform</i>	Sélectionnez cette option si vous souhaitez seulement configurer des types d'authentification qui concernent la Security Platform Solution. Dans ce cas, seuls les types suivants d'authentification sont affichés : <ul style="list-style-type: none">• Authentification Propriétaire• Authentification Clé (par ex. utilisé pour l'authentification Utilisateur de la Security Platform)• Authentification Données (par ex. utilisé par

	<p>Windows BitLocker en combinaison avec PIN)</p> <p>Décochez cette option si vous désirez configurer également autres types d'authentification qui ne sont pas pertinentes pour la solution Security Platform. Pour informations détaillées sur ces types d'authentification, consultez les spécifications des Trusted Computing Group (TCG) et celles des votre fournisseur Trusted Platform Module.</p> <p>Des mesures de défense contre les attaques de type dictionnaires sont prises lorsqu'on dépasse le nombre de tentatives permises pour un certain compteur, sans tenir compte si le type d'authentification respectif est pertinent pour la solution Security Platform ou non.</p>
<input type="radio"/> <i>Compteur global d'authentification</i>	<p>Sélectionnez cette option si vous souhaitez déterminer un compteur global d'authentification pour tous les types d'authentification. Tout échec d'authentification conduit à augmenter ce compteur, indépendamment du type d'authentification.</p>
<input type="checkbox"/> <i>Types d'authentification</i>	<p>Cette liste affiche tous les types d'authentification avec les valeurs minimum, maximum et configurées actuellement pour le nombre d'essais d'authentification autorisés.</p> <p>Changez le nombre d'essais autorisé selon vos souhaits. Assurez-vous d'entrer seulement des chiffres entiers dans la limite autorisée du minimum au maximum.</p>
<input checked="" type="checkbox"/> <i>Désactiver la plateforme temporairement</i>	<p>Sélectionnez cette option, si vous souhaitez que les mesures de défense comprennent temporairement la désactivation de la Security Platform.</p>



Infineon Security Platform Solution

Réinitialisation du niveau de défense contre les attaques de type dictionnaire



Remarques :

- Ce sujet s'applique seulement aux Security Platforms avec un Infineon Trusted Platform Module 1.2. Les détails pour le mécanisme de défense contre les attaques de type dictionnaire Security Platform ne sont valides que pour les Security Platforms avec un Infineon Trusted Platform Module 1.2.
- Ce sujet s'adresse principalement au propriétaire de Security Platform.

La réinitialisation du niveau de défense commence à afficher des renseignements sur l'état des attaques de type dictionnaire. Un message est présenté au propriétaire du Security Platform.

Étapes de la réinitialisation du niveau de défense

Étape	Commentaires
1. Renseignements sur l'état des attaques de type dictionnaire	<p>Cette page fournit les informations détaillées suivantes nécessaires pour décider si le niveau de défense doit être réinitialisé ou non :</p> <p>Etat général d'attaque par dictionnaire : indique si des mesures de défense d'attaque par dictionnaire sont actuellement en vigueur ou pas.</p> <p>Temps restant de verrouillage : Affiche le temps restant, si un verrouillage est actuellement en vigueur.</p> <p>Liste de type d'authentification : Affiche les informations relatives à l'état pour plusieurs types d'authentification, par exemple types d'authentification pour clés (par ex. utilisés pour Authentification Utilisateur de Security Platform), propriétaire et pour l'accès aux données verrouillées (par ex. utilisés par Windows BitLocker en combinaison avec PIN).</p> <p>Les informations suivantes sont affichées pour chaque type d'authentification :</p> <ul style="list-style-type: none">• Essais Autorisés : Nombre d'essais autorisés du Trusted Platform Module, avant que des mesures de défense d'attaque par dictionnaire ne soient prises (voir Interface Utilisateur Attaque par Dictionnaire, section "Configuration du seuil pour les attaques de type dictionnaire").• Compteur Courant : Nombre de tentatives courantes manquées effectives.• Temps suivant de verrouillage : Cela indique le temps de verrouillage après le prochain échec d'authentification, si le compteur courant est déjà au-dessous du nombre d'essais autorisés. Sinon, il indique le temps de verrouillage lorsque le seuil est en voie d'être dépassé. <p>Le compteur courant et le prochain temps de verrouillage dépendent du nombre d'essais autorisés, du nombre total</p>

d'authentification échouées dans le passé et du temps écoulé depuis la dernière authentification échouée (voir [baisse automatique de niveau de défense](#)).

Réactualiser : Cliquez sur ce bouton ou appuyez sur la touche "F5" afin de réactualiser les informations relatives à l'état d'attaque par dictionnaire.

Afficher types d'authentification non critiques : Par défaut, seuls les types d'authentification avec les compteurs courants supérieurs à zéro sont affichés. Vérifiez cette option pour afficher également les types d'authentification avec le compteur courant à zéro.

 Les informations sur l'état des attaques de type dictionnaires sont affichées seulement si elles peuvent être récupérées du Trusted Platform Module.

2. Saisir le mot de passe du propriétaire de Security Platform

Le mot de passe du propriétaire est nécessaire pour réinitialiser le niveau de défense. Vous pouvez soit taper le Mot de Passe Propriétaire soit donner un Fichier de Sauvegarde de Mot de Passe Propriétaire.

-  Assurez-vous de fournir le mot de passe correct. Des mesures de défense contre les attaques de type dictionnaires peuvent être prises. Dans ce cas, vous ne pourrez plus réinitialiser le niveau de défense contre les attaques de type dictionnaire.



Infineon Security Platform Solution

Outils de la solution Infineon Security Platform



Il y a quelques différences dans le comportement des outils de la solution Security Platform en [mode serveur](#).

Le logiciel de la solution Infineon Security Platform fournit les outils d'administration suivants :

Outil solution Security Platform	But
Outil de paramétrage Security Platform	<ul style="list-style-type: none">• Obtention des informations variées sur le Trusted Platform Module de votre système.• Exécution de quelques tâches d'administration. <p>Cette composante est conçue comme un applet Control Panel. Il représente un point central d'accès pour l'administration de l'Infineon Security Platform.</p>
Assistant d'Initialisation Rapide de Security Platform	<ul style="list-style-type: none">• Installez rapidement votre Infineon Security Platform et Utilisateur (recommandé pour la plupart des utilisateurs).
Assistant Initialisation de Security Platform	<ul style="list-style-type: none">• Configuration de votre Infineon Security Platform (pour utilisateurs experts).
Assistant Initialisation de l'utilisateur de Security Platform	<ul style="list-style-type: none">• Configuration de vos utilisateurs d'Infineon Security Platform.
Assistant Migration de Security Platform	<ul style="list-style-type: none">• Migration de clés et certificat utilisateur d'Infineon Security Platform d'une Infineon Security Platform vers une autre d'une manière sécurisée et assurant le caractère privé.
Assistant Sauvegarde de Security Platform	<ul style="list-style-type: none">• Effectuer les opérations de sauvegarde et restauration pour des données de la Security Platform.
Assistant Réinitialisation du	<ul style="list-style-type: none">• Réinitialisation des mots de passe utilisateur de base.

mot de passe de Security Platform	
Assistant d'Importation PKCS #12 de Security Platform	<ul style="list-style-type: none"> • Importation des fichiers d'échange d'informations personnels dans la Security Platform.
Visualisateur du certificat et sélection du certificat de Security Platform	<ul style="list-style-type: none"> • Gestion de certificats.
Pictogramme Zone de notification barre de tâches de Security Platform	<ul style="list-style-type: none"> • Exécuter des tâches administratives de Security Platform et obtenir des informations sensibles.
Administration de stratégie d'Infineon Security Platform	<ul style="list-style-type: none"> • Administrer des stratégies système et utilisateur liées à l'Infineon Security Platform.
Services d'intégration de Security Platform	<ul style="list-style-type: none"> • Permettre aux applications standards d'utiliser la fonction Trusted Platform Module.
Services de Security Platform	<ul style="list-style-type: none"> • Fournir une pile logicielle compatible avec le Trusted Computing Group (TCG).



©Infineon

Infineon Security Platform Solution

Utilisation des assistants de Security Platform

La solution Security Platform utilise l'outil de paramétrage comme un point central d'accès pour l'administration de l'Infineon Security Platform. Les tâches de configuration initiale et ultérieure sont facilitées par des assistants.

Pages assistant

Page d'accueil

C'est la première page de l'assistant. Elle vous explique le but de l'assistant. Cette page est affichée seulement lorsque la fonction complète de l'assistant est nécessaire. Elle n'est pas affichée lorsque l'assistant est lancé à partir de l'outil de paramétrage pour exécuter une tâche d'administration définie.

Pages internes de l'assistant

Ces pages demandent une saisie de la partie de l'utilisateur pour collecter les informations demandées pour exécuter la tâche de l'assistant.

Page de confirmation

La page de confirmation liste toutes les informations pertinentes et les actions à exécuter.



Jusqu'à ce moment aucun changement n'a pas été effectué. Les actions présentées seront exécutées lorsque vous cliquez sur **Suivant**.

Page de finalisation

C'est la dernière page de l'assistant. Elle vous informe sur la finalisation de l'assistant (succès ou échec) et liste toutes les actions finalisées.

Lorsque le processus général de configuration demande le démarrage d'un autre assistant avant d'utiliser les fonctions de la Security Platform, vous pouvez sélectionner de continuer automatiquement l'exécution avec l'assistant suivant.

Exemple : Après avoir initialisée ou restaurée votre Security Platform (Assistant Initialisation de la Platform), vous pouvez éventuellement continuer avec l'initialisation des utilisateurs (Assistant d'initialisation de l'utilisateur).

Dans la page finale de **l'Assistant Initialisation de Security Platform** vous pouvez décider lorsque la [sauvegarde automatique](#) peut être exécutée pour mettre à jour la sauvegarde de secours du système en cas des changements significatifs. Cette option n'est pas disponible lorsque la stratégie [Appliquer la sauvegarde de système immédiate](#) n'est pas configurée.

Indication du progrès de l'assistant

L'Identification de Progrès de l'Assistant dans la partie haute à droit de la page de l'assistant visualise les étapes de l'assistant demandées et souligne l'étape actuelle. L' Identification de Progrès de l'Assistant est prise en charge par tous les Assistant ayant des pages et étapes de configuration multiples. Cela vous donne des informations sur les étapes à réaliser pour exécuter une certaine tâche :

- Chaque pas est représenté par une petit rectangle.
- Le rectangle représentant le pas actuel est mis en évidence.
- Déplacez votre souris sur les rectangles pour visualiser les informations pour les pas individuels.

Comportement de l'assistant en cas d'échec

En cas d'échec, les changements prévus pour la Security Platform ne sont pas exécutés. Un message d'erreur est affiché.

Conditions préalables générales pour l'exécution d'un assistant

Condition préalable	Explication
Droits d'administration Windows et stratégies Windows	Assistant Initialisation de Security Platform/Assistant d'Initialisation Rapide de Security Platform (si la plateforme n'est pas encore initialisée) : L'utilisateur actuel doit avoir des droits d'administration Windows (c.-à-d. il doit être membre du groupe Administrateurs). Pour un système avec un Trusted Platform Module désactivé, l'utilisateur actuel doit pouvoir redémarrer l'ordinateur.
Stratégies Security Platform	L'accès aux assistants de la Security Platform peut être limité par les stratégies Permettre l'inscription de la plateforme et Permettre l'inscription de l'utilisateur .
Etat de l'utilisateur	Assistent Réinitialisation mot de passe, Assistant Import PKCS #12 : L'utilisateur actuel doit être un utilisateur initialisé de la Security Platform.
Etat Security Platform et Trusted Platform Module	Assistant Initialisation de Security Platform : Les sources possibles d'erreur sont : <ul style="list-style-type: none">• Le propriétaire de l'Infineon Security Platform est modifié après la configuration de la Security Platform.• le Trusted Platform Module a un propriétaire, mais l'Infineon Security Platform n'est pas encore configurée. La configuration ne peut pas être exécutée dans ce cas. Tous les assistants : Une connexion à le Trusted Platform Module est exigé. Les sources possibles d'erreur sont : <ul style="list-style-type: none">• Trusted Platform Module désactivé ou désactivé temporairement

	<ul style="list-style-type: none">• Trusted Platform Module manquant• Problèmes avec le logiciel du pilote <p> Informations détaillées sur l'état de l'Infineon Security Platform sont disponibles ici.</p>
Cohérence générale de la configuration	<p>Tous les assistants : La configuration de la Security Platform doit être cohérente.</p> <p>Exemples de sources possibles d'erreur :</p> <ul style="list-style-type: none">• Paramètres non valides pour la configuration de la sauvegarde de secours.• Le jeton de récupération d'urgence ou le jeton de réinitialisation du mot de passe ne peut pas être créé.



Infineon Security Platform Solution

Dialogues Mot de passe utilisateur de base et Authentification

La gestion de la Security Platform et l'utilisation de ses fonctions exigent votre authentification sur la Security Platform. Le dialogue d'authentification est fonction du mode d'authentification et de l'action exigeant votre authentification.

- [Présentation](#)
- [Stratégies pour les mots de passe utilisateur de base et la complexité du mot de passe](#)
- [Dialogues pour l'utilisation des fonctions de la Security Platform](#)
- [Dialogues pour la gestion de la Security Platform](#) - [Configuration mot de passe utilisateur de base](#)
 - [Changement mot de passe utilisateur de base](#)
 - [Vérification du mot de passe utilisateur de base](#)

Présentation

La table suivante présente les types différents de dialogues mot de passe et authentification affichés dans des circonstances différentes.

Type d'action	Actions utilisateur exigées	Exemples solution Security Platform
Configuration du mot de passe utilisateur de base	<p>Mode d'authentification du mot de passe :</p> <ul style="list-style-type: none">• Saisissez et confirmez le mot de passe. <p>Mode d'authentification étendue :</p> <ul style="list-style-type: none">• Entrez et confirmez mot de passe.• Insérez le dispositif d'authentification et saisissez le numéro d'identification personnel (ou prenez l'action adéquate, selon le type du dispositif d'authentification, par exemple mettez le doigt sur le capteur d'empreinte).	<ul style="list-style-type: none">• Initialisation utilisateur (Assistant d'Initialisation Rapide ou Assistant d'Initialisation Utilisateurs)• Réinitialisation mot de passe (Outil de paramétrage - Réinitialisation mot de passe - Réinitialiser...)
Modifier le mot de passe utilisateur de base	<p>Mode d'authentification du mot de passe :</p> <ul style="list-style-type: none">• Saisissez le mot de passe ancien.• Saisissez et confirmez le nouveau mot de passe. <p>Mode d'authentification étendue :</p>	<ul style="list-style-type: none">• Changement mot de passe (Outil de paramétrage - Paramètres utilisateur - Modifier...)

	<ul style="list-style-type: none"> • Insérez le dispositif d'authentification et saisissez le numéro d'identification personnel (ou prenez l'action adéquate, selon le type du dispositif d'authentification, par exemple mettez le doigt sur le senseur empreinte). • Saisissez et confirmez la nouvelle phrase de passe. 	
<p>Vérification du mot de passe utilisateur de base</p>	<p>Mode d'authentification du mot de passe :</p> <ul style="list-style-type: none"> • Saisissez le mot de passe. <p>Mode d'authentification étendue :</p> <ul style="list-style-type: none"> • Insérez le dispositif d'authentification et saisissez le numéro d'identification personnel (ou prenez l'action adéquate, selon le type du dispositif d'authentification, par exemple mettez le doigt sur le senseur empreinte). Alternativement, lorsque vous ne désirez pas utiliser le dispositif d'authentification étendue, saisissez la phrase de passe. 	<ul style="list-style-type: none"> • Authentification de l'utilisateur exigée pour utiliser les fonctions de la Security Platform (par exemple cryptage fichiers ou messagerie sécurisée) • Activer réinitialisation mot de passe (Outil de paramétrage - Réinitialisation mot de passe - Activer...) • Exportation sauvegarde données migration (Outil de paramétrage - Migration - Exporter...) • Importation sauvegarde données migration (Outil de paramétrage - Migration - Importer...) • Restauration informations d'identification utilisateur (Outil paramétrage - Sauvegarde - Restaurer...)



Stratégies pour les mots de passe utilisateur de base et la complexité du mot de passe

Les informations concernant les stratégies mot de passe et la complexité mot de passe sont disponibles dans la [gestion des mots de passe](#).

Dialogues pour l'utilisation des fonctions de la Security Platform

Les tables suivantes expliquent les dialogues exigés pour utiliser les fonctions de la Security Platform (par exemple cryptage fichiers ou messagerie sécurisée)

Authentification du mot de passe

<input type="password"/> <i>Mot de passe utilisateur de base</i>	Saisissez le mot de passe actif actuel d'utilisateur de base.
<input checked="" type="checkbox"/> <i>Mémoriser le mot de passe pour toutes les applications</i>	Cochez cette case pour empêcher les demandes multiples d'authentification déterminées par les applications différentes utilisant les fonctions de la Security Platform.
<input type="checkbox"/> <i>Détails...</i>	Cliquez pour afficher les détails de l'application exigeant votre authentification sur la Security Platform.
Authentification étendue avec la phrase de passe	
<input type="password"/> <i>Phrase de passe utilisateur de base</i>	Saisissez la phrase de passe active actuelle d'utilisateur de base.
<input type="checkbox"/> <i>Authentification</i>	Modifiez la méthode d'authentification lorsque vous désirez utiliser votre dispositif d'authentification et non saisir votre phrase de passe.
<input checked="" type="checkbox"/> <i>Cachez la saisie</i>	Décochez cette case pour voir la phrase de passe entrée.
<input checked="" type="checkbox"/> <i>Mémoriser la phrase de passe pour toutes les</i>	Cochez cette case pour empêcher les demandes multiples d'authentification déterminées par les applications différentes utilisant les fonctions de la Security Platform.

<i>applications</i>	
<input type="checkbox"/> <i>Détails...</i>	Cliquez pour afficher les détails de l'application exigeant votre authentification sur la Security Platform.
Authentification étendue avec Carte à puce ou clé USB sécurisé	
<input type="checkbox"/> <i>PIN</i>	Insérez votre carte à puce ou la clé USB sécurisé. Entrez votre numéro d'identification personnel.
<input type="checkbox"/> <i>Authentification</i>	Modifiez la méthode d'authentification lorsque vous désirez saisir votre phrase de passe et non utiliser votre dispositif d'authentification.
<input checked="" type="checkbox"/> <i>Mémoriser le numéro d'identification personnel pour toutes les applications</i>	Cochez cette case pour empêcher les demandes multiples d'authentification déterminées par les applications différentes utilisant les fonctions de la Security Platform.
<input type="checkbox"/> <i>Détails...</i>	Cliquez pour afficher les détails de l'application exigeant votre authentification sur la Security Platform.
Authentification étendue avec un autre dispositif d'authentification	
<input type="checkbox"/> <i>Authentifiez-vous</i>	Utilisez votre dispositif d'authentification pour vous authentifier (par exemple mettez le doigt sur le senseur empreintes).  Pour plusieurs informations, consultez l'aide en ligne de votre plugiciel d'authentification étendue.

<input type="checkbox"/> <i>Authentification</i>	Modifiez la méthode d'authentification lorsque vous désirez saisir votre phrase de passe et non utiliser votre dispositif d'authentification.
<input checked="" type="checkbox"/> <i>Mémoriser pour toutes les applications</i>	Cochez cette case pour empêcher les demandes multiples d'authentification déterminées par les applications différentes utilisant les fonctions de la Security Platform.
<input type="checkbox"/> <i>Détails...</i>	Cliquez pour afficher les détails de l'application exigeant votre authentification sur la Security Platform.



Dialogues pour la gestion de la Security Platform

Les tables suivantes expliquent les dialogues d'authentification et mot de passe utilisateur de base exigés pour la gestion de la Security Platform.

Configuration mot de passe utilisateur de base (Initialisation utilisateur, Réinitialisation mot de passe)

Authentification du mot de passe	
 <i>Mot de passe</i>	Saisissez un mot de passe répondant aux paramètres à la stratégie mot de passe . Ce mot de passe sera votre nouveau mot de passe utilisateur de base.
 <i>Confirmer mot de passe</i>	Saisissez à nouveau le mot de passe pour confirmation.
Authentification étendue avec Carte à puce ou clé USB sécurisé	
 <i>Phrase de passe</i>	Saisissez une phrase de passe répondant aux paramètres à la stratégie mot de passe . Cette phrase de passe sera votre nouvelle phrase de passe utilisateur de base.
 <i>Confirmer phrase de passe</i>	Saisissez à nouveau la phrase de passe pour confirmation.
 <i>PIN</i>	Insérez votre carte à puce ou la clé USB sécurisé. Entrez votre numéro d'identification personnel.
Authentification étendue avec un autre dispositif d'authentification	

 <i>Phrase de passe</i>	Saisissez une phrase de passe répondant aux paramètres à la stratégie mot de passe . Cette phrase de passe sera votre nouvelle phrase de passe utilisateur de base.
 <i>Confirmer phrase de passe</i>	Saisissez à nouveau la phrase de passe pour confirmation.
 <i>Authentifiez-vous</i>	Utilisez votre dispositif d'authentification pour vous authentifier (par exemple mettez le doigt sur le senseur empreintes).  Pour plusieurs informations, consultez l'aide en ligne de votre plugiciel d'authentification étendue.



Modifier le mot de passe utilisateur de base

Authentification du mot de passe	
 <i>Ancien mot de passe</i>	Saisissez le mot de passe actif actuel d'utilisateur de base.
 <i>Nouveau mot de passe</i>	Saisissez un mot de passe répondant aux paramètres à la stratégie mot de passe . Ce mot de passe sera votre nouveau mot de passe utilisateur de base.
 <i>Confirmation nouveau mot de passe</i>	Saisissez à nouveau le nouveau mot de passe pour confirmation.
Authentification étendue avec Carte à puce ou clé USB sécurisé	
 <i>PIN</i>	Insérez votre carte à puce ou la clé USB sécurisé. Entrez votre numéro d'identification personnel.

 <i>Nouvelle phrase de passe</i>	Saisissez une phrase de passe répondant aux paramètres à la stratégie mots de passe . Cette phrase de passe sera votre nouvelle phrase de passe utilisateur de base.
 <i>Confirmation nouvelle phrase de passe</i>	Saisissez à nouveau la phrase de passe pour confirmation.
Authentification étendue avec un autre dispositif d'authentification	
 <i>Nouvelle phrase de passe</i>	Saisissez une phrase de passe répondant aux paramètres à la stratégie mots de passe . Cette phrase de passe sera votre nouvelle phrase de passe utilisateur de base.
 <i>Confirmation nouvelle phrase de passe</i>	Saisissez à nouveau la phrase de passe pour confirmation.
 <i>Authentifiez-vous</i>	Utilisez votre dispositif d'authentification pour vous authentifier (par exemple mettez le doigt sur le senseur empreintes).  Pour plusieurs informations, consultez l'aide en ligne de votre plugiciel d'authentification étendue.



Vérification mot de passe utilisateur de base (Activation réinitialisation mot de passe, Exportation/Importation sauvegarde données migration, Restauration informations d'identification utilisateur)

Authentification du mot de passe	
 <i>Mot de passe</i>	Saisissez le mot de passe actif actuel d'utilisateur de base.

Authentification étendue	
<ul style="list-style-type: none"> ⦿ Dispositif d'authentification ⦿ <i>Phrase de passe</i> 	Spécifiez lorsque vous désirez utiliser votre dispositif d'authentification ou saisissez votre phrase de passe.
Authentification étendue avec phrase de passe	
☒ <i>Phrase de passe</i>	Saisissez la phrase de passe active actuelle d'utilisateur de base.
Authentification étendue avec Carte à puce ou clé USB sécurisé	
☒ <i>PIN</i>	Insérez votre carte à puce ou la clé USB sécurisé. Entrez votre numéro d'identification personnel.
Authentification étendue avec un autre dispositif d'authentification	
☒ <i>Authentifiez-vous</i>	<p>Utilisez votre dispositif d'authentification pour vous authentifier (par exemple mettez le doigt sur le senseur empreintes).</p> <p> Pour plusieurs informations, consultez l'aide en ligne de votre plugiciel d'authentification étendue.</p>



Infineon Security Platform Solution

Gestion du mot de passe

Mots de passe utilisés dans la solution Security Platform

La solution Infineon Security Platform utilise quelques mots de passe différents. Quelques-uns sont pour les administrateurs de Security Platform, autres sont pour les utilisateurs de Security Platform. Ne faites pas une confusion entre les mots de passe différents.



En [mode serveur](#), les mots de passe administratifs et le Code autorisation réinitialisation ne sont pas valides, car Trusted Computing Management Server gère la préparation et la fourniture pour ces mots de passe.

La table suivante présente les mots de passe de Security Platform et leur utilisation.

Mot de passe	Utilisé par...	But/Explication
Mot de passe propriétaire	Administrateur	Ceci est paramétré pendant l'initialisation de la Security Platform, et demandé d'exécuter des tâches importantes d'administration de la Security Platform. Peut être configuré manuellement, ou un Mot de Passe Propriétaire aléatoire peut être créé. Peut être enregistré dans un Fichier de Sauvegarde du Mot de Passe Propriétaire (au lieu de saisir le Mot de Passe Propriétaire). Ce fichier est compatible avec le Fichier de Sauvegarde du Mot de Passe Propriétaire généré par l'application Microsoft "Trusted Platform Module (TPM) Management".
Mot de passe jeton de récupération d'urgence	Administrateur	Protège le jeton de récupération d'urgence exigé pour effectuer une récupération d'urgence.
Jeton réinitialisation	Administrateur	Protège le jeton de réinitialisation du

du mot de passe		mot de passe exigé lorsqu'un utilisateur doit modifier son mot de passe utilisateur de base .
Mot de passe utilisateur de base (nommé également "Mot de passe" dans le mode Authentification étendue nommé également "phrase de passe utilisateur de base")	Utilisateur	<p>Protège la clé utilisateur de base exigée pour accéder les données spécifiques à l'utilisateur d'Infineon Security Platform. C.à.d aucune fonctionnalité de Security Platform ne peut être utilisée sans ce mot de passe.</p> <p>Le mot de passe utilisateur de base est exigé également pour restaurer et migrer les données utilisateur et pour configurer quelques paramètres utilisateur. Le mot de passe peut être réinitialisé lorsque l'administrateur et également l'utilisateur ont configuré cette fonctionnalité.</p> <p>Dans le mode Authentification étendue, ce mot de passe est remplacé par une « phrase de passe » protégée par le dispositif d'authentification.</p> <p> C'est le mot de passe principal de l'utilisateur de Security Platform. Pour simplifier les choses, il est nommé souvent « mot de passe ».</p>
Mot de passe PKCS #12	Utilisateur	Protège la clé privée d'un utilisateur stockée dans un fichier PKCS #12.
Code autorisation réinitialisation	Utilisateur	Ce code n'est pas vraiment un mot de passe, mais il est similaire du point de vue de l'utilisateur. Créé automatiquement au cours de la préparation de la réinitialisation du mot de passe d'un utilisateur. Exigé pour réinitialiser un mot de passe utilisateur de base.

Généralités sur les mots de passe

- Utilisez des mots de passe différents pour des objectifs différents. Ne réutilisez surtout pas votre mot de passe Windows. Si vous avez réutilisé votre mot de passe Windows pour tous les mots de passe relatifs à la Security Platform, le niveau de sécurité renforcé basé sur le matériel n'est plus en vigueur. L'attaqueur connaissant votre Mot de Passe Windows pourrait accéder à vos données EFS et PSD, utilisez vos informations d'identification pour l'identification et autorisation et modifiez les paramètres de la Security Platform.
- L'utilisation de caractères spéciaux est fortement recommandée pour améliorer la qualité des mots de passe. Cependant, vous ne devez pas oublier que certains caractères changent de position sur le clavier en fonction des paramètres régionaux. Certains caractères risquent même de ne pas être disponibles, en fonction de la langue du système d'exploitation. Il est également possible que quelques caractères ne soient pas permis dans les mots de passe, en fonction du système d'exploitation et des composantes logicielles.
- Evitez d'utiliser comme mots de passe des termes figurant dans le dictionnaire, même lorsque le mot de passe se compose de plusieurs termes.
- L'ajout de chiffres et l'utilisation de minuscules/majuscules améliorent la qualité d'un mot de passe.
- Les longueurs minimale et maximale des mots de passe restent habituellement inchangées après la configuration du système. Ainsi, l'apparence des mots de passe pourra varier d'un système à l'autre. Cependant, les aspects généraux restent valables pour chaque installation du logiciel.
- Pour empêcher les attaques d'espionnage des mots de passe, la copie à partir des zones d'entrée du mot de passe n'est pas supportée.

Complexité du Mot de passe

La table suivante présente une présentation générale des exigences de complexité du Mot de passe :

Exigences de complexité du mot de passe

Caractères depuis 3 des 4 catégories demandés :

- Caractères anglais majuscules (**A** à **Z**)
- Caractères anglais minuscules (**a** à **z**)
- Chiffres dans la base 10 (**0** à **9**)
- Caractères non-alphanumériques (par ex. **!**, **\$**, **#**, **%**)

Stratégies pour le Mot de passe Propriétaire et la Complexité du Mot de passe

Il y a des exigences spéciales concernant la longueur du Mot de passe du Propriétaire et la complexité du Mot de passe du Propriétaire. La table suivante présente les paramètres par défaut à la stratégie mot de passe :

Longueur minimale par défaut	6 caractères
Complexité du mot de passe demandé	Non

Stratégies pour les Mots de passe utilisateur de base et la Complexité du Mot de passe

Il y a des exigences spéciales concernant la longueur des Mots de passe utilisateur de base et la Complexité des Mots de passe utilisateur de base. La table suivante présente les paramètres par défaut à la stratégie mot de passe :

	Authentification du mot de passe - aucun dispositif d'authentification utilisé	Authentification étendue - le dispositif d'authentification protège une phrase de passe
Longueur minimale par défaut	6 caractères	20 caractères
Complexité du mot de passe demandé	Non	Non

Votre administrateur peut modifier ces paramètres. Les détails sur les stratégies mot de passe utilisateur de base sont disponibles dans la description des [Stratégies utilisateur](#) d'Infineon Security Platform.



Demandez votre administrateur pour les stratégies effectives mot de passe utilisateur de base, lorsque les droits d'accès ne permettent pas la configuration ou la visualisation des stratégies mot de passe.



Les options à l'intérieur du champ du mot de passe peuvent être restreintes en fonction de la stratégie de système [Activation de la sécurité du champ de mot de passe obligatoire](#).



Infineon Security Platform Solution - Outil de paramétrage

Outil de paramétrage d'Infineon Security Platform

Avec l'outil de paramétrage de la Security Platform vous pouvez obtenir des informations diverses sur le Trusted Platform Module de votre système. Vous pouvez également exécuter quelques tâches administratives. Cette composante est conçue comme un applet Control Panel. Il représente un point central d'accès pour l'administration de l'Infineon Security Platform.

La table suivante présente les pages de l'outil de paramétrage :

Page	Explication
Info	<ul style="list-style-type: none">• Détermine les paramètres les plus importants de l'Infineon Security Platform
Paramètres utilisateur	<ul style="list-style-type: none">• Modifier le mot de passe utilisateur de base• Configuration des fonctions de la Security Platform spécifiques à l'utilisateur• Gestion des certificats de la Security Platform• Désactivation temporaire de Security Platform
Sauvegarde	<ul style="list-style-type: none">• Configuration des sauvegardes automatiques (tâche d'administration)• Exécution des sauvegardes manuelles et de la restauration• Création des dispositifs d'authentification de sauvegarde <p> Trusted Computing Management Server gère la sauvegarde et restauration en mode serveur. Si Personal Secure Drive (PSD) a été configuré, la sauvegarde et restauration manuelle peut être exécutée.</p>
Migration	<ul style="list-style-type: none">• Exportation des clés et certificats utilisateurs de la Security Platform• Importation des clés et certificats utilisateurs de la Security Platform <p> Cette page n'est pas disponible dans le mode serveur, car la migration des clés et certificats utilisateur est gérée par Trusted Computing Management Server, donc vous ne devez pas exécuter cette tâche.</p>
Réinitialisation	<ul style="list-style-type: none">• Configuration pour tous les utilisateurs (tâche

[mot de passe](#)

d'administration)

- Activation de l'utilisateur actuel
- Préparation de la réinitialisation du mot de passe pour un certain utilisateur (tâche d'administration)
- Réinitialisation du mot de passe pour l'utilisateur actuel



En [mode serveur](#), Trusted Computing Management Server gère la configuration, l'activation et la préparation du code autorisation réinitialisation du mot de passe, donc l'administrateur et l'utilisateur ne doivent pas exécuter cette tâche. Par suite toutes les options sont désactivées, sauf pour *Réinitialiser* et *Activer*.

[BitLocker](#)

- Utilisez le Chiffrement de lecteur BitLocker ensemble avec Trusted Platform Module pour chiffrer les données sur votre disque



- Cette page n'est disponible que si le système d'exploitation accepte le chiffrement de lecteur BitLocker (par ex. pour les éditions Enterprise et Ultimate de Windows 7 et de Windows Vista) et si l'utilisateur courant possède des droits d'administration.
- Cette page n'est pas disponible en [mode serveur](#). Vous pouvez toutefois configurer BitLocker via l'applet Panneau de configuration Microsoft BitLocker.

[Avancé](#)

- Changement de Mot de Passe du Propriétaire
- Configuration des fonctions de la Security Platform spécifiques à la plate-forme
- Désactivation/activation de la Security Platform
- Configuration des stratégies de la Security Platform
- Réinitialisez le niveau de défense d'attaque par dictionnaire



- Cette page est visible seulement lorsque l'utilisateur actuel possède des droits d'administration.

- Cette page n'est pas disponible dans le [mode serveur](#), car Trusted Computing Management Server gère la configuration des fonctions et stratégies d'Security Platform.

Démarrage de l'application

- **Gestion de Security Platform**

Lancez l'Outil de configuration à partir de [l'icône de notification de la barre des tâches](#).



Dans les systèmes d'exploitation avec Contrôle des comptes utilisateurs (par exemple Windows 7 et Windows Vista), l'Outil de configuration est lancé sans privilèges élevés.

-  **Gestion de Security Platform**

Lancez l'Outil de configuration à partir de [l'Icône de notification de la barre des tâches](#) avec des privilèges élevés.



Disponible seulement pour les utilisateurs avec droits d'administration dans les systèmes d'exploitation avec contrôles des comptes utilisateurs (par exemple Windows 7 et Windows Vista).



Infineon Security Platform Solution - Outil de paramétrage

Informations sur l'Infineon Security Platform

Cette page affiche les paramètres les plus importants de l'Infineon Security Platform.

Lorsque l'Infineon Security Platform est désactivée, les informations disponibles seront limitées.

La table suivante présente toutes les informations et fonctions.

Eléments de la page	Explication
 <i>Solution Security Platform</i>	Version du produit Security Platform Solution et le mode d'opération pour l'utilisateur actuellement connecté.
 <i>État de Security Platform</i>	Les états du microprocesseur, du propriétaire, de l'utilisateur et du mode d'exploitation sont décrits dans la vue d'ensemble de l'État de Security Platform .
 <i>Trusted Platform Module</i>	Le fabricant et la version du matériel et le logiciel d'Trusted Platform Module.
 <i>Autotest</i>	Cliquez pour vérifier la fonctionnalité d'Trusted Platform Module. Le résultat est affiché.
 <i>Plusieurs détails...</i>	Cliquez pour visualiser des informations supplémentaires détaillées sur la configuration d'Infineon Security Platform.



Infineon Security Platform Solution - Outil de paramétrage

Plusieurs détails

Ce dialogue présente les informations de système les plus importantes. Ces informations incluent :

- Version du produit
- [Mode d'opération](#)
- [État de Security Platform](#)
- Informations composante
- Informations d'assistance avancée

Vous pouvez sauvegarder ces informations dans un fichier :

Bouton	Explication
<input type="checkbox"/> <i>Enregistrer...</i>	Les informations de diagnose peuvent être stockées dans un fichier pour une analyse hors connexion. Un dialogue de sélection du fichier est affiché, vous pouvez y définir le lecteur, le dossier et le nom du fichier. Le format du fichier pour le fichier de diagnose de la Security Platform est le fichier texte standard (extension *.txt). Ceci permet la visualisation du fichier avec une large gamme d'applications.



©Infineon

Infineon Security Platform Solution - Outil de paramétrage

État de Security Platform

L'état actuel d'Infineon Security Platform est défini par l'état actuel des quatre composantes suivantes :

État du Chip (état du Trusted Platform Module)

Fournit des informations sur l'état du Trusted Platform Module. Les états suivants peuvent être signalés :

- **Activée** - le Trusted Platform Module est accessible et utilisé par le logiciel Infineon Security Platform.
- **Désactivée** - L'utilisation de le Trusted Platform Module est bloquée. Cela s'effectue par un réglage de paramètre, soit dans le BIOS système, soit dans le logiciel Infineon Security Platform.
Solution possible : Lorsque le Trusted Platform Module est désactivé dans le BIOS, consultez la documentation de votre BIOS système. Sinon, [activez](#) Trusted Platform Module dans le logiciel Infineon Security Platform.
- **Temporairement désactivé** - le Trusted Platform Module est accessible, mais son utilisation est bloquée tant que le système n'a pas été redémarré. Les fonctions de sécurité utilisant le circuit ne sont pas disponibles.
Solution possible: [Activez](#) Trusted Platform Module dans le logiciel Infineon Security Platform et redémarrer le système.

État propriétaire

Fournit des informations sur l'état général d'Infineon Security Platform. Les états suivants peuvent être signalés :

- **Non initialisé** - Soit l'Infineon Security Platform n'a pas encore été initialisée, ni aucun propriétaire défini, soit l'état d'initialisation n'est pas cohérent (par ex. causé par une interruption en raison d'une coupure de courant).
Solution possible : Initialisez la Security Platform avec [l'Assistant d'Initialisation Rapide de la Security Platform](#) ou [l'Assistant d'Initialisation de Security Platform](#).
- **Initialisé** - Les premières opérations de configuration ont été effectuées, le Trusted Platform Module est opérationnel et la propriété de l'Infineon Security Platform définie. Il existe un propriétaire Infineon Security Platform dans le Trusted Platform Module.
- **Initialisé mais changé** - La propriété de l'Infineon Security Platform a été définie mais, après cette opération le Propriétaire d'Infineon Security Platform a été changé . La fonction d'administration de Security Platform le signale par l'état du propriétaire **Initialisé (mode échec 1)**.
Solution possible: Démarrez l'[assistant Initialisation de Security Platform](#) et suivez les instructions affichées à l'écran.
- **TPM initialisé, Security Platform non initialisée** - Nommé "**Autre SE initialisé**" dans les versions précédentes du logiciel de la solution Infineon Security Platform.
1er scénario: Pour les systèmes d'exploitation Windows 7 et Windows Vista, une situation possible est la suivante le Trusted Platform Module a été initialisé avec l'application Microsoft [Gestion de module de plateforme sécurisée](#), donc la possession de Trusted Platform Module a été prise, mais Infineon Security Platform n'est pas configurée.
2ème scénario: Pour les ordinateurs multi-plateforme avec plusieurs versions de système d'exploitation installées, où la possession a été prise en utilisant un système, mais un autre système a été lancé.
Dans les deux scénarios, la configuration d'Infineon Security Platform demeure active. La fonction d'administration de Security Platform le signale par l'état du propriétaire **Initialisé (mode échec 2)**.
Solution possible: Démarrez l'[assistant Initialisation de Security Platform](#) et suivez les instructions affichées à l'écran.

État utilisateur

Fournit des informations sur l'état de l'utilisateur actuellement connecté. Les états suivants peuvent être signalés :

- **Non initialisé** - Soit l'utilisateur actuellement connecté n'est pas encore un utilisateur de l'Infineon Security Platform, soit l'état d'initialisation de l'utilisateur n'est pas cohérent (par ex., en raison d'une interruption due à une coupure de courant).
Solution possible : Initialisez l'utilisateur avec [l'Assistant d'Initialisation Rapide de Security Platform](#) ou [l'Assistant d'Initialisation d'Utilisateur de Security Platform](#).
- **Initialisé** - L'utilisateur actuellement connecté est un utilisateur valide d'Infineon Security Platform. C.à.d., la configuration de l'utilisateur actuellement connecté a bien été effectuée. La clé utilisateur de base a été générée et stockée dans la sauvegarde de restauration d'urgence si elle existe.
- **Initialisé mais changé** - L'utilisateur d'Infineon Security Platform a été configuré, mais la propriété de l'Infineon Security Platform a été modifiée par la suite. La clé utilisateur de base de l'utilisateur actuellement connecté ne peut pas être utilisée sur l'Infineon Security Platform. L'administration de Security Platform présente l'état du propriétaire comme **Initialisé (Mode erreur 3)**.

Solution possible :

Contactez votre Administrateur pour démarrer l'[Assistant Initialisation d'Infineon Security Platform](#) et cochez *Restaurer une Security Platform depuis une sauvegarde de récupération d'urgence*. Ainsi, les informations d'identification d'un utilisateur peuvent être préparées pour être restaurées à partir d'une sauvegarde de récupération d'urgence précédemment créée. Connectez-vous ensuite à l'aide de votre propre compte utilisateur et démarrez l'[Assistant Initialisation de l'utilisateur](#). (consultez le [Guide pas à pas pour effectuer une récupération d'urgence](#)).

Si aucune sauvegarde de récupération d'urgence n'est disponible, une réinitialisation forcée de l'utilisateur devra être effectuée. Cela pourra se faire en démarrant l'[Assistant Initialisation de l'utilisateur](#) avec le paramètre de commande **-forceinit**.

 Le paramètre **SpUserWz.exe /forceinit** de ligne de commande n'est pas supporté dans le [mode serveur](#).

État session utilisateur

Cet état n'est disponible qu'en [mode serveur](#).

Les états de session utilisateur contrôlent l'accès en écriture pour les informations d'identification et configuration de l'utilisateur. Ainsi les changements conflictuels simultanés depuis plusieurs plateformes ne sont pas possibles. Un état de session fait référence à un certain utilisateur sur une certaine plateforme. Vous pouvez modifier l'état de session en utilisant le sous-menu *Informations d'identification / Configuration utilisateur* dans le [menu Notification de la barre des tâches](#). Les états suivants sont utilisés :

- **Lecture seule** : Aucun accès en écriture. L'accès en écriture est possible en changeant l'état *Lecture/Écriture temporaire* ou *Lecture/Écriture permanente*, car aucune autre plateforme n'est pas dans un des deux états Lecture/Écriture possibles. État par défaut.
- **Lecture/Écriture temporaire** : État utilisé par défaut par Trusted Computing Management Server pour accès en écriture. Bloque les changements provenant d'autres plateformes. Après l'accès en écriture, l'état *Lecture seule* sera rétabli.
- **Lecture/Écriture permanente** : L'utilisateur entre explicitement dans cet état en utilisant l'élément du menu Notification de la barre des tâches nommé *Informations d'identification / Configuration utilisateur - Demander une copie locale de travail*. Permet le changement hors connexion des informations d'identification et configuration de l'utilisateur, dans une copie locale de travail. Bloque les changements provenant d'autres plateformes. Cet état peut être changé dans *Lecture seule* en utilisant l'élément du menu Notification de la barre des tâches nommé *Informations d'identification / Configuration utilisateur - Accepter les changements locaux* ou *Informations d'identification / Configuration utilisateur - Annuler les changements locaux*.



Infineon Security Platform Solution - Outil de paramétrage

Paramètres utilisateur d'Infineon Security Platform

Dans cette page vous pouvez configurer tous les paramètres concernant la sécurité pour l'utilisateur de l'Infineon Security Platform actuellement connecté.



Disponibilité de la page:

- Cette page est disponible seulement sur une Security Platform initialisée.
- Sur une Infineon Security Platform non configurée, une boîte de message vous informe sur cette situation et l'[Assistant Rapide d'Initialisation](#) peut être lancé. Dans ce cas, l'outil de paramétrage est fermé. Aucun message présenté en [mode serveur](#), car Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée.
- pour un utilisateur non initialisé une boîte de message vous informe sur cette situation et l'[Assistant Rapide d'Initialisation](#) peut être lancé. Dans ce cas, l'outil de paramétrage est fermé. En [mode serveur](#), une boîte de message informe sur cette situation seulement si l'utilisateur actuel est membre du groupe d'inscription utilisateurs et l'[Assistant Rapide d'Initialisation](#) peut être lancé.

Boutons :

- Dans ce cas l'Infineon Security Platform est désactivée, l'utilisateur non configuré encore ou l'utilisateur connecté n'est pas initialisé, les boutons sont désactivés.
- L'activation de quelques fonctions est fonction de vos [paramètres stratégie utilisateur](#).

La table suivante décrit toutes les fonctions paramètres utilisateur.

Bouton	Explication
<input type="checkbox"/> <i>Changer...</i>	<p>Cliquez ici pour modifier votre mot de passe utilisateur de base.</p> <p> L'archive contenant les données de récupération d'urgence sera mise à jour pour refléter le changement du mot de passe.</p>
<input type="checkbox"/> <i>Configurer...</i>	Cliquez ici pour configurer les fonctions suivantes :

	<ul style="list-style-type: none"> • Messagerie électronique sécurisée • Cryptage de fichiers et dossiers avec le système de fichiers de cryptage (EFS) et personal Secure Drive (PSD). • Authentification étendue <p>En fonction de l'état de configuration de fonctions d'utilisateurs, soit l'Assistant Rapide d'Initialisation soit l'Assistant d'Initialisation Utilisateur sera lancé.</p>
<input type="checkbox"/> <i>Gérer...</i>	<p>Cliquez pour visualiser, importer ou supprimer les certificats protégés par la Security Platform.</p> <p>Le visualisateur du certificat d'Infineon Security Platform sera lancé.</p>
<input type="checkbox"/> <i>Désactiver/Activer...</i>	<p>Fonction de l'état actuel de l'Infineon Security Platform, cette opération peut être exécutée. Désactiver arrête fonctionnalité d'Infineon Security Platform jusqu'au prochain démarrage du système. Les applications désignées à utiliser le Security Platform n'auront plus accès aux données protégées par le Trusted Platform Module, incluant les données protégées par l'EFS, le personal Secure Drive et autres. L'accès aux données protégées est restauré une fois la Security Platform est réactivée.</p> <p>Le redémarrage du système vous sera demandé lorsque vous désirez activer l'Infineon Security Platform.</p> <p> Lorsque la fonctionnalité est bloquée par les paramètres de la stratégie utilisateur, ce bouton est désactivé.</p> <p>Cette fonction n'est disponible que pour les Security Platform avec un Trusted Platform Module 1.2.</p>

Infineon Security Platform Solution - Outil de paramétrage

Sauvegarde d'Infineon Security Platform

Dans cette page vous pouvez sauvegarder et restaurer les informations d'identification et les paramètres de la Security Platform et les Personal Secure Drive.

Lorsque l'[authentification étendue](#) est activée, vous pouvez créer également des sauvegardes pour votre dispositif d'authentification.



Boutons :

- Les boutons pour les tâches d'administration sont désactivés pour les utilisateurs sans droits d'administration.
- Les boutons sont désactivés lorsque les fonctions correspondantes ne sont pas disponibles dans un certain état de la Security Platform.

La table suivante décrit toutes les informations et fonctions de sauvegarde et restauration.

Bouton	Explication
 <i>Configurer...</i>	<p>Cliquez ici pour configurer les sauvegardes automatiques de la Security Platform. L'assistant d'initialisation d'Infineon Security Platform sera lancé.</p> <p> • Cette fonction est disponible seulement lorsque le compte utilisateur actuel possède des droits d'administration.</p> <p>• Ce bouton est désactivé en mode serveur, car la sauvegarde automatique est gérée par Trusted Computing Management Server, donc aucune configuration explicite n'est nécessaire de la part de l'utilisateur.</p>
 <i>Restaurer tous...</i>	<p>Cliquez ici pour restaurer votre configuration de Security Platform et les pièces d'identité à partir d'une Archive de sauvegarde système. De plus, une Restauration de Récupération d'Urgence peut être effectuée.</p> <p>Vous pouvez également restaurer depuis une archive écrite</p>

manuellement, si vous n'avez pas de système Archive de Sauvegarde. Dans ce cas, Restauration de Récupération d'Urgence est seulement possible, si l'archive écrite manuellement comprend les données correspondantes. Si vous avez des sauvegardes de vos fichiers d'image de Personal Secure Drive, vous pouvez également. Dans ce cas, vous pouvez soit restaurer un fichier d'image pour un PSD déjà configuré soit installer un nouveau PSD afin d'utiliser ce fichier d'image restauré.

La partie de restauration de l'[assistant Sauvegarde d'Infineon Security Platform](#) sera lancé.



- Ce bouton est désactivé si Infineon Security Platform est désactivée ou si l'utilisateur n'a pas les privilèges d'administration.
- Ce bouton est désactivé en [mode serveur](#), car la restauration après une sauvegarde système est gérée par Trusted Computing Management Server, donc aucune configuration explicite n'est nécessaire de la part de l'utilisateur.

Sauvegarder...

Cliquez pour démarrer une sauvegarde manuelle de vos paramètres et informations d'identification de la Security Platform.

Si vous avez installé des Personal Secure Drives, vous pouvez les sauvegarder également.

L'[assistant Sauvegarde d'Infineon Security Platform](#) sera lancé.



- Ce bouton est désactivé si Infineon Security Platform est désactivée ou n'a pas encore été paramétrée.
- En [mode serveur](#), vous pouvez sauvegarder seulement votre Personal Secure Drives. En plus des conditions citées ci-dessus, ce bouton est désactivé si votre Personal Secure Drive (PSD) n'est pas configuré.

Restaurer...

Cliquez pour démarrer une sauvegarde manuelle de vos

paramètres et informations d'identification sauvegardées de la Security Platform.

Si vous avez des sauvegardes de vos fichiers d'image de Personal Secure Drive, vous pouvez également. Dans ce cas, vous pouvez soit restaurer un fichier d'image pour un PSD déjà configuré soit installer un nouveau PSD afin d'utiliser ce fichier d'image restauré.

La partie de restauration de l'[assistant Sauvegarde d'Infineon Security Platform](#) sera lancé.



- Ce bouton est désactivé si Infineon Security Platform est désactivée ou n'a pas encore été paramétrée.
- Dans le mode [autonome](#), si vous avez les privilèges d'administration vous pouvez effectuer la Restauration Récupération d'urgence.
- En plus des conditions citées ci-dessus, dans le [mode serveur](#), ce bouton est désactivé si l'utilisateur n'est pas initialisé et Personal Secure Drive (PSD) n'est pas configuré.

Créer...

Cliquez pour créer un dispositif d'authentification de sauvegarde.



Cette fonction est disponible seulement lorsque l'[authentification étendue](#) est activée.



Infineon Security Platform Solution - Outil de paramétrage

Migration d'Infineon Security Platform

La migration implique la copie et le transfert des informations d'identification d'un utilisateur pour une plate-forme source vers une plate-forme cible. Fonction de la configuration actuelle du système, l'utilisateur d'Infineon Security Platform peut migrer les clés et certificats utilisateurs vers ou d'une plate-forme locale Infineon Security Platform.

La fonction est couverte par l'Assistant Migration d'Infineon Security Platform.



Disponibilité de la page:

- Cette page est disponible seulement sur une Security Platform initialisée.
- Cette page n'est pas disponible en [mode serveur](#) car la migration des informations d'identification de sécurité de l'utilisateur depuis une plateforme source vers une plateforme de destination est gérée par Trusted Computing Management Server, donc l'administrateur et l'utilisateur sur le système client local ne doivent pas exécuter cette tâche.

[Migration pas à pas](#)

La table suivante décrit toutes les fonctions de migration.

Bouton	Explication
<input type="checkbox"/> <i>En savoir plus...</i>	Cliquez pour visualiser un guide pas à pas pour l'exécution de la migration.
<input checked="" type="radio"/> <i>Ce système est la plate-forme source</i>	Cochez cette option pour indiquer que vous désirez exporter les informations d'identification depuis cette Security Platform. Les actions Exporter... et Autoriser... pour la plate-forme source peuvent être exécutées.
<input type="checkbox"/> <i>Exporter...</i>	Exporte les clés et certificats utilisateur vers une plate-forme cible. L'export est exécuté par la fonction d'exportation de

	<p>l'Assistant Migration d'Infineon Security Platform. La plate-forme cible doit être autorisée par l'utilisateur de la plate-forme avant l'exportation.</p> <p> Le bouton est désactivé lorsqu'une des situations suivantes s'applique :</p> <ul style="list-style-type: none"> • L'Infineon Security Platform est désactivée. • L'Infineon Security Platform n'est pas initialisé. • L'utilisateur d'Infineon Security Platform n'est pas encore initialisé.
<p><input type="checkbox"/> <i>Autoriser...</i></p>	<p>Chaque migration de clés et certificats utilisateur depuis une Infineon Security Platform vers une autre exige l'autorisation de la migration sur la plate-forme Security Platform source par le propriétaire Infineon Security Platform. Ce bouton affiche le dialogue d'autorisation.</p> <p> Le bouton est désactivé lorsqu'une des situations suivantes s'applique :</p> <ul style="list-style-type: none"> • L'Infineon Security Platform est désactivée. • L'Infineon Security Platform n'est pas initialisée. • L'utilisateur actuel ne possède pas des droits d'autorisation.
<p><input checked="" type="radio"/> <i>Ce système est la plate-forme de destination</i></p>	<p>Cochez cette option pour indiquer que vous désirez importer les informations d'identification vers cette Security Platform. Les actions importer... et Enregistrer... pour la plate-forme cible peuvent être exécutées.</p>
<p><input type="checkbox"/> <i>Importer...</i></p>	<p>importe les clés et certificats utilisateur depuis une plate-forme source. L'import est exécuté par la fonction d'importation de l'Assistant Migration d'Infineon Security Platform.</p> <p> Le bouton est désactivé lorsqu'une des situations suivantes s'applique :</p> <ul style="list-style-type: none"> • L'Infineon Security Platform est désactivée.

	<ul style="list-style-type: none">• L'Infineon Security Platform n'est pas initialisée.
<input type="checkbox"/> Enregistrer...	<p>Les informations de migration d'une Infineon Security Platform peuvent être exportées dans un fichier peuvent être importées vers une Infineon Security Platform destination. Les informations de migration sont dans un fichier dans le format XML.</p> <p>C'est le pas initial vers la migration des clés utilisateur.</p> <p> Le bouton est désactivé lorsqu'une des situations suivantes s'applique :</p> <ul style="list-style-type: none">• Le propriétaire Infineon Security Platform est modifié (information indiquée également dans la page info).• L'Infineon Security Platform n'est pas initialisée, mais une du propriétaire Infineon Security Platform existe.• Les utilisateur de base de l'administrateur d'Infineon Security Platform connecté ne correspondent pas à la clé du propriétaire Infineon Security Platform.• L'Infineon Security Platform est désactivée.

Infineon Security Platform Solution - Outil de paramétrage

Réinitialisation mot de passe de l'Infineon Security Platform

Cette page fournit toutes les tâches pour la configuration et l'exécution de la réinitialisation des mots de passe utilisateur de base.



Disponibilité de la page:

- Dans le [mode autonome](#), cette page est disponible seulement sur une Security Platform initialisée.

Boutons :

- Les boutons pour les tâches d'administration sont désactivés pour les utilisateurs sans droits d'administration.
- Les boutons sont désactivés lorsque les fonctions correspondantes ne sont pas disponibles dans un certain état de la Security Platform : Si la réinitialisation du mot de passe n'a pas été configurée par l'administrateur, vous ne pouvez pas l'activer et la réinitialisation du mot de passe ne peut pas être exécutée.
- En [mode serveur](#) Trusted Computing Management Server gère la création d'un jeton de réinitialisation du mot de passe pour tous les utilisateurs, l'activation de la réinitialisation du mot de passe et la préparation et la fourniture d'un Code autorisation réinitialisation du mot de passe pour utilisateurs spécifiques, donc l'administrateur et l'utilisateur ne doivent pas exécuter cette tâche. Par suite tous les boutons sont désactivés, sauf pour *Réinitialisation*.

La table suivante décrit toutes les fonctions de réinitialisation du mot de passe.

Bouton	Explication
<input type="checkbox"/> Configurer...	Cliquez pour créer un jeton de réinitialisation du mot de passe pour tous les utilisateurs. Cette opération exige des droits d'administration.
<input type="checkbox"/> Activer...	Cliquez pour activer la réinitialisation du mot de passe pour l'utilisateur actuel. Cette opération est possible seulement lorsqu la réinitialisation du mot de passe a été configurée auparavant par un administrateur.

<input type="checkbox"/> <i>préparer...</i>	Cliquez pour préparer et fournir le code d'autorisation pour la réinitialisation du mot de passe pour un utilisateur spécifique. Vous pouvez préparer et réinitialiser également votre compte dans un seul pas. Les deux options exigent des droits d'administration.
<input type="checkbox"/> <i>Réinitialiser...</i>	Cliquez pour réinitialiser le mot de passe utilisateur de base pour le compte utilisateur actuel. Cette opération est possible seulement lorsque la réinitialisation du mot de passe a été préparée pour le compte utilisateur actuel.

Infineon Security Platform Solution - Outil de paramétrage

BitLocker

Cette page permet d'utiliser le Chiffrement de lecteur BitLocker en liaison avec Trusted Platform Module pour crypter les données sur votre disque. La configuration de BitLocker est effectuée à l'aide de l'Applet du panneau de configuration BitLocker de Microsoft.



Disponibilité de la page :

- Cette page n'est disponible que si le système d'exploitation accepte le chiffrement de lecteur BitLocker (par ex. pour les éditions Enterprise et Ultimate de Windows 7 et de Windows Vista) et si l'utilisateur courant possède des droits d'administration.
- Cette page n'est pas disponible en [mode serveur](#).

La table suivante décrit les fonctions de BitLocker.

Bouton	Explication
 <i>État courant...</i>	État courant du Chiffrement du lecteur BitLocker. Les états possibles sont : <i>Configuré, Non configuré, Reconfiguration nécessaire, Chiffrage en cours</i> ou <i>Déchiffrage en cours</i> .
 <i>Configurer...</i>	Cliquez ici pour démarrer l'Applet du panneau de configuration BitLocker de Microsoft.  Ce bouton est désactivé si Trusted Platform Module n'est pas Initialisé.



©Infineon

Technologies AG

Infineon Security Platform Solution - Outil de paramétrage

Paramètres avancés d'Infineon Security Platform

Dans cette page vous pouvez configurer tous les paramètres pour le propriétaire Security Platform et pour la stratégie.

Les paramètres pouvant être modifiés sont limités pour l'ordinateur local.

Les [paramètres stratégie](#) d'Infineon Security Platform sont inclus dans le fichier modèles de stratégie d'Infineon Security Platform.



Disponibilité de la page :

- Cette page est disponible seulement lorsque l'utilisateur actuel possède des droits d'administrateur.
- Cette page n'est pas disponible en [mode serveur](#).

Boutons :

- Les boutons pour l'administration des stratégies système et utilisateur ne sont pas disponibles dans les éditions Windows ne prenant pas en charge la Gestion des stratégies de groupe, par exemple les éditions familiales de Windows.
- Les boutons sont désactivés lorsque les fonctions correspondantes ne sont pas disponibles dans un certain état de la Security Platform.

La table suivante décrit toutes les fonctions avancées.

Bouton	Explication
<input type="checkbox"/> <i>Modifier...</i>	<p>Cliquez pour modifier le mot de passe exigé Security Platform (voir changement de Mot de Passe du Propriétaire).</p> <p> • Cette fonction n'est pas disponible lorsque l'Infineon Security Platform est désactivée ou elle n'est pas encore initialisée.</p> <p>• Cette fonctionnalité n'est pas disponible en mode serveur, car Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée.</p>
<input type="checkbox"/> <i>Configurer...</i>	Cliquez ici pour configurer les fonctions suivantes :

- Sauvegarde automatique (inclut la récupération d'urgence)
- Réinitialisation mot de passe
- Authentification Renforcée
- Défense d'Attaque par Dictionnaire

L'[Assistant d'initialisation d'Infineon Security Platform](#) sera lancé.



- Cette fonction n'est pas disponible lorsque l'Infineon Security Platform est désactivée ou elle n'est pas encore initialisée.
- Cette fonctionnalité n'est pas disponible en [mode serveur](#), car la réinitialisation du mot de passe et la sauvegarde et restauration sont gérées par le Trusted Computing Management Server.
- Notez que la caractéristique *Défense d'Attaque par Dictionnaire* est seulement disponible sur les Security Platforms avec un Infineon Trusted Platform Module 1.2, si la stratégie [Configurer seuil d'attaque par dictionnaire](#) n'est pas configurée.



Désactiver/Activer...

Cliquez pour désactiver ou activer la Security Platform. Fonction de l'état actuel de l'Infineon Security Platform, cette opération peut être exécutée. Pour cette opération, le mot de passe du propriétaire est exigé.

Désactivation de la Security Platform : Les applications désignées à utiliser le Security Platform n'auront plus accès aux données protégées par le Trusted Platform Module, incluant les données protégées par l'EFS, le Personal Secure Drive et autres. L'accès aux données protégées est restauré une fois Security Platform réactivée.



Sur un système supportant Chiffrement de lecteur BitLocker (par exemple Windows Vista Enterprise ou

Ultimate), si vous désactivez Security Platform lorsque BitLocker est activé, le système d'exploitation vous demandera de saisir le mot de passe BitLocker au redémarrage du système.

Activer la Security Platform dans le BIOS : Pour quelques états de la plate-forme vous devez activer explicitement la Security Platform dans le BIOS. Lorsqu'un redémarrage est demandé pour l'activation de la Security Platform n'est pas activée après le redémarrage, activez explicitement la Security Platform dans le BIOS (voir [Activation du Module Trusted Platform](#)).



- Cette caractéristique n'est pas disponible, si Infineon Security Platform est désactivée dans BIOS.
- Cette caractéristique n'est pas disponible, si Infineon Security Platform n'est pas encore initialisée.
- Cette fonctionnalité n'est pas disponible en [mode serveur](#), car l'activation/désactivation du Trusted Platform Module en fonction du propriétaire n'est pas possible dans ce mode.

▣ Réinitialiser...

Cliquez ici pour [réinitialiser](#) le niveau de défense d'attaque par dictionnaire.
L'Assistant d'Initialisation de Security Platform *SpTPMWz.exe* est lancé avec le paramètre de la ligne de commande *-resetattack*.



- Ce bouton n'est disponible que sur les Security Platforms avec un Trusted Platform Module 1.2.
- En [mode serveur](#), il s'agit de la seule utilisation autorisée de l'Assistant d'Initialisation de Security Platform.

▣ Système...

Cliquez pour administrer les paramètres pour les stratégies système.
L'[Administration de stratégie de système](#) pour l'Infineon

Security Platform sera lancée.



- Les stratégies ne sont pas disponibles dans les éditions Windows ne prenant pas en charge la Gestion des stratégies de groupe, par exemple les éditions familiales de Windows.
- Cette fonctionnalité n'est pas disponible en [mode serveur](#), car l'administrateur local ne doit pas configurer et gérer les paramètres de stratégie. Les stratégies sont configurées au niveau du domaine par un administrateur de domaine, en utilisant Trusted Computing Management Server.

Utilisateur...

Cliquez pour administrer les paramètres pour les stratégies utilisateur.
L'[Administration de stratégie d'utilisateur](#) pour l' Infineon Security Platform sera lancée.



- Les stratégies ne sont pas disponibles dans les éditions familiales de Windows.
- Cette fonctionnalité n'est pas disponible en [mode serveur](#), car l'administrateur local ne doit pas configurer et gérer les paramètres de stratégie. Les stratégies sont configurées au niveau du domaine par un administrateur de domaine, en utilisant Trusted Computing Management Server.



Solution Infineon Security Platform - Outil de Paramétrage

Changement de Mot de Passe du Propriétaire

Ce dialogue permet de changer le Mot de Passe du propriétaire.



Disponibilité du dialogue :

- Ce dialogue est seulement disponible à partir de la page *Avancé* de l'Outil de Paramétrage.
- Ce dialogue n'est pas disponible en [mode serveur](#) car le Trusted Computing Management Server gère les Mot de Passe du Propriétaire.

Merci de noter des indices relatifs à la [gestion de mot de passe](#).

Le tableau suivant indique des indices comment utiliser ce dialogue :

Élément de Dialogue	Explication
<input type="text"/> Ancien Mot de Passe	Indiquez ici l'ancien Mot de Passe du Propriétaire. Vous pouvez soit taper le mot de passe soit donner un fichier de Sauvegarde de Mot de Passe du Propriétaire. Afin de garantir que le Mot de Passe du Propriétaire saisi manuellement remplisse les principales conditions de qualité, un jeu de règles de base pour la gestion de mot de passe devrait être pris en considération.
<input type="checkbox"/> Depuis le Fichier...	Cliquez ici pour fournir un fichier de Sauvegarde de Mot de Passe du Propriétaire, si vous avez enregistré votre Mot de Passe dans un fichier de sauvegarde et si vous ne souhaitez pas taper le mot de passe.
<input type="text"/> Nouveau mot de passe	Indiquez ici le nouveau ancien Mot de Passe du Propriétaire. Vous pouvez soit taper le mot de passe ou générer un mot de passe aléatoire.
<input type="checkbox"/> Aléatoire	Cliquez ici pour générer un Mot de Passe Propriétaire aléatoire au lieu de taper un nouveau mot de passe. Ainsi, vous pouvez facilement garantir d'utiliser un mot de passe sûr remplissant les conditions relatives à

	<p>la complexité et la longueur du mot de passe.</p> <p> Assurez-vous de démasquer, d'imprimer ou d'enregistrer le mot de passe aléatoire avant de fermer ce dialogue.</p>
<input type="checkbox"/> <i>Confirmer nouveau mot de passe</i>	Entrez le mot de passe encore une fois pour confirmer (pas nécessaire si vous avez généré un nouveau mot de passe aléatoire).
<input type="checkbox"/> <i>To Fichiers...</i>	Cliquez ici pour enregistrer le nouveau Mot de Passe Propriétaire vers un fichier de sauvegarde. Vous serez en mesure d'utiliser ce fichier pour l'authentification du Propriétaire au lieu de taper le mot de passe.
<input type="checkbox"/> <i>Imprimer...</i>	<p>Cliquez sur ce bouton pour imprimer le nouveau Mot de Passe Propriétaire.</p> <p> Assurez-vous de stocker l'impression dans un emplacement sûr.</p>
<input checked="" type="checkbox"/> <i>Décochez les mots de passe</i>	Décochez cette case, si vous souhaitez voir les mots de passe.

 Pour information, du police, [Activation de sécurité rigoureuse du champs de mot de passe](#) vous n'avez pas l'autorisation de couper, copier, coller ni de voir des mots de passe en texte clair.



Solution Infineon Security Platform - l'Assistant d'Initialisation Rapide

L'Assistant d'Initialisation Rapide Infineon Security Platform

L'Assistant Rapide d'Initialisation de l'Infineon Security Platform est destiné pour la plupart des utilisateurs d'initialiser rapidement la Security Platform et l'Utilisateur avec les paramètres par défaut. Ces opérations sont nécessaires afin d'activer la fonction Infineon Security Platform et de fournir la base pour toutes les autres activités sur l'Infineon Security Platform.

Si vous souhaitez initialiser votre Security Platform et Utilisateur avec des paramètres avancés, il vous est recommandé d'utiliser l' [Assistant d'Initialisation de Security Platform](#) et l'[Assistant d'Initialisation Utilisateur de Security Platform](#) à la place.



Disponibilité de l'assistant :

- Cet assistant exige des droit administratifs, tant que la Security Platform n'est pas encore initialisée.
- Si la Security Platform est déjà initialisée, l'assistant exécute seulement les tâches de configuration spécifiques à l'utilisateur qui n'exige pas de droits administratifs
- L'utilisation de cet assistant peut être contrôlée avec la [politique Initialisation Rapide de Contrôle](#).
- Les étapes d'initialisation de plateforme de cet assistant sont seulement disponibles si la [politique Autoriser l'Inscription de Plateforme](#) est activée avec l'option *Autoriser fournisseur et assistant de Management*, ou si cette politique n'est pas configurée (les mêmes conditions s'appliquent si vous lancez cet assistant depuis l' [Icône de Notification de la Barre d'Outils](#)). Pour information, cette politique est seulement en vigueur, si la Security Platform n'a pas été initialisée avant.
- Les étapes d'initialisation de l'utilisateur de cet assistant sont seulement disponibles si la [politique Autoriser l'Inscription de l'Utilisateur](#) est activée avec l'option *Autoriser fournisseur et assistant de Management*, ou si cette politique n'est pas configurée (les mêmes conditions s'appliquent si vous lancez cet assistant depuis l' [Icône de Notification de la Barre d'Outils](#)). Pour information, cette politique s'appliquent seulement pour les utilisateurs qui ne sont pas encore initialisés.
- Les étapes d'initialisation de plateforme de cet assistant ne sont pas

disponibles en [mode serveur](#) car la Security Platform est automatiquement initialisée si le système client est intégré dans un Trust Domain avec une gestion centralisée.

Etapes et Pages de l'Assistant

Page/ Etape	Commentaire
1. Bienvenue	Sélection d'une initialisation rapide ou avancée.
2. Paramètres	Configuration de Security Platform spécifique à l'Utilisateur : Encrypting File System (EFS), Personal Secure Drive (PSD), Mot de Passe Utilisateur de Base (si la Security Platform de l'Utilisateur n'est pas encore initialisée).
3. Résumé	Confirmation des paramètres et étapes d'assistant demandées.
4. Achèvement	
5. Fichier Protocole	Affichage, impression et enregistrement du fichier de protocole.
6. Données Secrètes	Affichage des données secrètes générées.

Si votre Trusted Platform n'est pas activée actuellement, vous devez l'activer immédiatement, avant de pouvoir établir votre plateforme (voir [Activation du Module Trusted Platform](#)).

Si votre Trusted Platform a déjà un Propriétaire, mais n'est pas encore initialisée sur votre système d'opération actuel, votre authentification de Propriétaire est demandée (voir [Mot de Passe Propriétaire](#)).

Démarrage de l'application

Lorsque Security Platform n'est pas encore initialisée :

Depuis l' [Icône de Notification de la Barre d'Outils](#), cliquez sur l'élément de menu [Initialisation de la Security Platform](#).

Si la Security Platform est déjà initialisée, et l'utilisateur n'est pas encore initialisé ou initialisé, mais les fonctions EFS et PSD ne sont pas configurées :

Depuis l' [Icône de Notification de la Barre d'Outils](#), cliquez sur l'élément de menu [Initialisation Utilisateur de Security Platform](#).



©Infineon Technologies AG

Solution Infineon Security Platform - l'Assistant d'Initialisation Rapide

Bienvenue

Cette page de l'assistant demande si vous souhaitez exécuter une initialisation rapide ou avancée.

Initialisation Rapide

Une initialisation Rapide, recommandée pour la plupart des utilisateurs, comine une initialisation de plateforme et d'utilisateur avec des emplacements de fichier de données par défaut et des paramètres de fonction par défaut. Les étapes spécifiques à la plateforme sont automatiquement exécutées sans entrée d'utilisateur. Quelques données secrètes et fichiers demandés pour l'administration et les urgences sont générés automatiquement.

Stockage de données et fichiers secrets automatiquement générés

Il vous est recommandé d'utiliser un support amovible (par ex. USB flash drive) afin de stocker des [données secrètes et fichiers](#) automatiquement générés. Si aucun support amovible n'est disponible, les données de sortie doivent être stockées sur le lecteur local du disque dur. Cela exige une protection supplémentaire de données. Par conséquent, vous devez mémoriser ou enregistrer les données secrètes supplémentaires dont vous n'avez pas besoin pour stocker les données sur un support amovible.

Initialisation Avancée

Une initialisation avancée, recommandée pour les utilisateurs experts lance l'[Assistant d'Initialisation de Security Platform](#) afin d'exécuter les étapes de configuration spécifiques à la plateforme. Depuis la fin de cet assistant, vous pouvez continuer avec les étapes de configuration spécifiques à l'utilisateur via l'[Assistant d'Initialisation Utilisateur de Security Platform](#). L'initialisation avancée permet une configuration avancée de données secrètes, d'emplacements de fichiers de données et de fonctions.

Choisissez ce type d'initialisation, si vous souhaitez utiliser [Authentification Renforcée](#) ou [BitLocker](#), ou si vous souhaitez créer un [Personal Secure Drive \(PSD\)](#) sur un support amovible (par ex. USB flash drive).



©Infineon Technologies AG

Solution Infineon Security Platform - Assistant Initialisation rapide

Paramètres

Cette page vous permet de configurer les paramètres de la Security Platform spécifique à l'utilisateur.



Disponibilité des fonctions :

- Cette page d'assistant est seulement disponible, si la politique *Autoriser Inscription Utilisateur* est activée avec l'option *Autoriser fournisseur et assistant de Gestion*.
- EFS n'est pas pris en charge dans les éditions familiales de Windows.
- La configuration d'EFS pourrait être bloquée via la politique d'utilisateur [Autoriser Configuration EFS](#).
- La configuration de PSD pourrait être bloquée via la politique d'utilisateur [Autoriser Configuration PSD](#).
- Pour une nouvelle configuration de ces fonctions, cliquez sur [Outil de Paramétrage - Paramètres Utilisateur - Configurer...](#)

Le tableau suivant explique les Fonctions de la Security Platform.

Fonction	Explication
<input checked="" type="checkbox"/> <i>Encrypting File System (EFS) basé sur le matériel</i>	<p>EFS fait partie de la technologie de sécurité du système fichier Microsoft NTFS. EFS permet de chiffrer vos fichiers et dossiers. La Security Platform Solution élargit la sécurité d'EFS en protégeant l'accès aux clés de chiffrement EFS avec le Trusted Platform Module.</p> <p>Si vous cochez cette case, l'Assistant d'Initialisation Rapide permet l'activation d'EFS, la création d'un dossier chiffré <i>Documents\Données chiffrées</i> ou <i>Mes Documents\Données chiffrées</i> (en fonction de votre système d'exploitation), et la création d'un raccourci de bureau vers ce dossier.</p> <p>Apprendre plus de détails sur EFS</p>
<input checked="" type="checkbox"/> <i>Personal Secure Drive (PSD)</i>	<p>PSD est un lecteur chiffré sur votre PC. Il apparaît comme tout autre lecteur de disque dur. L'accès aux fichiers et dossiers sur le PSD est le même que tout autre lecteur. La seule différence est que le contenu de PSD est totalement chiffré et seulement</p>

	<p>accessible après avoir expressément chargé PSD. Le chargement de PSD exige votre authentification d'utilisateur. Les données PSD sont stockées dans le fichier d'image PSD.</p> <p>Si vous cochez cette case, l'Assistant d'Initialisation Rapide crée un PSD et un raccourci de bureau vers ce PSD. Le fichier image PSD sera créé dans la partition système, dans le dossier <i>Security Platform</i> (sauf si cet emplacement est configuré en utilisant la stratégie Emplacement fichier pour Personal Secure Drive).</p> <p>Apprendre plus de détails sur PSD</p>
<p> <i>Mot de passe utilisateur de base</i></p>	<p>Configurez le Mot de Passe Utilisateur de Base qui est demandé pour l'utilisation des Fonctions de Security Platform.</p>

Où utiliser EFS ou PSD ?

Le tableau suivant compare EFS et PSD. Il fournit également des indices où utiliser laquelle des deux fonctions.

Critère	EFS	PSD
<i>Type de Chiffrement</i>	Basés sur fichier et dossier, c'est-à-dire fichiers et dossiers discrets sont chiffrés.	Basé sur dispositif, c'est-à-dire tous les fichiers sur le lecteur sont chiffrés.
<i>Systèmes d'Operation pris en charge</i>	Tous les systèmes d'exploitation pris en charge par Security Platform Solution excepté les éditions familiales de Windows.	Tous les systèmes d'exploitation pris en charge par Security Platform Solution.
<i>Accès et Gestion des Données</i>	Toujours visible. Le chiffrement et déchiffrement ne sont possibles qu'après l'authentification de l'utilisateur. Le chiffrement et déchiffrement sont bloqués	Seulement visible et accessible après avoir expressément chargé le lecteur (exige une authentification de l'utilisateur). PSD peut

	après la déconnexion d'EFS. De plus, les droits d'accès au système de fichier NTFS peuvent être configurés si vous souhaitez partager des fichiers.	expressément être déchargé. De plus, les droits d'accès au système NTFS peuvent être configurés.
<i>Récupération de Données</i>	Via Agents de Récupération EFS.	<ul style="list-style-type: none"> • Sur les systèmes d'exploitation qui prennent en charge EFS: Via Agents de Récupération EFS. • Sur les systèmes d'exploitation qui ne prennent pas en charge EFS: Via Agents de Récupération PSD.
<i>Partage de Données</i>	Peut être utilisé en commun avec de multiples utilisateurs en ajoutant le certificat d'un autre utilisateur.	Pas de partage de données, utilisateur unique.
<i>Emplacement de Données</i>	Lecteurs locaux ou dossiers web, système de fichier NTFS.	Support amovible ou disque dur local.
<i>Sauvegarde de Données</i>	Via toute méthode de sauvegarde ou logiciel.	Via Sauvegarde de Security Platform Solution .
<i>Quand utiliser EFS ou PSD</i>	Si les données à chiffres se trouvent dans des dossiers spéciaux (par ex. <i>Mes Documents</i> ou dossiers de données spécifiques à l'application.	<ul style="list-style-type: none"> • Si votre système d'exploitation est une édition familiale de Windows et ne prend donc pas en charge EFS. • Si les données à chiffres se trouvent sur un lecteur amovible que vous souhaitez utiliser sur plusieurs PC. Dans le mode serveur, Personal Secure Drive sur

supports amovibles peut être itinéré sans problèmes. Dans le [mode autonome](#) vous devez migrer les informations d'identification et paramètres ou vous pouvez restaurer ou ajouter une sauvegarde du fichier image.

- Si les données à chiffrer se trouvent sur un système de fichier FAT32.



Solution Infineon Security Platform - l'Assistant d'Initialisation Rapide

Résumé

Sur la page de résumé figurent les étapes à exécuter.

Les étapes demandées dépendent de la plateforme actuelle et de l'état de l'utilisateur. Par exemple, sur une Security Platform qui est déjà initialisée, les étapes propres à la plateforme sont ignorées, et seules les étapes spécifiques à l'utilisateur sont exécutées.



Pour information, l'initialisation et la configuration de la Security Platform pourrait prendre un peu de temps. La création en particulier d'un large lecteur PSD peut prendre beaucoup de temps.



©Infineon Technologies AG

Solution Infineon Security Platform - l'Assistant d'Initialisation Rapide

Achèvement

La page finale montre le résultat de toutes les étapes d'initialisation et de configuration. Vous pouvez trouver des informations détaillées dans le fichier de protocole de l'assistant. Cliquez sur *Détails...* pour accéder au fichier de protocole.



En fonction de la plateforme précédente et de l'état d'utilisateur précédent et de votre sélection de l'emplacement de stockage de la production de l'assistant, l'assistant peut avoir créé des données secrètes. Cela est nécessaire pour l'administration et les urgences. Surtout, si vous n'avez pas sélectionné de support amovible (par ex. USB flash drive) afin de stocker la production de l'assistant, vous devez imprimer, enregistrer ou mémoriser toutes les données secrètes dans tous les cas, avant de terminer l'assistant. Pour cela, cliquez sur *Détails*.

Options Avancées

Si vous souhaitez changer vos paramètres propres à l'utilisateur ou utiliser des fonctions supplémentaires, vérifiez **Continuer avec options avancées**. Dans ce cas, [Assistant Initialisation de l'Utilisateur](#) est lancé après l'achèvement de cet assistant.



©Infineon

Technologies AG

Solution Infineon Security Platform - l'Assistant d'Initialisation Rapide

Fichier de Protocole

Ce dialogue affiche le protocole de toutes les étapes effectuées par l'assistant.

Élément de la boîte de dialogue	Explication
<input type="checkbox"/> <i>Imprimer...</i>	<p>Cliquez ici pour imprimer le fichier de protocole. Vous pouvez décider si vous souhaitez inclure les données secrètes générées demandées pour l'administration et les urgences dans l'impression du protocole.</p>
<input type="checkbox"/> <i>Enregistrer...</i>	<p>Cliquez ici pour enregistrer le fichier de protocole. Vous pouvez décider si vous souhaitez inclure les données secrètes générées demandées pour l'administration et les urgences dans le protocole à enregistrer.</p> <p> Pour information, une version du protocole sans les données secrètes a déjà été enregistrée automatiquement (<i>SpProtocol_<PCName>_<UserName>.txt</i> pour utilisateurs locaux) ou (<i>SpProtocol_<PCName>_<UserName>.<DomainName>.txt</i> pour utilisateurs de domaine). Le chemin du fichier de protocole enregistré automatiquement est affiché dans ce dialogue.</p>
<input type="checkbox"/> <i>Afficher</i>	<p>Cliquez ici pour afficher les données secrètes générées.</p> <p> Pour information, le montant et le type de données secrètes dépendent de la précédente plateforme et de l'état de l'utilisateur, et de votre sélection où stocker la production de l'assistant. Si la plateforme a déjà été initialisée avant le lancement de l'assistant, et vous avez sélectionné un support amovible (par ex. USB flash drive) pour stocker la production de l'assistant, aucune donnée secrète n'est créée.</p>
	<p>Après avoir terminé cet assistant, vous n'avez plus de possibilité d'accéder aux données secrètes générées. Assurez-vous d'avoir imprimé, enregistré ou archivé avec succès les données secrètes sous n'importe quelle forme</p>

avant de terminer l'assistant. Ceci est particulièrement important, si vous n'avez pas sélectionné de support amovible (par ex. USB flash drive) pour stocker la production de l'assistant.



©Infineon

Technologies AG

Solution Infineon Security Platform - l'Assistant d'Initialisation Rapide

Secrets d'Authentification

Ce dialogue affiche les données secrètes générées.



Si vous n'avez pas sélectionné de support amovible (par ex. USB flash drive) afin de stocker la production de l'assistant, vous devez imprimer, enregistrer ou mémoriser toutes les données secrètes générées. Vous en avez besoin pour exécuter certaines tâches administratives ou urgentes importantes.

Pour information, le montant et le type de données secrètes dépendent de l'ancienne plateforme et de l'état de l'utilisateur, et de votre sélection de l'emplacement de stockage.

Le tableau suivant fournit des détails sur les données secrètes générées et les fichiers correspondants. Les noms **USB** et **HD** indiquent si les données secrètes concernées ou le fichier est créé et enregistré, si vous avez sélectionné un support amovible (par ex. USB flash drive) ou un disque dur (**HD**) afin de stocker la production de l'assistant.

Type	Objectif	Etendue	Fichier correspondant
Mot de Passe Propriétaire (USB, HD)	Exigé pour exécuter des tâches importantes administratives de Security Platform.	Propre à Plateforme. Création automatique pendant les étapes d'initialisation propres à la plateforme, si la plateforme n'a pas encore été initialisée lorsque cet assistant a été lancé.	Fichier de Sauvegarde Mot Propriétaire (USB) Nom de fichier par défaut : <i>SpOwner_<PC>.tpm</i> où <PC> est le nom de la pla Seulement créé et enregistré, avez sélectionné un support a (par ex. USB flash drive) afin stocker la production de l'assi Dans ce cas, vous n'avez pas connaître expressément le Mo Propriétaire, car vous pouvez Fichier de Sauvegarde de Mo Propriétaire depuis votre amc ex. USB flash drive).
Mot de Passe pour Récupération	Protection du combiné Récupération	Propre à Plateforme. Création	Fichier Combiné de Récupération d'Urgence / Jeton de Réinitialisation de Mot de Passe (USB, HD)

<p>d'Urgence / Jeton de Réinitialisation de Mot de Passe (HD)</p>	<p>d'Urgence / Jeton de Réinitialisation de Mot de Passe qui est exigé pour exécuter une Récupération d'Urgence et pour réinitialiser un Mot de Passe Utilisateur de Base.</p>	<p>automatique pendant les étapes de configuration propres à la plateforme, si vous n'avez pas sélectionné un support amovible (par ex. USB flash drive) afin de stocker la production de l'assistant et la plateforme n'avait pas été initialisée lorsque cet assistant a été lancé.</p>	<p>Nom de fichier par défaut : <i>SpToken_<PC>.xml</i> où <PC> est le nom de la plateforme. Pour information, ce jeton n'est pas un mot de passe dédié, s'il est utilisé sur un support amovible (par ex. USB flash drive).</p>
<p>Mot de Passe Secret Réinitialisation (USB, HD)</p>	<p>Un secret personnel d'utilisateur qui est exigé pour réinitialiser son Mot de Passe Utilisateur de Base.</p>	<p>Propre à l'utilisateur. Création automatique pendant les étapes de configuration propres à l'utilisateur, si l'utilisateur n'a pas encore été initialisé lorsque cet assistant a été lancé.</p>	<p>Fichier Secret de Réinitialisation de Passe (USB) Nom de fichier par défaut : <i>SpPwdResetSecret_<PC>_<User></i> où <PC> est le nom de la plateforme (pour les utilisateurs locaux) ou une combinaison de nom d'utilisateur et de nom de domaine (pour les utilisateurs de domaine). Seulement créé et enregistré, si vous avez sélectionné un support amovible (par ex. USB flash drive) afin de stocker la production de l'assistant. Dans ce cas, vous n'avez pas besoin de connaître expressément le Se</p>

			Réinitialisation Mot de Passe pouvez utiliser le Fichier de S Réinitialisation Mot de Passe Propriétaire depuis votre supp amovible (par ex. USB flash
--	--	--	--

Indices généraux sur la gestion de données secrètes : Voir [Gestion de Mot de Passe](#).



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Initialisation

Assistant d'initialisation de l'Infineon Security Platform

L'Assistant d'Initialisation d'Infineon Security Platform est destiné pour les experts à initialiser la Security Platform et à configurer les Fonctions de Security Platform (sauvegarde y compris Récupération d'Urgence, Réinitialisation du Mot de Passe, Authentification Renforcée, BitLocker). Ces opérations sont nécessaires pour activer la fonctionnalité de l'Infineon Security Platform et fournir les fonctions de base liées à l'utilisation de l'Infineon Security Platform.

Si vous souhaitez initialiser rapidement votre Security Platform et Utilisateur avec les paramètres par défaut, il vous est recommandé d'utiliser à la place [l'Assistant d'Initialisation Rapide](#).

A la place de l'initialisation d'une nouvelle Security Platform, vous pouvez également restaurer une Security Platform endommagée en sélectionnant *Restaurer une Security Platform depuis une sauvegarde de secours*.

C'est le premier assistant à exécuter pour configurer une Infineon Security Platform.



Disponibilité de l'assistant :

- Cet assistant est disponible seulement si l'utilisateur actuel possède droits d'administration.
- Cet assistant est disponible seulement si la stratégie *Permettre l'inscription de la plate-forme* est activée avec l'option *Autorisation pour l'interface et l'assistant de gestion* ou cette stratégie n'est pas configurée (les mêmes conditions s'appliquent si vous lancez cet assistant à partir de [l'Icône de notification de la barre des tâches](#)). Cette stratégie s'applique uniquement si la Security Platform n'a pas été initialisée auparavant.
- Si la Security Platform a été initialisée auparavant, la stratégie n'est pas appliquée et cet assistant peut être utilisé pour configurer les fonctions de Security Platform (les mêmes conditions s'appliquent si vous lancez cet assistant à partir de [l'Icône de notification de la barre des tâches](#)).
- Cet assistant n'est pas disponible en [mode serveur](#), car Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée.

Etapes de l'assistant

Étape	Commentaire
1. Activer le Trusted Platform Module	Seulement si le Trusted Platform Module n'est actuellement activé.
2. Initialisation ou restauration ?	Seulement si la Security Platform n'est pas encore initialisée.
3. Configuration de la propriété ou Mot de passe utilisateur	Seulement si la Security Platform n'est pas encore initialisée. Fonction de l'état de la Security Platform, le mot de passe propriétaire est configuré ou vérifié.
4. Fonctions	Sauvegarde avec réinitialisation d'urgence, Réinitialisation mot de passe, Authentification étendue, Bitlocker.
5. Sauvegarde	Seulement la fonction <i>Sauvegarde</i> a été sélectionnée.
6. Récupération d'urgence	Seulement la fonction <i>Sauvegarde</i> a été sélectionnée.
7. Réinitialisation du mot de passe	Seulement la fonction <i>Réinitialisation du mot de passe</i> a été sélectionnée.
8. BitLocker	<p>Seulement si la fonction <i>BitLocker</i> a été sélectionnée. Seulement si l'état de <i>BitLocker</i> est <i>Configuré</i>, <i>Reconfiguration nécessaire</i>, <i>Chiffrage en cours</i> ou <i>Déchiffrage en cours</i>.</p> <p> • Cette fonction n'est disponible que si le système d'exploitation accepte le chiffrement de lecteur BitLocker (par ex. pour Windows 7 et Windows Vista Enterprise ou Ultimate).</p> <p>• Cette page n'est pas disponible en mode serveur. Vous pouvez toutefois configurer BitLocker via l'applet Panneau de configuration Microsoft BitLocker.</p>

9. [Authentification étendue](#)

Seulement lorsque la Security Platform est déjà initialisée lorsque l'assistant a été lancé.
Seulement lorsque la fonction *Authentification étendue* a été sélectionnée.

10. [Défense d'Attaque par Dictionnaire](#)

Seulement disponible sur les Security Platforms avec un Infineon Trusted Platform Module 1.2.
Seulement si la caractéristique *Défense d'Attaque par Dictionnaire* a été sélectionnée.

Démarrage de l'application

Lorsque Security Platform n'est pas encore initialisée : Depuis l'Icône de [Notification de la Barre d'Outils](#), cliquez sur l'élément de menu **Initialisation de la Security Platform**. [L'assistant Initialisation rapide](#) démarre. Sur la page d'Accueil, sélectionnez **l'Initialisation Avancée**. L'Assistant d'Initialisation de Security Platform est lancé.

Lorsque Security Platform est déjà initialisé : Démarrez l'assistant d'initialisation de la Security Platform via l'outil de paramétrage.

- Pour configurer les fonctions de la Security Platform (Sauvegarde avec réinitialisation d'urgence, Réinitialisation mot de passe, Authentification étendue) : [Outil de paramétrage - Avancé - Configuration...](#)
- Pour configurer la fonction Réinitialisation mot de passe : [Outil de paramétrage - Réinitialisation mot de passe - Configuration...](#)
- Pour configurer la fonction Sauvegarde : [Outil de paramétrage - Sauvegarde - Configuration...](#)



Infineon Security Platform Solution - Assistant Initialisation

Activer le Trusted Platform Module

Trusted Platform Module doit être activé pour mettre en service la fonctionnalité principale. Seulement après cela, on peut initialiser Security Platform et effectuer d'autres opérations de configuration initiale. La procédure d'activation de Trusted Platform Module dépend de la version du Trusted Platform Module, du matériel de Security Platform et de BIOS.

Sur **les systèmes de Trusted Platform Module 1.2 qui prennent en charge la Physical Presence Interface (PPI)** cette interface est utilisée afin d'activer le Trusted Platform Module. Selon le matériel et le BIOS, ceci est possible soit sans interaction d'utilisateur, ou vous devez exécuter quelques étapes additionnelles.

Sur **tous les autres systèmes**, vous devez redémarrer et accéder au BIOS du système.

Une description du mode d'activation du microprocesseur est disponible ici :

En tout cas, l'assistant détecte automatiquement la façon de laquelle l'activation de Trusted Platform Module est possible sur votre système et il vous guide en conséquence.

La table suivante montre comment activer Trusted Platform Module sur des différents types de Security Platform.

Type de Security Platform	Bouton	Explication
Trusted Platform Module 1.2 PPI demande un redémarrage	<input type="checkbox"/> <i>Redémarrer</i>	Le système est redémarré. Lors du redémarrage veuillez suivre les instructions de l'écran de démarrage pour activer Trusted Platform Module.

Trusted Platform Module 1.2 PPI demande fermeture	<input type="checkbox"/> <i>Fermer</i>	Le système est fermé et doit être redémarré manuellement. Lors du démarrage du système veuillez suivre les instructions de l'écran de démarrage pour activer Trusted Platform Module.
Trusted Platform Module 1.2 PPI ne demande pas de redémarrage ni de fermeture	<input type="checkbox"/> <i>Activer</i>	L' <i>Interface de Présence Physique</i> est utilisée pour activer le Trusted Platform Module. Aucun redémarrage ni arrêt n'est exigé.  En fonction de votre système, quelques étapes additionnelles pourraient être nécessaires de votre part pour activer Trusted Platform Module. Veuillez trouver plus d'informations dans votre manuel du système.
Tous les autres types (par ex. Trusted Platform Module 1.1 et / ou PPI non prise en charge)	<input type="checkbox"/> <i>Redémarrer</i>	Le système est redémarré et Trusted Platform Module doit être activé dans le BIOS du Système.



Note concernant le redémarrage et la fermeture du système :

Tous les applications ouvertes sont fermées sans autres indications. Pour éviter la perte de données, tous les applications devraient être fermées avant le redémarrage du système.



Infineon Security Platform Solution - Assistant Initialisation

Initialisation ou restauration d'une Security Platform

Cette page d'assistant vous demande lorsque vous désirez l'initialisation ou la restauration d'une Security Platform.



Cette page d'assistant n'est pas disponible dans le [mode serveur](#), car Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée, c'est-à-dire l'administrateur ne doit pas exécuter cette tâche.

Élément de la page assistant	Explication
⦿ <i>Initialisation de Security Platform</i>	Cliquez lorsque vous désirez configurer une nouvelle Security Platform. Dans ce cas, une nouvelle plate-forme et nouvelles informations d'identification utilisateur seront créées.
⦿ <i>Restauration de Security Platform à partir d'une Sauvegarde de secours</i>	Cliquez lorsque vus désirez restaurer une Security Platform après une erreur du matériel, une erreur d'un support de stockage ou une erreur Trusted Platform Module. La restauration de la Security Platform rétablit l'accès aux fonctions de la Security Platform pour tous les utilisateurs.



Infineon Security Platform Solution - Assistant Initialisation

Créer le propriétaire de Security Platform

Une fois le Trusted Platform Module activé, le propriétaire doit être configuré, au cours d'une étape unique, pour établir une association logique entre le circuit et l'ordinateur en vue d'une utilisation ultérieure. Pendant cette opération, le Propriétaire d'Infineon Security Platform est créé et stocké dans le Trusted Platform Module ensemble avec le secret du Propriétaire d'Infineon Security Platform. Cela est protégé par le [Mot de Passe Propriétaire](#) qui doit être défini ici. Vous pouvez soit entrer le Mot de Passe Propriétaire ou générer un Mot de Passe Propriétaire aléatoire. Vous pouvez enregistrer ce Mot de Passe Propriétaire dans un fichier et utiliser ce fichier de sauvegarde avec le Mot de Passe Propriétaire, ou même l'imprimer. Si vous avez choisi l'option de générer un Mot de Passe Propriétaire aléatoire, vous pouvez aussi le rendre visible afin de le mémoriser ou le noter. Vous avez besoin du Mot de Passe Propriétaire ou du fichier de sauvegarde avec le Mot de Passe Propriétaire afin d'administrer la Security Platform.



Cette page n'est pas disponible dans le [mode serveur](#), car Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée, c'est-à-dire l'administrateur ne doit pas exécuter cette tâche.



L'échange du propriétaire avec l'assistant d'initialisation de la Security Platform crée une nouvelle clé SRK. Généralement vous devez configurer le propriétaire de la Security Platform une seule fois pour un Trusted Platform Module. Car tous les certificats clé publique sont liés par la clé SRK du Trusted Platform Module, vous ne pourrez plus utiliser ces certificats avec la nouvelle clé SRK.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
 <i>Mot de Passe</i>	Paramétrez un Mot de Passe Propriétaire ici. Vous pouvez soit entrer un Mot de Passe Propriétaire de votre choix ou générer un Mot de Passe Propriétaire aléatoire.

	 Afin de garantir que le Mot de Passe du Propriétaire saisi manuellement remplisse les principales conditions de qualité, un jeu de règles de base pour la gestion de mot de passe devrait être pris en considération.
<input type="text" value="xxx"/> <i>Entrez le mot de passe</i>	Entrez le mot de passe encore une fois pour confirmer (pas nécessaire si vous avez généré un mot de passe aléatoire).
<input type="checkbox"/> <i>Aléatoire</i>	<p>Cliquez ici pour générer un Mot de Passe Propriétaire aléatoire au lieu de taper un nouveau mot de passe. Ainsi, vous pouvez facilement garantir d'utiliser un mot de passe sécurisé remplissant les conditions relatives à la complexité et la longueur du mot de passe.</p> <p> Assurez-vous de démasquer, d'imprimer ou d'enregistrer le mot de passe aléatoire avant de continuer.</p>
<input type="checkbox"/> <i>Vers Fichier...</i>	Cliquez ici pour enregistrer le nouveau Mot de Passe Propriétaire vers un fichier de sauvegarde. Vous serez en mesure d'utiliser ce fichier pour l'authentification du Propriétaire au lieu de taper le mot de passe.
<input type="checkbox"/> <i>Imprimer...</i>	<p>Cliquez sur ce bouton pour imprimer le Mot de Passe Propriétaire.</p> <p> Assurez-vous de stocker l'impression dans un emplacement sûr.</p>
<input checked="" type="checkbox"/> <i>Décochez les mots de passe</i>	Décochez cette case, si vous souhaitez voir les mots de passe.

 Notez que dû à la stratégie [Activer la sécurité rigoureuse du champ mot de passe](#) vous n'êtes pas autorisé à couper, copier, coller et voir les mots de passe en texte clair.



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Initialisation

Mot de passe propriétaire

Le [Mot de Passe propriétaire](#) est demandé pour exécuter des tâches importantes d'administration de la Security Platform.

Cette page est affichée dans l'[Assistant d'Initialisation de Security Platform](#) et l'[Assistant d'Initialisation Rapide](#), si le Mot de Passe Propriétaire existe déjà, mais la Security Platform n'est pas encore initialisée.

C'est le cas sous les circonstances suivantes :

- Si le Mot de Passe Propriétaire a été paramétré via l'application Microsoft du [Trusted Platform Module \(TPM\) Management](#).
- Si le processus d'initialisation de la Security Platform a été interrompu, probablement en raison d'une coupure de courant ou pour une autre raison.
- Si la Security Platform est initialisée et qu'elle a un propriétaire sur l'autre système d'exploitation.
- Si la Security Platform est initialisée sur un système d'exploitation et qu'ensuite l'utilisateur l'initialise sur l'autre SE en passant par le BIOS.

Pour authentification, vous pouvez soit taper le mot de passe soit donner un fichier de Sauvegarde de Mot de Passe du Propriétaire.



Cette page n'est pas disponible en [mode serveur](#) car la Security Platform est automatiquement initialisée si le système client est intégré dans un Trust Domain avec une gestion centralisée, i.e. l'administrateur ne doit pas exécuter cette tâche.



©Infineon

Infineon Security Platform Solution - Assistant Initialisation

Fonctionnalités de Security Platform

Avec cette page vous pouvez configurer les fonctions de la Security Platform pour tous les utilisateurs, par exemple la sauvegarde.



Cette page d'assistant n'est pas disponible dans le [mode serveur](#), car Trusted Computing Management Server gère la configuration des fonctions de Security Platform, par exemple la *sauvegarde*, la *réinitialisation du mot de passe* et l'*Authentification étendue*. La fonction *BitLocker* peut être configurée en utilisant l'applet Microsoft Panneau de configuration.

La table suivante explique toutes les fonctions de la Security Platform.

Fonction	Explication
<input checked="" type="checkbox"/> <i>Sauvegarde automatique (inclut la récupération d'urgence)</i>	<p>Cochez cette fonction lorsque vous désirez configurer les sauvegardes automatiques de la Security Platform. La configuration de la <i>Sauvegarde</i> est vivement recommandée. Autrement toutes les données utilisateur seront perdues en cas d'urgence.</p> <p> Vous ne pouvez pas décocher cette option lorsque la stratégie Application de la configuration de sauvegarde incluant la récupération d'urgence est activée.</p>
<input checked="" type="checkbox"/> <i>Réinitialisation mot de passe</i>	<p>Cochez cette option lorsque vous désirez créer un jeton de réinitialisation du mot de passe pour tous les utilisateurs. La configuration de la <i>Réinitialisation mot de passe</i> est vivement recommandé. Autrement les mots de passe utilisateurs de base ne peuvent pas être réinitialisés.</p> <p> Vous ne pouvez pas décocher cette option lorsque la stratégie Application de la configuration de la réinitialisation du mot de passe est activée. Cette fonction ne peut pas être configurée qu'une seule fois. La sélection est désactivée lorsque la <i>Réinitialisation mot de passe</i> a été déjà configurée.</p>
<input checked="" type="checkbox"/> <i>BitLocker</i>	<p>Cochez cette fonction si vous désirez utiliser le Chiffrement</p>

	<p>de lecteur BitLocker ensemble avec Trusted Platform Module pour chiffrer les données sur votre disque.</p> <p> Cette fonction n'est disponible que si le système d'exploitation accepte le chiffrement de lecteur BitLocker (par ex. pour Windows 7 et Windows Vista Enterprise ou Ultimate).</p>
<p><input checked="" type="checkbox"/> <i>Authentification Renforcée</i></p>	<p>Cochez cette fonction lorsque vous désirez activer l'authentification étendue pour tous les utilisateurs et vous désirez modifier la sélection des dispositifs d'authentification.</p> <p> Cette fonction est disponible seulement lorsqu'au moins un plugiciel de l'authentification étendue est installé. Ce service n'est pas encore disponible tant que la Security Platform n'a pas été initialisée avant le démarrage de l'assistant.</p>
<p><input checked="" type="checkbox"/> <i>Défense d'Attaque par Dictionnaire</i></p>	<p>Vérifiez cette caractéristique, si vous souhaitez configurer combien d'essais d'authentification devraient être autorisés pour plusieurs types d'authentification avant que des mesures de défense d'attaque par dictionnaire ne soient prises. Voir Configurer Paramètres de Défense d'Attaque par Dictionnaire.</p> <p> Notez que cette caractéristique est seulement disponible sur les Security Platforms avec un Infineon Trusted Platform Module 1.2, si la stratégie Configurer seuil d'attaque par dictionnaire n'est pas configurée. Ce service n'est pas encore disponible tant que la Security Platform n'a pas été initialisée avant le démarrage de l'assistant.</p>



Infineon Security Platform Solution - Assistant Initialisation

Sauvegarde

Avec cette page vous pouvez configurer les sauvegardes automatiques de la Security Platform. Voir [Sauvegarde et restauration de données Security Platform](#).



Cette page n'est pas disponible en [mode serveur](#), car la sauvegarde automatique est gérée par Trusted Computing Management Server, donc aucune configuration explicite n'est nécessaire de la part de l'utilisateur.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Elément de la page assistant	Explication
 <i>Emplacement de la sauvegarde :</i>  <i>Parcourir...</i>	Vos informations d'identification et paramètres de Security Platform seront sauvegardés régulièrement dans une sauvegarde de secours. Entrez le chemin et le nom du fichier ou naviguez jusqu'au fichier. Un fichier de sauvegarde écrit automatiquement, représenté par un fichier XML et un dossier avec le même nom, sera créé, par ex. un fichier SPSystemBackup.xml et un dossier SPSystemBackup .  Veuillez utiliser l'extension *.xml.
 <i>Planifier...</i>	Une sauvegarde planifiée sera créée. Cliquez pour visualiser et modifier la planification de la sauvegarde.  Les sauvegardes automatiques sont exécutées seulement lorsque votre ordinateur n'est pas arrêté au moment de la planification. Le compte utilisateur choisi pour la sauvegarde planifiée doit être membre du groupe "Administrateurs" ou "Opérateurs sauvegarde".



Infineon Security Platform Solution - Assistant Initialisation

Récupération d'urgence

Avec cette page vous pouvez configurer la partie Récupération d'urgence des sauvegardes automatiques de la Security Platform.



Disponibilité de la page :

- Cette page est disponible seulement lorsque vous avez sélectionnée la configuration des sauvegardes automatiques de Security Platform.
- Cette page n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration automatique sont gérées par Trusted Computing Management Server, donc aucune configuration explicite n'est nécessaire de la part de l'utilisateur.

Eléments de la page assistant



Vos options dans la page de l'assistant peuvent être limitées selon les [stratégies système](#).

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<input type="radio"/> <i>Créer nouveau jeton récupération</i>	Sélectionnez cette option lorsque vous désirez créer un nouveau jeton à utiliser pour la récupération d'urgence. Le jeton sera enregistré dans l'emplacement spécifié par vous. Vous devrez configurer un nouveau mot de passe jeton.
<input type="radio"/> <i>Utiliser jeton récupération existant</i>	Sélectionnez cette option lorsque les conditions suivantes sont remplies : <ul style="list-style-type: none">• En cas d'urgence, vous devez restaurer votre système en utilisant le jeton de récupération d'urgence créé auparavant.• Ce jeton et le mot de passe jeton sont actuellement disponibles. Vous devrez vérifier le mot de passe jeton, c.à.d. vous devez saisir le mot de passe une seule fois.
<input type="checkbox"/> <i>Location fichier</i> <input type="checkbox"/> <i>Parcourir...</i>	Lorsque vos paramètres stratégie autorisent la spécification manuelle de l'emplacement du fichier, vous pouvez modifier le nom du fichier et le chemin. Entrez le chemin et le nom du fichier ou naviguez jusqu'au fichier. Le fichier est en format XML. Lorsque vous avez sélectionné <i>Créer nouveau jeton récupération</i> : Le jeton de récupération d'urgence doit être sauvegardé dans un emplacement sûr, par exemple un support amovible stocké dans un environnement sécurisé. Ne stockez

	<p>pas le jeton de récupération sur votre disque dur. Autrement, en cas d'erreur système ou erreur du disque dur, votre jeton ne sera plus disponible et des données seront perdues. Stockez le jeton de récupération sur un support de secours, par exemple un lecteur de mémoire ou un CD, pour empêcher la perte du jeton et pour assurer votre accès exclusif au jeton de récupération.</p>
<p> <i>Mot de passe</i></p>	<p>Lorsque vous avez sélectionné <i>Créer nouveau jeton de récupération</i>, vous devez configurer un nouveau mot de passe jeton. Entrez un mot de passe pour le jeton de récupération d'urgence. Consultez les Généralités sur les mots de passe.</p> <p>Lorsque vous avez sélectionné <i>Utiliser jeton récupération existant</i>, vous devez vérifier le mot de passe jeton. Saisissez le mot de passe du jeton actuel.</p> <p>Lorsque vous avez sélectionné <i>Utiliser archive récupération existante</i>, vous ne devez pas saisir un mot de passe.</p>
<p> <i>Confirmer mot de passe</i></p>	<p>Lorsque vous avez sélectionné <i>Créer nouveau jeton de récupération</i>, vous devez confirmer le nouveau mot de passe. Entrez à nouveau le mot de passe pour confirmation.</p>



Infineon Security Platform Solution - Assistant Initialisation

Réinitialisation du mot de passe

Avec cette page vous pouvez créer un jeton de réinitialisation du mot de passe pour tous les utilisateurs.



Disponibilité de la page :

- Cette page est seulement disponible lorsque vous avez configuré la Réinitialisation du mot de passe.
- Cette page n'est pas disponible dans le [mode serveur](#), car le Trusted Computing Management Server la gère.

Eléments de la page assistant



Vos options dans la page de l'assistant peuvent être limitées selon les [stratégies système](#).

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<input type="radio"/> <i>Créer jeton nouveau</i>	<p>Sélectionnez cette option lorsque vous désirez créer un nouveau jeton à utiliser pour la réinitialisation du mot de passe.</p> <p>Le jeton sera enregistré dans l'emplacement spécifié par vous. Vous devrez configurer un nouveau mot de passe jeton.</p>
<input type="radio"/> <i>Utiliser jeton existant</i>	<p>Sélectionnez cette option lorsque les conditions suivantes sont remplies :</p> <ul style="list-style-type: none">• Vous désirez réinitialiser des mots de passe en utilisant un jeton créé auparavant.• Ce jeton et le mot de passe jeton sont actuellement disponibles. <p>Vous devrez vérifier le mot de passe jeton, c.à.d. vous devez saisir le mot de passe une seule fois.</p>
<input type="checkbox"/> <i>Location fichier</i> <input type="checkbox"/> <i>Parcourir...</i>	<p>Lorsque vos paramètres stratégie autorisent la spécification manuelle de l'emplacement du fichier, vous pouvez modifier le nom du fichier et le chemin.</p> <p>Entrez le chemin et le nom du fichier ou naviguez jusqu'au fichier. Le fichier est en format XML.</p> <p> Lorsque vous avez sélectionné <i>Créer nouveau jeton</i> : Le jeton de réinitialisation du mot de passe doit être sauvegardé dans un emplacement sûr, par exemple un support amovible stocké dans un environnement sécurisé. Ne stockez pas le</p>

	<p>jeton sur votre disque dur. Autrement, en cas d'erreur système ou erreur du disque dur, votre jeton ne sera plus disponible et les mots de passe utilisateur de base ne peuvent pas être réinitialisés. Stockez le jeton sur un support de secours, par exemple un lecteur de mémoire ou un CD, pour empêcher la perte du jeton et pour assurer votre accès exclusif au jeton.</p>
<p>☒ <i>Mot de passe</i></p>	<p>Lorsque vous avez sélectionné <i>Créer jeton nouveau</i>, vous devez configurer un nouveau mot de passe jeton. Entrez un mot de passe pour le jeton de réinitialisation du mot de passe. Consultez les Généralités sur les mots de passe.</p> <p>Lorsque vous avez sélectionné <i>Utiliser jeton existant</i>, vous devez vérifier le mot de passe jeton. Saisissez le mot de passe du jeton actuel.</p> <p>Lorsque vous avez sélectionné <i>Utiliser archive existante</i>, vous ne devez pas saisir un mot de passe.</p>
<p>☒ <i>Confirmer mot de passe</i></p>	<p>Lorsque vous avez sélectionné <i>Créer jeton nouveau</i>, vous devez confirmer le nouveau mot de passe. Entrez à nouveau le mot de passe pour confirmation.</p>

Infineon Security Platform Solution - Assistant Initialisation

BitLocker

Cette page permet d'utiliser le Chiffrement de lecteur BitLocker en liaison avec Trusted Platform Module pour crypter les données sur votre disque.



Disponibilité de la page :

- Cette page n'est disponible que si le système d'exploitation accepte le chiffrement de lecteur BitLocker (par ex. pour Windows 7 et Windows Vista Enterprise ou Ultimate).
- Cette page est disponible seulement si l'état de BitLocker est *Configuré*, *Reconfiguration nécessaire*, *Chiffrage en cours* ou *Déchiffrage en cours*, et cette fonction est sélectionnée par l'utilisateur.
- Cette page n'est pas affichée lorsque l'état de BitLocker est "*Non configuré*" car la configuration de BitLocker pour la première fois nécessite un redémarrage du système. En échange, l'Applet du panneau de configuration BitLocker est lancé automatiquement après la fin de l'Assistant Initialisation.
- Cette page n'est pas disponible en [mode serveur](#).

Eléments de la page Assistant

La table suivante explique comment utiliser cette page de l'assistant.

<input type="checkbox"/> <i>Configurer</i>	En cliquant sur ce bouton, on démarre l'Applet du panneau de configuration BitLocker de Microsoft.
--	--



©Infineon

Technologies AG

Infineon Security Platform Solution- Assistant Initialisation

Authentification étendue

Avec cette page vous pouvez activer l'authentification étendue pour tous les utilisateurs ou modifier la sélection des dispositifs d'authentification.



Disponibilité de la page :

- Cette page est disponible seulement dans le mode [autonome](#), si au moins un plugiciel d'authentification étendue est installé.
- Cette page n'est pas disponible dans le [mode serveur](#), car Trusted Computing Management Server gère la configuration de l'Authentification étendue par la stratégie serveur, donc l'administrateur ne doit pas exécuter cette tâche.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<input type="checkbox"/> Liste de dispositifs d'authentification	<p>Cochez le(s) dispositif(s) d'authentification qui vous désirez activer pour tous les utilisateurs de la Security Platform.</p> <p>Une fois un dispositif d'authentification activé, les utilisateurs peuvent le sélectionner pour authentification.</p> <p> • Lorsque vous désirez vérifier si les utilisateurs de la Security Platform utilisent vraiment l'authentification étendue, vous devez activer la stratégie utilisateur Application de l'authentification étendue.</p> <p>• Dans le mode autonome, si la stratégie Fournisseurs d'authentification étendue est configurée, seulement les fournisseurs dans la liste des fournisseurs d'authentification étendue permis sont disponibles pour configuration ; cette liste est fournie par la stratégie. Si la stratégie n'est pas configurée, tous les fournisseurs d'authentification étendue enregistrés seront disponibles pour</p>

configuration.



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Initialisation utilisateur

Assistant Initialisation de l'utilisateur d'Infineon Security Platform

L'Assistant d'Initialisation d'Infineon Security Platform est destiné pour les utilisateurs experts à initialiser les Utilisateurs de la Security Platform et à configurer les fonctions spécifiques à l'utilisateur (Messagerie électronique sécurisé, chiffrement de fichier et dossier avec EFS et PSD, Authentification Renforcée). Cet assistant doit être lancé pour chaque utilisateur de PC qui a l'intention d'utiliser les Fonctions personnalisées d'Infineon Security Platform (c'est-à-dire qui sera l'Utilisateur de la Security Platform).

Si vous souhaitez initialiser rapidement votre Utilisateur de la Security Platform avec les paramètres par défaut, il vous est recommandé d'utiliser à la place [l'Assistant d'Initialisation Rapide](#).



Disponibilité de l'assistant :

- Cet assistant n'est disponible que si la stratégie *Autorisation de l'enregistrement des utilisateurs* est activée avec l'option *Autorisation de l'interface et de l'assistant du fournisseur de services de gestion* ou si cette stratégie n'est pas configurée (les mêmes conditions s'appliquent si vous lancez cet assistant à partir de [l'Icône de notification de la barre des tâches](#)). Cette stratégie s'applique seulement pour les utilisateurs non initialisés encore.
- Si un utilisateur a été initialisé auparavant, la stratégie n'est pas appliquée et cet assistant peut être utilisé pour configurer les fonctions spécifiques pour l'utilisateur (les mêmes conditions s'appliquent si vous lancez cet assistant à partir de [l'Icône de notification de la barre des tâches](#)).
- Cet assistant est disponible en [mode serveur](#) seulement si l'utilisateur actuel est membre du groupe d'inscription utilisateurs.

Etapes de l'assistant

La table suivante présente les étapes de l'assistant pour un utilisateur non encore initialisé. Pour un utilisateur déjà initialisé sont exécutées seulement les étapes exigées pour une tâche spéciale de l'assistant (par exemple la configuration des fonctions de la Security Platform spécifique à l'utilisateur).

Etape	Comment
1. Dispositif d'authentification	<p>Seulement si l'administrateur de la Security Platform a activé au moins un dispositif d'authentification. Seulement si l'utilisateur de la Security Platform n'est pas encore initialisé. Autrement cette page est disponible via Fonctions de la Security Platform.</p> <p> Si vous avez déjà configuré l'authentification étendue, mais votre dispositif d'authentification et votre Security Platform ont Phrases de passe utilisateur de base, vous devrez synchroniser votre phrase de passe utilisateur de base.</p>
2. Mot de passe utilisateur de base	Seulement si l'utilisateur de la Security Platform n'est pas encore initialisé.
3. Réinitialisation mot de passe utilisateur de base	Seulement si l'administrateur de la Security Platform a configuré la fonction Réinitialisation mot de passe.
4. Fonctions de la Security Platform	Messagerie sécurisée, cryptage de fichiers et de dossiers avec l'EFS et PSD, authentification étendue
5. Demande d'un certificat	Seulement si l'option <i>messagerie sécurisée</i> ou <i>cryptage de fichiers et de dossiers</i> (EFS ou PSD) a été sélectionnée.
6. Configuration messagerie sécurisée	Seulement si l'option <i>messagerie sécurisée</i> a été sélectionnée.

7. Certificat de cryptage	Seulement si l'option <i>cryptage de fichiers et de dossiers</i> (EFS ou PSD) a été sélectionnée.
8. Personal Secure Drive	Seulement si l'option <i>cryptage de fichiers et de dossiers avec Personal Secure Drive</i> a été sélectionnée.

Démarrage de l'application

Lorsque l'utilisateur actuel n'est pas encore initialisé : Depuis [l'Icône de Notification de la Barre d'Outils](#), cliquez sur l'élément de menu **Initialisation d'Utilisateur de la Security Platform**. [L'Assistant d'Initialisation Rapide](#) est lancé. Sur la page d'Accueil, sélectionnez **l'Initialisation Avancée**. L'Assistant d'Initialisation de Security Platform est lancé.

Lorsque l'utilisateur actuel est déjà initialisé : Démarrez l'assistant d'initialisation de l'utilisateur via l'outil de paramétrage.

- Pour configurer les fonctions personnalisées d'Infineon Security Platform (messagerie sécurisée, cryptage de fichiers et de dossiers avec l'EFS et PSD, authentification étendue) : [Outil de paramétrage - Paramètres utilisateur - Configuration...](#)
- Pour activer la fonction Réinitialisation mot de passe pour l'utilisateur actuel : [Outil de paramétrage - Réinitialisation mot de passe - Activation...](#)
- Pour créer un dispositif d'authentification de sauvegarde : [Outil de paramétrage - Sauvegarde - Créer...](#)

Description du paramètre ligne de commande : Vous pouvez démarrer l'assistant également via Windows Explorer en double cliquant sur le fichier *SpUserWz.exe* dans le répertoire d'installation de la solution Security Platform. Le paramètre ligne de commande suivant est pris en charge :

Paramètre	Comment
-forceinit ou /forceinit	<p>Forcer la réinitialisation d'un utilisateur.</p> <p> Toutes les informations d'identification existantes pour l'utilisateur sont perdues. Utilisez ce paramètre de la ligne de commande seulement si aucune sauvegarde de secours n'est pas disponible.</p> <p> Ce paramètre de ligne de commande n'est pas supporté dans le mode serveur car :</p>

- L'utilisateur n'a pas besoin d'utiliser ce paramètre.
- Un utilisateur dans un environnement Trust Domain ne devrait pas l'utiliser.



Infineon Security Platform Solution - Assistant Initialisation utilisateur

Dispositif d'authentification

Cette page vous permet de sélectionner un dispositif d'authentification.



Disponibilité de la page : Cette fonction est disponible seulement si votre administrateur a activé au moins un dispositif d'authentification.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<input type="checkbox"/> Liste de dispositifs d'authentification	<p>Sélectionnez le dispositif d'authentification à utiliser. Lorsque la stratégie Application de l'authentification étendue par les mots de passe utilisateur de base n'est pas activée, vous pouvez sélectionner également <i>Mot de passe</i>. Ca vaut dire que vous n'utilisez aucun dispositif d'authentification.</p> <p> Vous ne pouvez pas modifier votre sélection d'un dispositif d'authentification à un autre. Si vous le désirez, modifiez d'abord le <i>Mot de passe</i>. Si vous lancez à nouveau l'assistant, vous pourrez modifier le dispositif d'authentification.</p>



Infineon Security Platform Solution - Assistant Initialisation de l'utilisateur

Synchronisation phrase de passe utilisateur de base

Dans cette page vous pouvez indiquer la modalité de synchronisation de votre phrase de passe utilisateur de base, lorsque votre dispositif d'authentification et votre Security Platform ont des phrases de passe utilisateur de base.



Disponibilité de la page : Cette page est affichée seulement lorsque les conditions suivantes sont remplies :

- Vous avez configuré l'authentification étendue.
- Votre dispositif d'authentification et votre Security Platform ont des phrases de passe utilisateur de base différentes.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément page assistant	Explication
<i>Utilisation de la phrase de passe de Security Platform, mise à jour du dispositif d'authentification</i> -	Sélectionnez cette option lorsque votre dispositif d'authentification sera mise à jour avec la phrase de passe utilisateur de base utilisée actuellement par votre Security Platform. Nécessaire si vous avez réinitialisé votre phrase de passe utilisateur de base sans mettre à jour votre dispositif d'authentification.
<i>Utilisation phrase de passe depuis le dispositif d'authentification, mise à jour Security Platform</i> -	Sélectionnez cette option si votre Security Platform doit être mise à jour avec la phrase de passe utilisateur de base utilisée actuellement par votre dispositif d'authentification. Nécessaire si vous utilisez votre dispositif d'authentification sur plusieurs Security Platforms et vous avez modifié votre phrase de passe utilisateur de base sur un autre Security Platform.



Infineon Security Platform Solution - Assistant Initialisation utilisateur

Réinitialisation du mot de passe utilisateur de base

Dans cette page vous pouvez réinitialiser votre mot de passe utilisateur de base en cas d'urgence (par exemple vous avez oublié votre mot de passe actuel utilisateur de base).



Disponibilité de la page : Cette page est seulement disponible lorsque votre administrateur a configuré la Réinitialisation du mot de passe.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<input checked="" type="checkbox"/> <i>Activation de la réinitialisation de mon mot de passe utilisateur de base en cas d'urgence</i>	Cochez cette case pour vous assurer que votre mot de passe utilisateur de base peut être réinitialisé en cas d'urgence.  Vous ne pouvez pas décocher cette case lorsque vous avez déjà activée la réinitialisation du mot de passe ou si la stratégie Application de l'activation de la réinitialisation mot de passe est activée.
<input type="checkbox"/> <i>Secret personnel</i> <input type="checkbox"/> <i>Parcourir...</i>	Un secret personnel sera enregistré dans un fichier. Entrez le chemin et le nom du fichier ou naviguez jusqu'au fichier.  Gardez le fichier dans un emplacement sûr. Vous en avez besoin pour réinitialiser votre mot de passe en cas d'urgence.



Infineon Security Platform Solution - Assistant Initialisation utilisateur

Confirmer vos paramètres (étape 1)

Votre administrateur système peut activer une fonction permettant la récupération de votre clé utilisateur de base. Dans ce cas, les entrées supplémentaires seront créées dans la sauvegarde de secours existante.

Remarque : La clé utilisateur de base est toujours gérée dans un format protégé, même au cours du processus de récupération.

Le système est désormais prêt à générer votre clé utilisateur de base. Dans le cas où la fonction de récupération d'urgence est activée, un fichier de données de récupération d'urgence supplémentaire peut être créé. Il contiendra les informations nécessaires à une récupération en toute sécurité de votre clé.

Lorsque vous cliquez sur le bouton **Suivant**, votre clé utilisateur de base est générée.

Remarque :

En aucun cas, vous ne devez vous déconnecter, arrêter le système ou débrancher l'alimentation lorsque l'opération est en cours.



©Infineon

Technologies AG

Infineon Security Platform Solution - Assistant Initialisation de l'utilisateur

Fonctionnalités de Security Platform

Avec cette page vous pouvez configurer les fonctions de la Security Platform, par exemple le cryptage de fichiers et dossiers.



Disponibilité de la page : Cette page est disponible seulement si vos stratégies utilisateur permettent la configuration d'au moins une fonction.
Disponibilité des fonctions : Fonction de vos [paramètres stratégie utilisateur](#).

La table suivante explique toutes les fonctions de la Security Platform.

Fonction	Explication
<input checked="" type="checkbox"/> <i>Messagerie électronique sécurisée</i>	<p>Opérations de cryptage et/ou de signature, spécifiques à l'utilisateur, pour éviter la lecture ou la modification de vos messages par des personnes non autorisées. L'utilisation de cette fonction garantit que seul le créateur du message e-mail et les destinataires spécifiés seront autorisés à décrypter et à lire le message ou à valider l'identité de l'émetteur.</p> <p>Lorsque vous choisissez de configurer cette fonction, vous pouvez exiger un certificat pour la messagerie sécurisée (si l'adresse web de demande de certificat est configuré dans vos paramètres stratégie). L'assistant fournit l'information Comment configurer le courrier électronique sécurisé. La configuration de votre client de messagerie ne fait pas partie de cet assistant. Par conséquent, l'état ne peut pas être affiché ici.</p>
<input checked="" type="checkbox"/> <i>Chiffrement de Fichier et dossier - Certificat de Chiffrement</i>	<p>Sélectionnez cette caractéristique, si vous souhaitez visualiser ou changer votre Certificat de Chiffrement. Si vous choisissez de configurer cette caractéristique, vous pouvez sélectionner un certificat. Vous pouvez également demander ou créer un nouveau certificat.</p> <p> <i>Certificat de Chiffrement</i> est seulement affiché en tant que caractéristique d'utilisateur séparée, si EFS ou PSD sont déjà configurés. La page du Certificat de Chiffrement est également affichée pendant la première configuration de EFS</p>

	ou PSD.
<input checked="" type="checkbox"/> <i>Chiffrement de Fichier et de dossier - Système de Fichier chiffré (EFS)</i>	<p>Le système d'exploitation comporte une fonctionnalité permettant de procéder à un cryptage spécifique à l'utilisateur du contenu des dossiers et fichiers sur l'ordinateur local, à l'aide du Système de fichiers de cryptage Microsoft (EFS). Seul l'utilisateur ayant créé un fichier dans ces dossiers peut accéder au contenu de ce fichier. Les autres utilisateurs doivent obtenir des droits d'accès à un dossier EFS, au cours d'une opération d'administration explicite, pour pouvoir utiliser les fichiers qu'il contient.</p> <p> EFS n'est pas pris en charge dans les éditions familiales de Windows.</p>
<input checked="" type="checkbox"/> <i>Chiffrement de fichier et de dossier - Personal Secure Drive (PSD)</i>	<p>Personal Secure Drive présente un cryptage de fichiers et dossiers similaire à l'EFS. Contrairement à EFS, PSD est reconnu sur tous les systèmes d'exploitation pris en charge par Security Platform Solution.</p> <p>Une unité logique est fournie pour les utilisateurs habilités. Cette unité dispose d'une protection contre les accès non autorisés et d'un cryptage pour l'ensemble du contenu. Le cryptage est effectué automatiquement. L'accès à l'unité PSD pour l'obtention de données lisibles ne peut pas se faire par l'intermédiaire de son identificateur UNC. L'accès réseau est impossible.</p> <p>Si vous choisissez de configurer cette fonction, vous pouvez gérer vos Personal Secure Drives.</p>
<input checked="" type="checkbox"/> <i>Authentification Renforcée</i>	<p>Sélectionnez cette fonction lorsque vous désirez visualiser ou modifier vos paramètres d'authentification. Si vos stratégies le permettent, vous pouvez sélectionner un dispositif d'authentification ou l'authentification mot de passe.</p> <p> Cette fonction est disponible seulement si votre administrateur a activé au moins un dispositif d'authentification. Cette fonction n'est pas disponible lorsque la Security Platform n'a pas été initialisée avant le démarrage</p>

de l'assistant.

Reconfiguration de fonction : Dans quelques circonstances spéciales, vous devez reconfigurer une fonction. Exemples:

- Lorsque l'état de *Chiffrement de fichier et de dossier - Certificat de Chiffrement* est *Reconfiguration exigée*, vous devez d'abord résoudre ceci. Si le certificat de chiffrement n'est pas valide ou n'est plus disponible, vous pouvez créer un nouveau certificat de chiffrement ou restaurer les titres d'utilisateur. Ce certificat est ensuite automatiquement reverrouillé pour votre EFS et / ou PSD configuré.
- Si le certificat de chiffrement n'est pas disponible et vous n'avez pas de sauvegarde de titres d'utilisateur, vous devez créer un nouveau certificat de chiffrement. Ce nouveau certificat est ensuite automatiquement reverrouillé pour votre EFS configuré. Mais ce certificat ne peut pas être reverrouillé automatiquement pour votre PSD configuré, alors vous devez supprimer l'ancien PSD et créer un nouveau PSD avec le certificat de chiffrement.
- Votre certificat l'EFS ou le PSD est non valide ou ne plus disponible. C'est arrive dans le cas du *Chiffrement de Fichier et de dossier - Système de Fichier chiffré (EFS)*, si lorsque vous avez configuré l'EFS et également le PSD, et puis avez modifié des paramètres ultérieurement.
- Une restauration a été effectuée, mais votre PSD n'est plus disponible (par exemple, le fichier image de PSD n'est pas trouvé).
- Vous avez configuré *l'authentification étendue*, mais le dispositif d'authentification ne plus disponible ou votre dispositif d'authentification et votre Security Platform ont des phrases de passe utilisateur de base différentes.



Infineon Security Platform Solution - Assistant Initialisation utilisateur

Demande de certificat

Pour pouvoir exécuter les fonctions spécifiques à l'utilisateur d'Infineon Security Platform, un certificat doit être obtenu. Ces certificats permettent à l'utilisateur de prouver son identité par un moyen électronique. Ces certificats sont générés en-dehors du logiciel Infineon Security Platform et doivent être transférés dans le système à l'aide de mécanismes définis.



Disponibilité de la page : Cette page est disponible seulement lorsqu'au moins une fonction de sécurité a été sélectionnée et la stratégie d'inscription de certificats est activée ([URL à lancer à partir de l'assistant pour l'inscription de certificats](#)). Contactez votre administrateur pour plusieurs informations.

Élément de la page assistant	Explication
<input type="checkbox"/> <i>Demande de certificat...</i>	Dans les stratégies d'Infineon Security Platform, l'administrateur a établi la nécessité d'obtenir un certificat et il a indiqué la méthode pour l'obtenir. Cette fonction est activée en cliquant sur ce bouton. L'action de cliquer sur le bouton fait accéder l'utilisateur à une page indépendante de l'assistant pour inscrire le certificat. Cette page a été définie par l'administrateur. Une fois le processus d'inscription terminé, continuez avec les étapes suivantes de l'assistant.

[Comment inscrire des certificats](#)



Infineon Security Platform Solution - Assistant Initialisation utilisateur

Configuration de la messagerie électronique sécurisée

La sécurisation de la messagerie désigne les opérations de cryptage et/ou de signature, spécifiques à l'utilisateur, pour éviter la lecture ou la modification de vos messages par des personnes non autorisées. L'utilisation de cette fonction garantit que seul le créateur du message e-mail et les destinataires spécifiés seront autorisés à décrypter et à lire le message ou à valider l'identité de l'émetteur.

Le cryptage et la signature des messages sont pris en charge pour la plupart des applications de messagerie les plus courantes. Si la sécurisation de la messagerie doit être utilisée, l'aide disponible pour les clients de messagerie pris en charge est affichée et vous pouvez y obtenir des informations complémentaires.

Pour l'instant, les clients de messagerie pris en charge sont les suivants :

- Microsoft Windows Mail/Outlook Express
- Microsoft Outlook 2003
- Microsoft Outlook XP
- Microsoft Outlook 2000
- Mozilla Thunderbird

Le client de messagerie électronique doit être configuré pour utiliser le certificat numérique protégé par la Security Platform afin de bénéficier de la messagerie sécurisée. Contactez votre administrateur système pour qu'il envoie une demande de certificat à l'autorité de certification appropriée ou pour qu'il effectue une demande à l'aide d'une autorité de certification sur Internet.

Pour chacun des clients de messagerie énumérés, un guide de configuration et un guide d'utilisation détaillée sont accessibles par l'intermédiaire du bouton approprié.

Remarque : Si vous ne possédez pas encore de certificat numérique susceptible d'être utilisé pour la sécurisation de la messagerie, procurez-vous un tel certificat avant de continuer les étapes de configuration.

[Informations détaillées](#)



©Infineon

Technologies AG

Infineon Security Platform Solution - Assistant Initialisation de l'utilisateur

Certificat de cryptage

Cette page permet de sélectionner un certificat de chiffrement à utiliser pour [EFS](#) et/ou [PSD](#). Un tel certificat est identifié par son empreinte digitale et est toujours affecté à un Utilisateur d'Infineon Security Platform sous une forme certaine.

Si aucun certificat valide n'est enregistré actuellement, mais un autre certificat approprié est déjà disponible, l'assistant propose de sélectionner ce certificat automatiquement. Si un tel certificat n'est pas disponible, l'assistant propose de créer un nouveau certificat et de le sélectionner automatiquement.

Si vous ne souhaitez pas que l'assistant crée et/ou sélectionne automatiquement de certificat, vous pouvez également le faire manuellement.

La table suivante explique comment utiliser cette page de l'assistant.

Element de la page de l'assistant	Explication
 <i>Certificat actuel</i>	Vous trouvez ici des informations sur le certificat de chiffrement enregistré actuellement (si vous avez déjà sélectionné un certificat avant).
 <i>Nouveau certificat</i>	Vous trouvez ici des informations sur le certificat de chiffrement qui est utilisé à l'avenir (si un autre certificat que l'actuel doit être utilisé partout). Cela peut être soit un certificat qui est créé et/ou sélectionné automatiquement par l'assistant, ou un certificat que vous avez créé et/ou sélectionné manuellement via le bouton <i>Modifier...</i>
 <i>Modifier...</i>	Cliquez sur ce bouton pour la création et/ou la sélection manuelle d'un certificat de chiffrement. Le dialogue Sélection de certificat est affiché.  Reverrouillage pour données chiffrées existantes : Notez que votre ancien certificat de chiffrement est toujours exigé afin de déchiffrer vos données chiffrées existantes. Le processus de reverrouillage demandé pour utiliser le nouveau certificat également pour des données existantes

	<p>dépend de votre système d'opération :</p> <p>Sur les systèmes d'opération comprenant l'assistant de verrouillage Système de Chiffrement de Fichier Microsoft (par ex. Windows 7 et Windows Vista), vous devez effectuer le verrouillage manuellement. Sur tous les autres systèmes d'opération, vous devez utiliser l'outil de la ligne de commande "cipher.exe", ou accéder aux fichiers concernés afin de les verrouiller automatiquement.</p> <p>Plus d'informations sont disponibles dans le Microsoft TechNet (recherche après "assistant de verrouillage" ou "cipher.exe").</p>
 <i>Longueur de la clé pour les nouveaux certificats</i>	<p>Vous pouvez sélectionner ici la longueur de clé pour les certificats de chiffrement nouvellement créés, par ex. <i>1024 bits</i> ou <i>2048 bits</i>.</p>



Solution Infineon Security Platform - l'Assistant d'Initialisation Utilisateur

Configuration de votre Système de fichiers de cryptage (EFS)

Cette page de l'assistant vous permet de configurer un accès facile à vos données chiffrées EFS. Elle permet également de revenir à Microsoft EFS sans protection de Security Platform.

Le tableau suivant indique des astuces comment utiliser cette page de l'assistant.

Élément de Page de l'Assistant	Explication
<input checked="" type="checkbox"/> <i>Dossier EFS</i>	<p>Sélectionnez cette option de création d'un dossier chiffré <i>Documents\Données Chiffrés</i> ou <i>Mes Documents\Données Chiffrés</i> (en fonction de votre système d'opération).</p> <p> Cette option n'est pas toujours disponible (par exemple, si vous avez déjà créé le dossier EFS, ou en raison des paramètres desktop.ini ou du type de système de fichiers FAT32).</p>
<input checked="" type="checkbox"/> <i>Raccourci de bureau</i>	<p>Sélectionnez cette option si vous souhaitez accéder à votre <i>dossier EFS</i> via un raccourci de bureau.</p> <p> Si vous décochez la case une fois que vous avez créé le <i>Raccourci de bureau</i> avant, l'assistant supprime le raccourci existant (tant qu'il n'a pas été renommé ou déplacé entre-temps).</p>
<input type="checkbox"/> <i>Revenir...</i>	<p>Cliquez ici pour revenir à la fonction EFS par défaut (Microsoft EFS) sans protection Security Platform.</p> <p>Après le retour à Microsoft EFS, le chiffrement de fichier et de dossier fonctionne comme suit :</p> <ul style="list-style-type: none">• vous pouvez accéder à toutes les données chiffrées, tant que votre certificat EFS et la clé privée sont utilisables. Après le retour EFS, le premier accès à un fichier chiffré avec la Solution Security Platform exigé votre certificat EFS, votre clé privée et

l'[authentification d'utilisateur](#). Une fois que l'accès à un tel fichier a été mis en place, il est automatiquement chiffré de nouveau avec le nouveau certificat Microsoft EFS.

- Les nouveaux fichiers sont chiffrés avec Microsoft EFS y compris dans votre système d'opération (sans protection Security Platform).

Recommandation: [Déchiffrez](#) les fichiers EFS existants, si vous ne pouvez pas garantir que votre certificat EFS et la clé privée soient utilisables, tant que vous souhaitez accéder à ces fichiers.

 Ce bouton n'est disponible que si vous avez déjà configuré EFS avant et sélectionné encore une fois sa configuration.



©Infineon

Solution Infineon Security Platform

Personal Secure Drive

Les pages de l'assistant du Personal Secure Drive permettent de changer les paramètres d'un Personal Secure Drive existant, de supprimer un Personal Secure Drive existant ou de créer un nouveau Personal Secure Drive. La configuration de Personal Secure Drive fait partie de l' [Assistant Initialisation de l'Utilisateur](#). Les pages concernées sont affichées si vous avez sélectionné la fonctionnalité *Chiffrement de fichier et dossier avec Personal Secure Drive (PSD)*.

Etapes et Pages de l'Assistant

Le tableau suivant affiche les étapes et pages de l'assistant concernant Personal Secure Drive.

Action	Etapes / Pages de l'Assistant
Changement des paramètres d'un PSD existant	<ol style="list-style-type: none">1. Gestion de vos Personal Secure Drives2. Changement de vos paramètres de Personal Secure Drive
Suppression d'un PSD existant	<ol style="list-style-type: none">1. Gestion de vos Personal Secure Drives2. Suppression de votre Personal Secure Drive
Création d'un nouveau PSD	<ol style="list-style-type: none">1. Gestion de vos Personal Secure Drives (seulement si vous avez déjà au moins un PSD)2. Définition d'une lettre de lecteur et nom pour votre Personal Secure Drive3. Configuration de votre Personal Secure Drive



Solution Infineon Security Platform

Définition d'une lettre de lecteur et nom pour votre Personal Secure Drive

Cette page vous permet de configurer votre lettre et nom de lecteur de votre Personal Secure Drive, et les options pour charger le PSD lors de la connexion et pour utiliser un raccourci de bureau.

Le tableau suivant indique des astuces comment utiliser cette page de l'assistant.

Element de la page de l'assistant	Explication
 <i>Mon Personal Secure Drive sera affecté au lecteur</i>	Afin de définir la lettre de lecteur de votre Personal Secure Drive, sélectionnez une lettre non utilisée dans le menu déroulant de lettres disponibles (voir Administration de Personal Secure Drive).
 <i>Nom de lecteur pour mon Personal Secure Drive</i>	Afin de définir le nom du lecteur, entrez le nom dans le champ disponible. Le nom ne devrait pas excéder une longueur de 32 caractères. Vous pouvez, par exemple entrer le nom "Mon Lecteur Sécurisé".
<input checked="" type="checkbox"/> <i>Chargez mon Personal Secure Drive lors de la connexion</i>	Sélectionnez cette option si vous souhaitez charger votre PSD lors de la connexion.
<input checked="" type="checkbox"/> <i>Création de raccourci de bureau</i>	Sélectionnez cette option si vous souhaitez accéder à votre PSD via un raccourci de bureau. Ce nom de raccourci contient la lettre de lecteur et son nom.



Infineon Security Platform Solution

Configuration de votre Personal Secure Drive

Lorsque vous l'utilisez, le Personal Secure Drive ressemble et se comporte comme n'importe quel autre lecteur, mais il ne s'agit pas d'un lecteur matériel connecté à votre ordinateur : c'est un fichier crypté enregistré sur l'un des lecteurs locaux de votre ordinateur. A l'installation du Personal Secure Drive, vous devez indiquer sa taille et sur quel lecteur local il doit être enregistré.

Le tableau suivant indique des astuces comment utiliser cette page de l'assistant.

Éléments de Dialogue	Explication
<input type="checkbox"/> <i>Espace de stockage</i>	<p>Afin de définir une taille de lecteur, entrez le nombre de mégaoctets (Mo) de mémoire que vous nécessitez dans le champ fourni, ou utilisez les flèches en haut et en bas à droite du champ pour sélectionner la taille. Pour information, les lecteurs locaux avec un support amovibles (par ex. USB flash drive) sont également pris en charge.</p> <p>La taille demandée d'espace sur le disque est réservée sur ce lecteur local pour une utilisation exclusive par le Personal Secure Drive. Assurez-vous qu'il y ait assez d'espace disponible sur le lecteur local pour votre Personal Secure Drive.</p> <p> En mode serveur, il vous est recommandé de créer votre PSD sur un support amovible, si vous souhaitez l'utiliser sur plus d'une plateforme (voir Introduction à votre Personal Secure Drive). Dans ce cas, utilisez une lettre de lecteur disponible sur toutes les plateformes.</p>
<input type="checkbox"/> <i>Sélectionnez le lecteur où le fichier d'image PSD doit être enregistré</i>	<p>Sélectionnez un lecteur où le fichier d'image PSD doit être enregistré.</p> <p> La sélection du lecteur est désactivée si la politique Emplacement du Fichier pour Personal Secure Drive est configurée.</p>

Taille maximum PSD

La taille maximum autorisée pour votre Personal Secure Drive est ne peut plus être modifiée une fois l'installation terminée. Ainsi, vous devez vous assurer que la taille indiquée suffit à vos besoins.

Vous ne pouvez pas utiliser la taille maximale du lecteur, car le système de fichiers affecte de l'espace. Cela dépend du système d'exploitation et peut être significatif pour des petites dimensions des lecteurs. Le stockage de quelques données internes PSD réduit aussi légèrement la taille maximum PSD.

La taille maximale du lecteur PSD est également limitée :

- La taille maximale pour les lecteurs PSD sur les volumes FAT16 est 2 Go.
- La taille maximale pour les lecteurs PSD sur les volumes FAT32 est 4 Go.
- La taille maximale pour le lecteur PSD sur la partition système peut être limitée par la stratégie [*Espace disponible minimale après la création du PSD.*](#)



Solution Infineon Security Platform

Gestion de vos Personal Secure Drives

Cette page permet de changer les paramètres d'un Personal Secure Drive existant, de supprimer un Personal Secure Drive existant ou de créer un nouveau Personal Secure Drive. Cette page est affichée, si vous avez sélectionné la fonction *Chiffrement de fichier et de dossier avec Personal Secure Drive (PSD)* et si vous avez au moins un Personal Secure Drive. Vous devez exécuter l'assistant plusieurs fois afin de réaliser des actions différentes ou de créer plusieurs Personal Secure Drives.

Le tableau suivant indique des astuces comment utiliser cette page de l'assistant.

Élément de Page d'Assistant	Explication
<input type="checkbox"/> <i>Personal Secure Drive(s) existant(s)</i>	Cette liste affiche tous vos Personal Secure Drives et leurs états actuels. Vous pouvez mettre à jour la liste en cliquant sur la touche "F5". Si vous souhaitez changer les paramètres d'un Personal Secure Drive existant ou supprimer un Personal Secure Drive existant, sélectionnez le lecteur concerné.
<input checked="" type="radio"/> <i>Changez les paramètres du PSD sélectionné</i>	Sélectionnez cette option si vous souhaitez changer les paramètres du Personal Secure Drive sélectionné (par ex. la lettre de lecteur, le nom, et les options pour charger le PSD lors de la connexion et pour utiliser un raccourci de bureau). L'assistant continue avec la page Changement de vos Paramètres du Personal Secure Drive .
<input checked="" type="radio"/> <i>Supprimez le PSD sélectionné</i>	Sélectionnez cette option si vous souhaitez supprimer le Personal Secure Drive sélectionné. L'assistant continue avec la page Suppression de votre Personal Secure Drive .
<input checked="" type="radio"/> <i>Créez un nouveau PSD</i>	Sélectionnez cette option si vous souhaitez créer un nouveau Personal Secure Drive. L'assistant continue avec les pages pour la création d'un nouveau PSD .



TPM

©Infineon Technologies AG

Solution Infineon Security Platform

Changement de vos paramètres de Personal Secure Drive

Cette page vous permet de changer votre lettre et nom de lecteur de votre Personal Secure Drive, et les options pour charger le PSD lors de la connexion et pour utiliser un raccourci de bureau.

Le tableau suivant indique des astuces comment utiliser cette page de l'assistant.

Elément de Page d'Assistant	Explication
 <i>Mon Personal Secure Drive sera affecté au lecteur</i>	Afin de changer la lettre de lecteur de votre Personal Secure Drive, sélectionnez une lettre non utilisée dans le menu déroulant de lettres disponibles (voir Administration de Personal Secure Drive).
 <i>Nom de lecteur pour mon Personal Secure Drive</i>	Afin de changer le nom du lecteur, entrez un autre nom dans le champ disponible. Le nom ne devrait pas excéder une longueur de 32 caractères. Vous pouvez, par exemple entrer le nom "Mon Lecteur Sécurisé".
<input checked="" type="checkbox"/> <i>Chargez mon Personal Secure Drive lors de la connexion</i>	Sélectionnez cette option si vous souhaitez charger votre PSD lors de la connexion.
<input checked="" type="checkbox"/> <i>Raccourci de bureau</i>	Sélectionnez cette option si vous souhaitez accéder à votre PSD via un raccourci de bureau. Ce nom de raccourci contient la lettre de lecteur et son nom.  Si vous décochez la case une fois que vous avez créé le raccourci de bureau, l'assistant supprime le raccourci existant (tant qu'il n'a pas été renommé ou déplacé entre-temps).



Infineon Security Platform Solution

Suppression de votre Personal Secure Drive

Si vous choisissez de supprimer votre Personal Secure Drive, vous avez la possibilité de créer une copie non cryptée du lecteur entier avant qu'il soit supprimé définitivement.

Remarque : Si vous appuyez sur **Suivant**, vous allez supprimer *définitivement* votre Personal Secure Drive – vous *ne* serez pas en mesure de restaurer les données.

Pour créer une copie non cryptée de votre Personal Secure Drive avant de le supprimer, cliquez sur la case d'option *Je veux enregistrer une copie non cryptée du contenu de mon Personal Secure Drive avant de le supprimer définitivement*, puis indiquez un emplacement où les fichiers et les dossiers de votre Personal Secure Drive doivent être enregistrés dans un format non crypté.

Pour supprimer définitivement votre Personal Secure Drive sans créer de copie non cryptée, cliquez sur la case d'option *Je veux supprimer définitivement mon Personal Secure Drive sans enregistrer de copie non cryptée de son contenu*.



©Infineon

Technologies AG

Infineon Security Platform Solution - Assistant Migration

Assistant Migration d'Infineon Security Platform

L'assistant migration de l'Infineon Security Platform est utilisé pour transférer d'une manière sécurisée des clés et certificats spécifiques à l'utilisateur de l'Infineon Security Platform d'une Infineon Security Platform vers une autre.

Chaque cible de migration doit être autorisée par le propriétaire de l'Infineon Security Platform avant l'exécution de l'opération d'exportation. Ainsi vous disposez d'une méthode administrative pour suivre la distribution des utilisateurs d'Infineon Security Platform même dans les réseaux locaux à grande échelle.

L'opération de migration doit être exécutée par l'utilisateur de l'Infineon Security Platform et elle est formée de l'opération d'exportation sur l'Infineon Security Platform source et l'opération correspondante d'importation sur l'Infineon Security Platform cible sélectionnée. Une migration ne peut jamais être exécutée pour un autre compte que le compte de l'utilisateur connecté actuellement. Ainsi la fiabilité de l'Infineon Security Platform du point de vue de l'utilisateur est assurée.

Lorsque l'utilisateur connecté actuellement n'a pas la clé utilisateur de base ou l'Infineon Security Platform est désactivée (de façon permanente ou temporaire), aucune opération de migration n'est possible.



Disponibilité de l'assistant :

- Dans le mode [autonome](#), cet assistant est disponible seulement sur une Security Platform initialisée.
- Cette page n'est pas disponible en [mode serveur](#), car Trusted Computing Management Server gère la migration en conditions de sécurité des clés et certificats utilisateur depuis une Infineon Security Platform vers une autre plateforme.

Etapes de l'assistant

Pas	Comment
1. Importation ou exportation ?	Spécifiez lorsque vous désirez importer vos clés et certificats depuis une autre Security Platform ou les exporter vers une autre Security Platform.
2. Cible de l'exportation	Spécifiez l'ordinateur cible de la migration (seulement lorsque l'option <i>Exportation</i> a été sélectionnée).
3. Location du fichier d'importation ou Location du fichier d'exportation	Spécifiez le répertoire du fichier contenant les données de migration.
4. Entrée mot de passe ou authentification	Authentifiez-vous pour autoriser la migration.

Démarrage de l'application

Démarrez l'assistant Migration via l'outil de paramétrage : [Outil de paramétrage - Migration - Exportation...](#) ou [Outil de paramétrage - Migration - Importation...](#)

Lorsque vous désirez exporter vos clés et certificats, sélectionnez *Ce système est la plate-forme source*.

Lorsque vous désirez importer vos clés et certificats, sélectionnez *Ce système est la plate-forme cible*.



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Migration

Importation ou Exportation

L'opération de migration pour les clés utilisateur doit être définie. Spécifiez lorsque vous désirez importer vos clés et certificats depuis une autre Security Platform ou les exporter vers une autre Security Platform.



Cette page d'assistant n'est pas disponible dans le [mode serveur](#), car la migration est gérée par Trusted Computing Management Server.

Elément de la page assistant	Explication
<input checked="" type="radio"/> <i>Importer</i>	Les opérations suivantes vont importer des certificats et clés spécifiques à un utilisateur de l'Infineon Security Platform depuis un fichier de migration vers l'Infineon Security Platform locale. Le répertoire du fichier de migration doit être connue.
<input checked="" type="radio"/> <i>Exporter</i>	Les opérations suivantes vont créer un fichier de migration contenant les certificats et clés de l'utilisateur d'Infineon Security Platform connecté actuellement. L'Infineon Security Platform cible doit être connue et autorisée pour cette opération par le propriétaire Infineon Security Platform.



©Infineon

Infineon Security Platform Solution - Assistant Migration

Spécification de le répertoire du fichier d'importation

La sauvegarde de secours contenant vos clés et certificats, créée au cours de l'opération d'exportation, sera demandée ici.



Cette page d'assistant n'est pas disponible dans le [mode serveur](#), car la migration est gérée par Trusted Computing Management Server.

Élément de la page assistant	Explication
 <i>Emplacement sauvegarde données migration</i>  <i>Parcourir...</i>	Les données de migration seront lues d'un fichier. Entrez le chemin et le nom du fichier contenant les données de migration ou naviguez jusqu'au celui-ci.  Le fichier de migration est dans le format XML.



Infineon Security Platform Solution - Assistant Migration

Spécification de le répertoire du fichier d'exportation

Les clés et certificats à migrer sont stockés d'une manière sécurisée dans le fichier de sauvegarde des données de migration. Le fichier est nécessaire pour finaliser l'opération de migration et il peu être importé seulement sur un ordinateur autorisé par le propriétaire de la plate-forme.



Cette page d'assistant n'est pas disponible dans le [mode serveur](#), car la migration est gérée par Trusted Computing Management Server.

Elément de la page assistant	Explication
<input type="text" value="abc"/> <i>Location de la sauvegarde</i> <input type="button" value="Parcourir..."/>	Les données de migration seront enregistrées dans un fichier. Entrez le chemin et le nom du fichier contenant les données de migration ou naviguez jusqu'au celui-ci. Le fichier de migration est dans le format XML.



Infineon Security Platform Solution - Assistant Migration

Spécification de la destination de l'exportation

Chaque Infineon Security Platform prévue comme une destination valide pour une opération de migration doit être autorisée d'abord par le propriétaire Infineon Security Platform. Cette opération doit être exécutée sur chaque Infineon Security Platform d'un réseau.



Cette page d'assistant n'est pas disponible dans le [mode serveur](#), car la migration est gérée par Trusted Computing Management Server.

Élément de la page assistant	Explication
<input type="checkbox"/> <i>Sélection de votre Infineon Security Platform cible</i>	<p>La liste de sélection contient tous les systèmes Infineon Security Platform représentant des cibles valides pour les certificats et clés utilisateur de l'Infineon Security Platform locale. Sélectionnez une entrée de cette liste comme cible pour l'opération de migration actuelle.</p> <p> Lorsqu'aucune cible n'est pas disponible dans la liste, l'assistant Migration de l'Infineon Security Platform doit être arrêté en utilisant le bouton Annuler. Le propriétaire de l'Infineon Security Platform locale doit autoriser la migration depuis l'Infineon Security Platform locale via l'outil de paramétrage de l'Infineon Security Platform.</p>



©Infineon

Infineon Security Platform Solution - Assistant Sauvegarde

Assistant Sauvegarde d'Infineon Security Platform

L'Assistant Sauvegarde d'Infineon Security Platform permet d'exécuter les opérations de sauvegarde ou de restauration des [informations relatives à la Security Platform](#). Ces opérations servent à protéger les données de toute perte accidentelle en cas d'urgence.

Le fichier de sauvegarde contient des informations concernant l'identification de l'ordinateur ("Platform ID") et les informations d'identification de l'utilisateur ("User ID"). Ces informations sont utilisées pour faire la correspondance entre le nom de l'ordinateur et le nom de l'utilisateur avec l'ordinateur et l'utilisateur actuel au cours du processus de restauration.



Lorsque la Clé utilisateur de base est autre que la Clé utilisateur de base à restaurer, le procès de restauration remplacera les informations d'identification et les paramètres sur l'emplacement de destination. Par conséquent, il est recommandé de faire migrer les informations d'identification d'un utilisateur dans un nouveau compte utilisateur (sur le système de destination) pour lequel les étapes d'initialisation de l'utilisateur de Security Platform n'ont pas encore été exécutées.



Trusted Computing Management Server gère la sauvegarde et restauration en [mode serveur](#), donc aucune configuration explicite n'est nécessaire. Si Personal Secure Drive (PSD) a été configuré, vous pouvez manuellement sauvegarder et restaurer les fichiers d'image de Personal Secure Drive.



Cette icône bouclier est visible seulement pour les utilisateurs avec droits d'administration dans les systèmes d'exploitation avec [Contrôle des comptes utilisateurs](#) (par exemple Windows 7 et Windows Vista).

Etapes de l'assistant

Scénario	Etapes de l'assistant	Explication
Sauvegarde Manuelle	Configurer paramètres de sauvegarde	Étape exigée.
	Configurez les paramètres de sauvegarde PSD	Seulement si les Personal Secure Drives doivent être compris dans la sauvegarde.
Restauration	Configurer paramètres de restauration	Non exigé, si seuls les Personal Secure Drives doivent être restaurés.
	Confirmez l'ordinateur ou sélectionnez l'ordinateur	Seulement si votre ordinateur n'est pas indiqué dans les données de sauvegarde. Non exigé, si seuls les Personal Secure Drives doivent être restaurés.
	Sélection du jeton de récupération d'urgence	Seulement si vous avez les droits administratifs, et la sauvegarde comprend des données de Récupération d'Urgence, et les données de Récupération d'Urgence sont restaurées. Non exigé, si seuls les Personal Secure Drives doivent être restaurés.
	Confirmez l'utilisateur	Seulement si vous allez restaurer les titres et paramètres de votre compte d'utilisateur courant, et l'utilisateur dans les données de Sauvegarde est différent de l'utilisateur courant.

		Non exigé, si seuls les Personal Secure Drives doivent être restaurés.
	Sélectionnez les utilisateurs	Seulement si vous avez des droits administratifs, et vous allez préparer la restauration pour d'autres utilisateurs. Non exigé, si seuls les Personal Secure Drives doivent être restaurés.
	Configurez les paramètres de restauration PSD	Seulement si les Personal Secure Drives doivent être restaurés.

Notez que vous n'avez pas besoin d'utiliser l'Assistant de Sauvegarde afin d'effectuer une Sauvegarde de Système, car une tâche planifiée de sauvegarde configurée via Assistant Initialisation Security Platform ou Assistant Rapide Initialisation effectue automatiquement la Sauvegarde de Système.

Démarrage de l'application

Sauvegarde manuelle : Démarrez l'assistant Sauvegarde via l'outil de paramétrage : [Outil de paramétrage - Sauvegarde - Sauvegarde...](#)

Restauration manuelle : Démarrez l'assistant Sauvegarde via l'outil de paramétrage : [Outil de paramétrage - Sauvegarde - Restauration...](#)

Restauration incluant la récupération d'urgence (tâche d'administration) : Démarrez d'abord l'assistant initialisation de Security Platform. Cochez [Restaurer une Security Platform depuis une sauvegarde de récupération d'urgence](#) dans la page *initialisation ou restauration d'une Security Platform* de l'assistant.

Démarrer l'assistant depuis l'info-bulle ou la pictogramme Notification barre de tâches : Dans quelques états de Security Platform vous pouvez démarrer l'assistant Sauvegarde depuis une info-bulle ou depuis la [pictogramme Notification barre de tâches](#) (par ex. quand l'administrateur de Security Platform a préparé la restauration pour l'utilisateur actuel).



Infineon Security Platform Solution - Assistant Sauvegarde

Sauvegarde ou restauration

Choisissez une option pour soit sauvegarder, soit restaurer vos données.

Élément de la page assistant	Explication
<p> <i>Création d'une sauvegarde manuelle</i></p>	<p>Les opérations suivantes créeront une sauvegarde de secours de vos informations d'identification de l'Infineon Security Platform locale sur un support sûr, amovible de préférence, tel qu'un lecteur de disquette, un disque dur ou sur le serveur. Une procédure de récupération pourra être lancée en cas de perte de données. L'emplacement du fichier de sauvegarde devra être connu.</p> <p> En mode serveur, vous pouvez sauvegarder seulement votre Personal Secure Drive (PSD).</p>
<p> <i>Restaurer après une sauvegarde manuelle</i></p>	<p>Les opérations suivantes vont restaurer, sur l'Infineon Security Platform, les informations d'identification précédemment sauvegardées. L'utilisateur doit spécifier l'emplacement du fichier de sauvegarde pour lancer le processus de restauration.</p> <p> Dans le mode serveur vous pouvez seulement sauvegarder votre Personal Secure Drive (PSD).</p>
<p> <i>Restaurer après une sauvegarde système</i></p>	<p>Les opérations suivantes vont restaurer les données des pièces d'identification sauvegardées préalablement sur l'Infineon Security Platform. L'utilisateur doit indiquer l'emplacement du fichier de sauvegarde pour le processus de restauration. Vous pouvez aussi restaurer d'une archive écrite manuellement, si vous n'avez pas une Archive de sauvegarde système. En plus, on peut effectuer une Restauration Récupération d'urgence.</p> <p> <ul style="list-style-type: none">• Ce bouton n'est pas disponible si l'utilisateur n'a pas des droits</p>

d'administration.

- Ce bouton n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.



Solution Infineon Security Platform - Assistant Sauvegarde

Configurer les Paramètres de Sauvegarde

Cette page vous permet de déterminer l'Archive de Sauvegarde.



En [mode serveur](#), cette page n'est pas disponible, comme la sauvegarde est traitée par le Trusted Computing Management Server.

Le tableau suivant indique des conseils comment utiliser cette page d'assistant.

Élément de Page d'Assistant	Explication
 <i>Emplacement de Sauvegarde</i> <input type="text"/> <i>Parcourez...</i>	Votre Security Platform Les informations d'identification et paramètres sont enregistrés dans une Archive de Sauvegarde Entrez le chemin et le nom du fichier ou parcourez.  Le fichier de sauvegarde est un fichier en format XML.



Solution Infineon Security Platform - Assistant Sauvegarde

Configuration des Paramètres de Sauvegarde du Personal Secure Drive

Cette page vous permet de sauvegarder les fichiers d'image du Personal Secure Drive. Vos paramètres PSD sont toujours pris en compte lors de la sauvegarde, si vous avez configuré un PSD, cependant les fichiers d'image doivent expressément être sélectionnés pour être pris en compte pendant la sauvegarde.

Le tableau suivant indique des astuces comment utiliser cette page de l'assistant.

Élément de Page d'Assistant	Explication
<p> <i>Destination de sauvegarde par défaut du Personal Secure Drive</i> <input type="checkbox"/> <i>Browse...</i></p>	<p>Si vous souhaitez sauvegarder un ou plusieurs fichiers d'image de Personal Secure Drive, spécifiez le chemin cible par défaut pour la sauvegarde des fichiers d'image. Si vous souhaitez sauvegarder plusieurs fichiers d'image à de différents emplacements, utilisez alors le bouton <i>Changer...</i> afin de configurer les chemins individuellement.</p> <p>Si vous ne souhaitez pas sauvegarder du tout un Personal Secure Drive, vous pouvez ignorer la sélection d'emplacement.</p>
<p><input type="checkbox"/> <i>Sélectionnez les Personal Secure Drives à inclure dans la sauvegarde</i></p>	<p>Cette liste affiche tous vos Personal Secure Drives configurés sur votre plateforme. Sélectionnez les lecteurs à inclure dans la sauvegarde. Assurez-vous qu'un fichier d'image de sauvegarde valide soit défini pour chaque lecteur sélectionné, et qu'il y ait assez d'espace disponible dans le dossier cible.</p> <p>Si vous ne souhaitez pas sauvegarder du tout un fichier d'image de Personal Secure Drive, assurez-vous qu'aucun Personal Secure Drive soit vérifié.</p> <p>Menu contextuel : Cliquez avec le bouton droit de la souris sur la liste pour afficher un menu contextuel avec toutes les actions prises en charges.</p>

 *Changer...*

Cliquez sur ce bouton afin de changer l'emplacement de sauvegarde et/ou le nom du fichier d'image de sauvegarde.

Un dialogue s'affiche. Effectuez vos modifications et fermez de nouveau le dialogue.

 Ne changez pas l'extension *.fsb du fichier d'image de sauvegarde.



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Sauvegarde

Configuration des paramètres de restauration

Vous pouvez spécifier à l'aide de cette page la sauvegarde de récupération d'urgence source de la restauration. Lorsque vous avez des droits d'administrateur, vous pouvez spécifier également un motif de la restauration.



Disponibilité de la page : Cette page n'est pas disponible en [mode serveur](#), car Trusted Computing Management Server gère la sauvegarde et restauration, donc aucune configuration explicite n'est nécessaire.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<ul style="list-style-type: none">⦿ <i>Disc dur brisé ou données perdues</i>⦿ <i>Trusted Platform Module nouveau</i>⦿ <i>Security Platform nouvelle à initialiser</i>	<p>Fonction de l'état Security Platform, un des motifs de restaurations suivants est sélectionné :</p> <ul style="list-style-type: none">• <i>Disque dur brisé ou données perdues</i> : La Security Platform a un propriétaire. Cet état survient d'habitude lorsque la solution Security Platform est initialisée et prête à utiliser, mais quelques données utilisateur ne sont plus disponibles.• <i>Trusted Platform Module nouveau</i> : La Security Platform n'a pas un propriétaire, mais les paramètres ou informations d'identification anciennes de Security Platform existent. Cet état survient d'habitude lorsque le logiciel de la solution Security Platform a été installé auparavant et ensuite le Trusted Platform Module a été remplacé ou réinitialisé dans la BIOS.• <i>Security Platform nouvelle à initialiser</i> : La Security Platform n'a pas un propriétaire. Aucun paramètre ou informations d'identification anciennes de Security Platform n'ont pas été trouvées.

	<p>Cet état survient d'habitude lorsque vous allez effectuer la restauration sur un ordinateur sur lequel le logiciel de la solution Security Platform n'a pas été installé auparavant.</p> <p>Vous ne pouvez pas modifier cette sélection.</p> <p> Le motif de la restauration est affiché seulement pour les utilisateurs aux droits d'administration.</p>
<p> <i>Spécifier le chemin et nom du fichier pour la sauvegarde de récupération d'urgence à restaurer</i></p> <p><input type="text"/> <i>Parcourir...</i></p>	<p>Vous devez spécifier la sauvegarde de récupération d'urgence source de la restauration. Entrez le chemin et le nom du fichier ou naviguez jusqu'au fichier.</p> <p> Le fichier de sauvegarde est dans le format XML.</p>



Solution Infineon Security Platform - Assistant Sauvegarde

Configuration des Paramètres de Restauration du Personal Secure Drive

Cette page permet de restaurer des Personal Secure Drives. Vous pouvez soit utiliser la sauvegarde d'un fichier d'image PSD pour un PSD déjà configuré, ou pouvez créer un nouveau PSD pour utiliser ce fichier d'image restauré.

Le tableau suivant indique des astuces comment utiliser cette page de l'assistant.

Elément de Page de l'Assistant	Explication
<p> <i>Emplacement de sauvegarde par défaut du Personal Secure Drive</i></p> <p> <i>Parcourir...</i></p>	<p>Si vous souhaitez restaurer un ou plusieurs Personal Secure Drive, alors définissez le chemin par défaut des sauvegardes de fichiers d'image PSD à restaurer. Ce chemin est considéré comme chemin de restauration par défaut pour tous les fichiers d'image PSD. Si vous souhaitez restaurer plusieurs fichiers d'image depuis différents emplacements, utilisez alors le bouton <i>Changer...</i> afin de configurer les chemins individuellement.</p> <p>Si vous ne souhaitez pas restaurer du tout un Personal Secure Drive, vous pouvez ignorer la sélection de chemin.</p>
<p><input type="checkbox"/> <i>Sélectionnez les Personal Secure Drives à restaurer</i></p>	<p>Cette liste affiche tous vos Personal Secure Drives configurés sur votre plateforme. Sélectionnez les lecteurs à restaurer, et assurez-vous qu'une sauvegarde de fichier d'image valide soit définie pour chaque lecteur sélectionné.</p> <p>Cette liste peut comprendre des lecteurs avec des statuts différents :</p> <ul style="list-style-type: none">• Personal Secure Drives qui sont complètement fonctionnels (c'est-à-dire les paramètres PSD et le fichier d'image sont disponibles). Vous souhaitez restaurer un lecteur complètement fonctionnel par exemple, si vous avez supprimé quelques fichiers

dans votre PSD par erreur, et la sauvegarde de fichier d'image comprend ces fichiers. Il est à noter que vos données PSD actuelles sont complètement écrasées dans ce cas.

- Personal Secure Drives avec le fichier d'image manquant (par exemple si vous avez seulement restauré les paramètres PSD depuis une Archive de Sauvegarde, mais le fichier d'image est toujours à restaurer). Dans ce cas, vous devez restaurer cette sauvegarde de fichier d'image avant que vous ne puissiez accéder à vos données PSD.
- Personal Secure Drives pour lesquels aucune clé n'est disponible. Dans ce cas, vous pouvez restaurer une sauvegarde de fichier d'image utilisant la clé prévue. Considérez la restauration d'informations d'identification et des paramètres d'abord, ensuite vous ne devrez plus restaurer le fichier image.

Si vous ne souhaitez pas restaurer du tout un Personal Secure Drive, assurez-vous qu'aucun Personal Secure Drive ne soit vérifié.

Menu contextuel : Cliquez avec le bouton droit de la souris sur la liste pour afficher un menu contextuel avec les actions prises en charge.

Ajouter...

Cliquez sur ce bouton pour ajouter un autre Personal Secure Drive à la liste des lecteurs. Cette façon pour restaurer un Personal Secure Drive depuis une sauvegarde de fichier d'image, sans avoir une sauvegarde des paramètres correspondants. Une boîte de [dialogue](#) sera affichée vous permettant de configurer tous les paramètres concernés de PSD.

Changer...

Cliquez sur ce bouton afin d'initialiser ou de changer les paramètres de restauration du Personal Secure Drive sélectionné.

Vous devez le faire par exemple dans les cas suivants :

- Aucune sauvegarde de fichier d'image appropriée n'a pu être trouvé sur l'emplacement de sauvegarde PSD par défaut.
- Une sauvegarde de fichier d'image appropriée a pu être trouvé sur l'emplacement de sauvegarde PSD par défaut, mais vous souhaitez sélectionner une autre sauvegarde valide du fichier d'image.
- L'état local du PSD sélectionné exige que la destination du fichier d'image ou de la lettre de lecteur soit changée.

Une boîte de [dialogue](#) sera affichée vous permettant de configurer tous les paramètres concernés de PSD.



Infineon Security Platform Solution - Assistant de Sauvegarde

Changer les Paramètres de Restauration / Ajouter Personal Secure Drive

Avec cette boîte de dialogue vous pouvez initialiser ou changer les paramètres de restauration pour un Personal Secure Drive, ou ajouter un autre Personal Secure Drive qui doit être restauré. En fonction de l'action à effectuer, uniquement les contrôles exigés sont activés.

Le tableau suivant indique des conseils sur la manière d'utilisation de cette boîte de dialogue :

Elément Page Assistant	Explication	Changer	Ajouter
<input type="text"/> <i>Chemin de Sauvegarde du fichier d'image</i> <input type="button" value="Parcourir..."/>	Déterminez le chemin de la sauvegarde du fichier d'image à être restauré.	Doit être initialisé si aucune sauvegarde de fichier d'image appropriée n'a pu être trouvée dans l'emplacement de la sauvegarde PSD par défaut. Sinon, le chemin peut être modifié.	Doit être initialisé
<input type="checkbox"/> <i>Lecteur de destination du fichier d'image</i>	Sélectionnez un lecteur où le fichier d'image PSC doit être restauré.	Doit être initialisé s'il n'est pas possible de restaurer la sauvegarde du fichier d'image vers le lecteur de destination stocké dans les paramètres locaux. Sinon le lecteur	Doit être initialisé

		de destination ne peut pas être modifié.	
 <i>Lettre de lecteur</i>	Afin de déterminer la lettre de lecteur pour votre Personal Secure Drive, sélectionnez une lettre non utilisée depuis la liste déroulante des lettres disponibles (voir Administration de Personal Secure Drive).	Doit être initialisé s'il n'est pas possible d'utiliser la lettre de lecteur stockée dans les paramètres locaux. Sinon la lettre de lecteur ne peut pas être modifié.	Doit être initialisé
 <i>Étiquette de lecteur</i>	Afin de déterminer l'étiquette de lecteur, entrez l'étiquette dans le champ donné. L'étiquette ne devrait pas avoir plus de 32 caractères en longueur. Par exemple, vous pourriez initialiser l'étiquette à "Mon Secure Drive".	Ne peut pas être modifié	Doit être initialisé
<input checked="" type="checkbox"/> <i>Chargement à l'ouverture</i>	Sélectionnez cette option si vous souhaitez charger votre PSD lors de l'ouverture.	Ne peut pas être modifié	Optionnel
<input checked="" type="checkbox"/> <i>Créer un raccourci de bureau</i>	Sélectionnez cette option si vous souhaitez accéder à votre PSC via un raccourci de bureau. Le nom du raccourci contiendra la lettre du lecteur et l'étiquette.	Ne peut pas être modifié	Optionnel



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Sauvegarde

Confirmation de l'ordinateur

Cette page vous invite à confirmer que l'ordinateur des Données de sauvegarde spécifiées doit être récupéré sur votre ordinateur.



Disponibilité de la page :

- Cette page est affichée seulement si les Données de sauvegarde contiennent des données pour un autre ordinateur que le vôtre.
- Cette page n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<i>Votre ordinateur : Nom de l'ordinateur / ID plate-forme</i>	<p>Le nom de l'ordinateur et l'ID de la plate-forme pour votre ordinateur sont affichés.</p> <p> Le nom de l'ordinateur peut être modifié depuis la sauvegarde, car il peut être renommé. L'ID de la plate-forme est donc affichée également.</p>
<i>Ordinateur dans les données de sauvegarde : Nom de l'ordinateur / ID plate-forme</i>	<p>Le nom de l'ordinateur et l'ID de la plate-forme sont affichés pour l'ordinateur sur lequel la sauvegarde a été effectuée.</p>



©Infineon

Infineon Security Platform Solution - Assistant Sauvegarde

Sélection de l'ordinateur

Vous pouvez sélectionner à l'aide de cette page l'ordinateur à restaurer.



Disponibilité de la page :

- Cette page est affichée seulement si les Données de sauvegarde contiennent des données pour plusieurs ordinateurs, mais pas pour le vôtre.
- Cette page n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
 <i>Votre ordinateur : Nom de l'ordinateur / ID plate-forme</i>	Le nom de l'ordinateur et l'ID de la plate-forme pour votre ordinateur sont affichés.  Le nom de l'ordinateur peut être modifié depuis la sauvegarde, car il peut être renommé. L'ID de la plate-forme est donc affichée également.
 <i>Ordinateur dans les données de sauvegarde : Nom de l'ordinateur / ID plate-forme</i>	Le nom de l'ordinateur et l'ID de la plate-forme sont affichés pour les ordinateurs sur lesquels les sauvegardes ont été effectuées. Sélectionnez un tel ordinateur pour être restauré.



Infineon Security Platform Solution - Assistant Sauvegarde

Sélection du jeton de récupération d'urgence

Lorsque le processus de restauration inclus la récupération d'urgence, vous devez spécifier un jeton de récupération d'urgence. Vous pouvez spécifier ce jeton à l'aide de cette page.

Les données de récupération d'urgence dans une archive peuvent être utilisées seulement en combinaison avec un jeton de récupération protégé avec un mot de passe dédié. Ce jeton a été écrit dans un fichier lorsque l'administrateur de Security Platform a configuré les données de récupération d'urgence pour tous les utilisateurs.



Disponibilité de la page :

- Cette page est affichée seulement si l'administrateur de Security Platform va restaurer les informations d'identification et configuration de la plateforme en utilisant une sauvegarde de secours créée automatiquement.
- Cette page est affichée seulement si une Récupération d'urgence est exigée (c'est-à-dire le motif de la restauration est *Trusted Platform Module nouveau* ou *Security Platform nouvelle à initialiser*).
- Cette page n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
 <i>Location du jeton de récupération d'urgence</i> <input type="text"/> <i>Parcourir...</i>	Entrez le chemin et le nom du fichier ou naviguez jusqu'au fichier.  Le fichier est en format XML.
 <i>Mot de passe</i>	Entrez le mot de passe protégeant le jeton de récupération d'urgence.



Infineon Security Platform Solution - Assistant Sauvegarde

Confirmation de l'utilisateur

Cette page vous invite à confirmer que l'utilisateur des Données de sauvegarde spécifiées doit être récupéré pour le compte utilisateur actuel.



Disponibilité de la page :

- Cette page est affichée pour un utilisateur qui n'a pas des droits d'administration, si les Données de sauvegarde spécifiées contiennent des données pour un autre utilisateur que le compte utilisateur actuel.
- Cette page n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
 <i>Votre compte utilisateur : Nom utilisateur / ID utilisateur</i>	Le nom d'utilisateur et l'ID utilisateur pour le compte utilisateur actuel sont affichés.  Le nom d'utilisateur peut être modifié depuis la sauvegarde, car il peut être renommé. L'ID de l'utilisateur est donc affiché également.
 <i>Utilisateur dans les données de sauvegarde : Nom utilisateur / ID utilisateur</i>	Le nom d'utilisateur et l'ID utilisateur sont affichés pour l'utilisateur qui a effectué la sauvegarde.



©Infineon

Infineon Security Platform Solution - Assistant Sauvegarde

Sélection des utilisateurs

Cette page vous invite à sélectionner les utilisateurs de Données de sauvegarde à récupérer.



Disponibilité de la page :

- Cette page est affichée pour un administrateur, si les utilisateurs des Données de récupération spécifiées ne peuvent pas être mappés aux utilisateurs de votre ordinateur.
- Cette page n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.

La table suivante présente des conseils sur l'utilisation de cette page de l'assistant.

Élément de la page assistant	Explication
<p> <i>Nom utilisateur actuel</i>  <i>Utilisateur dans les données de sauvegarde</i></p>	<p>Le compte utilisateur actuel est affiché ici. Lorsque vous désirez restaurer votre compte utilisateur actuel, cliquez sur la flèche à droite du champ texte et sélectionnez dans la liste un utilisateur à restaurer.</p>
<p> <i>Nom utilisateur</i>  <i>Utilisateur dans les données de sauvegarde</i></p>	<p>D'autres relevés utilisateur valides qui ont été connectés à cet ordinateur au moins une fois sont affichés. Pour ajouter d'autres utilisateurs qui ne sont pas affichés dans la liste, double-cliquez sur "<AJOUTER UTILISATEUR>". Lorsque vous désirez préparer la restauration pour autres utilisateurs, cliquez pour chaque utilisateur sur la flèche à droite du champ texte et sélectionnez dans la liste un utilisateur à restaurer.</p> <p> Une infobulle est affichée pour chaque utilisateur après leur prochaine ouverture de session, en leur</p>

demandant de finaliser la restauration. Une entrée Menu de notification barre de tâches sera fournie aux utilisateurs pour finaliser la restauration.



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Réinitialisation du mot de passe

Assistant de réinitialisation du mot de passe de Infineon Security Platform

L'assistant Réinitialisation du mot de passe de Infineon Security Platform est utilisé pour réinitialiser les mots de passe de l'utilisateur de base. La réinitialisation du mot de passe utilisateur de base inclus des étapes administratives et des étapes utilisateur. Avec l'Assistant de réinitialisation du mot de passe vous pouvez exécuter d'étapes administratives et des étapes utilisateur.



Disponibilité de l'assistant :

- Dans le mode [autonome](#), cet assistant est disponible seulement sur une Security Platform initialisée.
- Dans le [mode serveur](#), aucune tâche administrative n'est disponible dans cet assistant, car le Trusted Computing Management Server gère ces tâches.



Cette icône bouclier est visible seulement pour les utilisateurs avec droits d'administration dans les systèmes d'exploitation avec [Contrôle des comptes utilisateurs](#) (par exemple Windows 7 et Windows Vista).

Étapes de l'assistant

Étapes administratives : Les pages de l'assistant pour préparer la réinitialisation du mot de passe pour un utilisateur sont destinées pour les administrateurs de la Security Platform ou pour le personnel de support technique. Le mot de passe qui protège le jeton de réinitialisation est exigé. Lorsque le mot de passe utilisateur de base de l'administrateur actuel doit être réinitialisé, l'assistant continue avec les étapes utilisateur.

Étapes utilisateur : Les pages de l'assistant pour la réinitialisation du mot de passe de l'utilisateur actuel a comme condition préalable la préparation antérieure de la réinitialisation du mot de passe pour cet utilisateur.

Étape	Commentaire
1. Sélection du jeton réinitialisation du mot de passe	Tâche d'administration
2. Sélection de l'utilisateur dont le mot de passe doit être réinitialisé	Tâche d'administration
3. Affichage et sauvegarde du code d'autorisation de la réinitialisation	Tâche d'administration (disponible seulement lorsque l'utilisateur sélectionné n'est pas l'utilisateur actuel)
4. Fournir les secrets pour la réinitialisation de votre mot de passe utilisateur de base	Tâche utilisateur
5. Configuration du nouveau mot de passe utilisateur de base	Tâche utilisateur  Lorsque vous avez configuré l'authentification étendue, mais votre dispositif d'authentification n'est pas opérationnel ou disponible, vous pouvez annuler la mise à jour de votre dispositif d'authentification avec la nouvelle phrase de passe utilisateur de base.

Démarrage de l'application

Démarrez l'assistant Réinitialisation mot de passe de l'Infineon Security Platform via l'outil de paramétrage : [Outil de paramétrage - Réinitialisation mot de passe](#)



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Réinitialisation mot de passe

Préparation ou exécution de la réinitialisation du mot de passe

Cette page d'assistant vous demande lorsque vous désirez exécuter les étapes administratives ou les étapes utilisateur de la réinitialisation du mot de passe.

Élément de la page assistant	Explication
<p>⦿ <i>Préparer et fournir le code d'autorisation pour la réinitialisation du mot de passe pour un utilisateur spécifique.</i> <i>Préparer et réinitialiser pour le compte administrateur dans un seul pas.</i></p>	<p>Exécution d'étapes administratives de la réinitialisation du mot de passe. Lorsque le mot de passe utilisateur de base de l'administrateur actuel doit être réinitialisé, l'assistant continue avec les étapes utilisateur.</p> <p> Cet élément de page d'assistant n'est pas disponible dans le mode serveur, car le Trusted Computing Management Server gère cette tâche.</p>
<p>⦿ <i>Réinitialiser mon mot de passe (la réinitialisation du mot de passe est déjà préparée pour mon compte utilisateur)</i></p>	<p>Exécution d'étapes utilisateur de la réinitialisation du mot de passe.</p>

 Cette page est affichée seulement lorsque l'assistant n'est pas lancé via l'outil de paramétrage de la Security Platform.



Infineon Security Platform Solution - Assistant Réinitialisation mot de passe

Sélection de l'utilisateur dont le mot de passe doit être réinitialisé

Cette page d'assistant vous permet de sélectionner l'utilisateur dont le mot de passe doit être réinitialisé.



Disponibilité de la page: Cette page n'est pas disponible dans le [mode serveur](#), car le Trusted Computing Management Server la gère.

Elément de la page assistant	Explication
 Utilisateurs	La liste affiche les utilisateurs de la Security Platform dont la fonction Réinitialisation a été activée pour le mot de passe utilisateur de base (voir Assistant d'Initialisation Rapide ou Assistent d'initialisation de l'utilisateur). Sélectionnez l'utilisateur dont le mot de passe doit être réinitialisé.



Cette page fait partie des étapes administratives de la réinitialisation du mot de passe.



Infineon Security Platform Solution - Assistant Réinitialisation mot de passe

Sélection du jeton réinitialisation du mot de passe

Cette page d'assistant vous demande le jeton de réinitialisation de mot de passe.



Disponibilité de la page: Cette page n'est pas disponible dans le [mode serveur](#), car le Trusted Computing Management Server la gère.

Elément de la page assistant	Explication
<i>Location jeton réinitialisation</i>	Entrez le chemin et nom de fichier pour le jeton de réinitialisation du mot de passe créé lorsque les données de réinitialisation du mot de passe ont été configurées pour tous les utilisateurs (voir Assistant Initialisation).
<i>Parcourir...</i>	Cliquez pour naviguer à la recherche du jeton de réinitialisation du mot de passe.
<i>Mot de passe</i>	Entrez le mot de passe protégeant le jeton de réinitialisation du mot de passe indiqué lorsque les données de réinitialisation du mot de passe ont été configurées pour tous les utilisateurs. Remarque : Le jeton de réinitialisation du mot de passe est exigé pour réinitialiser les mots de passe utilisateur de base. Ce fichier est protégé par un autre mot de passe.



Cette page fait partie des étapes administratives de la réinitialisation du mot de passe.



Infineon Security Platform Solution - Assistant Réinitialisation mot de passe

Affichage et sauvegarde du code d'autorisation de la réinitialisation

Cette page d'assistant affiche de code d'autorisation de la réinitialisation, qui autorise un utilisateur à réinitialiser son mot de passe utilisateur de base.



Disponibilité de la page : Cette page n'est pas disponible dans le [mode serveur](#), car le Trusted Computing Management Server la gère.

Élément de la page assistant	Explication
 <i>Code autorisation réinitialisation</i>	Ce code doit être transmis à l'utilisateur qui doit réinitialiser son mot de passe utilisateur de base. Le code sera exigé pour la réinitialisation du mot de passe.
<input type="checkbox"/> <i>Enregistrer dans fichier...</i>	Avec ce bouton vous pouvez sauvegarder le code d'autorisation de la réinitialisation dans un fichier. Vous pouvez ensuite transmettre ce fichier et l'utilisateur peut lire le fichier. Lorsque l'utilisateur est hors connexion (et donc vous ne pouvez pas lui transmettre un fichier), vous devez transmettre les données et le panneau de contrôle comme affichés (par téléphone, par exemple). Dans ce cas l'utilisateur doit saisir manuellement son code d'autorisation de la réinitialisation.
 <i>Panneau de contrôle</i>	Le panneau de contrôle aide un utilisateur à saisir manuellement son code d'autorisation de la réinitialisation. Le panneau de contrôle de la chaîne saisie est affiché à l'utilisateur. Lorsque le panneau de contrôle correspond au panneau de contrôle saisie avec le code d'autorisation de la réinitialisation, vous avez saisi la chaîne correct.



Cette page fait partie des étapes administratives de la réinitialisation du mot de passe. Ce code doit être transmis à l'utilisateur qui doit réinitialiser son mot de passe utilisateur de base. Lorsque vous devez réinitialiser le mot de passe utilisateur de base de votre compte utilisateur, cette page n'est pas affichée. Dans ce cas l'assistant continue avec les étapes utilisateur et vous pouvez réinitialiser

immédiatement votre clé utilisateur de base.



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Réinitialisation mot de passe

Fournir les secrets pour la réinitialisation de votre mot de passe utilisateur de base

Cette page d'assistant vous exige de fournir les secrets pour la réinitialisation de votre mot de passe utilisateur de base : votre "Secret personnel" et le "Code autorisation réinitialisation".

Élément page assistant	Explication
<input type="text"/> <i>Secret personnel</i>	<p>Votre Secret personnel a été créé lors de l'activation de la fonction de réinitialisation pour votre mot de passe utilisateur de base (voir l'Assistant d'Initialisation Rapide ou l'Assistant d'Initialisation d'Utilisateurs).</p> <p>Vous pouvez soit entrer manuellement le Secret Personnel soit fournir un fichier du Secret Personnel.</p>
<input type="checkbox"/> <i>A partir du fichier...</i>	<p>Si vous avez enregistré le Secret Personnel dans un fichier, cliquez sur ce bouton pour fournir le fichier de Secret Personnel.</p>
<input checked="" type="checkbox"/> <i>Masquer secret</i>	<p>Décochez cette case, si vous souhaitez rendre le secret visible en texte clair.</p> <p> Cette option dans le champ Secret Personnel peut être limitée en fonction de la politique du système Activer une sécurité rigoureuse du champ de mot de passe.</p>
	<p>Remarque : Les éléments de la page suivante ne sont pas affichés lorsque vous venez de préparer la réinitialisation du mot de passe pour votre compte utilisateur. Dans ce cas le code d'autorisation de la réinitialisation n'est pas nécessaire.</p>
<input type="text"/> <i>Code autorisation réinitialisation</i>	<p>Ce code vous a été transmis par l'administrateur de la Security Platform ou par le personnel de support technique. Vous pouvez lire d'un fichier ou saisir directement le code d'autorisation de la réinitialisation.</p>
<input type="checkbox"/> <i>Obtenir du fichier...</i>	<p>Cliquez sur ce bouton lorsque vous avez reçu un fichier avec le code d'autorisation de la réinitialisation. Autrement vous</p>

	devez le saisir.
 <i>Obtenir depuis serveur</i>	<p>Cet élément d'assistant n'est disponible qu'en mode serveur. Cliquez sur ce bouton pour obtenir le Code autorisation réinitialisation depuis le serveur.</p> <p> Le système client doit être intégré dans un Trust Domain à gestion centralisée.</p>
 <i>Panneau de contrôle</i>	<p>Le panneau de contrôle vous aide à saisir manuellement le code d'autorisation de la réinitialisation. Lorsque le panneau de contrôle affiché correspond au panneau de contrôle reçu avec le code d'autorisation de la réinitialisation, vous avez saisi la chaîne correct.</p>

 Cette page fait partie des étapes utilisateur de la réinitialisation du mot de passe. Lorsque vous devez réinitialiser le mot de passe utilisateur de base de votre compte utilisateur, cette page est affichée après l'exécution des étapes administratives.

Infineon Security Platform Solution - Assistant d'Importation PKCS #12

Assistant d'Importation PKCS #12 d'Infineon Security Platform

L'Assistant d'Importation PKCS #12 d'Infineon Security Platform est utilisé pour importer les fichiers d'échange d'informations personnelles dans la Security Platform.

Un fichier d'échange d'informations personnelles (PKCS #12) a l'extension ".pfx" ou ".p12". Un fichier PKCS #12 créé pour vous contient votre certificat et votre clé privée. En plus il peut contenir également une chaîne de certificat, par exemple tous les certificats d'autorité de certification nécessaires pour valider votre certificat. Pour des raisons de sécurité, la clé privée est protégée dans un fichier PKCS #12 par un mot de passe.

Différences envers l'assistant d'Importation certificat Microsoft

Ordinateur sans la Security Platform : Les fichiers PKCS #12 sont importés en utilisant l'*Assistant d'Importation certificat Microsoft*. Votre clé privée est sécurisée par le logiciel.

Ordinateur avec Security Platform : Les fichiers PKCS #12 sont importés en utilisant l'*Assistant d'Importation PKCS #12 de la Security Platform*. Votre clé privée est sécurisée par le Trusted Platform Module. Ainsi la protection de votre clé privée est améliorée.

Etapes de l'assistant

Etape	Comment
1. Fichier PKCS #12 à importer	Spécifiez le fichier vous désirez importer
2. Options	Configuration d'options d'importation PKCS #12

Démarrage de l'application

Pour démarrer l'assistant Importation PKCS #12 d'Infineon Security Platform cliquez sur **Importer...** dans le Visualisateur du certificat de la Security Platform. Démarrez le Visualisateur du certificat de la Security Platform via l'outil de paramétrage ([Outil de paramétrage - Paramètres utilisateur - Gestion...](#)).



©Infineon

Technologies AG

Infineon Security Platform Solution - Assistant d'Importation PKCS #12

Fichier PKCS #12 à importer

Cette page d'assistant vous demande de spécifier le fichier PKCS #12 à importer.

Elément de la page assistant	Explication
<input type="text"/> <i>Nom fichier</i>	Vous pouvez saisir ou copier le chemin ici, par exemple D:\certificates\MyPKCS12file.pfx ou D:\certificates\MyPKCS12file.p12.
<input type="button" value="Parcourir"/>	Cliquez pour naviguer à la recherche du fichier PKCS #12 sans saisir ou copier le chemin.
<input type="password"/> <i>Saisissez le mot de passe protégeant le fichier</i>	Pour des raisons de sécurité, la clé privée est protégée dans un fichier PKCS #12 par un mot de passe. Saisissez ici le mot de passe.



Infineon Security Platform Solution - Assistant d'Importation PKCS #12

Options

Cette page d'assistant vous demande de configurer les options d'importation PKCS #12.

Elément de la page assistant	Explication
<input type="checkbox"/> <i>Stockage certificat</i>	Le fichier PKCS #12 sera enregistré dans un certain stockage de certificats, par exemple <i>Personnel</i> . Le stockage certificat est affiché ici.
<input type="checkbox"/> <i>Parcourir...</i>	Cliquez pour modifier le stockage certificat.  Vous pouvez importer un certificat dans n'importe quel stockage certificat. Le plus souvent vous importez les certificats soit dans le dépôt <i>Personnel</i> ou dans le dépôt <i>Autorités de certification racine de confiance</i> , fonction du but prévu du certificat - certificat autorité de certification racine ou non. Recommandation : Lorsque vous importez votre certificat, sélectionnez <i>Personnel</i> .
<input checked="" type="checkbox"/> <i>Inclure chaîne complète certificat si inclut dans le fichier PKCS #12</i>	Un fichier PKCS #12 peut contenir non seulement votre certificat, mais une chaîne complète de certificats. Une chaîne de certificats inclut tous les certificats de l'autorité de certification nécessaires pour valider votre certificat. Cochez cette case lorsque vous désirez importer la chaîne complète de certificats (si inclut dans le fichier PKCS #12).  Lorsque la chaîne complète de certification est importée, les certificats de l'autorité de certification seront stockés automatiquement dans les dépôts de certificats appropriés. Exemple : Vous allez importer un PKCS #12 incluant votre

	<p>certificat et votre clé privée, un certificat d'autorité de certification intermédiaire et un certificat d'autorité de certification de racine de confiance.</p> <p>Vous avez sélectionné le dépôt de certificats <i>Personnel</i>.</p> <ul style="list-style-type: none">→ Votre certificat sera enregistré dans le dépôt certificats <i>Personnel</i>.→ Le certificat d'autorité de certification intermédiaire sera enregistré dans le dépôt certificats <i>Autorités de certification intermédiaires</i>.→ Le certificat d'autorité de certification racine de confiance sera enregistré dans le dépôt certificats <i>Autorités de certification racine de confiance</i>.
<p><input checked="" type="checkbox"/> <i>Activation du niveau élevé de protection de clé privée</i></p>	<p>Cochez cette case lorsque vous désirez vous assurer que la clé privée ne soit pas utilisée sans vous la savoir.</p> <p>Lorsque vous activez le <i>niveau élevé de protection de clé privée</i>, on vous demande le mot de passe chaque fois la clé privée est utilisée.</p>



**Infineon Security Platform Solution - pictogramme Zone de notification
barre de tâches**

Security Platform pictogramme Zone de notification barre de tâches

La pictogramme Zone de notification barre de tâches est un point d'entrée sensible pour les tâches d'administration de Security Platform. Cette pictogramme vous permet d'accéder le menu notification barre de tâches. En plus, des info-bulles vous aideront avec les informations sensibles.

Pictogramme Zone de notification barre de tâches

Cette pictogramme est affichée dans la zone de notification barre de tâches. Point d'entrée sensible pour les tâches d'administration de Security Platform.

L'aspect visuel de la pictogramme indique l'état actuel de Security Platform :

 La Security Platform est en cours d'utilisation.

 La Security Platform est initialisée, mais désactivée ou désactivée temporairement. L'utilisateur actuel peut activer la Security Platform.

 La Security Platform n'est pas initialisée pour l'utilisateur actuel.

 La Security Platform est désactivée ou désactivée temporairement ou l'autotest a échoué. L'utilisateur actuel ne peut pas modifier l'état de la Security Platform.

 La Security Platform n'est pas initialisée.

Menu Notification barre de tâches

Ce menu est affiché en cliquant sur Notification barre de tâches.

Il fournit tâches administratives concernant l'état, par ex. :

- Initialisation de Security Platform
- Initialisation utilisateur Security Platform
- Administration Security Platform
- Aide sur l'exécution de quelques tâches

	 Quelques éléments de menu ne sont pas disponible en mode serveur .
Bulles	<p>Les info-bulles vous informent sur les changements de l'état de Security Platform et vous suggèrent quelques tâches dans les états de Security Platform.</p> <p> Dans le mode serveur, les tâches n'exigeant pas l'intervention de l'utilisateur sont gérées par Trusted Computing Management Server. Les bulles associées pour ces tâches ne sont pas disponibles.</p>
Info-bulles	Une courte information sur l'état est affichée comme une info-bulle lorsque la souris se déplace sur la pictogramme Notification barre de tâches.



**Infineon Security Platform Solution - Pictogramme Zone de notification
barre de tâches**

Éléments menu notification barre de tâches

Fonction de l'état actuel de Infineon Security Platform et de l'état de l'utilisateur connecté actuellement, le menu notification barre de tâches vous offre des éléments de menu différents.

En utilisant ce menu, tous les outils de la solution Security Platform permis pour l'utilisateur connecté actuellement peuvent être lancés. Lorsque l'utilisateur connecté actuellement n'est pas autorisé à lancer un outil de la solution, l'élément de menu respectif n'est pas contenu dans le menu.



Cette icône bouclier est visible seulement pour les utilisateurs avec droits d'administration dans les systèmes d'exploitation avec [Contrôle des comptes utilisateurs](#) (par exemple Windows 7 et Windows Vista).

La table suivante présente tous les éléments de menu.

Élément du menu	Explication
<i>Gestion de Security Platform</i>	Démarez l' Outil de paramétrage d'Infineon Security Platform .  Dans les systèmes d'exploitation avec Contrôle des comptes utilisateurs, l'Outil de configuration est lancé sans privilèges élevés.
<i>Initialisation de la Security Platform</i>	Démarez l' Assistant Initialisation Rapide d'Infineon Security Platform . Cet élément de menu est disponible lorsque la configuration d'Infineon Security Platform n'a pas encore été exécutée. Cette entrée est désactivée lorsque la stratégie <i>Permettre l'inscription de la plate-forme</i> est désactivée (cette stratégie s'applique si la Security Platform n'a pas été initialisée auparavant).  Cet élément de menu n'est pas disponible en mode serveur , car Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée.

<p><i>Initialisation de l'utilisateur de la Security Platform</i></p>	<p>Démarrez l'Assistant Initialisation Rapide d'Infineon Security Platform.</p> <p>Cet élément de menu est disponible lorsque l'utilisateur connecté actuellement n'a pas été encore configuré comme utilisateur de l'Infineon Security Platform. Cette entrée est grisée si la Security Platform n'est pas initialisée et la stratégie <i>Permettre inscription utilisateur</i> est désactivée (cette stratégie n'est disponible que pour les utilisateurs non initialisés encore).</p> <p> Cet élément de menu n'est pas disponible en mode serveur si l'utilisateur courant n'est pas membre du groupe d'inscription utilisateurs.</p>
<p><i>Activer la sauvegarde de vos fonctions de la Security Platform</i></p>	<p>Inclure vos clés et informations d'identification dans les sauvegardes automatiques. Vous devez vous authentifier dans la Security Platform.</p> <p>Cet élément de menu est disponible lorsque l'administrateur de la Security Platform a configuré la fonction Sauvegarde, mais l'utilisateur actuel n'a pas encore activé cette fonction.</p> <p> Cet élément de menu n'est pas disponible en mode serveur, car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.</p>
<p><i>Activer la fonction Réinitialisation du mot de passe</i></p>	<p>Activer la fonction Réinitialisation du mot de passe pour votre compte utilisateur.</p> <p>Cet élément de menu est disponible lorsque l'administrateur de la Security Platform a configuré la fonction Réinitialisation du mot de passe, mais l'utilisateur actuel n'a pas encore activé cette fonction.</p>
<p><i>Personal Secure Drive - Chargement ou Personal Secure Drive - <Lecteur de lecteur:Etiquette</i></p>	<p>Chargement de votre Personal Secure Drive. Lorsque vous avez configuré plusieurs PSD, ce menu affichera tous les lecteurs (<Lettre de lecteur:Etiquette de lecteur>).</p> <p>Cet élément du menu est disponible, si vous avez configuré au moins un PSD (qui n'est pas chargé actuellement).</p>

<p>de lecteur> - Chargement</p>	
<p>Personal Secure Drive - Déchargement ou Personal Secure Drive - <Lettre de lecteur:Etiquette de lecteur> - Déchargement</p>	<p>Déchargement de votre Personal Secure Drive. Lorsque vous avez configuré plusieurs PSD, ce menu affichera tous les lecteurs (<Lettre de lecteur:Etiquette de lecteur>). Cet élément du menu est disponible, si vous avez configuré au moins un PSD (qui est chargé actuellement).</p>
<p>Personal Secure Drive – Chargement lors de la connexion ou Personal Secure Drive - <Lettre de lecteur:Etiquette de lecteur> - Chargement lors de la connexion</p>	<p>Déterminez si vous souhaitez charger votre PSD automatiquement après votre connexion Windows. Lorsque vous avez configuré plusieurs PSD, ce menu affichera tous les lecteurs (<Lettre de lecteur:Etiquette de lecteur>). Si une marque est affichée ici, votre PSD est chargé. Cliquez ici pour ajouter / enlever la marque. Cet élément du menu est disponible, si vous avez configuré au moins un PSD.</p>
<p>Personal Secure Drive - Créez / Gérez</p>	<p>Créez, changez ou supprimez un Personal Secure Drive via Assistant d'Initialisation Utilisateur.</p>
<p>Personal Secure Drive - Déchargez tous</p>	<p>Déchargement de tous les Personal Secure Drives qui sont chargés actuellement.</p>
<p>Fermeture de session du système de fichiers de cryptage</p>	<p>Cliquez pour fermer la session du système de fichiers de cryptage. Ça veut dire que vous devez vous authentifier à nouveau pour accéder à vos données protégées EFS. Cet élément de menu est disponible lorsque vous êtes authentifié avant d'accéder à quelques données protégées</p>

	par l'EFS.
<i>Modifier le mot de passe utilisateur de base</i>	<p>Cliquez ici pour modifier votre mot de passe utilisateur de base.</p> <p>Cet élément de menu est disponible si votre mot de passe utilisateur de base est expiré. L'expiration du mot de passe utilisateur de base peut être configurée par la stratégie d'utilisateur Age maximal mot de passe utilisateur de base.</p>
<i>Synchronisation phrase de passe utilisateur de base</i>	<p>Cliquez pour synchroniser votre phrase de passe utilisateur de base sur le dispositif d'authentification et Security Platform.</p> <p>Cet élément de menu est disponible lorsque votre dispositif d'authentification et votre Security Platform ont des phrases de passe utilisateur de base différentes. Les motifs possibles sont :</p> <ul style="list-style-type: none"> • Vous avez réinitialisé votre phrase de passe utilisateur de base sans mettre à jour votre dispositif d'authentification. • Vous utilisez votre dispositif d'authentification sur plusieurs Security Platform et vous avez modifié votre phrase de passe sur une autre Security Platform.
<i>Reconfigurez les caractéristiques de l'utilisateur</i>	<p>Cliquez ici pour reconfigurer les caractéristiques de votre Security Platform. Cet élément de menu est disponible lorsque votre PSD ou EFS doit être reconfiguré. Les motifs possibles sont :</p> <ul style="list-style-type: none"> • Votre certificat l'EFS ou le PSD est non valide ou n'est plus disponible. Cela se produit également lors du <i>cryptage de fichiers et de dossiers à l'aide de Encrypting File System (EFS), si vous avez configuré l'EFS et également le PSD, et puis modifié vos paramètres PSD par la suite.</i> • Une restauration a été effectuée et votre PSD ne peut plus être chargé (par ex. car la lettre de lecteur est déjà utilisée).
<i>Désactiver temporairement la Security</i>	<p>Cliquez ici pour suspendre la fonctionnalité de Infineon Security Platform jusqu'au prochain redémarrage du système. Les applications qui utilisent Security Platform</p>

<p><i>Platform jusqu'au prochain démarrage du système</i></p>	<p>n'auront plus accès aux données protégées par Trusted Platform Module, incluant les données protégées par EFS, Personal Secure Drive et autres. L'accès aux données protégées est restauré une fois Security Platform réactivée. Cet élément de menu est disponible lorsque l'Infineon Security Platform est initialisée et activée. Cette fonction n'est pas disponible pour les Security Platforms avec un Trusted Platform Module 1.2.</p>
<p><i>Activez le fonctionnement de Security Platform</i></p>	<p>Cet élément de menu est disponible pour les administrateurs sur une Security Platform initialisée en mode autonome, dans le cas où la Security Platform a été désactivée par le propriétaire. Le mot de passe du propriétaire est exigé pour activer la Security Platform.</p> <p>Cet élément de menu est également disponible pour les utilisateurs sur une Security Platform initialisée disposant d'une version de Trusted Platform Module inférieure à la version 1.2, si la Security Platform a été temporairement désactivée par l'utilisateur. Dans ce cas, l'utilisateur doit redémarrer le système.</p> <p> Cet élément de menu n'est pas disponible en mode serveur, car Security Platform est initialisée automatiquement si le système client est intégré dans un Trust Domain à gestion centralisée.</p>
<p><i>Restaurer la Security Platform</i></p>	<p>Restaurer les informations d'identification et les paramètres de la Security Platform depuis une sauvegarde de secours. Cet élément de menu est disponible pour un administrateur lorsque la Security Platform n'a pas été initialisée ou elle a été initialisée avec un autre système d'exploitation ou lorsque le propriétaire de la plate-forme est modifié.</p> <p> Cet élément de menu n'est pas disponible en mode serveur, car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.</p>
<p><i>Restaurer les fonctions de la Security</i></p>	<p>Restaurez vos informations d'identification et les paramètres depuis une sauvegarde de secours. Cet élément de menu est disponible lorsque votre clé</p>

Platform

utilisateur de base ne peut pas être chargée, par exemple vos fonctions Security Platform ne peuvent pas être utilisées.



Cet élément de menu n'est pas disponible en [mode serveur](#), car la sauvegarde et restauration sont gérées par Trusted Computing Management Server.

*Informations
d'identification /
Configuration
utilisateur -
Demande une
copie locale de
travail*

Obtenir du Trusted Computing Management Server une copie locale de travail de vos informations d'identification et configuration de l'utilisateur. Bloque les changements de tous les ordinateurs tandis que vous n'avez pas accepté ou annulé les changements locaux (par ex. l'état de la session utilisateur en mode serveur est configuré à « Lecture/Écriture permanente »).



Cet élément de menu n'est disponible qu'en [mode serveur](#).

Exécutez cette action avant de mettre la plateforme hors connexion si vous désirez changer vos informations d'identification et configuration d'utilisateur sans une connexion réseau avec Trusted Computing Management Server. Un exemple typique est le changement ou la réinitialisation de votre mot de base d'utilisateur de base sur ordinateur portable qui est hors connexion.

Conditions préalables :

- L'utilisateur actuel a été initialisé en mode serveur.
- Votre plateforme est connectée au Trusted Computing Management Server.
- Aucune copie locale de travail active n'existe sur la même plateforme (par ex. l'état de la session utilisateur sur la même plateforme n'est pas « Lecture/Écriture permanente »).

Lorsqu'un accès actuel en écriture utilisant vos informations d'identification existe déjà ou lorsque vos informations d'identification ne sont pas mises à jour, vous serez informé que vous ne pouvez pas demander actuellement une copie

	<p>de travail locale. Dans le premier cas, attendez et réessayez. Dans le deuxième cas, une bulle vous demandera d'actualiser vos informations d'identification.</p> <p>Détails sur les états de session utilisateur.</p>
<p><i>Informations d'identification / Configuration utilisateur - Accepter les changements locaux</i></p>	<p>Envoyer les changements des vos informations d'identification et configuration d'utilisateur vers Trusted Computing Management Server. Permettre de nouveau les changements depuis l'autre plateforme.</p> <p> Cet élément de menu n'est disponible qu'en mode serveur.</p> <p>Exécutez cette action lorsque votre plateforme est de nouveau en ligne, après avoir modifié localement vos informations d'identification et configuration.</p> <p>Conditions préalables :</p> <ul style="list-style-type: none"> • L'utilisateur actuel a été initialisé en mode serveur. • Votre plateforme est connectée au Trusted Computing Management Server. • Une copie locale de travail active existe (par ex. l'état de la session utilisateur sur cette plateforme est « Lecture/Écriture permanente »).
<p><i>Informations d'identification / Configuration utilisateur - Annuler les changements locaux</i></p>	<p>Annule les changements des vos informations d'identification et configuration d'utilisateur. Permettre de nouveau les changements depuis l'autre plateforme.</p> <p> Cet élément de menu n'est disponible qu'en mode serveur.</p> <p>Exécutez cette action lorsque votre plateforme est de nouveau en ligne et vous n'avez pas modifié vos informations d'identification et configuration ou vous désirez annuler les changements.</p> <p>Conditions préalables :</p> <ul style="list-style-type: none"> • L'utilisateur actuel a été initialisé en mode serveur.

	<ul style="list-style-type: none"> • Votre plateforme est connectée au Trusted Computing Management Server. • Une copie locale de travail active existe (par ex. l'état de la session utilisateur sur cette plateforme est « Lecture/Écriture permanente »).
<i>Mettre à jour les informations d'identification et configuration d'utilisateur</i>	<p>Exécutez cette tâche pour mettre à jour vos informations d'identification et configuration d'utilisateur sur la plateforme actuelle.</p> <p> Cet élément de menu n'est disponible qu'en mode serveur.</p> <p>Conditions préalables :</p> <ul style="list-style-type: none"> • L'utilisateur actuel a été initialisé en mode serveur. • Votre plateforme est connectée au Trusted Computing Management Server. <p>Détails sur la mise à jour des informations d'identification et configuration d'utilisateur</p>
<i>Réactualisez</i>	Réactualisez l'Icône de Notification de la Barre des Tâches et le Menu de Notification de la Barre des Tâches.
<i>Supprimez Authentification Cache</i>	<p>Annulation de l'effet du <i>Rappel de mot de passe pour toutes les applications</i>, qui a été configuré dans le dialogue d'authentification du Mot de Passe Utilisateur de Base. Ainsi, vous devez immédiatement vous authentifier encore une fois si nécessaire.</p> <p> Cet élément du menu n'est disponible que si <i>Rappel du mot de passé pour toutes les applications</i> a été vérifié avant dans le dialogue d'authentification du Mot de Passe Utilisateur de Base.</p>
<i>Activez Infineon TPM Strong Cryptographic Provider</i>	Afin d'activer Infineon TPM Strong Cryptographic Provider une clé doit être générée. Cliquez ici afin d'autoriser la génération de clé.

<i>Aide</i>	L'aide de l'Infineon Security Platform est démarrée.
Eléments de menu divers pour l'aide contextuels	L'aide contextuelle pour l'état actuel de la plate-forme et les actions utilisateur nécessaires sont affichées.



©Infineon Technologies AG

**Infineon Security Platform Solution - pictogramme Zone de notification
barre de tâches**

Désactivation du Trusted Platform Module

Il y a deux possibilités pour désactiver le Trusted Platform Module.

- **Désactivation temporaire**

Cette opération désactive le chip jusqu'au prochain redémarrage du système. Un changement de l'utilisateur connecté actuellement n'affecte pas l'état du chip.

- **Désactivation permanente**

Cette opération désactive physiquement le chip. Lorsque l'Infineon Security Platform est déjà configurée, la désactivation peut être exécutée via l'[Outil de paramétrage d'Infineon Security Platform](#).

La réactivation d'Infineon Security Platform est exécutée via le même outil de paramétrage. Lorsque l'Infineon Security Platform n'est pas configurée, le chip doit être activée dans la BIOS du système.



©Infineon

Technologies AG

**Infineon Security Platform Solution - pictogramme Zone de notification
barre de tâches**

Désactivation temporaire d'Infineon Security Platform

Un mécanisme a été prévu pour désactiver l'Infineon Security Platform jusqu'au prochain redémarrage du système. La désactivation temporaire reste active lorsque l'utilisateur d'Infineon Security Platform se déconnecte et se reconnecte.

Toutes les fonctions Infineon Security Platform et le circuit correspondant sont bloqués pour assurer une protection contre toute utilisation dans cet état.



Technologies AG

Solution Infineon Security Platform - Icône de Notification de la barre d'outils

Activation d'Infineon Security Platform

Pour activer Security Platform, allez dans **Avancé** dans l'Outil de paramétrage et cliquez sur **Activer...** (voir [Paramètres avancés](#)). Notez que seul le [propriétaire de Security Platform](#) peut effectuer cette action, car celle-ci exige des droits d'administration et la connaissance du mot de passe du propriétaire.

Après avoir activé Security Platform, procédez à la configuration initiale de la Security Platform et des utilisateurs via l'[Assistant Initialisation rapide](#) (recommandé pour la plupart des utilisateurs), ou via l'[Assistant Initialisation](#) et l'[Assistant Initialisation utilisateur](#) (recommandé pour les utilisateurs experts).



©Infineon

Technologies AG

Infineon Security Platform Solution - Administration stratégie

Administration de stratégie d'Infineon Security Platform

Le Local Group Policy Editor vous aide à administrer les aspects suivants d'Infineon Security Platform :

Stratégies système	Paramètres de sécurité pour l'ordinateur
Stratégies utilisateur	Paramètres de sécurité pour les ordinateurs sur l'ordinateur
	Dans le mode serveur , les stratégies sont configurées au niveau du domaine par un administrateur de domaine via Trusted Computing Management Server.

Conditions préalables et limitations



- Seul un administrateur est en mesure de changer les stratégies système et utilisateur.
- L'éditeur de stratégie de groupe local n'est pas disponible dans les éditions familiales de Windows.

Comment inscrire la Stratégie de Security Platform

Sur les systèmes d'exploitation prenant en charge le format de politique ADMX (par ex. Windows 7 et Windows Vista), la Stratégie de Security Platform est automatiquement inscrite (modèle administratif de fichier **IfxSpPol.admx**).

Sur d'autres systèmes d'exploitation, vous devez exécuter les étapes suivantes pour inscrire les Politiques de Security Platform manuellement (modèle administratif de fichier **IfxSpPol.adm**), avant d'avoir accès aux politiques depuis l'[Outil de Paramétrage](#) :

1. Démarrez Editeur de Stratégie de Groupe Local (gpedit.msc)
2. Cliquez avec la touche droite de la souris sur **Modèles Administratifs de Configuration Ordinateur** ou **Configuration Utilisateur**.
3. Dans le menu contextuel, cliquez sur **Ajouter / Enlever modèles...** .
Le dialogue "Ajouter / Enlever Modèles" est affiché.
4. Cliquez sur **Ajouter**.
Le dialogue à parcourir "Modèles de Stratégie" est affiché.
5. Sélectionnez le modèle **IfxSpPol.adm**, et cliquez sur **Ouvrir** afin d'ajouter le modèle "Security Platform".
6. Cliquez sur **Fermer** afin d'inscrire le nouveau modèle administratif.

Comment éditer les Stratégies de Systèmes et d'Utilisateurs

1. Démarrez l'[Outil de Paramétrage](#) depuis l'[Icône de Notification de la Barre d'Outils](#).

Sur les systèmes d'exploitation avec le Contrôle de Compte d'Utilisateur (par ex. Windows 7 et Windows Vista), cliquez sur  **Gérer Security Platform**.

Sur d'autres systèmes d'exploitation, cliquez sur **Gérer Security Platform**.

2. Afin d'éditer Stratégies de Système, cliquez sur **Système...** sur l'onglet **Avancé**.

Afin d'éditer Stratégies Utilisateurs, cliquez sur **Utilisateur...** sur l'onglet **Avancé**.

Editeur de Stratégie de Groupe Local est lancé. Il affiche Stratégies Système Infineon Security Platform ou Stratégies Utilisateurs.

Plusieurs informations

Des informations détaillées sur les stratégies système et utilisateur sont disponibles dans la Présentation de la stratégie de groupe Microsoft et sur Microsoft TechNet. Pour obtenir les informations demandées en Aide Microsoft, minimiser toutes les fenêtres déjà ouvertes pour visualiser le Bureau Windows. Ensuite, appuyez sur F1 pour rechercher le mot-clé convenable.



©Infineon Technologies AG

Infineon Security Platform Solution - Administration stratégie

Stratégies système d'Infineon Security Platform

Les paramètres de stratégie ordinateur suivants sont pris en charge par le logiciel de la solution Infineon Security Platform.



Dans le [mode serveur](#), les stratégies système sont configurées au niveau du domaine par un administrateur de domaine via Trusted Computing Management Server. Notez que les paramètres autorisés uniquement pour le mode serveur sont décrits dans le fichier modèle administratif fourni par Trusted Computing Management Server.



Valeur par défaut: Lorsqu'une stratégie n'a pas été encore configurée explicitement (par exemple l'éditeur de Stratégie de groupe parent affiche l'état **Non configuré**), alors le logiciel de la solution Security Platform applique implicitement une valeur par défaut.

Paramètres pour toutes les versions

Paramètre valables pour la version en mode autonome ET pour la version en mode serveur.

Stratégie	Explication	Valeur par défaut
<i>Préparer l'inscription TPM</i>	<p>Activé : Pour les plates-formes non initialisées avec un Trusted Platform Module désactivé prenant en charge l'Interface de présence physique (Physical Presence Interface, PPI), Trusted Platform Module est préparé automatiquement pour activation. Les utilisateurs seront guidés pour finaliser l'activation.</p> <p>Désactivé : Trusted Platform Module n'est pas préparé pour activation automatique.</p>	Désactivé
<i>Autorisation donnée aux administrateurs d'utiliser les clés de la plate-forme à distance</i>	<p>Activé : Un administrateur peut utiliser les clés de la plate-forme non seulement localement, mais également à distance.</p> <p>Désactivé : L'utilisation des clés plate-forme à distance n'est pas permise. Pour des raisons de sécurité, l'accès à ces clés est limité comme établi par le Trusted Computing Group (TCG). Ainsi toutes les clés pouvant permettre l'identification de votre Security Platform ne sont pas disponibles pour accès à</p>	Désactivé

	<p>distance. Cette stratégie demande que tous les ordinateurs impliqués soient membres des domaines autorisés. S'applique seulement pour les systèmes d'exploitation prenant en charge la propriété des domaines.</p> <p> L'administration et l'opération de la Security Platform ne sont pas limitées par ce paramètre.</p>	
<p><i>Permettre la lecture de la mémoire NV TPM non protégée</i></p>	<p>Détermine qui peut lire la mémoire non-volatile (NV) non protégée stockée dans un Trusted Platform Module 1.2. La mémoire NV peut contenir des données confidentielles.</p> <p>Activé : Spécifie lorsque seulement les administrateurs locaux, ou les administrateurs locaux et les administrateurs à distance, ou tous les utilisateurs locaux, ou tous les utilisateurs peuvent lire les données NV non protégées.</p> <p>Désactivé : Aucun utilisateur ne peut lire les données NV non protégées.</p> <p> Cette stratégie est valable pour les Security Platform avec un Trusted Platform Module 1.2.</p> <p>L'administration et l'opération</p>	<p>Activée/Administrateurs locaux</p>

	<p>de Security Platform ne sont pas restrictionnées par ce paramètre.</p>	
<p><i>Configurer le seuil pour les attaques de type dictionnaire</i></p>	<p>Détermine le nombre d'essais d'authentification de Trusted Platform Module autorisés avant que des mesures de défense d'attaque par dictionnaire ne soient prises.</p> <p>Activé : Déterminez combien d'essais d'authentification devraient être autorisés pour les clés (par ex. utilisé pour l'authentification de l'Utilisateur de Security Platform), le propriétaire, et pour l'accès aux données verrouillées (par ex. utilisé par Windows BitLocker en combinaison avec PIN), avant que des mesures de défense d'attaque par dictionnaire ne soient prises.</p> <p>Désactivé : Le seuil pour les attaques de type dictionnaire ne peut pas être configuré. Les valeurs par défaut sont appliquées.</p> <p> Cette stratégie s'applique uniquement aux Security Platforms équipée d'un Infineon Trusted Platform Module 1.2. Elle doit être configurée avant l'initialisation de Security Platform. Les changements ultérieurs de cette</p>	<p>Activé Propriétaire : 3 essais Clé : 5 essais Données : 10 essais</p>

stratégie ne seront appliqués qu'après la suivante [réinitialisation du niveau de défense](#).

Si cette stratégie n'est pas configurée, les mêmes paramètres peuvent être configurés individuellement pour chaque plate-forme dans le mode autonome via l'assistant Initialisation (voir [Configurer les paramètres de la défense contre les attaques de type dictionnaire](#)). Dans ce cas, aucune réinitialisation du niveau de défense n'est nécessaire pour activation. Tous les utilisateurs de Security Platform partagent le nombre d'essais d'authentification utilisateur permis. A retenir lorsqu'il y a plusieurs utilisateurs sur un système (par ex. en utilisant Changement rapide utilisateur).

[Détails sur les attaques de type dictionnaire](#)

Activez la sécurité du champ de mot de passe obligatoire

Activé : La possibilité de couper, copier, coller et visualiser le mot de passe dans un texte en clair n'est pas disponible dans les champs des mots de passe.

Désactivé : La possibilité de coller est disponible dans les champs des mots de passe. En

Désactivé

	<p>plus, l'opération de coupe et copie est disponible lorsque le mot de passe est visible dans un texte en clair.</p>	
<p><i>Purge des clés lorsqu'on passe aux états d'économie d'énergie</i></p>	<p>Activé : Les clés de Security Platform sont purgées avant que l'ordinateur passe dans un des états d'économie d'énergie mise en veille (S3) ou veille prolongée (S4). Par conséquent, le niveau de sécurité pendant l'état d'économie d'énergie sera augmenté. Après avoir revenu de l'état d'économie d'énergie, les Fonctions Security Platform vont redemander une autre authentification.</p> <p>Désactivé : Les clés de Security Platform ne sont pas purgées.</p>	<p>Activé</p>
<p><i>Fournisseurs d'authentification étendue</i></p>	<p>Activé : Saisissez un class ID fournisseur d'authentification étendue (CLSID) ou plusieurs CLSID séparés par points-virgules. Seulement les fournisseurs spécifiés seront acceptés pour utiliser l'authentification étendue sur les systèmes client qui ne sont pas encore configurés. Si vous ne connaissez pas le class ID d'un fournisseur d'authentification étendue,</p>	<p>Le même comportement comme si désactivée.</p> <p>En mode autonome, le comportement est identique à celui des versions antérieures du produit, c'est-à-dire que les fournisseurs installés peuvent être utilisés.</p>

	<p>veuillez contacter le fournisseur d'authentification étendue. Exemple de ClassID : {76D8D888-B5AC-49FC-9408-8A45D37F3AC6}.</p> <p>Désactivé : Aucun fournisseur d'authentification étendue ne peut être spécifié. L'authentification évoluée ne peut pas être utilisée sur les systèmes client qui ne sont pas configurés.</p>	
<p><i>Autorisation donnée aux administrateurs de devenir propriétaire à distance</i></p>	<p>Activé : La présence locale d'un administrateur n'est pas exigée pour prendre la propriété d'un ordinateur. Cette fonctionnalité peut s'avérer très utile pour l'installation des clients dans les réseaux étendus.</p> <p>Désactivé : La prise à distance de la propriété n'est pas permise.</p> <p> Cette stratégie demande que tous les ordinateurs impliqués soient membres des domaines autorisés. S'applique seulement pour les systèmes d'exploitation prenant en charge la propriété des domaines.</p>	<p>Désactivé</p>
<p><i>Autorisation donnée aux</i></p>	<p>Détermine qui peut lire la clé publique SRK stockée dans un</p>	<p>Désactivé</p>

*administrateurs
de récupérer la
clé publique SRK
à distance*

Trusted Platform Module. La clé publique SRK nécessite une protection spéciale, lorsqu'elle peut identifier la Security Platform.

Activé : Un administrateur peut récupérer la clé publique SRK localement, mais également à distance.

Désactivé : La récupération à distance de la clé publique SRK n'est pas permise.



Le pas [Exportation et autorisation automatiques](#) de la migration exige l'activation de ce paramètre sur l'ordinateur cible de la migration.

Cette stratégie demande que tous les ordinateurs impliqués soient membres des domaines autorisés.

S'applique seulement pour les systèmes d'exploitation prenant en charge la propriété des domaines.

Paramètres pour la version en mode autonome

Paramètres valides seulement pour la version en mode autonome.

Stratégie	Explication
<i>Mot de passe du propriétaire - Longueur minimale du mot de passe</i>	<p>Activé : Saisissez la longueur minimal du Mot de passe utilisateur, par exemple 6. La longueur minimale des mots de passe est valable pour les Mots de passe du propriétaire qui sont configurées ou changées ultérieurement.</p> <p>Désactivé : La longueur minimale du mot de passe est 6 caractères.</p> <p> Ce paramètre s'applique uniquement aux mots de passe du propriétaire configurés sur une Security Platform autonome. La longueur minimale du mot de passe pour les mots de passe du propriétaire configurés en utilisant Trusted Computing Management Server est configurée pas la stratégie Trusted Computing Management Server avec le même nom.</p> <p>Détails sur la gestion du mot de passe</p>
<i>Mot de passe du propriétaire - Le mot de passe doit correspondre aux exigences de complexité</i>	<p>Activé : Les exigences de complexité du mot de passe sont imposées pour les Mots de passe du propriétaire qui sont configurés ou changés ultérieurement.</p> <p>Désactivé : Aucune demande concernant la complexité du mot de passe n'est pas appliquée.</p> <p> Ce paramètre s'applique uniquement aux mots de passe du propriétaire configurés sur une Security Platform autonome. La demandes de complexité pour les mots de passe du propriétaire configurés en utilisant Trusted Computing Management Server sont configurées pas la stratégie Trusted Computing Management Server avec le même nom. Détails sur la complexité du mot de passe</p>
<i>Permettre l'inscription de la plate-</i>	<p>Activé/Autorisation pour l'interface et l'assistant de gestion : L'administrateur peut utiliser l'assistant d'initialisation de la Security Platform et l'interface de</p>

<p><i>forme</i></p>	<p>management provider pour initialisation.</p> <p>Activer/Autoriser Management Provider uniquement : Les plateformes ne peuvent être initialisées qu'à l'aide de l'interface Management Provider.</p> <p>Désactivé : Les plates-formes ne peuvent pas être initialisées.</p>
<p><i>Application de la configuration de sauvegarde incluant la récupération d'urgence</i></p>	<p>Activé : La configuration des sauvegardes automatiques (y compris la récupération d'urgence) est obligatoire dans le processus d'initialisation de la Security Platform. Lorsque la Security Platform a été déjà initialisée sans configurer les sauvegardes automatiques, il n'y a aucune obligation pour la configuration des sauvegardes automatiques.</p> <p>Désactivé : Il n'y a aucune obligation pour la configuration des sauvegardes automatiques. La sauvegarde peut être configurée après l'initialisation de la Security Platform via Outil de paramétrage - Sauvegarde - Configurer...</p>
<p><i>Emplacement de la sauvegarde de secours</i></p>	<p>Activé : Saisissez un chemin, y compris un nom de fichier, par exemple \\BackupServer\SecurityPlatformShare\SPSystemBackup.xml. Ce chemin cible sera appliqué lorsque la fonction Sauvegarde est configurée. Un fichier de sauvegarde écrit automatiquement, représenté par un fichier XML et un dossier avec le même nom, sera créé, par ex. un fichier SPSysSystemBackup.xml et un dossier SPSysSystemBackup. Lorsque la fonction Sauvegarde est déjà configurée, le chemin de sauvegarde existant est gardé tant qu'une reconfiguration n'est pas exécutée.</p> <p> Vérifiez l'entrée d'un chemin valide, accessible pour tous les ordinateurs Security Platform, autrement la configuration de la sauvegarde échouera.</p> <p>Désactivé : Le chemin cible de sauvegarde peut être spécifié librement lorsque la fonction Sauvegarde est configurée.</p>
<p><i>Appliquer la</i></p>	<p>Activé : La sauvegarde secours du système sera mise à jour</p>

<p><i>sauvegarde système immédiate</i></p>	<p>immédiatement après les changements significatifs des données Security Platform.</p> <p> Conditions préalables : Les sauvegardes automatiques doivent être configurées. L'accès à la sauvegarde de secours du système doit être accordé.</p> <p>Désactivé : La sauvegarde secours du système ne sera pas mise à jour immédiatement après les changements significatifs des données Security Platform. Lorsque des sauvegardes automatiques sont configurées et l'accès en écriture à la sauvegarde de secours du système est permis, la sauvegarde sera mise à jour à la prochaine sauvegarde planifiée du système.</p>
<p><i>Utilisation de la clé publique du jeton de récupération d'urgence depuis l'archive</i></p>	<p>Activé : Entrez un chemin incluant le nom du fichier de clé publique, par exemple \\NomServeur\NomDossier\NomFichier.xml. Ce chemin cible sera appliqué lorsque la fonction Sauvegarde est configurée. Lorsque la fonction Sauvegarde est déjà configurée, ce paramètre n'aura aucun effet pour cet ordinateur.</p> <p> Vérifiez l'entrée d'un chemin valide, accessible pour tous les ordinateurs Security Platform, autrement la configuration de la récupération d'urgence échouera.</p> <p>Désactivé : Le jeton de récupération d'urgence peut être créé ou sélectionné lorsque la fonction Récupération d'urgence est configurée.</p> <p>Détails sur la configuration de la récupération d'urgence Comment créer un fichier archive de clé publique à partir d'un fichier jeton ?</p>
<p><i>Application de la configuration de réinitialisation mot de passe</i></p>	<p>Activé : La configuration de la réinitialisation du mot de passe est obligatoire dans le processus d'initialisation de la Security Platform. Lorsque la Security Platform a été déjà initialisée sans configurer la réinitialisation du mot de passe, il n'y a aucune obligation pour la configuration de la réinitialisation du mot</p>

de passe.

Désactivé : Aucune obligation pour la configuration de la réinitialisation du mot de passe. La réinitialisation du mot de passe peut être configurée après l'initialisation de la Security Platform via [Outil de paramétrage - Réinitialisation mot de passe - Configurer...](#).

Utilisation de la clé publique du jeton de réinitialisation du mot de passe depuis l'archive

Activé : Entrez un chemin incluant le nom du fichier de clé publique, par exemple
\\NomServeur\NomDossier\NomFichier.xml.

Ce chemin sera appliqué lorsque la fonction Réinitialisation mot de passe est configurée.

Lorsque la fonction Réinitialisation mot de passe est déjà configurée, ce paramètre n'aura aucun effet pour cet ordinateur.



Vérifiez l'entrée d'un chemin valide, accessible pour tous les ordinateurs Security Platform, autrement la configuration de la réinitialisation mot de passe échouera.

Désactivé : Le jeton de réinitialisation du mot de passe peut être créé ou sélectionné lorsque la fonction Réinitialisation du mot de passe est configurée.

[Détails sur la configuration de la réinitialisation du mot de passe](#)

[Comment créer un fichier archive de clé publique à partir d'un fichier jeton ?](#)

Paramètres versions antérieures produit

Paramètres valides seulement pour les versions antérieures du produit.

Stratégie	Explication	Valeur par défaut
<i>Emplacement de fichier pour la sauvegarde de récupération d'urgence</i>	<p>Ce paramètre est applicable seulement pour les versions précédentes du logiciel de la solution Security Platform.</p> <p>Pour les versions précédentes, l'emplacement de fichier pour la sauvegarde de récupération d'urgence peut être configuré explicitement au cours de l'initialisation de la Security Platform. Avec cette stratégie, l'emplacement de fichier peut être appliqué obligatoirement.</p> <p>Pour la version actuelle, l'emplacement de fichier est configuré automatiquement.</p>	---
<i>URL à lancer à partir de l'assistant pour l'inscription de certificats</i>	Voir stratégies utilisateur .	Désactivé



Infineon Security Platform Solution - Administration stratégie

Stratégies utilisateur d'Infineon Security Platform

Les paramètres de stratégie utilisateur suivants sont pris en charge par le logiciel de la solution Infineon Security Platform.



Dans le [mode serveur](#), les stratégies utilisateur sont configurées au niveau du domaine par un administrateur de domaine via Trusted Computing Management Server. Notez que les paramètres autorisés uniquement pour le mode serveur sont décrits dans le fichier modèle administratif fourni par Trusted Computing Management Server.



Valeur par défaut: Lorsqu'une stratégie n'a pas été encore configurée explicitement (par exemple l'éditeur de Stratégie de groupe parent affiche l'état **Non configuré**), alors le logiciel de la solution Security Platform applique implicitement une valeur par défaut.

Paramètres pour toutes les versions

Paramètre valables pour la version en mode autonome ET pour la version en mode serveur.

Stratégie	Explication	Valeur par défaut
<i>Mot de passe utilisateur de base - Longueur minimale du mot de passe</i>	<p>Activé : Entrez la longueur minimale désirée pour le mot de passe utilisateur de base, par exemple 6. La longueur minimale du mot de passe est valide pour les mots de passe utilisateur de base configurés ou modifiés ultérieurement.</p> <p>Désactivé : La longueur minimale du mot de passe est 6 caractères.</p> <p>Détails sur la gestion du mot de passe</p>	Activé , 6 caractères
<i>Mot de passe utilisateur de base - Le mot de passe doit correspondre aux exigences de complexité</i>	<p>Activé : Les demandes concernant la complexité du mot de passe sont appliquées pour les mots de passe utilisateur de base configurées ou modifiées ultérieurement.</p> <p>Désactivé : Aucune demande concernant la complexité du mot de passe n'est pas appliquée.</p> <p>Détails sur la complexité du mot de passe</p>	Désactivé
<i>Mot de passe utilisateur de base - Age maximal mot de passe utilisateur de base</i>	<p>Détermine l'intervalle (en jours) d'utilisation d'un mot de passe utilisateur de base avant que le système exige son changement à l'utilisateur.</p> <p>Activé :</p> <ul style="list-style-type: none">• <i>Age maximal mot de passe utilisateur de base:</i> Saisissez l'âge maximal désiré pour le mot de passe utilisateur de base, par ex. 42 jours.• <i>Avertissement expiration mot de passe utilisateur de base :</i> Spécifiez avec combien jours avant l'expiration du mot de passe utilisateur de base doit-on notifier les utilisateurs, par ex. 7 jours.	Désactivé

	<p>Désactivé : Pas d'âge maximal mot de passe utilisateur de base, c.à.d les mots de passe n'expirent pas.</p>	
<p><i>Phrase de passe utilisateur de base - Longueur minimale de la phrase de passe</i></p>	<p>Activé : Entrez la longueur minimale désirée pour la phrase de passe utilisateur de base, par exemple 20. La longueur minimale de la phrase de passe est valide pour les phrases de passe utilisateur de base configurés ou modifiés ultérieurement.</p> <p>Désactivé : La longueur minimale de la phrase de passe est 20 caractères.</p> <p> Cette stratégie est pertinente seulement lorsque l'authentification étendue est utilisée. Détails sur l'authentification étendue</p>	<p>Activé, 20 caractères</p>
<p><i>Phrase de passe utilisateur de base - La phrase de passe doit correspondre aux exigences de complexité</i></p>	<p>Activé : Les demandes concernant la complexité sont appliquées pour les phrases de passe utilisateur de base configurées ou modifiées ultérieurement.</p> <p>Désactivé : Aucune demande concernant la complexité n'est pas appliquée</p> <p> Cette stratégie est pertinente seulement lorsque l'authentification étendue est utilisée. Détails sur la complexité du mot de passe Détails sur l'authentification étendue</p>	<p>Désactivé</p>
<p><i>Initialisation Rapide de Contrôle</i></p>	<p>Activé/Autoriser : Assistant Rapide d'Initialisation ou Assistant d'Initialisation de Security Platform et Assistant d'Initialisation Utilisateur peuvent être utilisés pour initialiser les plates-formes et utilisateurs.</p> <p>Activée / Renforcer : Assistant Rapide d'Initialisation doit être utilisé pour initialiser les plates-formes et / ou utilisateurs. Les fonctions disponibles (EFS, PSD) doivent également être</p>	<p>Activée / Autoriser</p>

	<p>configurées initialement avec l'Assistant Rapide d'Initialisation.</p> <p>Désactivé : Assistant Rapide d'Initialisation ne peut pas être utilisé pour initialiser les plates-formes et utilisateurs. L'Assistant d'Initialisation de Security Platform et l'Assistant Rapide Utilisateur doivent être utilisés à la place.</p>	
<p><i>Désactivation temporaire de la fonction Security Platform par l'utilisateur</i></p>	<p>Activé : L'utilisateur d'Infineon Security Platform peut désactiver les fonctions de sécurité activées jusqu'au prochain redémarrage de l'ordinateur.</p> <p>Désactivé : L'option de désactiver temporairement Infineon Security Platform n'est pas disponible dans l'interface utilisateur du logiciel de la solution Security Platform.</p> <p> Cette stratégie s'applique uniquement aux Security Platforms équipée d'un Infineon Trusted Platform Module 1,1.</p> <p>Lorsque l'utilisateur se déconnecte et qu'un autre utilisateur se connecte à son tour, les fonctions de sécurité désactivées restent dans cet état jusqu'au redémarrage de l'ordinateur.</p>	<p>Activé</p>
<p><i>Autorisation de la configuration de la messagerie électronique sécurisée</i></p>	<p>Activé : L'utilisateur peut configurer le fonction <i>Messagerie électronique sécurisée</i> de la Security Platform.</p> <p>Désactivé : L'utilisateur ne peut pas configurer cette fonction, mais une configuration antérieure peut être utilisée.</p>	<p>Activé</p>
<p><i>Autorisation de la configuration de l'EFS</i></p>	<p>Activé : L'utilisateur peut configurer la fonction <i>Cryptage de fichiers et de dossiers avec le système de fichiers de cryptage (EFS)</i> de la Security Platform.</p> <p>Désactivé : L'utilisateur ne peut pas configurer cette fonction, mais une configuration antérieure</p>	<p>Activé</p>

	<p>peut être utilisée.</p> <p> EFS n'est pas pris en charge dans les éditions familiales de Windows.</p>	
<i>Autorisation de la configuration du PSD</i>	<p>Activé : L'utilisateur peut configurer le fonction <i>Cryptage de fichiers et de dossiers (EFS) avec le Personal Secure Drive (PSD)</i> de la Security Platform.</p> <p>Désactivé : L'utilisateur ne peut pas configurer cette fonction, mais une configuration antérieure peut être utilisée.</p>	Activé
<i>Application de l'activation de la réinitialisation mot de passe</i>	<p>Activé : L'activation de la réinitialisation du mot de passe est obligatoire dans le processus d'initialisation de l'utilisateur. Lorsqu'un utilisateur de la Security Platform a été déjà initialisé sans activer la réinitialisation du mot de passe, il n'y a aucune application pour activer la réinitialisation du mot de passe.</p> <p>Désactivé : Aucune application pour l'activation de la réinitialisation du mot de passe. La réinitialisation du mot de passe peut être activée après l'initialisation de l'utilisateur via Outil de paramétrage - Réinitialisation mot de passe - Activer...</p>	Désactivé
<i>Application de l'authentification étendue</i>	<p>Activé : Les utilisateurs de la Security Platform doivent utiliser l'authentification étendue (avec la phrase de passe utilisateur de base).</p> <p>Désactivé : Les utilisateurs de la Security Platform peuvent décider lorsqu'ils désirent utiliser l'authentification étendue (avec la phrase de passe utilisateur de base) ou authentification mot de passe (avec mot de passe utilisateur de base).</p> <p>Cette stratégie est relevante seulement lorsqu'au</p>	Désactivé

	<p>moins un dispositif d'authentification a été activé; pour tous les utilisateurs. Lorsqu'un utilisateur de Security Platform a été déjà initialisé sans sélectionner un dispositif d'authentification, il n'y a aucune obligation d'utiliser l'authentification étendue.</p> <p>Détails sur l'authentification étendue</p>	
<p><i>Permettre la mise en cache du mot de passe utilisateur de base</i></p>	<p>Activé : Le mot de passe utilisateur de base peut être mis en cache dans le logiciel Infineon Security Platform, en diminuant le numéro d'entrées du mot de passe au cours de la session ouverte actuellement. Ceci réduit le numéro d'entrées du mot de passe pour l'utilisateur.</p> <p>Désactivé : Le dialogue Mot de passe utilisateur de base n'offre pas la possibilité de mettre en cache le mot de passe utilisateur de base.</p>	<p>Activé</p>
<p><i>URL à lancer à partir de l'assistant pour l'inscription de certificats</i></p>	<p>Activé : Ce paramètre spécifie l'adresse web qui est utilisée par l'Assistant Initialisation de l'utilisateur d'Infineon Security Platform pour récupérer des certificats à l'aide d'un navigateur web.</p> <p>Cette page d'obtention d'un certificat est disponible seulement dans l'Assistant d'initialisation de l'utilisateur lorsque ce paramètre est activé et au moins une fonction de sécurité a été sélectionnée pour configuration.</p> <p>Désactivé : La page pour l'obtention d'un certificat n'est pas disponible dans l'assistant d'initialisation de l'utilisateur de l'Infineon Security Platform.</p> <p>Remarques:</p> <ul style="list-style-type: none"> • Ce paramètre est pris en charge également comme stratégie système pour être compatible avec les versions précédentes du logiciel de la solution Security Platform. 	<p>Désactivé</p>

	<ul style="list-style-type: none"> • Recommandation: Utilisez ce paramètre comme stratégie utilisateur. • Lorsque ce paramètre est indépendant de l'utilisation du certificat, il y a également une stratégie d'utilisateur spéciale pour les certificats EFS (<i>Type et inscription des certificats EFS</i>). 	
<p><i>Type et inscription des certificats EFS</i></p>	<p>Activé : Vous pouvez limiter le type de certificat EFS. Vous pouvez activer également l'inscription des certificats EFS externes en spécifiant l'adresse web de l'autorité de certification.</p> <p>1. Type certificat EFS : Indiquez si vous voulez permettre tous les types des certificats (certificats domaine, externes et auto-signés) ou seulement quelques types de certificats. Cette limitation est valide seulement lorsque les utilisateurs vont inscrire ou sélectionner les certificats.</p> <ul style="list-style-type: none"> • Certificat domaine : Un certificat inscrit via une autorité de certification dans votre domaine. • Certificat externe : Un certificat inscrit via une autorité de certification accessible via le web. • Certificat auto-signé : Un certificat créé sur votre ordinateur. <p>2. URL demande certificat : Entrez l'adresse web de demande certificat d'une autorité de certification à utiliser pour l'inscription du certificat EFS, par exemple https://www.companynome.com/foldername. Ce chemin cible sera utilisé lorsqu'un certificat EFS est demandé depuis une autorité de certification externe.</p> <ul style="list-style-type: none"> • L'URL de demande certificat est optionnel. 	<p>Désactivé</p>

	<ul style="list-style-type: none"> • Lorsque vous ne spécifiez pas un chemin ici, les utilisateurs ne pourront pas demander des certificats EFS externes. • Lorsque vous désirez activer les certificats EFS externes, entrez un chemin valide, accessible pour tous les ordinateurs Security Platform, autrement l'inscription du certificat EFS échouera. <p>Désactivé : Le type de certificat EFS n'est pas limité. L'adresse web à utiliser pour récupérer les certificats EFS n'est pas configurée, par exemple les utilisateurs ne peuvent pas demander des certificats EFS externes.</p> <p>Remarques:</p> <ul style="list-style-type: none"> • Les certificats EFS ne sont pas utilisés seulement pour l'EFS, mais également pour le PSD. • Lorsque ce paramètre est valable seulement pour les certificats EFS (à utiliser pour l'EFS ou le PSD), il y a également une stratégie utilisateur indépendant de l'utilisation du certificat (<i>URL à lancer à partir de l'assistant pour l'inscription de certificats</i>). <p>Comment inscrire et sélectionner un certificat EFS</p>	
<p><i>Apparition de l'avertissement expiration du certificat EFS</i></p>	<p>Activé : Les utilisateurs de Security Platform seront avertis par une info-bulle avant l'expiration de leur certificat EFS. Spécifiez quand l'avertissement doit se produire, par exemple 14 jours avant l'expiration du certificat EFS.</p> <p>Désactivé : Aucun avertissement sur l'expiration du certificat.</p>	<p>Les utilisateurs sont avertis 14 jours avant l'expiration du certificat.</p>
<p><i>Intervalle de validité pour les</i></p>	<p>Activé : Spécifiez la durée pour laquelle les certificats EFS auto-signés doivent être valides.</p>	<p>Activée avec une</p>

<i>certificats EFS autosignés</i>	Désactivé : La période de validité est de 10 ans.	période de validité de 10 ans.
<i>Emplacement fichier pour Personal Secure Drive</i>	<p>Activée/Lecteur PSD par défaut : Ce paramètre définit le lecteur par défaut dans lequel les fichiers image du Personal Secure Drive seront créés. Saisissez une lettre de lecteur valide dans le champ d'édition avec un deux-points sans spécifier de chemin supplémentaire (p.ex. C:). Si la lettre de lecteur n'est pas valide, l'utilisateur ne pourra pas créer le fichier image du Personal Secure Drive.</p> <p>Désactivé : L'utilisateur peut sélectionner le lecteur cible dans lequel les fichiers image du Personal Secure Drive seront créées.</p>	Désactivé
<i>Espace minimale disponible après la création du PSD</i>	<p>Activé : Lorsqu'un PSD est sauvegardé sur le lecteur système (sur lequel est localisé le système d'exploitation actuel), alors une quantité d'espace disponible doit être laissée après la configuration du PSD. Spécifiez combien d'espace disponible doit être laissé sur le lecteur système après la configuration du PSD.</p> <p>Désactivé : Il n'y a aucune exigence concernant l'espace disponible sur la partition système après la création du PSD.</p> <p><u>Exemple :</u> La stratégie est activée et configurée à 5000 Mo. La taille minimale de l'unité PSD est de 20 Mo pour Windows 7 et Windows Vista et 10 Mo pour tous les autres systèmes d'exploitation.</p> <ul style="list-style-type: none"> • Si l'espace disponible avant la création du PSD est 5050 Mo, alors la taille maximale du PSD sera 50 Mo. • Si l'espace libre est 5000 Mo, vous ne pourrez pas créer un PSD sur le lecteur système. 	La stratégie est activée et configurée à 5000 Mo.

<p><i>Autorisation de l'importation de la clé pour l'utilisateur</i></p>	<p>Activé : Les utilisateurs de la Security Platform peuvent importer les clés privées dans la Security Platform. Les clés privées sont importées avec les certificats par le Visualisateur du certificat et sélection du certificat.</p> <p>Désactivé : Les utilisateurs de la Security Platform ne peuvent pas importer les clés privées dans la Security Platform.</p>	<p>Activé</p>
<p><i>Application du niveau élevé de protection de clé privée pour les clés de signature MS-CAPI</i></p>	<p>Activé : Toutes les clés utilisées exclusivement pour la signature d'opérations par l'interface MS-CAPI sont protégées par une protection de clé privée renforcée. Dans ce cas, la clé est protégée par son propre mot de passe, que soit être saisie chaque fois la clé est utilisée pour une opération de signature.</p> <p>Désactivé : Il n'y a pas de protection particulière pour les clés de signature.</p> <p> Ce mot de passe spécifique peut être mis en cache pour éviter des saisies répétées. Puisque le mot de passe n'est pas lié à la clé utilisateur de base, le mécanisme de mise en cache utilisé pour le mot de passe de cette clé n'affecte pas ce mot de passe.</p>	<p>Désactivé</p>
<p><i>Création de Clé Utilisateur de Base non migrable</i></p>	<p>Activé/ Sur demande : Les utilisateurs sont invités à créer leur Clé Utilisateur de Base non migrable, lorsqu'ils vont utiliser Infineon TPM Strong Cryptographic Provider pour la première fois. Notez que Strong Cryptographic Provider exige une Clé Utilisateur de Base non migrable.</p> <p>Activé / Automatique : Pour les nouveaux utilisateurs, la Clé Utilisateur de Base non migrable est automatiquement créée pendant l'initialisation de l'utilisateur. Pour les utilisateurs qui sont déjà initialisés, la Clé Utilisateur de Base</p>	<p>Activé/ Sur demande</p>

non migrable est créée sur demande.

Désactivé : Aucune Clé Utilisateur de Base non migrable n'est créée, c'est-à-dire qu'Infineon TPM Strong Cryptographic Provider ne peut pas être utilisé.

Paramètres pour la version en mode autonome

Paramètres valides seulement pour la version en mode autonome.

Stratégie	Explication	Valeur par défaut
<i>Apparition avertissement sauvegarde</i>	<p>Activé : Les utilisateurs de la Security Platform seront informés par une info-bulle lorsque la sauvegarde des informations d'identification et clés spécifiques à l'utilisateur a échoué (par exemple parce que le répertoire de sauvegarde n'est pas disponible). Spécifiez tous les combien doit-on exécuter cette notification, par exemple tous les 2 jours après l'échec de la sauvegarde, jusqu'à une sauvegarde est réussie.</p> <p>Désactivé : Aucune notification pour l'échec de la sauvegarde.</p>	Les utilisateurs sont notifiés quotidiennement.
<i>Permettre l'inscription de l'utilisateur</i>	<p>Activé/Autorisation pour l'interface et l'assistant de gestion : Les utilisateurs peuvent être initialisés via l'interface Management Provider, l'Assistant Initialisation rapide ou l'Assistant Initialisation utilisateur.</p> <p>Activer/Autoriser Management Provider uniquement : L'utilisateur peut seulement invoquer l'interface Management Provider, mais il ne peut pas exécuter les outils de la solution Security Platform.</p> <p>Désactivé : La Security Platform ne permet pas l'exécution d'aucune fonction.</p>	Activé/Autorisation pour l'interface et l'assistant de gestion



©Infineon Technologies AG

Infineon Security Platform Solution

Services d'intégration de Security Platform

Les services d'intégration de la Security Platform permettent aux applications standards d'utiliser la fonction Trusted Platform Module. Cela est possible pour les applications prenant en charge le Microsoft Crypto-API, Microsoft Cryptography Next Generation (CNG) API, ou le PKCS #11 Crypto-API.

La table suivante présente toutes les composantes des services d'intégration disponibles :

Nom du fournisseur	Explication	Crypto-API	Application/services pris en charge (exemples)
Infineon TPM Cryptographic Provider (CSP utilisateur, sans prendre en charge AES)	Utilisé pour les certificats utilisateurs. L' authentification utilisateur est exigée pour utiliser la clé privée du certificat. La clé privée du certificat utilisateur peut être migrée, par exemple elle peut être transférée vers un autre Trusted Platform Module.	Microsoft Crypto-API	<ul style="list-style-type: none">• Cryptage de fichiers et dossiers avec EFS et PSD• Sécurisation de la messagerie électronique (S/MIME) avec Outlook et Windows Mail/Outlook Express• Authentification client SSL/TLS avec Internet Explorer• Inscription du certificat via le composant logiciel enfichable certificat Microsoft via des autorités de certification prenant en charge Internet Explorer
Infineon TPM RSA et AES Cryptographic Provider (CSP utilisateur, prenant en charge AES. pas disponible sous Windows 2000.)			

			<ul style="list-style-type: none"> • Macros signés dans Microsoft Word • Checkpoint VPN utilisant Microsoft Crypto-API • Applications client prenant en charge Microsoft Crypto-API • Signature numérique Adobe et cryptage fichier Adobe • Authentification utilisateur avec EAP-TLS
<p>Infineon TPM PKCS #11 Provider (nommé également "TPM Cryptoki Token")</p>		<p>PKCS #11 Crypto-API</p>	<ul style="list-style-type: none"> • Sécurisation de la messagerie (S/MIME) avec Mozilla Thunderbird • Authentification client SSL/TLS avec Mozilla Firefox • Inscription du certificat via autorités de certification publiques prenant en charge Mozilla Firefox • Inscription du certificat via une autorité de certification fondée sur Sun

			<p>Certificate Server</p> <ul style="list-style-type: none"> • Accès web sécurisé et accès à distance avec RSA SecurID • Applications client prenant en charge l'interface PKCS #11
<p>Infineon TPM Strong Cryptographic Provider (sans support AES)</p>	<p>Utilisé pour Certificats d'Utilisateurs. L'authentification d'Utilisateurs est exigée pour chaque utilisation de la clé privée du certificat. La clé privée du Certificat d'Utilisateurs ne peut pas être migrée, c'est-à-dire, lié au Trusted Platform Module.</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> • Spécialement destiné à l'authentification d'utilisateur dans un VPN.
<p>Infineon TPM Platform Cryptographic Provider (CSP plate-forme)</p>	<p>Utilisé pour les certificats ordinateur. Aucune autorisation dédiée exigée pour utiliser la clé privée du certificat, car la clé privée du certificat ordinateur est protégée par le Trusted Platform Module. La clé privée du certificat ordinateur ne peut pas être migrée, par exemple liée au Trusted Platform</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> • Authentification IEEE 802.11 EAP-TLS entre le client réseau local sans fil et le serveur RADIUS (dans la phase d'établissement d'une liaison TLS), dans une entreprise administrée, côté client du réseau local sans fil • Authentification

	<p>Module.</p> <p>Pour utiliser le CSP plate-forme, vous devez être un administrateur ou membre du groupe Administrateurs.</p>		<p>IEEE 802.1X EAP-TLS dans les réseaux locaux dans fil entre le client et le serveur RADIUS (dans la phase d'établissement d'une liaison TLS), dans une entreprise administrée, côté client</p> <ul style="list-style-type: none"> • Authentification ordinateur IPSec, côté client VPN
<p>Infineon TPM Key Storage Provider (KSP)</p>	<p>Key Storage Provider Limité.</p> <p>Fournit l'accès à d'autres Infineon TPM Cryptographic Service Providers seulement. Prend en charge seulement les opérations de signature et de chiffrement, mais non la création de paire de clé TPM RSA.</p>	<p>Microsoft Cryptography Next Generation (CNG) API</p>	<ul style="list-style-type: none"> • Microsoft .NET 3.0 • Pour plus d'exemples, voir d'autres Cryptographic Service Providers.

Pour autres application prises en charge, contactez votre assistance technique.



Infineon Security Platform Solution

Services de Security Platform

Les services de la Security Platform vous offrent une pile logicielle compatible avec le Trusted Computing Group (TCG).

La pile logicielle TCG (TSS) est représentée par les modules suivants :

- Fournisseur service couche logicielle TCG
- TSS Core Service
- Bibliothèque pilotes dispositif TSS

La pile logicielle TCG est une partie intégrante d'une plate-forme compatible TCG et elle fournit des fonctions qui peuvent être utilisées par les systèmes d'exploitation et les applications étendues.



Recommandation :

Contactez votre assistance technique pour vérifier lorsqu'une mise à jour est disponible pour le logiciel de votre Trusted Platform Module.



Infineon Security Platform Solution - Assistant Sauvegarde

Server Integration Services

La composante *Server Integration Services* communique avec Trusted Computing Management Server. Elle active l'intégration de Security Platform avec Trusted Computing Management Server (voir [mode serveur](#)).

Il s'agit d'une composante interne sans interface graphique utilisateur. Client Side Control Agent est une composante principale des Server Integration Services.

Nom de la composante	Explication
<i>Client Side Control Agent</i>	Synchronise l'état de la plateforme et les informations d'identification de l'utilisateur avec Trusted Computing Management Server (voir les états de session utilisateur).

Si Server Integration Services n'est pas inclus dans votre version d'Infineon TPM Professional Package logiciel, veuillez contacter votre distributeur pour les obtenir.

Pour en savoir comment installer Server Integration Services, veuillez consulter *ReadmeServerIntegrationServices.txt*. Pour identifier la version installée, consultez la version *Client Side Control Agent* listée dans *Plusieurs détails* dans [Outil de paramétrage](#).



Infineon Security Platform Solution

Utilisation des fonctionnalités de Security Platform dans vos applications

La solution Infineon Security Platform prend en charge la [fonctionnalité de clé publique fournie par Windows 2000/Windows XP](#) ainsi que la [fonctionnalité PKI basée sur la norme PKCS #11](#). Cette prise en charge englobe la chaîne complète de processus dont l'[inscription](#) des [certificats numériques](#), la configuration des services disponibles à l'aide de certificats, et l'administration des fonctions spécifiques à l'utilisateur de l'Infineon Security Platform.

Les applications utilisant des certificats numériques sont les suivantes :

- [Personal Secure Drive \(PSD\)](#)
- [Système de fichiers de cryptage \(EFS\)](#)
- [Messagerie électronique sécurisée](#)
- [Macros signés dans Microsoft Word](#)
- [Sécuriser les connexions réseau](#)



©Infineon

Infineon Security Platform Solution

Certificats et Infrastructure clé publique (PKI)

Pour pouvoir utiliser les fonctions de la Security Platform dans vos applications, vous devez demander un ou plusieurs certificats. Lorsque vous n'utilisez pas des certificats auto-signés ou des certificats d'une autorité de certification de votre domaine, vous avez besoin d'accéder une infrastructure clé publique.

Les certificats sont gérés par le [Visualisateur du certificat et sélection du certificat de la Security Platform](#).



Les sujets suivants fournissent des informations générales concernant les certificats et l'infrastructure clé publique, opérations conçues pour les administrateurs.

[Certificats numériques](#)

[L'infrastructure clé publique dans les systèmes d'exploitation Windows](#)

[L'infrastructure clé publique dans PKCS #11](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Certificats numériques

Les certificats numériques sont des informations d'identification électroniques confirmant l'identité d'un individu ou d'une société. Un certificat numérique crée le lien entre l'identité du propriétaire du certificat et une paire de clés électroniques qui peuvent être utilisées pour signer des informations numériques.

Un certificat numérique doit contenir les informations suivantes :

- Clé publique de l'utilisateur
- Nom de l'utilisateur
- Date d'expiration du certificat numérique
- Numéro de série du certificat numérique
- Nom de l'autorité de certification ayant émis le certificat
- Certificat numérique de l'autorité de certification ayant émis le certificat numérique

En plus de ces données, un certificat numérique peut aussi contenir d'autres informations fournies par l'utilisateur, telles que :

- Adresse postale
- Adresse électronique (pour certaines applications, le remplissage de ce champ est obligatoire)
- Informations d'inscription de base (telles que pays, âge, sexe, etc.)

Les certificats numériques sont généralement émis et gérés par une tierce partie de confiance appelée Autorité de certification. La procédure d'[obtention d'un certificat](#) peut être uniformisée pour la plupart de ces autorités. Il existe un nombre important de CA qui satisfont à la demande sans cesse croissante de certificats numériques en émettant des certificats dont l'utilisation va de la sécurisation du courrier électronique jusqu'à la sécurisation des communications par Internet ou sur un intranet.



©Infineon

Infineon Security Platform Solution

Obtention d'un certificat numérique depuis un CA publique

Pour utiliser la technologie clé publique fournie par Microsoft, vous devez obtenir d'abord un **ID numérique**. Suite à la demande croissante pour les ID numériques, une gamme large d'autorités de certification commerciales telles que VeriSign et Thawte offrent des certificats numériques pouvant être utilisés pour la sécurisation de la messagerie ou la signature des macros.

Les autorités de certification commerciales distribuent une gamme variée de types de certificats, incluant ici :

- Certificats personnels pour la signature numériques de la messagerie et l'échange sécurisé de l'information dans un réseau publique.
- Certificats d'authentification de clients et de serveurs, utilisés pour la transmission sécurisée de l'information entre les clients et les serveurs.
- Certificats d'éditeur de logiciels, utilisés par les compagnies commerciales fournissant leurs progiciels avec des signatures numériques.

Les autorités de certification distribuent également d'autres types de certificats. Chaque autorité de certification possède son propre déclaration sur les stratégie de certification, la base de son opération. Visitez le site web d'une autorité de certification et lisez sa déclaration sur les stratégie de certification avant de décider l'autorité à utiliser pour obtenir votre certificat.

Lorsque vous choisissez une autorité de certification, posez-vous les questions suivantes :

- Est-ce que l'autorité de certification est une organisation digne de confiance, fonctionnant avec une stratégie de certification répondant à vos besoins et d'une manière efficace dans votre région ?
- Est-ce que l'autorité de certification est connue ? Est-ce que la plus part du monde reconnaît votre autorité de certification comme une compagnie de bonne réputation est digne de confiance ? Lorsque vous choisissez une autorité de certification dont la réputation est dubitative, il est possible que les utilisateurs rejètent votre certificat.
- Est-ce que l'autorité de certification exige des informations détaillées de vous pour vérifier vos informations d'identification ?
- Est-ce que l'autorité de certification dispose d'un système de réception en ligne de demandes de certificats, par exemple demandes générées par un serveur de gestion des clés ? Un tel système pourrait économiser beaucoup

du temps et accélérer le processus de demande, obtention et installation de certificats.

- Est-ce que le coût du service de l'autorité de certification correspond à vos demandes ?

Une fois prise la décision sur l'identité de l'autorité de certification commerciale vous fournissant le certificat, vous pouvez lancer une demande pour cette autorité. Beaucoup d'autorités de certification prennent en charge la procédure d'inscription en ligne.



Sélectionnez un des [Cryptographic Service Providers](#) délivrés avec votre solution Security Platform pour l'utiliser pour votre certificat.

Une fois votre demande traitée, vous recevrez des instructions pour son installation et utilisation.



©Infineon

Technologies AG

Infineon Security Platform Solution

L'infrastructure clé publique (PKI) dans les systèmes d'exploitation Windows

Le système d'exploitation Microsoft Windows 2000 a mis en place une infrastructure complète de clé publique sur la plateforme Windows. Cette infrastructure améliore les services cryptographiques pour la clé publique de Windows, introduits dans les dernières années, en fournissant un set intégré de services et outils administratifs pour la création, le déploiement et la gestion des applications fondées sur les clés publiques.

C'est-à-dire les développeurs des applications peuvent profiter des mécanismes de sécurité partageant les secrets ou les mécanismes de sécurité fondés sur les clés publiques, selon le cas. En plus, les compagnies pourront administrer leur environnement et leurs applications avec des outils et des stratégies cohérentes dans l'organisation entière.

L'infrastructure de clé publique remplace les mécanismes de confiance et autorisation Windows existantes, fondés sur le contrôleur de domaine et la centre de distribution de clés Kerberos. L'infrastructure de clé publique coopère avec ces services et fournit une amélioration permettant aux applications de répondre aux nécessités extranet et internet. L'infrastructure de clé publique répond à la nécessité d'avoir une identification et une authentification extensibles et distribuées, une intégrité et une confidentialité en fournissant un cadre pour les services, la technologie, les protocoles et les standards vous permettant de déployer et gérer un système puissant et extensible de sécurité de l'information. Le support pour la création, le déploiement et la gestion des applications fondées sur les clés publiques est fourni uniformément sur les stations de travail et serveurs utilisant Windows 2000 ou Windows NT4.

Les certificats numériques, les listes de révocation de certificats et les autorités de certification font partie des composants de base d'une infrastructure de clé publique. Les administrateurs des systèmes d'entreprise doivent s'assurer qu'une infrastructure de clé publique est en place avant de commencer à utiliser le cryptage par clé publique dans leurs réseaux.

Plusieurs informations sur les concepts d'infrastructure de clé publique de Microsoft et les services de certificat sont disponibles sur Microsoft TechNet.

La mise en place d'une clé publique (PKI) dans une organisation comprend les étapes suivantes :

- Configuration d'Active Directory
- Installation d'une autorité de certification
- Changement du modèle de certificat utilisateur
- Inscription des certificats

Ce document présente quelques éléments listés ci-dessus et vous indique les liens vous fournissant plusieurs informations sur ces sujets.



©Infineon

Technologies AG

Infineon Security Platform Solution

Configuration d'Active Directory

Active Directory et le service de dossiers utilisé par Microsoft Windows 2000. Il représente la base de réseaux distribués Windows 2000. Active Directory facilite le stockage sécurisé, structuré et hiérarchique de l'information concernant les éléments dans les réseaux des compagnies, tels que les utilisateurs, les ordinateurs, les services, etc.

Active Directory doit être installé dans le domaine où vous désirez configurer une infrastructure de clé publique, parce que toutes les informations concernant l'emplacement et les stratégies des autorités de certification, les certificats et les listes d'annulation sont stockés dans Active Directory.

Une fois Active Directory installé pour votre domaine, vous devez y ajouter des utilisateurs. Vous pouvez utiliser le composant logiciel enfichable « Utilisateurs et ordinateurs Active Directory » pour ajouter, déplacer, supprimer ou modifier les propriétés des éléments comme les utilisateurs, les contacts, les groupes, etc.

Plusieurs informations sur Active Directory sont disponibles sur Microsoft TechNet.

L'étape suivante de la configuration d'une infrastructure de clé publique est l'installation d'une autorité de certification installer une autorité de certification.



©Infineon

Technologies AG

Infineon Security Platform Solution

Installation d'une autorité de certification

Une autorité de certification est un service émettant les certificats nécessaires pour exécuter une infrastructure de clé publique. Ces certificats sont émis d'habitude pour les demandeurs basés sur des critères établis. Une autorité de certification garantit la validité de la liaison entre la clé publique du sujet et les informations d'identification du sujet stockées dans le certificat émis. Une autorité de certification peut être une autorité de certification externe commerciale ou une autorité de certification gérée par votre compagnie. (Lorsqu'une autorité de certification est un point important de confiance dans une organisation, la plus part des compagnies opteront pour avoir leur propre autorité de certification).

L'infrastructure de clé publique de Windows 2000 suppose un modèle d'autorité de certification hiérarchique caractérisé par son extensibilité, une administration facile et la prise en charge des certificats émis par les autorités de certification commerciales tiers.

Windows 2000 prend en charge deux types de services d'autorité de certification : d'entreprise et individuels. La différence principale entre les deux services d'autorité de certification réside dans la manière d'émission des certificats. Une autorité de certification indépendante émet des certificats sans authentifier le demandeur et d'habitude un administrateur de l'autorité de certification doit approuver les demandes selon quelques informations supplémentaires.

Une autorité de certification d'entreprise exige l'existence d'un domaine Windows 2000 et authentifie le demandeur selon ses informations d'identifications pour la connexion dans la domaine. De plus, une autorité de certification d'entreprise utilise des modèles de certificat pour faire la différence entre les types différents de certificats selon leur utilisation prévue. Les utilisateurs peuvent obtenir des types différents de certification selon leurs droits d'accès dans un domaine et le but de l'utilisation de certificats.

Vous devez installer une autorité de certification d'entreprise lorsque vous désirez émettre des certificats seulement pour les utilisateurs ou les ordinateurs se trouvant à l'intérieur d'une organisation qui fait part d'un domaine Windows 2000. Vous devez installer une autorité de certification indépendante lorsque vous désirez émettre des certificats seulement pour les utilisateurs ou les ordinateurs se trouvant à l'intérieur d'un domaine Windows 2000.

Remarque : Une autorité de certification entreprise possède un modèle spécial

de stratégie appliquant l'exécution et l'émission des certificats. Les informations de stratégie utilisées par ces modules de stratégie sont stockées dans un objet autorité de certification dans l'Active Directory. Vous devez donc posséder un Active Directory et un serveur DNS fonctionnels pour configurer votre autorité de certification d'entreprise.

Consultez Microsoft TechNet pour instructions concernant l'installation d'une autorité de certification pour votre domaine.

L'étape suivante dans la configuration d'une infrastructure clé publique est le changement du modèle certificat utilisateur pour permettre l'utilisation des [Cryptographic Service Providers](#) délivrés avec la solution Security Platform.



©Infineon

Technologies AG

Infineon Security Platform Solution

Changement du modèle de certificat utilisateur

Avec l'[Assistant de demande de certificat](#), un utilisateur peut sélectionner seulement un des Cryptographic Service providers (CSP) stockés dans l'Active Directory pour le modèle de certificat adéquat. pour activer l'utilisation des [Cryptographic Service Providers](#) délivrés avec la solution Security Platform pour une demande de certificat utilisateur, le modèle de certificat utilisateur correspondant doit être modifié.

Comment éditer le modèle de certificat utilisateur stocké dans l'Active Directory ?

1. **Installation d'ADSI Edit**

Le modèle de certificat utilisateur peut être modifié en utilisant l'éditeur d'interface de services Active Directory (éditeur ADSI). Cet éditeur est un composant logiciel enfichable de Microsoft Management, composant de Support Tools localisés dans le dossier Support\Tools du CD du système d'exploitation Windows 2000 Server pour installer les outils, double cliquez sur l'icône Setup (installation) du dossier. pour informations sur l'installation et l'utilisation de Support Tools Windows 2000 et l'aide de Support Tools, voir le fichier Readme.doc dans le dossier Support\Tools du CD du système d'exploitation Windows 2000. pour plusieurs informations sur l'ADSI Edit, voir l'aide de Microsoft Windows 2000 Resource Kit Tools.

2. **Démarrez ADSI Edit**

Adsiedit.msc (le composant logiciel enfichable MMC pour ADSI Edit) essaie automatiquement de charger le domaine actuel dans lequel l'utilisateur est connecté. Lorsque l'ordinateur est installé dans un groupe de travail ou il n'est pas connecté dans un domaine, un message d'erreur "Le domaine spécifié n'existe pas" sera affiché à plusieurs reprises. pour éviter les problèmes dans un tel cas, ouvrez mmc.exe, ajoutez le composant logiciel enfichable ADSI Edit manuellement, effectuez les connexions pour vous avec les informations d'identification nécessaires et ensuite sauvegardez le fichier console. Ainsi vous aurez votre console par défaut fonctionnant avec ADSI Edit.

3. **Sélection du modèle de certificat utilisateur**

Dans Adsiedit.msc les noeuds suivants doivent être modifiés pour étendre un modèle de certificat :

CN=<Nom de modèle>, CN=Modèles de certificats, CN=Services de Clés publiques, CN=Services, CN=Configuration, DC=<nom du domaine>.

4. **Modifier le modèle de certificat utilisateur**

Cliquez avec le bouton droit de la souris sur l'entrée **CN=User** et dans le menu contextuel affiché cliquez sur l'élément **propriétés**.

Sélectionnez la propriété à afficher : *PKIDefaultCSPs*.

Editer l'attribut :

Ajoutez le texte suivant : *<n> Infineon TPM Cryptographic Provider* (où *<n>* est le numéro suivant dans la Liste des **valeurs**).

Exemple : La liste des **valeurs** contient déjà deux éléments :

1,*Microsoft Enhanced Cryptographic Provider v1.0*

2,*Microsoft Base Cryptographic Provider v1.0*

Ajoutez le texte suivant :

3,*Infineon TPM Cryptographic Provider*

Cliquez sur **Ajouter** et ensuite sur **Appliquer** pour mémoriser le changement du modèle de certificat.

L'autorité de certification est maintenant prête à lancer l'[inscription d'utilisateurs pour les certificats Security Platform](#).

Remarque : Lorsque vous désirez utiliser les [Cryptographic Service providers](#) délivrés avec la solution Security Platform avec autres modèles, les pas demandés sont similaires aux pas décrits ci-dessus pour l'Active Directory.



Infineon Security Platform Solution

Inscription des certificats

Les certificats représentent un mécanisme pour obtenir la confiance dans la relation entre une clé publique et l'entité propriétaire de la clé privée respective. Un certificat représente une déclaration signée numériquement par son émetteur, garantissant qu'une clé privée appartient au sujet qui possède le certificat. Les certificats contiennent d'habitude des informations sur l'identification de l'entité ayant accès à la clé privée correspondant à la clé privée mentionnée dans le certificat.

Un certificat utilisateur associé à un des [Cryptographic Service Providers](#) délivrés avec la solution Security Platform peut être inscrit en utilisant

- Le composant logiciel enfichable certificat exécuté dans Microsoft Management Console ou
- L'application web fournie par des systèmes d'exploitation Microsoft Windows Server.



Technologies AG

Infineon Security Platform Solution

Inscription des certificats utilisant Microsoft Management Console

Cette méthode d'applique seulement lorsque l'ordinateur local et l'autorité de certification se trouvent dans la même domaine Windows.

1. Lancez le composant logiciel enfichable certificat exécuté dans Microsoft Management Console
Lancez la Microsoft Management Console et ajoutez le composant logiciel enfichable certificats pour gérer les certificats pour mon compte utilisateur.
2. Lancer l'Assistant de demande de certificat
Cliquez avec le bouton droit de la souris sur le magasin logique **Personnel** et lancez l'**Assistant de demande de certificat** en cliquant sur **Demander nouvel certificat...**
3. Traiter la demande de certificat
Cliquez sur **Suivant** pour continuer.
4. Sélectionner le type du certificat **Utilisateur** et cochez l'élément **Avancé**.
Ainsi vous pouvez assigner ultérieurement le certificat à un des [Cryptographic Service Providers](#) délivrés avec la solution Security Platform.

Cliquez sur **Suivant** pour continuer.

5. Sélectionnez un des Cryptographic Service Providers délivrés avec la solution Security Platform à utiliser par le certificat demandé.
La longueur de la clé est configurée automatiquement à la longueur par défaut de la clé du CSP.



Lorsque les Cryptographic Service Providers délivrés avec la solution Security Platform ne sont pas listés, vérifiez si le modèle certificat utilisateur a été modifié.

Cliquez sur **Suivant** pour continuer.

6. Sélectionnez l'autorité de certification destinataire de la demande.

Cliquez sur **Suivant** pour continuer.

7. Entrez le nom et la description du nouveau certificat.
Cliquez sur **Suivant** pour continuer.

8. Finalisez la demande de certificat en cliquant sur **Terminer**.

Une confirmation est affichée, indiquant que la demande de certificat a été bien exécutée.



©Infineon Technologies AG

Infineon Security Platform Solution

Inscription des certificats en utilisant le navigateur web

Les sections suivantes présentent l'enregistrement de certificat en utilisant le standard Microsoft CA, qui peut être installé sur les systèmes d'exploitation Microsoft Windows Server (par ex. Microsoft Windows Server 2003).

Les autorités de certification publiques peuvent utiliser des interfaces web différentes.

1. **Démarrez Internet Explorer** Démarrez votre Internet Explorer et ouvrez la page d'accueil de votre autorité de certification entreprise. Sélectionner **Demandez un certificat** et cliquez sur **Suivant** pour continuer.
2. **Traiter la demande de certificat**
Sélectionner **demande certificat utilisateur** et cliquez sur **Suivant** pour continuer.



Lorsque vous sélectionnez **Demande avancée** votre demande est plus flexible et vous pouvez sélectionner ou configurer des paramètres d'une large gamme. Cette option doit être utilisée d'habitude pour pouvoir sélectionner un des [Cryptographic Service Providers](#) délivrés avec la solution Security Platform.

Cliquez sur **Plusieurs options** pour permettre l'association du Cryptographic Service Provider avec le certificat demandé.

Lorsque vous cliquez sur **Soumettre** les valeurs par défaut suivantes sont utilisées pour la demande de certificat :

CSP :	<i>MS Base Cryptographic Provider V1</i>
Longueur clé :	<i>Valeur par défaut par CSP</i>
Niveau élevé de protection de clé privée :	<i>Non</i>
Nom du conteneur :	<i>Un GUIDE aléatoire</i>

Le certificat sera assigné à *MS Base Cryptographic Provider V1*.

Sélectionnez un des Cryptographic Service Providers délivrés avec la solution Security Platform à utiliser par le certificat demandé.
La longueur de la clé est configurée automatiquement à la longueur par

défaut de la clé du CSP et le nom du conteneur est un GUID aléatoire.



Lorsque les Cryptographic Service Providers délivrés avec la solution Security Platform ne sont pas listés, vérifiez si le modèle certificat utilisateur a été modifié.

Finalisez la demande de certificat avec un clic sur **Soumettre**.

Une confirmation est affichée, indiquant que la demande de certificat a été bien exécutée.

Une fois reçu, le certificat peut être installé sur votre système en cliquant sur **Installer ce certificat**.



©Infineon Technologies AG

Infineon Security Platform Solution

L'infrastructure de clé publique (PKI) dans PKCS #11

La norme PKCS #11 définit une interface commune pour créer, utiliser et administrer des certificats et clés de cryptage. Chaque implémentation de cette interface fournit une approche spécifique de la technologie sous-jacente, PKCS #11 ne spécifiant pas le jeton de cryptage servant à la mise en oeuvre de la fonction centrale. Les solutions proposées sur le marché sont basées, tant sur des logiciels que sur des cartes à puce ou des circuits spécialisés de cryptage. Chaque bibliothèque conforme à PKCS #11 met en oeuvre sa propre façon d'inclure de tels dispositifs spéciaux et de les utiliser pour générer et traiter les données de cryptage appropriées.

Comme PKCS #11 définit une interface indépendante d'une plate-forme, il existe diverses solutions proposées par un large éventail de fabricants. Ainsi, la norme est prise en charge sur de nombreuses plates-formes et systèmes d'exploitation.

Les bibliothèques conformes à PKCS #11 proposent leur fonctionnalité à l'aide d'une interface bien définie. Selon l'objectif principal d'une mise en oeuvre, une bibliothèque PKCS #11 ne peut prendre en charge qu'un sous-ensemble de l'interface définie.

Pour créer une infrastructure de clé publique (PKI), les applications utilisant un module PKCS #11 requièrent l'accès à un stockage persistant, offrant un emplacement d'enregistrement des données sécurisé et fiable pour les certificats utilisateurs et les clés privées. PKCS #11 ne spécifie pas ce mécanisme de stockage. En tant que mécanisme fréquemment utilisé, les services d'annuaire ont prouvé leur utilité pour offrir la fonctionnalité requise. L'accès à de tels services d'annuaire est très souvent mis en oeuvre par le protocole d'accès LDAP.

Windows 2000 / XP ne contient pas de bibliothèque native PKCS #11, si bien que cette fonctionnalité doit être ajoutée en faisant appel à des produits tiers. Le logiciel de la solution Security Platform comprend une bibliothèque mettant en oeuvre l'interface PKCS #11 qui utilise le circuit Security Platform pour exécuter les opérations de cryptage les plus sensibles telles que générer des clés.

Plusieurs implémentations indépendantes de la norme peuvent se trouver sur le même système. Il est fréquent que les applications utilisant ces bibliothèques doivent être configurées lors d'une étape spécifique pour accéder correctement aux modules respectifs.

Les applications basées sur PKCS #11 doivent néanmoins mettre en oeuvre un

ensemble d'outils d'administration afin de générer les données requises pour gérer la fonctionnalité PKCS #11.

Les développeurs d'applications peuvent profiter de l'ensemble des fonctions des mécanismes de sécurité basés sur PK en utilisant différents modules de mise en oeuvre, sans devoir apporter le moindre changement à la plate-forme ou au système de logiciels sur la ou lequel(le) ils travaillent. Qui plus est, les entreprises seront également en mesure de gérer leurs environnement et applications avec des outils et stratégies cohérents pour toute l'organisation.

Pour que d'autres utilisateurs puissent lire les messages cryptés ou vérifier le courrier électronique signé, les certificats utilisateurs devront être stockés dans un répertoire public. Ce répertoire se trouve normalement sur un serveur accessible depuis l'intérieur de l'unité d'organisation concernée.

Les certificats numériques, les listes de révocation de certificats et les autorités de certification font partie des composants de base d'une infrastructure de clé publique. Les administrateurs des systèmes d'entreprise doivent s'assurer qu'une infrastructure de clé publique est en place avant de commencer à utiliser le cryptage par clé publique dans leurs réseaux.

La mise en place d'une clé publique (PKI) dans une organisation comprend les étapes suivantes :

- Installation d'un serveur de certificats
- Définition d'un fournisseur de services de certificats tiers
- Configuration de [Mozilla Firefox](#) pour utiliser la bibliothèque PKCS #11 d'Infineon Security Platform.
- Obtention de certificats auprès d'une autorité de certification pour l'authentification de clients.

Ce document de mise en route offre une vue générale sur certains des éléments listés ci-dessus et vous fournit des liens vers des sources d'information complémentaire sur ces sujets.



Après une mise à niveau du logiciel de solution Security Platform, les applications qui utilisent cette solution via l'interface PKCS#11 risquent de ne pas fonctionner comme prévu, car le fichier DLL PKCS#11 (*ifxtpmck.dll*) se trouve désormais dans le répertoire d'installation du logiciel de solution Security Platform. Dans les versions antérieures du produit, il se trouvait dans le répertoire *system32*. Les applications doivent donc être reconfigurées pour charger *ifxtpmck.dll* à partir du

nouvel emplacement.



©Infineon

Technologies AG

Infineon Security Platform Solution

Configuration de PKCS #11 dans Mozilla Firefox

La norme PKCS #11 définit des interfaces et technologies indépendantes d'une plate-forme pour la gestion d'éléments se rapportant à la sécurité pour un PKI dans un environnement distribué. Plusieurs solutions sont proposées par différents fabricants. Le logiciel de la solution Infineon Security Platform comprend une bibliothèque PKCS #11 (de fonctions logicielles) qui met en oeuvre l'ensemble des fonctions nécessaires à l'exécution d'un système Infineon Security Platform. Cette bibliothèque utilise le Trusted Platform Module pour la plupart des opérations se rapportant à la sécurité.

Mozilla Firefox a été conçu pour prendre en charge plusieurs bibliothèques PKCS #11. Une solution entièrement basée sur les mécanismes logiciels fait partie du produit standard.

La bibliothèque PKCS #11 contenue dans le logiciel de la solution Infineon Security Platform doit être configurée une seule fois dans Mozilla Firefox. Lors de cette opération, la bibliothèque PKCS #11 standard peut être désactivée, si elle n'est plus nécessaire. Cette décision doit être prise en accord avec l'administrateur de système.

Configuration de Mozilla Firefox

1. Démarrez Mozilla Firefox.
2. Sélectionnez **Outils > Options...** Le panneau Options s'ouvre.
3. Cliquez sur l'icône **Sécurité** dans le panneau Options.
4. Vérifiez **Utiliser un mot de passe master** afin de définir le mot de passe pour la protection de votre base de données du certificat.
5. Entrez un **nouveau mot de passe** deux fois pour confirmer. Seulement lorsque les valeurs entrées sont identiques, le bouton OK est active. Le **compteur de qualité du Mot de Passe** donne une indication du niveau de sécurité de la valeur actuellement saisie. Afin d'avoir le même niveau de sécurité pour ce mot de passe comme il est recommandé pour les mots de passe dans Infineon Security Platform Solution Software, certaines [règles de mot de passe](#) devraient être prises en considération. Si vous souhaitez changer un mot de passe déjà configuré, vous pouvez également saisir le **mot de passe actuel**.
6. Cliquez sur **OK**.

La configuration d'Messagerie électronique est décrite dans la section [Configuration d'messagerie électronique sécurisé](#).

Configuration de la gestion de certificat

Cette section explique la configuration de la manière de gérer les certificats dans Mozilla Firefox.

1. Cliquez sur l'icône **Avancé** dans le panneau Options afin de configurer l'environnement de gestion de certification.
2. Cliquez sur l'onglet **Chiffrement** . Pour la **Sélection de Certificat**, paramétrez le mode à **Demander à Tout Moment**. Cela garantit qu'aucune authentification client n'est faite sans connaissance de l'utilisateur.
3. Cliquez sur le bouton **Périphérique de Sécurité** afin d'ouvrir le Device Manager.
4. Cliquez sur le bouton **Chargement** afin d'ouvrir le dialogue de configuration pour un nouveau PKCS #11 Module.
5. Le **Nom du Module** est obligatoire, le **nom du fichier Module** est fixé à *IfxTPMCK.dll*. Si le module n'est pas localisé dans un dossier se trouvant dans le CHEMIN du système variable, vous pouvez utiliser le bouton **Parcourir** pour localiser le fichier. Confirmez vos paramètres avec **OK**.
6. Si le nom du module spécifié figure dans la liste des **Cryptographic Modules**, il est correctement configuré pour l'utiliser.



©Infineon

Infineon Security Platform Solution

Inscription des certificats

Les certificats représentent un mécanisme pour obtenir la confiance dans la relation entre une clé publique et l'entité propriétaire de la clé privée respective. Un certificat représente une déclaration signée numériquement par son émetteur, soulignant qu'une clé privée appartient à une personne ou entité qui possède le certificat. Les certificats contiennent d'habitude des informations sur l'identification de la personne ou de l'entité ayant accès à la clé privée correspondant à la clé privée mentionnée dans le certificat.

Un certificat utilisateur associé à un des [Cryptographic Service Providers](#) délivrés avec la solution Security Platform peut être inscrit en utilisant

- [Sun Certificate Server](#) ou
- [Autorités de certification publiques prenant en charge PKCS #11](#).



©Infineon

Technologies AG

Infineon Security Platform Solution

Inscription de certificats avec une autorité de certification utilisant le serveur de certificat Sun

Les sections suivantes décrivent la procédure d'inscription de certificats à l'aide de l'autorité de certification iPlanet. Ce produit est disponible pour différentes plates-formes (Windows 2000 / XP, Unix, Linux, ...).

L'accès est fourni à travers un navigateur web qui prend en charge la norme PKCS #11.

Inscription de certificats avec Mozilla Firefox

1. Vérifiez que Mozilla Firefox est bien installé.
2. Démarrez Mozilla Firefox.
3. Saisissez l'adresse web de votre serveur de certificat. Contactez votre administrateur de système si vous ne connaissez pas cette adresse. Le canal de communication est sécurisé par le cryptage SSL sur le port prédéfini 1025, si bien que l'adresse de votre certificat se présente ainsi : *https://nom_de_votre_serveur:1025*.
4. L'inscription du certificat peut s'effectuer juste après l'affichage de quelques messages.
5. Le certificat permet l'exécution d'une authentification de client auprès de l'autorité de certification. L'utilisateur peut définir le mode d'authentification.
 - Sélectionnez **Accepter ce certificat pour la session**, lorsque vous devez récupérer un nouveau certificat à chaque nouvelle session.
 - Sélectionnez ne pas **Accepter le certificat et ne pas connecter**, si vous voulez abandonner le certificat.
 - Sélectionnez **Accepter toujours ce certificat (jusqu'à son expiration)**, si vous voulez utiliser le certificat pour l'authentification de client jusqu'à son expiration.

Remarque: Un complément d'informations sur le niveau de sécurité des communications se trouve sur le serveur de l'autorité de certification.

Pour vérifier les propriétés d'une autorité de certification, exécutez les étapes suivantes :

1. Cliquez sur l'icône **Avancée** dans **Outils > Options...** et cliquez sur l'onglet **Chiffrement** .
2. Cliquez sur **Visualiser Certificats** afin d'ouvrir le Gestionnaire de Certificats et cliquez sur l'onglet **Autorités** .
3. Sélectionnez le mode de traitement de l'autorité de certification qui correspond à vos besoins ou qui a été défini par votre administrateur de système.

- Sélectionnez **Ce certificat permet d'identifier les sites webweb**, si vous voulez utiliser les certificats émis par l'autorité de certification pour une authentification à travers le web.
- Sélectionnez **Ce certificat permet d'identifier les utilisateurs mail**, si vous voulez utiliser les certificats émis par l'autorité de certification et qui sont utilisés pour signer et/ou crypter des messages électroniques.
- Sélectionnez **Ce certificat permet d'identifier les créateurs de logiciel**, si vous voulez utiliser les certificats émis par cette autorité de certification pour la gestion de logiciels certifiés.



Infineon Security Platform Solution

Inscription des certificats avec une autorité de certification publique prenant en charge PKCS #11

Les autorités de certification publiques offrent d'habitude une méthode d'inscription de certificats fondée sur une interface web.

L'interface web peut être identique avec, par exemple [Sun Certificate Server](#). L'adresse du service représente la différence. Les autorités de certification publiques offrent d'[habitude un service à](#) grande échelle pour les aspects de sécurité et certificats.

Le fournisseur du service peut offrir également un logiciel spécial à télécharger et installer qui automatise la communication et les demandes de certificats.



©Infineon

Technologies AG

Infineon Security Platform Solution

Présentation de votre Personal Secure Drive

Personal Secure Drive (PSD) provides fournit une zone de stockage protégé pour des données sensibles. Vous pouvez configurer un ou plusieurs Personal Secure Drives avec l'[Assistant d'Initialisation Utilisateur](#).

Lorsque vous configurez un Personal Secure Drive, il ressemble à tout autre lecteur sur votre PC : Vous pouvez créer des fichiers et dossiers sur votre Personal Secure Drive, et y accéder de la même manière qu'avec les fichiers et dossiers sur d'autres lecteurs. Il n'existe aucune limite quant aux types de fichiers pouvant être enregistrés sur le Personal Secure Drive.

Le Personal Secure Drive diffère cependant des lecteurs ordinaires sous deux aspects essentiels :

1. Les données sont cryptées
2. Ce lecteur ne peut être lu et accédé que par son utilisateur

Le cryptage

Les données sur le Personal Secure Drive sont automatiquement protégées à l'aide de techniques cryptographiques avancées basées sur les algorithmes d'AES et de RSA. Lorsque vous enregistrez un fichier ou dossier sur le Personal Secure Drive, il est immédiatement crypté. Vous pouvez créer des fichiers et dossiers sur le Personal Secure Drive, ou bien les copier des lecteurs ordinaires vers votre Personal Secure Drive. Dans les deux cas, ils seront automatiquement cryptés une fois enregistrés sur le Personal Secure Drive. De même, si vous accédez à des fichiers ou dossiers, ou si vous les copiez de votre Personal Secure Drive vers des lecteurs ordinaires, ils seront automatiquement décryptés. Il est inutile d'exécuter des procédures particulières pour protéger vos fichiers ou dossiers ; toutes les fonctions de cryptage et de décryptage sont traitées automatiquement.



Comment protéger les fichiers et dossiers existants : Déplacez les fichiers et dossiers existants vers votre PSD pour les protéger. Lorsque vous copiez des fichiers ou dossiers vers votre PSD sans les supprimer de leur emplacement original, les copies non cryptées resteront dans leur emplacement original.

Mode serveur

Dans le [mode serveur](#), les paramètres de PSD sont gérés par Trusted Computing Management Server. Les paramètres de PSD sont donc migrés automatiquement, comme les autres informations d'identification et certificats utilisateur (voir [La migration des clés vers autres systèmes](#)).



Le fichier image de l'unité PSD n'est pas migré.

Nous vous recommandons de configurer le PSD sur un support amovible (par ex. USB flash drive), ainsi vous pourrez prendre avec vous votre fichier image de l'unité PSD.

Si vous décidez configurer votre PSD sur un support fixe (par ex. votre disque dur local) et vous désirez l'utiliser sur une autre plateforme, vous devriez sauvegarder votre fichier image de l'unité PSD sur la première plateforme et le restaurer sur l'autre plateforme (Voir [Sauvegarde et restauration des données Security Platform](#)). Dans ce cas, vous travaillez sur copies physiques différentes de votre PSD.



©Infineon Technologies AG

Infineon Security Platform Solution

Avantages de l'utilisation du Personal Secure Drive

Que vous travailliez avec des données numériques à titre professionnel ou privé, vos données confidentielles doivent être sécurisées et protégées. L'unité personnelle sécurisée "Personal Secure Drive" offre une protection maximum parce que tous les fichiers de votre choix seront enregistrés sur un lecteur crypté et virtuel, créant ainsi un stockage de haute sécurité pour les données sensibles. Les avantages sont les suivants :

- Cryptage des lecteurs virtuels à l'aide d'une clé enregistrée de manière sécurisée AES (Advanced Encryption Standard).
- Codage de la clé de cryptage par l'intermédiaire de l'algorithme de RSA.
- Sécurité transparente - cryptage/décryptage automatique des données.
- Traitement de fichiers, même de grande taille, sans ralentissement apparent - parce que le cryptage et le décryptage sont effectués en même temps que l'opération.

Simplification de la protection des fichiers

Le Personal Secure Drive a été conçu pour fournir une interface utilisateur simple et intuitive, permettant de se concentrer sur le travail à faire sans être ralenti par des processus de sécurité fastidieux. Caractéristiques du Personal Secure Drive :

- Convivialité : Le Personal Secure Drive se comporte comme n'importe quel lecteur standard de Windows.
- Interface basée sur des assistants pour faciliter la gestion et la configuration.
- Intégration dans Microsoft EFS (Encrypting File System).

Sécurité élevée grâce au Trusted Platform Module

Le Personal Secure Drive est basé sur l'initiative la plus récente du consortium Trusted Computing Initiative - le Trusted Platform Module (TPM). Le Personal Secure Drive utilise le Trusted Platform Module comme noyau du processus de cryptage de fichier, garantissant ainsi que les données seront protégées contre tout accès non autorisé et qu'elles seront "verrouillées" sur le PC sur lequel elles ont été cryptées. Le Trusted Platform Module assure un degré de sécurité matériel pour vos données, surpassant toutes les méthodes logicielles de protection actuellement disponibles.

Avantages du Personal Secure Drive

- Permet le stockage sûr des données sur un PC local.
- Protection des données à l'aide du Trusted Platform Module (TPM) offrant une sécurité basée sur un circuit matériel.
- Interface conviviale facile à utiliser.
- Intégration complète dans l'environnement de Windows ; le Personal Secure Drive se comporte comme n'importe quel autre lecteur local.
- Cryptage/décryptage automatique des données pour les utilisateurs autorisés ; aucune action supplémentaire de protection des données n'est demandée aux utilisateurs finals.
- Sous-programmes de cryptage et décryptage très efficaces ; aucune perte de productivité ou de performance ressentie par l'utilisateur final.



©Infineon

Technologies AG

Infineon Security Platform Solution - Chargement et déchargement du PSD

Chargement et déchargement de votre Personal Secure Drive

Vous pouvez charger (monter) un décharger (démonter) explicitement votre Personal Secure Drive lorsque vous désirez limiter l'accès à vos données cryptées.

Avant que vous ne puissiez accéder à PSD, vous devez le charger. Le chargement d'un PSD exige votre autorisation. Une fois que le PSD est chargé, vous pouvez accéder à vos données chiffrées jusqu'à ce que vous déchargiez explicitement le PSD, ou sortiez ou fermiez votre ordinateur.

Comment charger votre PSD

Chargez votre PSD depuis la [pictogramme Zone de notification barre de tâches](#), élément menu **Personal Secure Drive - Charger** (si vous avez installé un Personal Secure Drive) ou **Personal Secure Drive - <Lettre de lecteur:Etiquette de lecteur> - Charger** (si vous avez installé plus qu'un Personal Secure Drives).

Après une authentification avec succès, Windows Explorer est lancé, en affichant votre PSD.

Chargement automatique du PSD à l'ouverture de session

Vous pouvez configurer le chargement automatique de votre PSD à l'ouverture de session Windows.

Configurez cette option via la [pictogramme Zone de notification barre de tâches](#), élément menu **Personal Secure Drive - Charger à l'ouverture de session** (si vous avez installé un Personal Secure Drive) ou **Personal Secure Drive - <Lettre de lecteur:Etiquette de lecteur> - Charger à l'ouverture de session** (si vous avez installé plus qu'un Personal Secure Drives). Lorsque cette option est configurée, un signe de coche est affiché à côté de **Charger à l'ouverture de session**.

Comment télécharger votre PSD

Déchargez votre PSD depuis la [pictogramme Zone de notification barre de tâches](#), élément menu **Personal Secure Drive - Télécharger** (si vous avez installé un Personal Secure Drive) ou **Personal Secure Drive - <Lettre de lecteur:Étiquette de lecteur> - Télécharger** (si vous avez installé plus qu'un Personal Secure Drive).

Dialogue Chargement du PSD

Lorsque votre PSD doit être chargé, le [dialogue d'authentification](#) pour l'utilisation des fonctionnalités de la Security Platform est affiché.

Dialogue Déchargement du PSD

Si votre PSD est déchargé, un dialogue affichant l'état de tous vos Personal Secure Drives chargés actuellement est affiché. Si vous continuez et un PSD à décharger dispose de fichiers ouverts, un message d'alerte est affiché.

Eléments de la boîte de dialogue Déchargement PSD	Explication
<input type="checkbox"/> <i>Personal Secure Drives</i>	Ici, vous pouvez voir l'état de tous les Personal Secure Drive chargés actuellement. Vérifiez tous les lecteurs que vous souhaitez décharger. Assurez-vous qu'aucun des lecteurs à décharger ne soit en cours d'utilisation. Vous pouvez mettre à jour la liste en cliquant sur la touche "F5".
<input checked="" type="checkbox"/> <i>Fermer ce dialogue après un déchargement réussi</i>	Cochez cette case, si vous souhaitez que le Dialogue de Déchargement de PSD soit automatiquement fermé après que les Personal Secure Drives ont été déchargés. Lorsque le déchargement du PSD échoue, le dialogue demeure et affiche un état d'erreur.
<input type="checkbox"/> <i>Décharger</i>	Cliquez sur Décharger pour continuer.
<input type="checkbox"/> <i>Fermer</i>	Cliquez sur ce bouton pour fermer le dialogue Déchargement PSD sans décharger votre PSD.



Infineon Security Platform Solution

Administration du Personal Secure Drive

Cette section traite les problèmes d'administration associés avec le Personal Secure Drive.

Stratégie

Les stratégies du Personal Secure Drive sont incluses dans l'[Administration de stratégie d'Infineon Security Platform](#).

Affectation des lettres lecteur au Personal Secure Drive

Lors de l'installation du Personal Secure Drive, vous êtes invité à choisir une lettre de lecteur dans une liste des lettres disponibles. Cette liste exclut les lettres des lecteurs actuellement utilisés ainsi que les lettres de lecteurs précédemment affectées à des périphériques remplaçables à chaud ou à des lecteurs amovibles. Ceci permet d'éviter des conflits de lettres de lecteur.

De plus, sept lettres non affectées sont marquées comme "non recommandées", afin de les réserver pour l'utilisation future par des périphériques échangeables qui n'ont pas encore été chargées. Ainsi, les conflits de lettres de lecteur peuvent être évités pour les périphériques remplaçables à chaud supplémentaires.

Le nombre de lettres de lecteur réservées à une utilisation future par les périphériques hot-swap supplémentaires est défini dans la clé de registre de Windows `HKEY_LOCAL_MACHINE\Software\Infineon\TPM Software\PSD\DLskip`. Pour augmenter ou diminuer le nombre de lettres de lecteur réservées, vous pouvez modifier la valeur de cette clé.

Remarque : La valeur par défaut pour cette clé de registre est 7; la valeur maximum autorisée est 9. Si la valeur de la clé dépasse ce maximum, elle sera par défaut remise à 9.



©Infineon

Technologies AG

Infineon Security Platform Solution

Récupération d'un Personal Secure Drive

Avec la Récupération du Personal Secure Drive vous pouvez récupérer vos données PSD lorsque les informations d'identification PSD sont perdues. La récupération de données est assurée par un agent de récupération. Un agent de récupération est un [rôle utilisateur](#) qui est autorisé à décrypter les données d'un autre utilisateur. Si l'utilisateur met à jour le système à partir d'une Home Edition vers un Système d'exploitation supérieur, par exemple de Windows XP Home à Windows XP Professional ou de Windows Vista Basic Home à Windows Vista Home Premium, les agents de récupération de Home deviennent invalides et l'utilisateur doit reconfigurer la récupération PSD comme décrit dans la table "Comment configurer et effectuer la Récupération PSD".



Conditions préalables pour la récupération du PSD :

- Au moins 1 agent de récupération PSD listé.
- Accès au fichier image PSD.

Un fichier image PSD perdu ou des données utilisateur perdues dans le fichier image peuvent être restaurées seulement à partir d'un fichier [sauvegarde d'image PSD](#).

Comment configurer et exécuter la récupération du PSD

Tâches de récupération PSD	Editions Windows ne prenant pas en charge EFS	Editions Windows prenant en charge EFS
Présentation	<ul style="list-style-type: none">• Des agents de récupération PSD dédiés sont utilisés. L'utilisateur de PSD doit enregistrer l'agent de récupération PSD.• Toutes les tâches sont exécutées dans l'outil ligne de commande Récupération PSD.	<ul style="list-style-type: none">• Des agents de récupération EFS sont utilisés.• Les agents de récupération sont gérés via Microsoft Security Settings.• La récupération PSD est exécutée via l'outil ligne de commande Récupération PSD.
Comment configurer les agents de récupération :		
Activation de la récupération	1. Configuration du PSD	1. Configuration du PSD

du PSD

2. Création du fichier certification de récupération et du fichier de récupération PKCS #12. Vous devez configurer un mot de passe pour protéger le fichier PKCS #12.

Ligne de commande :
PSDRecovery /R:filename

3. Enregistrement de l'agent de récupération PSD :
Ligne de commande :
PSDRecovery /A:filename.CER [/ID:driveID]

Remarque :
Vous pouvez exécuter d'abord l'étape 2 et ensuite l'étape 1.

2. Configuration d'agents de récupération EFS via Microsoft Security Settings :
Ligne de commande :
secpol.msc

3. [Chargement de votre PSD](#) pour faire les changements effectifs.

Remarques :
Vous pouvez exécuter d'abord l'étape 2 et ensuite l'étape 1. Dans ce cas l'étape 3 n'est plus nécessaire.
Windows 2000 EFS crée un agent de récupération par défaut ;
Windows 7, Windows Vista et Windows XP Professional ne le créent pas.

Afficher la

Visualiser les

<p>liste d'agents de récupération enregistrés</p>	<p>Afficher la liste d'agents de récupération enregistrés pour votre PSD. Ligne de commande : PSDRecovery /V [/ID:driveID]</p>	<p>agents de récupération EFS via Microsoft Security Settings : Ligne de commande : secpol.msc</p>	
<p>Suppression d'un agent de récupération enregistré</p>	<p>Supprimez un agent de récupération enregistré pour votre PSD. Ligne de commande : PSDRecovery /D:[name] [number] [/ID:driveID]</p>	<p>Supprimer les agents de récupération EFS via Microsoft Security Settings : Ligne de commande : secpol.msc</p>	
<p>Comment récupérer votre PSD :</p>	<ul style="list-style-type: none"> • Vérifiez que l'accès au certificat numérique de l'agent de récupération et à la clé privée affectée est assuré (par exemple vous devez importer le fichier de récupération PKCS #12). • Assurez l'installation de l'application du Personal Secure Drive. • Vérifiez l'accessibilité des données cryptées Personal Secure Drive à récupérer pour l'agent de récupération. 		
<p>Localisation du fichier image PSD</p>	<p>Les données cryptées pour un Personal Secure Drive sont localisées dans un seul fichier</p>	<p>Récupération des données PSD</p>	<p>Récupérez PSD dans u lecteur tem</p>

(avec l'extension * .FSF).
N'oubliez pas que les fichiers
* .FSF portent les attributs de
fichiers système et de fichiers
cachés et qu'ils ne sont
normalement accessibles qu'aux
utilisateurs possédant les droits
d'administrateur.

La localisation du fichier peut être
obtenue via l'outil ligne de
commande Récupération PSD :
PSDRecovery /L

Vous aurez
données PS
l'outil Récu
PSD est aci
vous pouve
vos donnée
copier dans
emplaceme
Ligne de co
PSDRecov
/M:DriveIn
[X:]

Syntaxe de l'outil ligne de commande Récupération PSD

PSDRecovery.exe est un outil ligne de commande similaire à cipher.exe d'EFS.



La syntaxe ne tient pas compte de la casse.

PSDRecovery /A:filename.CER [/ID:driveID]

Pris en charge seulement dans les éditions familiales de Windows ne prenant pas en charge EFS.

Enregistrement d'un agent de récupération en ajoutant le certificat du fichier spécifique *.CER à la liste d'agents de récupération à tous les Personal Secure Drives

filename.CER

Un nom de fichier avec l'extension .CER

/ID:driveID

Optionnel : Exécute l'action spécifique seulement pour le Personal Secure Drive avec l'ID du lecteur donné.

PSDRecovery /D:name [/ID:driveID]

PSDRecovery /D:number [/ID:driveID]

Pris en charge uniquement dans les éditions familiales de Windows.

Supprime l'agent de récupération spécifié de la liste d'agents de récupération PSD enregistrés. Le nom ou le numéro de séquence (affiché par PSDRecovery /V) doit être spécifié.

name

Le nom de l'agent de récupération est affiché avec PSDRecovery /V

number

Le numéro de séquence de l'agent de récupération est affiché avec PSDRecovery /V

Sans paramètre /ID, cette action est exécutée pour tous les Personal Secure Drives.

PSDRecovery /L

Listez ID, fichier d'image et chemin du fichier d'image pour tous vos Personal Secure Drives.

PSDRecovery /M:DriveImageFile.FSF [X:]

Récupère vos données PSD dans un nouveau lecteur temporaire non crypté.

DriveImageFile.FSF	Chemin complet du fichier image PSD comme affiché avec PSDRecovery /L
--------------------	---

X	La lettre de lecteur logique doit être affectée à un nouveau lecteur temporaire contenant les données récupérées (optionnel). Lorsqu'aucune lettre lecteur est fournie, la première lettre lecteur disponible sera utilisée.
---	--

PSDRecovery /R:filename

Pris en charge uniquement dans les éditions familiales de Windows.

Génère une clé et un certificat d'agent de récupération, ensuite elles sont écrites dans un fichier *.PFX (contenant le certificat et la clé privée) et un fichier *.CER (contenant seulement le certificat).

filename	Un nom de fichier (incluant facultativement le chemin complet) sans les extensions. Lorsque le chemin complet est spécifié, les fichiers de sortie seront écrits dans le répertoire spécifié. Autrement les fichiers de sortie seront écrits dans le répertoire courant.
----------	---

PSDRecovery /V [/ID:driveID]

Pris en charge uniquement dans les éditions familiales de Windows.

Affiche la liste d'agents de récupération PSD enregistrés. Les paramètres suivants sont affichés pour chaque agent de récupération : Un numéro de séquence, le nom de l'agent de récupération et une valeur de hachage du certificat.

Sans paramètre /ID, cette action est exécutée pour tous les Personal Secure Drives.



Infineon Security Platform Solution

Système de fichiers de cryptage

Les fonctions du système de fichiers cryptés (EFS) font partie de la technologie de sécurité des volumes NTFS. L'intégration se fait sans discontinuité et ne demande pas d'autre action qu'une unique étape de configuration. Utilisez EFS pour mettre vos documents à l'abri de tout intrus ayant éventuellement réussi à accéder physiquement et de façon non autorisée à vos données sensibles sauvegardées (en volant, par exemple, votre ordinateur portable). Lors de cette étape initiale, un volume ou un dossier est marqué comme étant crypté. A partir de là, tous les fichiers ou sous-dossiers à l'intérieur du volume ou dossier sélectionné sont cryptés.

Le travail avec un volume ou dossier crypté est tout à fait le même qu'avec un volume ou dossier non crypté - le cryptage est entièrement transparent pour l'utilisateur ayant l'autorisation d'accès.

Remarque :

- Il est recommandé d'utiliser le cryptage au niveau dossier ou volume, et non pas au niveau fichier. Pour simplifier, seuls ces éléments sont décrits ici.
- EFS n'est pas pris en charge dans les éditions familiales de Windows.



©Infineon

Technologies AG

Infineon Security Platform Solution

Fonctionnalité d'EFS

Il s'agit ici d'un extrait du chapitre original de l'aide de Microsoft sur l'EFS. Une aide complète est disponible sur la page d'aide de Microsoft. Pour obtenir les informations demandées en Aide Microsoft, minimiser toutes les fenêtres déjà ouvertes pour visualiser le Bureau Windows. Ensuite, appuyez sur F1 pour rechercher le mot-clé convenable.

- Les utilisateurs peuvent crypter leurs fichiers lorsqu'ils les sauvegardent sur disque. A cet effet, il suffit de cocher une case dans la boîte de dialogue des propriétés du fichier.
- L'accès aux fichiers cryptés est rapide et facile. Les utilisateurs voient leurs données en texte clair lorsqu'ils accèdent aux données à partir du disque.
- Le cryptage des données est effectué automatiquement et il est entièrement transparent pour l'utilisateur.
- Les utilisateurs peuvent décrypter un fichier en décochant la case de cryptage dans la boîte de dialogue des propriétés du fichier.
- Les administrateurs peuvent récupérer des données qui ont été cryptées par un autre utilisateur. Ainsi, les données restent accessibles même si l'utilisateur qui a crypté les données n'est plus disponible ou qu'il a perdu sa clé privée.
- Le système EFS ne crypte les données que si elles sont sauvegardées sur disque. Deux fonctions en option sont disponibles pour crypter les données lors de leur transmission sur un réseau TCP/IP : Internet Protocol Security (IPSec) et le cryptage PPTP.

Remarque : EFS n'est pas pris en charge dans les éditions familiales de Windows.



©Infineon

Technologies AG

Infineon Security Platform Solution

Utilisation du système de fichiers de cryptage

Quelques aspects doivent être pris en compte lorsque vous travaillez avec l'EFS. Certains d'entre eux n'intéressent que les administrateurs de système puisqu'ils sont importants lorsque l'EFS est installé.

Considérations de gestion

- Seuls les fichiers et dossiers sur volumes NTFS peuvent être cryptés
En principe, ce n'est pas une véritable restriction puisque le système de fichier NTFS est fortement recommandé comme système standard de fichier sous Windows 2000 ou XP. Un nombre considérable de fonctionnalités sans rapport avec la solution de sécurité est également basé sur NTFS.
- Un volume FAT invalide le cryptage dans tous les cas
Lorsqu'un fichier crypté est enregistré sur un volume FAT, la protection n'existe plus. Ceci s'applique en particulier aux disquettes qui sont généralement utilisées pour le transfert de petits fichiers. Mais les disques durs à multiples partitions peuvent également constituer un point faible si l'une des partitions est un volume FAT et que ce volume est utilisé pour le stockage de fichiers (même s'il s'agit d'un stockage temporaire).
- Les fichiers de système et les fichiers compressés ne peuvent pas être cryptés
Le dossier d'installation de Windows, tout comme un certain nombre de fichiers dans le dossier racine de la partition de démarrage, ne peuvent pas être protégés par le mécanisme d'EFS. Ceci n'invalide en aucun cas les fonctions de sécurité, car le système d'exploitation lui-même protège les fichiers système principaux avec des mécanismes spéciaux qui ne peuvent pas être arrêtés. Des informations supplémentaires sur ce sujet se trouvent dans les [Questions fréquentes](#).
- Les fichiers temporaires sont également une cible d'intérêt pour les attaquants potentiels
Pour empêcher toute faille dans la structure de sécurité de données, les dossiers et fichiers temporaires doivent aussi être cryptés. La plupart des applications utilisent les dossiers standard pour le stockage des fichiers temporaires. Le cryptage de ces dossiers augmente considérablement le niveau de sécurité d'un système. L'utilisation d'un dossier provisoire commun à tous les utilisateurs n'est pas recommandée puisque cela demande un effort administratif supplémentaire.

Considérations d'utilisation

Les utilisateurs travaillant avec des fichiers et dossiers cryptés doivent garder à l'esprit les informations et recommandations suivantes.

- Le cryptage est facile à configurer. Des informations plus détaillées sont disponibles dans l'aide EFS Microsoft.
- Seul l'utilisateur qui a crypté le fichier peut l'ouvrir. L'accès supplémentaire à d'autres utilisateurs est possible et doit être accordé manuellement, fichier par fichier.
- Les utilisateurs doivent utiliser les fonctions copier et coller pour conserver le cryptage lors du transfert des fichiers dans un dossier crypté. Si vous utilisez le mécanisme glisser - déplacer pour déplacer les fichiers, ceux-ci ne seront pas automatiquement cryptés dans le nouveau dossier.
- Si l'utilisation d'EFS est souhaitée sur des ordinateurs distants, cette fonctionnalité devra être manuellement configurée sur les systèmes distants.
- Il est recommandé aux utilisateurs de crypter le dossier **Mes documents** si c'est l'emplacement où ils sauvegardent la plupart de leurs documents. Ainsi, ils sont assurés que leurs documents personnels seront cryptés par défaut.

Les rubriques énumérées présentent une vue globale approximative sur la façon de travailler avec l'EFS. Des informations plus détaillées sont disponibles dans l'aide EFS Microsoft. Pour obtenir les informations demandées en Aide Microsoft, minimiser toutes les fenêtres déjà ouvertes pour visualiser le Bureau Windows. Ensuite, appuyez sur F1 pour rechercher le mot-clé convenable.

Quelques aspects techniques de l'EFS sont traités dans le chapitre [Dépannage](#).

Remarque : EFS n'est pas pris en charge dans les éditions familiales de Windows.



©Infineon Technologies AG

Infineon Security Platform Solution

Sécurisation de la messagerie

Le courrier électronique sécurisé est une des applications les plus populaires de toutes les applications activées par une clé publique car il permet aux utilisateurs de partager des informations de manière confidentielle et d'être sûrs que l'authenticité des informations a été préservée lors de leur transfert. Cette sécurité est obtenue grâce à des fonctions de cryptage et/ou de signature spécifiques à l'utilisateur, pour éviter la lecture ou la modification de vos messages par des personnes non autorisées. L'utilisation de cette fonction garantit que seul le créateur du message e-mail et les destinataires spécifiés seront autorisés à décrypter et à lire le message ou à valider l'identité de l'émetteur.

Dans ce document, on vous présente l'utilisation des [certificats numériques](#) et on vous explique, étape par étape, la configuration des applications [Microsoft Windows Mail/Outlook](#) et [Mozilla Thunderbird](#).



Technologies AG

Infineon Security Platform Solution

Sécurisez votre courriel avec Windows Mail /Outlook Express / Outlook

Ce chapitre décrit la façon de configurer Windows Mail / Outlook Express / Outlook pour sécuriser le courrier électronique et comment vous pouvez utiliser votre [certificat numérique](#) pour envoyer du courrier signé numériquement et des messages cryptés :

- [Configurez le Courriel sécurisé](#)
- [Envoi des Messages signés numériquement](#)
- [Envoi des Messages chiffrés](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Configurez le Courriel sécurisé

Vérifiez que vous avez déjà installé Windows Mail/Outlook Express/Outlook et vous l'avez configuré pour envoyer et recevoir les messages électroniques par votre serveur de courrier électronique. En outre, la présence d'au moins un certificat numérique est exigée pour continuer avec les instructions suivantes.

Remarque : Si vous ne possédez pas encore de certificat numérique susceptible d'être utilisé pour la sécurisation de la messagerie, procurez-vous un tel certificat avant de continuer les étapes de configuration.

☒ **Windows Mail/Outlook Express**

☒ **Outlook 2007**

☒ **Outlook 2003**

☒ **Outlook XP**

☒ **Outlook 2000**



©Infineon Technologies AG

Infineon Security Platform Solution

Envoi des Messages signés numériquement

⊕ **Windows Mail/Outlook Express**

⊕ **Outlook 2007**

⊕ **Outlook 2003**

⊕ **Outlook XP**

⊕ **Outlook 2000**



©Infineon Technologies AG

Infineon Security Platform Solution

Envoi des Messages chiffrés

Pour envoyer un message crypté à quelqu'un, vous devez avant tout disposer d'une copie de sa clé de cryptage publique ou de son certificat de cryptage (ce certificat contient une copie de sa clé publique). Assurez-vous de disposer du certificat de clé publique du destinataire et que celui-ci se trouve effectivement dans votre liste Contacts, avant d'effectuer les étapes mentionnées ci-dessous.

+ Windows Mail/Outlook Express

+ Outlook 2007

+ Outlook 2003

+ Outlook XP

+ Outlook 2000

Votre clé privée n'est pas nécessaire pour envoyer des messages électroniques, car le cryptage s'effectue à l'aide de la clé publique du destinataire. Par contre, vous avez besoin de votre clé privée pour lire un message électronique crypté, car le décryptage requiert la clé privée correspondant à votre clé publique qui a été utilisée pour crypter le courrier électronique.



Infineon Security Platform Solution

Sécurisez votre courriel avec Mozilla Thunderbird

Ce chapitre décrit la façon de configurer Mozilla Thunderbird Mail pour sécuriser le courrier électronique et comment vous pouvez utiliser votre [certificat numérique](#) pour envoyer du courrier signé numériquement et des messages cryptés :

- [Configurez le Courriel sécurisé](#)
- [Envoi des Messages signés numériquement](#)
- [Envoi des Messages chiffrés](#)



Technologies AG

Infineon Security Platform Solution

Configurez le Courriel sécurisé

Vérifiez si vous avez déjà installé Mozilla Thunderbird et si vous l'avez configuré pour envoyer et recevoir des messages à travers votre serveur électronique. La présence, en outre, d'au moins un certificat numérique est nécessaire avant de pouvoir exécuter les instructions suivantes.

Remarque : Si vous n'avez pas encore de certificat pouvant être utilisé pour la messagerie sécurisée, occupez-vous en avant de procéder aux étapes de configuration décrites ci-dessous.

Mozilla Thunderbird

1. Lancez le Mozilla Thunderbird.
2. Cliquez sur **Outils > Paramètres du Compte...** afin d'ouvrir le panneau des Paramètres du Compte.
3. Cliquez sur **Sécurité** dans le panneau à gauche sous votre nom du compte.
4. Cliquez sur le bouton **Sélectionner...** dans la zone **Signature numérique** afin de définir le certificat à utiliser pour la signature des messages électroniques. Une liste contenant tous les certificats disponibles apparaît. Sélectionnez un certificat, puis configurez la signature à l'aide du paramètre **Signer numériquement les messages (par défaut)**.
5. Dans la zone **Chiffrement**, vous pouvez configurer le niveau de cryptage.
 - A. Sélectionnez **Jamais (ne pas utiliser le chiffrement)** lorsque vous voulez définir le niveau de cryptage à la demande.
 - B. Sélectionnez **Obligatoire (Impossible d'envoyer un message sauf si tous les destinataires ont des certificats)** pour que tous vos messages électroniques soient cryptés automatiquement.

La configuration de PKCS #11 est décrite dans la section [Configuration de PKCS #11 pour Mozilla Firefox](#).



©Infineon

Technologies AG

Infineon Security Platform Solution

Envoi de Messages signés numériquement en utilisant Mozilla Thunderbird

1. Lancez le Mozilla Thunderbird.
2. Cliquez sur **Ecrire** dans la barre d'icônes ou **Fichiers > Nouveau > Message** pour obtenir un modèle de message vide.
3. Insérez la ou les adresse(s) du destinataire ou sélectionnez-les dans une liste à l'aide du bouton **A**.
4. Si vous voulez joindre une pièce, cliquez sur l'icône **Joindre** dans la barre d'icônes afin d'obtenir un dialogue de sélection de fichiers.
5. Saisissez votre texte dans le champ **Objet** et dans le **Contenu** du message.
6. Cliquez sur la petite **flèche à droite du bouton Sécurité** ou sélectionnez **Options > Sécurité** pour appeler le menu des options de sécurité. Sélectionnez **Signer ce message numériquement** pour signer votre courrier électronique. Il est représenté par un symbole de signature sur la partie droite de la barre d'état.

Infineon Security Platform Solution

Envoi de Messages chiffrés en utilisant Mozilla Thunderbird

1. Lancez le Mozilla Thunderbird.
2. Cliquez sur **Ecrire** dans la barre d'icônes ou **Fichiers > Nouveau > Message** pour obtenir un modèle de message vide.
3. Insérez la ou les adresse(s) du destinataire ou sélectionnez-les dans une liste à l'aide du bouton **A**.
4. Si vous voulez joindre une pièce, cliquez sur l'icône **Joindre** dans la barre d'icônes afin d'obtenir un dialogue de sélection de fichiers.
5. Saisissez votre texte dans le champ **Objet** et dans le **Contenu** du message.
6. Cliquez sur la petite **flèche à droite du bouton Sécurité** ou sélectionnez **Options > Sécurité** pour appeler le menu des options de sécurité. Cela est représenté par un symbole de signature dans la partie droite de la barre d'état.



©Infineon

Infineon Security Platform Solution

Macros signées dans Microsoft Word

Microsoft Word offre des mécanismes de sécurité qui permettent aux utilisateurs d'exécuter des macros, qu'elles soient ou non signées par un développeur de macros se trouvant sur une liste de sources approuvées. Un cachet numérique d'identification sur une macro confirme qu'elle provient du développeur qui l'a signée et qu'elle n'a pas été modifiée, garantissant ainsi l'authenticité de la macro et confirmant qu'elle ne contient pas de virus.

Le mécanisme de macros signées est pris en charge par Microsoft Word 2000 et Microsoft Word XP.



©Infineon

Technologies AG

Infineon Security Platform Solution

Configuration de Microsoft Word pour signer macros

Pour utiliser des macros signés, Microsoft Word doit être d'abord configuré. Cette fonction de sécurité est disponible seulement après la configuration?

Microsoft Word offre **trois niveaux de sécurité** pour vous permettre de réduire la possibilité d'infection de vos documents, modèles et suppléments par les virus de macro? Lorsque votre administrateur de système n'a pas appliqué un niveau de sécurité pour votre compagnie, vous pouvez modifier vous-même le niveau de sécurité. Lorsque le niveau de sécurité pour Microsoft Word est configuré à Moyenne ou Haute, vous pouvez gérer une liste de sources de macros de confiance. Lorsque vous ouvrez un document ou chargez un supplément contenant des macros développés par une de ces sources, les macros sont activés automatiquement.



©Infineon

Technologies AG

Infineon Security Platform Solution

Signature numérique d'un projet macro dans Microsoft Word

Niveaux de sécurité

1. Cliquez sur **Outils > Macro > Sécurité...** pour ouvrir la boîte de dialogue **Sécurité**.
2. Choisissez le niveau de sécurité dont vous avez besoin : élevé / moyen / bas.

Enregistrement d'une nouvelle macro

1. Ouvrez un nouveau document en cliquant sur **Nouveau document**.
2. Cliquez sur **Outils > Macro > Nouvelle macro...** (Commentaire dans **Microsoft Word 2007** : Cliquez sur **Visualiser > Macros > Record Nouveau Macro...**).
3. La boîte de dialogue **Enregistrer une macro** s'affiche.
4. Saisissez un nom de macro et cliquez sur le bouton **OK** pour fermer la boîte de dialogue.
5. Ecrivez le texte de la macro.
6. Cliquez sur **Arrêter l'enregistrement**.

Signer un (nouveau) Macro dans Microsoft Word 2007

1. Ouvrez le document ou modèle contenant le projet macro que vous souhaitez signer, si le fichier n'est pas ouvert.
2. Cliquez sur **Visualiser > Macros > Visualiser Macros**, le dialogue **Macros** apparaît.
3. Sélectionnez un **nom de Macro** dans la liste. Vous pouvez soit exécuter, éditer, créer ou supprimer un macro.
4. Cliquez sur le bouton **Editer** afin d'ouvrir une fenêtre **Visual Basic**. Maintenant éditez votre macro sélectionné.
5. Allez à l' **Explorateur de Projet** afin de sélectionner le projet que vous souhaitez signer.
6. Cliquez sur **Outils > Signature Numérique...** ans la fenêtre Visual Basic afin d'ouvrir le dialogue **Signature Numérique**.
7. Cliquez sur **Choisir...** afin d'ouvrir le dialogue **Sélectionner Certificat**.
8. Sélectionnez un certificat approprié dans la liste.
9. Cliquez sur **Visualiser Certificat** afin de visualiser les informations relatives au certificat dans le dialogue **Certificat**.
Commentaire : Cliquez sur l'onglet **Détails** afin de visualiser les informations relatives au certificat dans le dialogue **Certificat**. Cliquez sur le bouton **OK** afin de fermer ce dialogue.
10. Cliquez sur le bouton **OK** afin de fermer le dialogue **Sélectionner Certificat**.
11. Fermez le dialogue **Signature Numérique** en cliquant sur le bouton **OK**.
12. Afin d'enregistrer votre macro, cliquez sur **Enregistrer** et enregistrez le document ou modèle comme **Document Word Macro Activé**.
Commentaire : Comme **Microsoft Word** utilise votre clé privée afin de signer votre macro, vous devez insérer votre clé privée secrète.
13. Cliquez sur **Fichier > Fermer** pour retourner à Microsoft Word.

Signature d'une (nouvelle) macro

1. Ouvrez le document ou modèle contenant le projet de macro que vous voulez signer, si le fichier n'est pas ouvert.
2. Cliquez sur **Outils > Macro > Macros**. La boîte de dialogue **Macros** s'affiche.
3. Sélectionnez un **Nom de la macro** dans la liste. Vous pouvez exécuter, éditer, créer ou supprimer une macro.
4. Cliquez sur le bouton **Modifier** pour ouvrir une fenêtre **Visual Basic**. Vous pouvez maintenant modifier la macro sélectionnée.

Remarque: Vous pouvez également ouvrir la fenêtre **Visual Basic** en cliquant sur **Outils > Macro > Visual Basic Editor**.

5. Allez sur l'**Explorateur de projets** pour sélectionner le projet que vous voulez signer.
6. Cliquez sur **Outils > Signature numérique...** dans la fenêtre Visual Basic pour ouvrir la boîte de dialogue **Signature numérique**.
7. Cliquez sur **Choisir** pour ouvrir la boîte de dialogue **Sélectionner un certificat**.
8. Sélectionnez un certificat qui convient dans la liste.
9. Cliquez sur **Afficher le certificat** afin de visualiser les données de certificat dans la boîte de dialogue **Certificat**.

Remarque: Cliquez sur **Détails...** afin de visualiser les données de certificat dans la boîte de dialogue **Certificat**. Cliquez sur le bouton **OK** pour fermer cette boîte de dialogue.

10. Cliquez sur le bouton **OK** pour fermer cette boîte de dialogue.
11. Fermez la boîte de dialogue **Sélectionner un certificat** en cliquant sur le bouton **OK**.
12. Fermez la boîte de dialogue **Signature numérique** en cliquant sur le bouton **OK**.
13. Pour sauvegarder votre macro, cliquez sur **Enregistrement de Normal**.

Remarque: La macro peut être enregistrée dans le dossier de projet **Normal (Tous les documents (normal.dot))** ou dans le dossier de projet **Document**.

Etant donné que **Microsoft Word** utilise votre clé privée pour signer votre

- macro, vous devez saisir le code secret de votre clé privée.
14. Cliquez sur **Fichier** > **Fermer** pour revenir à Microsoft Word.



©Infineon Technologies AG

Infineon Security Platform Solution

Sécurisation des connexions réseau

Avec la solution Security Platform vous pouvez sécuriser les connexions réseau. Lorsque vous utilisez les services d'intégration de la Security Platform (par exemple les Cryptographic Service Providers pour Microsoft Crypto-API et PKCS #11 Crypto-API), alors les clés privées de vos certificats seront protégées par le Trusted Platform Module.

Les types suivants de réseaux sont pris en charge :

- [Navigateur Web /connexion serveur \(Authentification de clients\)](#)
- [Réseau privé virtuel \(VPN\)](#)
- [Réseau local sans fil \(WLAN\) ou réseau local câblé](#)

Vous pouvez utiliser les certificats utilisateurs pour vous authentifier et les certificats ordinateur pour authentifier votre ordinateur.

Les tables suivantes présentent les types de réseaux et certificats pris en charge :

Type de réseau	Service d'intégration de la Security Platform	Protocole	Type de certificat
Navigateur Web /connexion serveur (authentification de clients)	Infineon TPM Cryptographic Provider ou Infineon TPM RSA and AES Cryptographic Provider (fournisseurs de services cryptographiques utilisateur)	SSL/TLS	Certificat utilisateur
Navigateur Web /connexion serveur (authentification de clients)	Infineon TPM PKCS #11 Provider	SSL/TLS	Certificat utilisateur

VPN	Infineon TPM Cryptographic Provider ou Infineon TPM RSA and AES Cryptographic Provider (CSP utilisateur)	IPsec	Certificat utilisateur
VPN	Infineon TPM Platform Cryptographic Provider (Platform CSP)	IPsec	Certificat ordinateur
Réseau local sans fil ou câblé	Infineon TPM Cryptographic Provider ou Infineon TPM RSA and AES Cryptographic Provider (CSP utilisateur)	Réseau local sans fil : IEEE 802.11 EAP-TLS Réseau local câblé : IEEE 802.1X EAP-TLS	Certificat utilisateur
Réseau local sans fil ou câblé	Infineon TPM Platform Cryptographic Provider (Platform CSP)	Réseau local sans fil : IEEE 802.11 EAP-TLS Réseau local câblé : IEEE 802.1X EAP-TLS	Certificat ordinateur

Pur autres types de réseaux et zones applications, contactez votre assistance technique.



©Infineon Technologies AG

Infineon Security Platform Solution

Authentification des clients

Jusqu'à récemment, les réseaux informatiques ont utilisé une base de données centralisée des comptes pour gérer les utilisateurs, leurs privilèges et leurs contrôles d'accès. Cette technique est simple et efficace pour les réseaux de petite taille. Toutefois dans la situation actuelle, où les très grands réseaux avec des milliers d'utilisateurs sont monnaie courante, cette forme de contrôle centralisé devient difficile à administrer. Ce type de système est confronté à toute une gamme de problèmes allant de la difficulté de vérifier un compte par rapport à une base de données résidant sur Internet jusqu'à la gestion de listes interminables d'utilisateurs. Qui plus est, l'arrivée d'Internet a confronté les réseaux informatiques à d'éventuelles attaques provenant d'entités externes.

Utilisation du certificat

Les certificats de clé publique offrent une solution qui facilite sensiblement l'administration d'un grand nombre d'utilisateurs dans les réseaux de grande taille tout en réduisant le risque d'attaques sur les ID / mots de passe. Ces certificats peuvent être distribués à grande échelle, émis par de nombreuses autorités et vérifiés par un simple examen, sans devoir en référer à une base de données centralisée.

Les certificats peuvent être utilisés pour la sécurisation des communications et l'authentification utilisateur entre clients et serveurs sur le web. Ils permettent aux clients d'établir l'identité d'un serveur, car celui-ci présente un certificat d'authentification de serveur révélant sa source. Si vous connectez à un site web doté d'un certificat de serveur émis par une autorité de certification, vous pouvez être sûr que le serveur est vraiment géré par la personne ou société identifiée par le certificat. De la même manière, les certificats permettent aux serveurs de déterminer votre identité. Lorsque vous connectez à un site web, le serveur peut être sûr de votre identité s'il reçoit votre certificat de client. Le certificat utilisé pour authentifier l'identité d'un serveur s'appelle un **certificat de serveur** et la procédure de vérification de l'identité d'un serveur **Authentification serveur**. De même, le certificat utilisé pour authentifier l'identité d'un client s'appelle un **certificat de client** et la procédure de vérification de l'identité d'un client **Authentification client**.

Par exemple, si un serveur web veut restreindre l'accès aux informations ou services à des utilisateurs ou clients spécifiques, il demandera un certificat client au cours de l'établissement de la connexion sécurisée (par ex. SSL).

Alors que l'authentification serveur assure une transmission sécurisée des données, l'authentification client augmente la sécurité de telles transactions en ligne.

Assignation de certificats à des comptes utilisateurs

La technologie de clé publique a apporté des solutions à bon nombre de problèmes de sécurité des réseaux de grande taille. Des certificats peuvent être utilisés pour garantir l'identité d'une entité et vérifier son authenticité sans avoir besoin de grandes bases de données ainsi que de listes des comptes utilisateurs et de leurs privilèges d'accès.

Toutefois, les systèmes d'exploitation et outils d'administration existants sont équipés pour travailler uniquement avec des comptes utilisateurs et non pas avec des certificats. La meilleure solution pour conserver les avantages à la fois des certificats et des comptes utilisateurs est d'assigner (ou mapper) un certificat à un compte utilisateur. Cette procédure permet au système d'exploitation de continuer à utiliser les comptes tandis que le système (dans le sens plus large) et l'utilisateur font appel à des certificats.

Dans ce modèle, un certificat qui a été émis pour un utilisateur sera assigné au compte réseau de cet utilisateur. Lorsqu'un utilisateur présente son certificat, le système interroge le mappage (assignations) et détermine quel compte doit être connecté.

La présente documentation de mise en route présente des approches différentes sur ce thème. Elle explique comment IIS et Active Directory peuvent être préparés pour l'authentification client ainsi que l'utilisation de l'authentification client avec Internet Explorer.

- [Affectation de certificats aux comptes utilisateurs dans IIS et Active Directory](#)
- Authentification des clients avec Internet Explorer

Pour un environnement PKCS #11 avec Mozilla Firefox, l'assignation du certificat utilisateur et l'authentification client sont également traitées.

- [Affectation de certificats aux comptes utilisateurs dans Mozilla Firefox](#)
- [Authentification client avec Mozilla Firefox](#)



Infineon Security Platform Solution

Authentification de clients dans Internet Explorer

Lorsque le serveur web exige un certificat du client, Internet Explorer signe un message avec la clé privée correspondant au certificat client fourni pour assurer que l'utilisateur est le vrai propriétaire du certificat client.

Plusieurs informations sur l'authentification de clients avec Internet Explorer sont disponibles dans Microsoft TechNet.



Technologies AG

Infineon Security Platform Solution

Mappage des certificats pour les comptes utilisateurs dans IIS et Active Directory

Le mappage d'un certificat à l'utilisateur de Windows 2000 / XP est effectué soit avec le service Active Directory de Windows 2000 / XP, soit avec les règles définies dans Internet Information Services (IIS).

Vous pouvez choisir de mapper les certificats aux comptes utilisateurs dans IIS ou Active Directory, fonction de l'exécution de l'authentification de clients pour utilisateurs inclus dans votre domaine ou pour des entités externes n'étant pas partie de votre partie. Le mappage du certificat avec Active Directory sera idéal lorsque vous désirez authentifier les utilisateurs de votre domaine. Vous devez utiliser le mappage IIS lorsque vous désirez authentifier des utilisateurs qui ne font pas partie de votre domaine.

Remarque: L'authentification de clients avec IIS implique l'utilisation de Secure Sockets Layer (SSL) sur votre serveur web, c'est-à-dire vous devez obtenir un certificat serveur depuis une autorité de certification. Cette condition est nécessaire car l'authentification serveur utilisant un certificat serveur est obligatoire pour une connexion SSL et l'authentification client est seulement une mesure supplémentaire de sécurité.

Plusieurs informations sur le « Mappage des certificats pour les comptes utilisateurs dans IIS et Active Directory » et « Internet Information Service » sont disponibles dans Microsoft TechNet.



Infineon Security Platform Solution

Authentification des clients avec Mozilla Firefox

Si le serveur web demande un certificat de client, Mozilla Firefox signera un message avec la clé privée qui correspond au certificat de client configuré, afin de garantir que l'utilisateur est le vrai propriétaire du certificat de client.

Selon la configuration du cache de mots de passe, il se peut qu'on vous demande de saisir le mot de passe de la base de données de certificats chaque fois que le certificat de client est requis pour une authentification. Sinon, il ne sera demandé qu'à la première authentification.

Si vous avez déjà assigné l'utilisation d'un certificat à une page web spécifique, ce certificat sera sélectionné automatiquement. Sinon, il vous sera demandé de fournir le bon certificat. Les explications dans [Assignation de certificats à des comptes utilisateurs et pages web](#) vous aident à exécuter les étapes nécessaires pour configurer correctement votre environnement sécurisé.



©Infineon

Technologies AG

Infineon Security Platform Solution

Affectation de certificats aux comptes utilisateurs dans Mozilla Firefox

L'affectation d'un certificat à un compte utilisateur se fait automatiquement parce que le certificat est enregistré dans la base de données locale du certificat de l'utilisateur. L'accès à cette base de données est protégé par un mot de passe spécifique à l'utilisateur. Tant que l'ordinateur n'est pas modifié, les certificats se trouvant dans l'emplacement local des certificat restent disponibles.

Dans le réseau étendu d'une société, le besoin peut émerger d'avoir les certificats disponibles non seulement sur un ordinateur local, mais aussi sur chaque système connecté au réseau. Si les structures administratives ne fournissent pas de dossiers partagés pour l'enregistrement des profils utilisateur, les certificats utilisateurs devront être exportés de l'ordinateur de l'utilisateur vers un annuaire de l'entreprise. Ce service d'annuaire fournit alors un service central d'authentification ou bien permet la réimportation d'un certificat utilisateur sur un autre ordinateur.

Méthode alternative : Les profils utilisateur enregistrés dans un dossier partagé (profils itinérants) réduisent les efforts administratifs au strict minimum. La base de données des certificats utilisateurs ainsi que TOUTES les autres données spécifiques aux utilisateurs enregistrées dans un tel dossier, garantissent un accès cohérent à partir de n'importe quel point du réseau d'entreprise.

Remarque : L'authentification du client fait appel à l'utilisation de Secure Sockets Layer (SSL) de votre serveur web, ce qui signifie que vous devrez obtenir un certificat de serveur par une autorité de certification. Cela est dû au fait que l'authentification de serveur utilisant un certificat de serveur est obligatoire pour toute connexion SSL et que l'authentification du client n'est qu'une mesure de sécurité supplémentaire.

Infineon Security Platform Solution

Réseau privé virtuel (VPN)

Un VPN est un réseau privé virtuel qui utilise le réseau public (généralement l'Internet) pour interconnecter des sites ou utilisateurs distants. Au lieu d'utiliser une connexion matérielle dédiée telle qu'une ligne allouée, un VPN utilisera des connexions "virtuelles" routées via l'Internet depuis le réseau privé de l'entreprise jusqu'au site ou employé distant.

L'accès distant est également appelé réseau privé virtuel commuté (Virtual Private Dial-up Network -VPDN). Il s'agit d'une connexion utilisateur-LAN utilisée par les entreprises ayant, par exemple, des employés qui ont besoin de se connecter au réseau privé à partir de divers sites distants. En général, une société qui désire mettre en oeuvre un grand réseau VPN d'accès distant sous-traitera ces travaux à un prestataire de services ESP. L'ESP installera un serveur d'accès au réseau (NAS) et fournira un logiciel client pour les ordinateurs des utilisateurs distants.



Infineon Security Platform Solution

Protocole d'authentification extensible (EAP)

Le Protocole d'authentification extensible (EAP) permet de créer des configurations de réseau privé virtuel (VPN) mieux sécurisées.

Le protocole EAP fournit un niveau de sécurité supplémentaire aux technologies VPN. EAP est un composant technologique essentiel pour les connexions VPN sécurisées car, par rapport aux autres méthodes d'authentification, il offre plus de sécurité contre les attaques massives ou de dictionnaire et les tentatives de déchiffrement de mots de passe.

Pour la mise en oeuvre de ces fonctions de protection, EAP fait appel aux autorités de certification (CA) et à la technologie Security Platform. L'utilisation du protocole EAP avec un VPN exige que le serveur et le client soient configurés pour accepter l'authentification EAP comme méthode d'authentification valide et qu'ils disposent d'un certificat utilisateur (X.509).



©Infineon

Technologies AG

Solution Infineon Security Platform

Configuration d'un VPN pour utiliser EAP

La méthode d'authentification du certificat est utilisée par la solution d'Infinion Security Platform qui fournit l'authentification du client. Avant de procéder à la configuration du client, vous devez disposer d'un [certificat](#) approuvé par une autorité de certification. Le client et le serveur doivent avoir la même autorité de certification ou une autorité de certification dans une hiérarchie de confiance. Le client doit avoir également un module de plateforme sécurisée (TPM).



Lors de la demande d'un certificat, vous devez sélectionner un des [Fournisseurs de services cryptographiques](#) délivrés avec la solution Security Platform. Le certificat est utilisé pour l'**authentification du client**. Dans les grandes entreprises, l'administrateur a probablement déjà configuré de tels certificats.

Pour en savoir plus sur VPN, consultez les pages d'Aide Microsoft TechNet ou Microsoft VPN. Pour obtenir les informations de l'Aide Microsoft, réduisez toutes les fenêtres déjà ouvertes afin de visualiser le Bureau Windows. Appuyez ensuite sur F1 pour rechercher le mot-clé approprié.

Le Réseau privé virtuel utilise Internet ou l'intranet pour fonctionner. Avant d'établir une connexion VPN, l'utilisateur doit disposer d'une installation Internet ou intranet pour la connexion au serveur VPN.

Pour utiliser EAP, le client doit d'abord établir une connexion. Vous pouvez utiliser l'option **Connexions réseau** de votre système d'exploitation pour configurer les connexions VPN. Si vous avez besoin d'informations détaillées sur les étapes associées à votre système d'exploitation, consultez l'Aide Microsoft Windows ou Microsoft TechNet.

Après avoir établi la connexion, vous devez la configurer pour utiliser EAP. Pour cela, procédez comme suit :

- Cliquez avec le bouton droit sur la nouvelle connexion VPN et affichez ses propriétés.
- Configurez les paramètres d'authentification dans l'onglet Sécurité pour utiliser le protocole EAP (Extensible Authentication Protocol) avec l'option d'utilisation d'une SmartCard ou d'un autre certificat.
- Configurez les propriétés EAP pour utiliser un certificat sur votre ordinateur.



Si vous disposez de plusieurs certificats pour l'authentification du client et le cryptage, assurez-vous que le certificat approprié est utilisé pour la connexion VPN. Lorsque vous lancez la connexion VPN, sélectionnez un certificat associé avec l'un des [Fournisseurs de services cryptographiques](#) délivrés avec la solution Security Platform.

L'utilisateur doit être connecté à l'ordinateur pour utiliser EAP avec un certificat utilisateur.



©Infineon

Technologies AG

Infineon Security Platform Solution

Réseau local sans fil (WLAN)

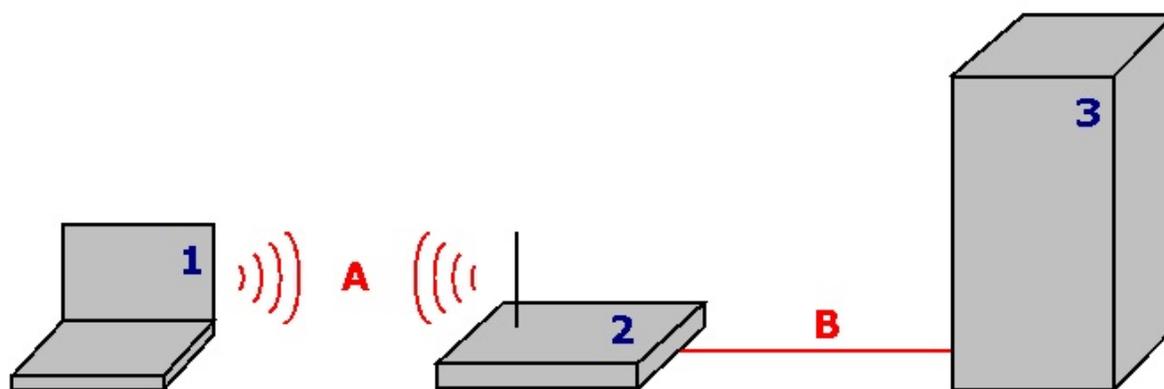
Avec la solution Security Platform vous pouvez protéger les clés privées des certificats utilisés pour les réseaux locaux sans fil (IEEE 802.11 EAP-TLS) et les réseaux locaux câblés (IEEE 802.1X EAP-TLS). La protection est assurée avec un des Cryptographic Service Providers (CSP) inclus dans la solution Security Platform.

Cette section met l'accent sur les réseaux locaux sans fil.

Introduction dans les réseaux locaux sans fil

Un réseau local sans fil utilise des ondes radioélectriques haute fréquence et non câbles pour la communication entre les noeuds. Les réseaux locaux sans fil n'ont pas besoin d'une visibilité directe entre l'expéditeur et le destinataire. Les points d'accès sans fil (les postes fixes) sont câblés à un réseau Ethernet et transmettent une fréquence radio sur un rayon d'une certaine étendue. Les réseaux locaux sans fil fonctionnent d'une manière similaire avec les systèmes de téléphonie cellulaire. Pour les systèmes conçus pour utilisation dans les compagnies, les utilisateurs peuvent se déplacer entre les points d'accès sans perdre la communication.

Le standard **IEEE 802.11** (fidélité sans fil, "Wi-Fi") spécifie les technologies pour les réseaux locaux sans fil. Le standard inclut les méthodes de cryptage Wi-Fi Accès protégé (**WPA**) et Wired Equivalent Privacy (**WEP**, Domaine privé équivalent aux réseaux sans fil).



1	Client réseau local sans fil	Voire ordinateur Security Platform. Le Trusted Platform Module protège la clé privée de votre certificat. Les clients du réseau local sans fil possèdent une connexion sans fil (A) vers un point d'accès.
2	Point d'accès	Appelé également poste fixe. Le point d'accès connecte les clients réseau local sans fil avec un réseau câblé (B).
3	Serveur RADIUS	Par exemple, l'Internet Authentication Service (IAS, Service d'authentification à Internet) inclus dans le Microsoft Windows 2003 Server.

Le serveur RADIUS gère votre authentification.

Informations générales plus détaillées

Des informations générales plus détaillées sur les réseaux locaux sans fil sont disponibles sur l'Internet.

- Le Microsoft Developer Network (MSDN) et l'aide Microsoft Windows (recherchez "connexion réseaux sans fil, wireless networking")
- Wi-Fi Alliance
- Association des réseaux locaux sans fil (WLANA)

La sécurisation de votre réseau local sans fil avec la solution Security Platform



Conditions préalables :

- A part le matériel et les logiciels demandés par les réseaux locaux sans fil, votre client réseau local sans fil doit être un ordinateur Security Platform avec un Trusted Platform Module.
- Vous devez inscrire un certificat protégé par la Security Platform.

[WLAN pas à pas](#)



©Infineon Technologies AG

Infineon Security Platform Solution

WLAN pas à pas

Cette section met l'accent sur les réseaux locaux sans fil. En ce qui concerne la configuration des réseaux locaux câblés (IEEE 802.1X), le seul pas spécifique à la Security Platform (la sélection du Cryptographic Service Provider) est le même que celui pour les réseaux locaux sans fil.

La configuration et l'utilisation des réseaux locaux sans fil pas à pas

Pas	A être exécuté par l'utilisateur
1. Obtention d'un certificat d'authentification client	Tous les utilisateurs de la Security Platform à utiliser le réseau local sans fil
2. Configuration du logiciel du réseau local sans fil	Un administrateur
3. Connexion de votre client réseau local sans fil	Tous les utilisateurs de la Security Platform à utiliser le réseau local sans fil

Obtention d'un certificat d'authentification client

Pour sécuriser votre connexion réseau local sans fil vous avez besoin d'un [certificat](#) approuvé par une autorité de certification. Le client du réseau local sans fil et le serveur RADIUS doivent utiliser une autorité de certification de confiance. Vérifiez l'utilisation d'un modèle de demande certificat pour l'*authentification client*.



Sélection du Cryptographic Service Provider :

Au cours de la demande de certificat vous devez sélectionner le Cryptographic Service Provider à être utilisé par votre certificat.

- Lorsque vous désirez vous authentifier, sélectionnez un CSP utilisateur (*Infineon TPM Cryptographic Provider* ou *Infineon TPM RSA et AES Cryptographic Provider*).
- Lorsque vous désirez authentifier votre ordinateur, sélectionnez CSP plate-forme (*Infineon TPM Platform Cryptographic Provider*).

Pour utiliser le CSP plate-forme, vous devez être un administrateur ou membre du groupe Administrateurs.

Configuration du logiciel du réseau local sans fil

Consultez la documentation de votre fournisseur du réseau local sans fil pour la configuration générale du réseau local sans fil. Le logiciel de votre fournisseur peut inclure un logiciel client configurant les connexions sans fil.

Vous pouvez utiliser l'option **Network Connections (Connexions réseau)** de votre système d'exploitation pour configurer les connexions sans fil :

- Configurez une connexion réseau sans fil sur votre client comme décrit dans l'aide de Microsoft Windows (recherchez "connexion réseaux sans fil, wireless networking").
- Utilisez les paramètres d'**Authentification** suivants :
 - Sélectionnez **Activer l'authentification IEEE 802.1x pour ce réseau**.
 - Dans **Type EAP**, sélectionnez **Carte à puce ou autre certificat**.
 - Dans Propriétés, sélectionnez **Utiliser un certificat sur cet ordinateur**.
 - Lorsque vous désirez sélectionner le certificat chaque fois vous configurez une connexion sans fil, décochez l'option **Utiliser la sélection de certificat simple**.



Pour configurer les paramètres d'**Authentification**, vous devez être un administrateur ou un membre du groupe Administrateurs.

Connexion de votre client réseau local sans fil

Consultez la documentation du votre fournisseur du réseau local sans fil pour les connexions réseau local sans fil.

Vous pouvez utiliser l'option **Network Connections (Connexions réseau)** de votre système d'exploitation pour connecter votre client réseau sans fil :

- Connectez votre client réseau local sans fil comme décrit dans l'aide de Microsoft Windows (recherchez "connexion réseaux sans fil, wireless networking").
- Vérifiez l'utilisation du certificat demandé dans le pas Obtention d'un certificat d'authentification client.



©Infineon Technologies AG

Infineon Security Platform Solution

Questions répétitives et dépannage

[Questions répétitives](#)

[Dépannage](#)

Technologies AG



Infineon Security Platform Solution

Questions répétitives

[Comment supprimer un utilisateur d'Infineon Security Platform ?](#)

[L'enregistrement de la sauvegarde de récupération d'urgence sur un système à distance pose-t-il un problème de sécurité ?](#)

[Le logiciel de la solution Infineon Security Platform peut-il être désinstallé et si c'est le cas, comment procéder ?](#)

[Quelles informations demeurent sur un système après une désinstallation réussie ?](#)

[Après l'inscription d'un certificat à l'aide d'Internet Explorer, le certificat ne peut pas être utilisé. Un message d'erreur est affiché.](#)

[La fonction du système d'exploitation pour comprimer les dossiers est utilisée pour la sauvegarde des données utilisateur. Comment activer l'EFS pour ce dossier comprimé ? Les fonctions peuvent-elles être associées ?](#)

[Le certificat attribué à un dossier d'EFS doit être modifié. Cela peut-il se faire sans risque pour les données contenues dans ce dossier ? Est-il possible d'assigner un certificat arbitraire au dossier ?](#)

[Comment préparer une Infineon Security Platform à une sauvegarde système réussie ? Quels fichiers sont essentiels pour restaurer avec succès une Infineon Security Platform à l'aide des mécanismes de système ?](#)

[Comment configurer et traiter la sauvegarde de secours, surtout en connexion avec les paramètres de stratégie ?](#)

[Comment créer un fichier archive de clé publique à partir d'un fichier jeton ?](#)



Les remarques sur EFS ne s'appliquent qu'aux éditions Windows prenant en charge EFS.

Comment supprimer un utilisateur d'Infineon Security Platform ?

Il existe deux types différents d'opérations de suppression :

- **La suppression complète d'un compte utilisateur du système d'exploitation est une opération simple, prise en charge par Windows. Lorsqu'un compte utilisateur est supprimé, la case de suppression du profil utilisateur doit être cochée. Cette opération supprime**

entièrement les données du compte utilisateur du système.

- **Pour ne supprimer que les données utilisateur de l'Infineon Security Platform sans toucher aux données de compte système, le dossier spécifique à l'utilisateur `\%AppData%\Infineon\TPM Software 2.0` doit être supprimé.**

Lorsque vous désirez supprimer toutes les données liées à un utilisateur de Security Platform, consultez les données spécifiques à l'utilisateur listées dans la section [Quelles informations demeurent sur un système après une désinstallation réussie ?](#).



S'il existe des données sur le système qui ont été cryptées avec une clé Infineon Security Platform spécifique à l'utilisateur, ces données ne pourront plus être décryptées une fois le compte utilisateur supprimé.



L'enregistrement de la sauvegarde de récupération d'urgence sur un système à distance pose-t-il un problème de sécurité ?

Cela ne pose pas de problème de sécurité. Les données sont protégées par le jeton de récupération d'urgence qui, à son tour, est protégé par le mot de passe du jeton de récupération d'urgence.



Aucun problème de sécurité en [mode serveur](#), car Trusted Computing Management Server gère la Récupération d'urgence.



Le logiciel de la solution Infineon Security Platform peut-il être désinstallé et si c'est le cas, comment procéder ?

Il peut être désinstallé à l'aide du processus standard de suppression de logiciel fourni par le système d'exploitation. Toutes les données utilisateur protégées par Security Platform doivent être auparavant sauvegardées. Sans cette sauvegarde, l'accès aux données ne pourra plus être établi une fois le logiciel de la solution Security Platform supprimé de votre système. La dernière étape consiste à désactiver le Trusted Platform Module du BIOS de l'ordinateur.

Une version nouvelle peut être installée sur une ancienne, sans la désinstaller. Dans ce cas, une sauvegarde complète des données utilisateur n'est pas nécessaire.



Quelles informations demeurent sur un système après une désinstallation réussie ?

Lorsque le logiciel de la solution Security Platform est désinstallé, quelques informations demeurent dans le système. En retenant les paramètres et les informations d'identification d'un utilisateur, après une réinstallation le système aura le même état comme auparavant. Ainsi aucune donnée cryptée auparavant ne sera perdue après une réinstallation du logiciel de la solution Security Platform.

Toutefois, lorsque ces données ne sont plus nécessaires et le système doit être nettoyé complètement, les données suivantes doivent être supprimées.

Sauvegardes de secours : L'emplacement des sauvegardes de récupération d'urgence écrites automatiquement est spécifié par les administrateurs. Un fichier de sauvegarde écrit automatiquement est représenté dans le système par un fichier XML et un dossier avec le même nom, par ex. un fichier `SPSystemBackup.xml` et un dossier `SPSystemBackup`. En plus, quelques sauvegardes de récupération d'urgence écrites manuellement peuvent exister.

Jeton de récupération d'urgence : L'emplacement est spécifié par le propriétaire Security Platform lors de l'initialisation de la Security Platform.

Sauvegarde de restauration d'urgence :

i) Windows 7 et Vista : `\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\RestoreData\\Users\\SHTempRestore.xml`

ii) Windows XP Professional, Windows 2000 et autres systèmes d'exploitation supportés: `\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\RestoreData\\Users\\SHTempRestore.xml`

Données système et fichiers clés système :

i) Windows 7 et Vista : `\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\PlatformKeyData`
`IFXConfigSys.xml`
`IFXFeatureSys.xml`
`TCSps.xml`
`TPMCPSys.xml`

ii) Windows XP Professional, Windows 2000 et autres systèmes

d'exploitation supportés: %ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software 2.0\PlatformKeyData
IFXConfigSys.xml
IFXFeatureSys.xml
TCSps.xml
TPMCPSys.xml

Fichiers de sauvegarde clichés instantanés locaux :

i) Windows 7 et Vista :

%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml
%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

ii) Windows XP Professional, Windows 2000 et autres systèmes

d'exploitation supportés:

%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml
%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

Fichiers clé utilisateur de base : %AppData%\Infineon\TPM Software 2.0\UserKeyData\TSPps.xml

TPM Cryptographic Service Provider Container:

%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMcp.xml

Fichier TPM PKCS #11 Provider : %AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMck.xml

Fichiers configuration utilisateur : %AppData%\Infineon\TPM Software 2.0\UserKeyData\
IFXConfig.xml
IFXFeature.xml

Clés de registre :

HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software
HKEY_CURRENT_USER\Software\Infineon\TPM software

Les clés **Personal Secure Drive** de registre suivantes doivent être supprimées manuellement lorsque la fonctionnalité Personal Secure Drive est désinstallée :
[HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]

[HKEY_CURRENT_USER\SOFTWARE\Infineon\TPM Software\PSD]

Personal Secure Drive Répertoires : En outre, les répertoires suivants doivent être supprimés manuellement :

x:\Security Platform\Personal Secure Drive\System Data

ou x: est le lecteur où des Personal Secure Drives sont enregistrés. Ce lecteur est sélectionné pendant la création du Personal Secure Drive (et peut donc être n'importe quel disque dur local) ou bien il est défini par la stratégie d'utilisateur locale du Personal Secure Drive.

Divers :

Pour certificats Trusted Platform Module enregistrés

Tâche de sauvegarde planifiée (par exemple C:\WINDOWS\Tasks\Security Platform Backup Schedule)



Après l'inscription d'un certificat à l'aide d'Internet Explorer, le certificat ne peut pas être utilisé. Un message d'erreur est affiché.

Le certificat est bloqué par Internet Explorer, bien qu'il soit déjà enregistré dans la sauvegarde de certificat de l'utilisateur. Fermez l'Internet Explorer et ouvrez-le à nouveau pour déverrouiller le certificat.



La fonction du système d'exploitation pour comprimer les dossiers est utilisée pour la sauvegarde des données utilisateur. Comment activer l'EFS pour ce dossier comprimé ? Les fonctions peuvent-elles être associées ?

Il n'est pas possible de combiner ces fonctions puisque le système d'exploitation ne permet pas à un dossier comprimé d'être également un dossier protégé d'EFS. La compression du dossier doit être d'abord révoquée. Ensuite la fonction d'EFS peut être activée pour le dossier.



Le certificat attribué à un dossier d'EFS doit être modifié. Cela peut-il se faire sans risque pour les données contenues dans ce dossier ? Est-il possible d'assigner un certificat arbitraire au dossier ?

En général, l'attribution d'un certificat supplémentaire à un dossier EFS ne pose

pas de problème. La première condition de limite est que tous les certificats doivent être contrôlés par le même [Cryptographic Service Provider](#). Tant que le(s) certificat(s) précédemment attribué(s) existe(nt), les données cryptées pourront être lues. Dès que le certificat protégeant un fichier EFS est supprimé du système, les fichiers correspondants sont perdus.



Comment préparer une Infineon Security Platform à une sauvegarde système réussie ? Quels fichiers sont essentiels pour restaurer avec succès une Infineon Security Platform à l'aide des mécanismes de système ?

Les fichiers fondamentaux de l'Infineon Security Platform n'incluent pas les applications du logiciel Infineon Security Platform. Il peut être réinstallé après la restauration d'une sauvegarde de système.

Les données spécifiques du logiciel de la solution Infineon Security Platform sont sauvegardées à l'aide de l'[Assistant Sauvegarde d'Infineon Security Platform](#).

L'Assistant Sauvegarde d'Infineon Security Platform ne sauvegarde pas les données protégées telles que vos fichiers et messages électroniques cryptés qui doivent être enregistrés avec d'autres outils de sauvegarde. Nous vous conseillons d'inclure la sauvegarde de secours de l'Assistant Sauvegarde d'Infineon Security Platform à votre sauvegarde de routine de données.

Si vous n'utilisez pas l'Assistant Sauvegarde d'Infineon Security Platform pour les données spécifiques au logiciel de la solution Security Platform, vérifiez la sauvegarde de toutes les données listées dans la section [Quelles informations demeurent sur un système après une désinstallation réussie ?](#).



- Les sauvegardes automatiques du système configurées par l'administrateur de la Security Platform incluent également les données de récupération d'urgence.
- Trusted Computing Management Server gère la sauvegarde et restauration en [mode serveur](#).



Comment configurer et traiter la sauvegarde de secours, surtout en connexion avec les paramètres de stratégie ?

Vous pouvez configurer toutes les Security Platforms de votre compagnie à utiliser une sauvegarde de secours commune en configurant la [stratégie](#) *Emplacement de la sauvegarde de secours*.

Si vous devez créer une nouvelle sauvegarde de secours, n'importez pas les stratégies avant l'initialisation de la première Infineon Security Platform

L'administration de la stratégie devra ensuite être lancée et la stratégie correctement configurée en définissant l'emplacement de la sauvegarde de récupération d'urgence précédemment créée. Le fichier configuré sera finalement utilisé automatiquement lorsque les autres Security Platforms sont initialisées.



Cette section ne s'applique pas en [mode serveur](#), car la sauvegarde et la restauration sont gérées par le Trusted Computing Management Server.



Comment créer un fichier archive de clé publique à partir d'un fichier jeton ?

Vous pouvez indiquer dans les paramètres de stratégie de groupe que la clé publique d'un jeton de dépannage d'urgence ou d'un jeton de réinitialisation du mot de passe est utilisée à partir d'un fichier archive (voir les [Stratégies système](#) *Utilisez la clé publique du Jeton de Dépannage d'Urgence de l'archive* et *Utilisez la clé publique du Jeton de Réinitialisation de Mot de Passe de l'archive*). Pour créer ce fichier archive à partir d'un fichier jeton existant, procédez comme suit :

- Initialisez complètement la plateforme (notamment Dépannage d'urgence et Réinitialisation du mot de passe) en utilisant les paramètres de stratégie par défaut sur le premier système (par exemple, un système de test).
L'Assistant Rapide d'Initialisation crée un fichier jeton pour Dépannage d'urgence et Réinitialisation du mot de passe.
L'Assistant Initialisation de plateforme crée un fichier jeton pour Dépannage d'urgence et un autre pour Réinitialisation du mot de passe.
- Exécutez le script ci-dessous sur le même système pour créer le fichier archive de clé publique requis à partir du fichier jeton correspondant.
- Copiez le fichier archive de la clé publique dans un emplacement approprié et activez les stratégies indiquées ci-dessus.

Script `GeneratePubKeyArchive.vbs` :

```
'GeneratePubKeyArchive.vbs <Chemin complet vers Token.xml> <Chemin
```

complet vers PubKeyArchive.xml>

'Le <Chemin complet vers Token.xml> peut être l'un des jetons suivants :

' - SPPwdResetToken.xml

' - SPEmRecToken.xml

' - SPGenericToken.xml

'Le <Chemin complet vers PubKeyArchive.xml> est le résultat, qui contient la clé publique extraite du jeton indiqué :

' - SPPwdResetTokenPubKeyArchive.xml

' - SPEmRecTokenPubKeyArchive.xml

' - SPGenericTokenPubKeyArchive.xml

'Pour une utilisation par la stratégie "Utilisez la clé publique du Jeton de Dépannage d'Urgence de l'archive" :

' - SPEmRecTokenPubKeyArchive.xml

' - SPGenericTokenPubKeyArchive.xml

'Pour une utilisation par la stratégie "Utilisez la clé publique du Jeton de Réinitialisation de Mot de Passe de l'archive" :

' - SPPwdResetTokenPubKeyArchive.xml

' - SPGenericTokenPubKeyArchive.xml

'Veillez à indiquer le chemin complet, par exemple :

' GeneratePubKeyArchive.vbs "c:\tmp\SPGenericToken.xml"

"c:\tmp\SPGenericTokenPubKeyArchive.xml"

If WScript.Arguments.Count <> 2 Puis

 WScript.Echo "Utilisation : " & Wscript.ScriptName & " ""<Chemin complet vers Token.xml>"" ""<Chemin complet vers PubKeyArchive.xml>"""

 WScript.Quit

End If

Set MPBase = WScript.CreateObject("IfxSpMgtPrv.MgmtProvider")

Set MPToken = MPBase.GetInterface(10)

' CreationFlags: conserver le fichier existant = 0, remplacer le fichier existant = 1

CreationFlags = 0

ReservedFlag = 0

MPToken.CreatePublicKeyFile WScript.Arguments(0), WScript.Arguments(1), CreationFlags, ReservedFlag

'Traitement des erreurs en cas d'échec à ajouter ici

WScript.Echo "Terminé"



Cette section ne s'applique pas en [mode serveur](#), car le Dépannage d'urgence et la Réinitialisation du mot de passe sont gérés par le Trusted Computing Management Server.



TPM
©Infineon Technologies AG

Infineon Security Platform Solution

Dépannage

La section suivante décrit les procédures pour les opérations de dépannage les plus probables sur un système Infineon Security Platform.

[Une plate-forme doit être configurée, mais le Trusted Platform Module a déjà un utilisateur.](#)

[Le système Infineon Security Platform a été configuré, mais le propriétaire Infineon Security Platform a été modifié.](#)

[Quels aspects doivent être pris en compte pour la récupération d'urgence à l'aide de l'Assistant Initialisation d'Infineon Security Platform ?](#)

[Un document enregistré dans un dossier protégé par EFS doit être restauré à partir d'une sauvegarde de système. L'utilisateur Infineon Security Platform n'existe pas sur le système cible. Comment cette situation peut-elle être traitée ?](#)

[Beaucoup d'applications communément utilisées créent des fichiers temporaires en dehors des dossiers "temp" standard. Généralement, tous les dossiers "temp" ne sont pas protégés par l'EFS. Comment les fichiers "temp" de telles applications peuvent-ils être sécurisés, d'autant plus que ces fichiers restent sur le disque dur lorsque l'application est fermée ?](#)

[Lorsqu'un utilisateur d'Infineon Security Platform accède pour la première fois à un dossier EFS, le mot de passe pour la clé utilisateur de base est demandé. Si cette boîte de dialogue est supprimée et un agent de récupération est configuré, l'utilisateur peut toujours accéder aux données dans le dossier EFS tant que la clé personnelle de l'agent de récupération est disponible à l'utilisateur. Est-ce une erreur du système ?](#)



Les remarques sur EFS ne s'appliquent pas aux éditions familiales de Windows qui ne le prennent pas en charge.

Une plate-forme doit être configurée, mais le Trusted Platform Module a déjà un utilisateur.

Dans ce cas, l'utilisateur existant de Security Platform sera utilisé pour initialiser la Security Platform. Cela exige la connaissance du Mot de Passe du Propriétaire existant ou l'accès au Fichier de Sauvegarde du Mot de Passe Propriétaire correspondant.

C'est une situation typique dans un environnement multi-système où plusieurs

installations de systèmes d'exploitation coexistent sur le même ordinateur. Le Propriétaire d'Infineon Security Platform ("Storage Root Key",SRK) ne peut pas être effacé dans le Trusted Platform Module, ni ne peut être introduit de l'extérieur, c'est-à-dire qu'une opération 'importation' n'est pas possible.

Selon l'existence ou non de clés utilisateur de base, une approche différente sera nécessaire lors de l'[initialisation de la Security Platform](#).

Si aucune clé utilisateur de base n'a été configurée pour la Security Platform, un nouvel fichier sauvegarde de secours (contenant les données de récupération d'urgence) pourra être créé. L'Infineon Security Platform est alors prêt pour d'autres opérations.

Si des clés utilisateur de base existent et une sauvegarde de secours (contenant les données de récupération d'urgence) est configurée, il est essentiel de ne pas écraser cette sauvegarde de secours lors de l'initialisation de la Security Platform.

 Dans le [mode serveur](#), vous devez effacer le propriétaire, lorsqu'un propriétaire existe déjà avant la connexion du système au Trust Domain. La Security Platform sera ensuite inscrite automatiquement dans le Trust Domain (voir [Inscription plateforme](#)).



Le système Infineon Security Platform a été configuré, mais l'utilisateur d'Infineon Security Platform a été modifié.

Si la Security Platform a été configurée avec une récupération d'urgence, les informations d'identification de votre Security Platform peuvent être réactivées en utilisant la [fonctionnalité de récupération d'urgence](#) de la solution Security Platform.

 Dans le [mode serveur](#), le Trusted Platform Module ne devrait pas avoir un propriétaire avant la connexion du système au Trust Domain, voir lorsqu'il n'a pas été initialisé encore (ni par Infineon TPM Professional Package dans le mode autonome, ni par le serveur Trusted Domain dans le mode serveur ou par un autre logiciel comme Windows Vista *Trusted Platform Module (TPM) Management*).



Quels aspects doivent être pris en compte pour la récupération d'urgence à

L'aide de l'Assistant Initialisation d'Infineon Security Platform ?

La récupération d'urgence d'un système peut s'effectuer si votre système est endommagé et une image de sauvegarde est disponible, vous permettant de restaurer vos données. Les données spécifiques à l'utilisateur relatives à la Security Platform et les données de récupération d'urgence sont sauvegardées par les sauvegardes automatiques du système.

L'administrateur d'Infineon Security Platform doit avoir accès à la sauvegarde de secours et au jeton de récupération d'urgence qui a été créé lors de la configuration du système. Il doit également être en possession du mot de passe protégeant ce jeton.

L'administrateur d'Infineon Security Platform doit restaurer le système, en démarrant l'[Assistant Sauvegarde d'Infineon Security Platform](#).

Si la récupération est effectuée sur un ordinateur dont le nom a été modifié, l'ancien nom de l'ordinateur ou le numéro d'identification plateforme (SID) de l'ordinateur doit être connu. Il est possible que la sauvegarde de secours inclut des données de récupération sur plusieurs ordinateurs. Dans ce cas, vous devez sélectionner l'ordinateur à restaurer depuis la sauvegarde de secours.



Trusted Computing Management Server gère la Récupération d'urgence en [mode serveur](#).



Un document enregistré dans un dossier protégé par EFS doit être restauré à partir d'une sauvegarde de système. L'utilisateur Infineon Security Platform n'existe pas sur le système cible. Comment cette situation peut-elle être traitée ?

Si la clé utilisateur de base n'est plus disponible et aucun certificat de récupération (pour un agent de récupération) n'a été configuré, le document est sans aucun doute perdu.

Sinon, la première étape est de restaurer le fichier à partir de la sauvegarde. Cela se fait sans toucher les propriétés se rapportant à la sécurité du fichier. Dans l'étape suivante, le certificat de récupération doit être utilisé pour activer un agent de récupération afin de décrypter le fichier.



Beaucoup d'applications communément utilisées créent des fichiers temporaires en dehors des dossiers "temp" standard. Généralement, tous les dossiers "temp" ne sont pas protégés par l'EFS. Comment les fichiers "temp" de telles applications peuvent-ils être sécurisés, d'autant plus que ces fichiers restent sur le disque dur lorsque l'application est fermée ?

C'est un problème commun à beaucoup d'applications. Selon l'application, il se peut que des fichiers temporaires soient créés à l'extérieur des dossiers EFS configurés. Quand il ne s'agit pas du dossier commun %AppData% dans le profil de l'utilisateur (généralement nommé "Données d'application"), c'est une fonctionnalité spécifique à l'application et aucune règle générale ne peut être établie sur la façon de traiter la situation. Lorsque l'emplacement est connu (et la configuration du dossier n'est pas prise en charge par l'application), il est éventuellement possible d'appliquer la sécurité de l'EFS sur le dossier respectif. Si cette approche n'est pas faisable, la suppression de tels fichiers à la fermeture de l'application peut au moins être garantie.

Plusieurs informations de dépannage sur le système de fichiers de cryptage sont disponibles dans Microsoft Developer Network (MSDN).



Lorsqu'un utilisateur d'Infineon Security Platform accède pour la première fois à un dossier EFS, le mot de passe pour la clé utilisateur de base est demandé. Si cette boîte de dialogue est supprimée et un agent de récupération est configuré, l'utilisateur peut toujours accéder aux données dans le dossier EFS tant que la clé personnelle de l'agent de récupération est disponible à l'utilisateur. Est-ce une erreur du système ?

Ce comportement est correct en raison de la conception de l'agent de récupération. Lorsqu'un certificat de récupération est configuré pour un dossier EFS, ce certificat est utilisé par l'agent de récupération lors du premier accès à ce dossier. Selon que l'ordinateur appartient ou non à un domaine, différentes solutions existent :

L'ordinateur appartient à un domaine : Dans ce cas, l'administrateur s'intéresse à l'affectation du certificat. Si aucune affectation à un utilisateur spécifique d'Infineon Security Platform n'existe, le comportement indiqué ne se produira pas.

L'ordinateur fonctionne sous Windows 2000 et n'est pas membre d'un domaine : Une manière possible est de s'assurer que la clé personnelle de

L'agent de récupération ne soit pas disponible pour les utilisateurs habituels de Security Platform.

L'ordinateur fonctionne sous un autre système d'exploitation pris en charge et n'est pas membre d'un domaine : Dans ce cas, le certificat de récupération n'existe généralement pas, si bien que le comportement ne se produira pas.



©Infineon Technologies AG

Infineon Security Platform Solution - Visualisateur du certificat et sélection du certificat

Visualisateur du certificat et sélection du certificat d'Infineon Security Platform

Le visualisateur du certificat et la sélection du certificat d'Infineon Security Platform sont utilisés pour la gestion des certificats.

Vue d'ensemble des particularités du certificat géré dans la Microsoft Management Console

Par contraste avec le [composant logiciel enfichable certificat exécuté dans Microsoft Management Console](#), vous pouvez relier les certificats de Security Platform avec le visualisateur du certificat et la sélection du certificat de Security Platform:

- Vous pouvez protéger les clés privées avec le Trusted Platform Module.
- Vous pouvez sélectionner les certificats à utiliser pour le cryptage de fichiers et dossiers avec le système de fichiers de cryptage (EFS) et Personal Secure Drive (PSD).

Différences entre le visualisateur du certificat et la sélection du certificat

Le visualisateur du certificat et la sélection du certificat partagent quelques fonctions communes de gestion de certificats, par exemple l'affichage d'une liste de certificats, la visualisation du certificat et des détails de la clé privée et l'importation des certificats PKCS #12 dans la Security Platform.

Les différences entre le visualisateur du certificat et la sélection du certificat sont :

Visualisateur du certificat : Le visualisateur du certificat est un outil spécial de gestion de certificat pour la solution Security Platform. Par exemple, vous pouvez protéger les clés privées avec le Trusted Platform Module.

Sélection du certificat : Le but de la sélection du certificat et de sélectionner un certificat pour le cryptage de fichiers et dossiers avec l'EFS ou le PSD. Vous pouvez créer un certificat auto-signé ou exiger un certificat d'une autorité de certification.

Comment enregistrer et sélectionner les certificats

L'enregistrement et la sélection de **certificats EFS** via **sélection du certificat** :

- Avec **Demander...** vous pouvez exiger un certificat depuis une autorité de certification externe.
- Avec **Créer** vous pouvez exiger un certificat depuis une autorité de certification de votre domaine ou créer un certificat auto-signé.
- Avec **Sélectionner** vous pouvez sélectionner les certificats à utiliser pour l'EFS ou le PSD.

La commande **Demander...** et la commande **Créer** sont fonction du [Type et inscription des certificats EFS](#).

Les certificats EFS ne sont pas utilisés seulement pour l'EFS, mais également pour le PSD.

Enregistrez les **certificats à utilisation générale** avec la page [Demander un certificat](#) de l'assistant d'initialisation de l'utilisateur.

Celle ci est fonction de la stratégie [URL à lancer à partir de l'assistant pour l'enregistrement de certificats](#).

[Plus amples détails sur l'enregistrement de certificats](#)

Eléments de la boîte de dialogue

Eléments habituels de la boîte de dialogue	Explication
<input type="checkbox"/> <i>Afficher les certificats au but prévu</i>	<p>Sélectionnez ici le but prévu pour filtrer la liste de certificats.</p> <p>Par exemple, vous pouvez afficher seulement les certificats de courrier électronique sécurisé ou vous pouvez afficher tous les certificats.</p> <p> Dans la sélection du certificat, cette sélection est configurée à <i>Système de fichiers de cryptage</i> et elle est désactivée. Cette valeur est utilisée pour l'EFS et également pour le PSD.</p>
<input type="checkbox"/> Liste de certificats	<p>Cette liste affiche tous les certificats sur votre ordinateur correspondant aux critères configurés par vous (par exemple <i>le but prévu</i>).</p> <p> Ce symbole est utilisé pour les certificats dont les clés privées sont accessibles.</p> <p> Ce symbole est utilisé pour les certificats dont les clés privées ne sont plus accessibles.</p> <p> Ce symbole est utilisé lorsqu'on ne connaît pas si la clé privée d'un certificat peut être accédée, par exemple si la clé privée est stockée sur une carte à puce. Dans ce cas, insérez la carte à puce et sélectionnez le certificat.</p> <p> Ce symbole est utilisé pour les certificats sans une clé privée correspondante.</p> <p>Dans Sélection du certificat, le certificat EFS ou PSD utilisé actuellement est affiché en caractères gras.</p>
<input type="checkbox"/> <i>Visualiser...</i>	Cliquez pour afficher les détails du certificat sélectionné.
<input type="checkbox"/> <i>Importer...</i>	Cliquez pour importer un certificat PKCS #12.

	<p>L'assistant d'Importation PKCS #12 de la Security Platform sera lancé.</p> <p>La clé privée du certificat sera protégée par le Trusted Platform Module.</p> <p> Ce bouton est activé seulement lorsque la stratégie Autorisation de l'importation de la clé pour l'utilisateur le permet.</p>
<input type="checkbox"/> <i>Clé privée</i>	Lorsque vous avez sélectionné un certificat contenant une clé privée, les propriétés de la clé sont affichées ici.
Eléments supplémentaires du dialogue dans le visualisateur du certificat	Explication
<input checked="" type="checkbox"/> <i>Afficher les certificats d'autres fournisseurs</i>	Cochez cette case pour afficher des certificats provenant également d'autres fournisseurs que l' <i>Infineon TPM Cryptographic Provider</i> .
<input checked="" type="checkbox"/> <i>Afficher également les certificats privés PKCS #11</i>	Lorsque vous cochez cette case, vous devrez vous authentifier sur la Security Platform lorsque le visualisateur du certificat accède un certificat privé PKCS #11.
<input type="checkbox"/> <i>Protéger</i>	<p>Cliquez pour protéger la clé privée du certificat sélectionné par le Trusted Platform Module.</p> <p> La protection de votre clé privée ne peut pas être désactivée. Lorsque vous désirez pouvoir restaurer une version non protégée, exportez d'abord le certificat avec la fenêtre Certificats Microsoft.</p>
<input type="checkbox"/> <i>Supprimer</i>	<p>Cliquez pour supprimer le certificat sélectionné et sa clé privée de votre ordinateur.</p> <p>Ce bouton est activé seulement lorsque le certificat sélectionné n'est pas utilisé pour EFS ou PSD, mais sa clé privée est protégée par le Trusted Platform</p>

	<p>Module.</p> <p> Vérifiez si le certificat est en cours d'utilisation. Vous ne pourrez plus l'utiliser.</p>
<input type="checkbox"/> <i>Fermer</i>	Cliquez pour fermer le visualisateur du certificat.
Eléments supplémentaires du dialogue dans la sélection du certificat	Explication
<input type="checkbox"/> <i>Demander...</i>	<p>Cliquez pour demander un certificat depuis une autorité de certification.</p> <p>Un dialogue de demande de certificat sera affiché. Suivez les instructions sur l'écran pour terminer la procédure de demande de certificat. Alors fermer la fenêtre de demande de certificat en cliquant sur le bouton Fermer dans le titre de la fenêtre.</p> <p> Ce bouton est désactivé lorsqu'aucune adresse web de demande de certificat n'est pas configurée dans la stratégie Type et enregistrement des certificats EFS.</p>
<input type="checkbox"/> <i>Créer</i>	<p>Cliquez pour obtenir un certificat de domaine ou créer un certificat auto-signé.</p> <p>Le logiciel de la solution Security Platform essaiera d'obtenir un certificat depuis l'autorité de certification Microsoft de votre domaine. Lorsqu'aucune autorité de certification n'est pas disponible, un certificat auto-signé sera créé.</p> <p> Remarques :</p> <ul style="list-style-type: none"> • En fonction de vos paramètres autorité de certification du domaine, il est possible que le certificat exigé ne peut pas être obtenu directement. Motifs possibles : Autorité de certification manuelle, certificat livré par courrier électronique. Dans ce cas, consultez votre opérateur d'autorité de

	<p>certification pour la disponibilité du certificat.</p> <ul style="list-style-type: none"> • En fonction de la configuration de la stratégie Type et enregistrement des certificats EFS, il est possible que vous ne pouvez pas créer des certificats auto-signés. <p>Lorsqu'aucune autorité de certification du domaine n'est disponible et des certificats auto-signés sont interdits par la stratégie, vous ne pouvez pas obtenir un certificat via <i>Créer</i>.</p> <ul style="list-style-type: none"> • La validité des certificats autosignés peut être configurée dans le paramètres de stratégie de Intervalle de validité pour les certificats EFS autosignés.
<input type="checkbox"/> <i>Sélectionner</i>	<p>Cliquez pour utiliser le certificat sélectionné dans la liste de certificats de la fenêtre comme certificat EFS ou PSD. La sélection du certificat sera fermée, vous serez de retour dans la page Certificat de cryptage dans l'assistant d'initialisation de l'utilisateur.</p>
<input type="checkbox"/> <i>Annuler</i>	<p>Cliquez pour fermer la sélection du certificat et être de retour dans la page Certificat de cryptage dans l'assistant d'initialisation de l'utilisateur sans modifier le certificat EFS ou PSD.</p>

Démarrage de l'application

Visualisateur du certificat : Démarrez le Visualisateur du certificat de la Security Platform via l'outil de paramétrage ([Outil de paramétrage - Paramètres utilisateur - Gérer...](#)).

Sélection du certificat : Pour démarrer la sélection du certificat de la Security Platform, cliquez sur **Sélectionner...** lors de la configuration du cryptage de fichiers et dossiers avec l'EFS ou PSD ([Assistant d'initialisation de l'utilisateur - Certificat de cryptage](#))



©Infineon Technologies AG

Infineon Security Platform Solution - Assistant Réinitialisation du mot de passe

Saut sur le dispositif d'authentification

Cette page d'assistant vous permet de ne mettre pas a jour votre dispositif d'authentification avec la nouvelle phrase de passe utilisateur de base. Utile si votre dispositif d'authentification ne fonctionne pas ou n'est pas disponible.



Disponibilité de la page : Cette page est seulement disponible lorsque vous avez configuré l'authentification étendue.

Élément page assistant	Explication
<input checked="" type="checkbox"/> <i>Saut sur le dispositif d'authentification</i> -	Ne pas mettre a jour votre dispositif d'authentification avec votre nouvelle phrase de passe utilisateur de base. Dans ce cas vous devez mettre a jour votre dispositif d'authentification quand il sera a nouveau disponible. Cette option peut être exécutée en configurant a nouveau Authentification étendue dans Outil de paramétrage : Outil de paramétrage - Paramètres utilisateur - Configuration...

