GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

GUIDE D'INSTALLATION ET DE MISE EN ŒUVRE

Version 10.1.1

Dernière mise à jour du document : 8 février 2023

Référence : sds-fr-sds_suite-guide_d_installation-v10

Table des matières

Dans la documentation, Stormshield Data Security Enterprise est désigné sous la forme abrégée : SDS.

Préface

A propos de ce guide

Ce document fournit les informations essentielles à l'utilisation de Stormshield Data Security Enterprise.

Audience

Ce guide s'adresse :

1. aux administrateurs système qui souhaitent installer Stormshield Data Security Enterprise.
2. aux utilisateurs du logiciel qui souhaitent protéger des fichiers confidentiels.

1. Environnement d'utilisation

Pour utiliser Stormshield Data Security Enterprise dans les conditions de son évaluation Critères Communs et de sa qualification au niveau standard, il est impératif de respecter les recommandations suivantes.

1.1 Recommandations sur la veille sécurité

1. Consultez régulièrement les alertes de sécurité diffusées sur https://advisories.stormshield.eu/.
2. Appliquez systématiquement une mise à jour du logiciel si elle contient la correction d'une faille de sécurité. Ces mises à jour sont disponibles sur votre espace client MyStormshield.

1.2 Recommandations sur les clés et les certificats

1. Les clés RSA des utilisateurs et des autorités de certification doivent être d'une taille minimale de 4096 bits, avec un exposant public strictement supérieur à 65536.
2. Les certificats et les CRL doivent être signés avec l'algorithme d'empreinte SHA-512.

1.3 Recommandations sur les algorithmes

1. Stormshield Data Security supporte différents algorithmes mais préconise l'utilisation de AES 256, RSA 2048, SHA 512.
2. Les algorithmes Triple DES, RC4 et RC5 sont également supportés.
3. Les mécanismes RC2 et DES sont supportés pour compatibilité mais il est déconseillé de les utiliser car ils comportent des faiblesses connues.

1.4 Recommandations sur les comptes utilisateurs

1. Les comptes utilisateurs doivent être protégés par l'algorithme de chiffrement AES et le standard de hachage cryptographique SHA-256.
2. Les mots de passe doivent être soumis à une politique de sécurité empêchant les mots de passe faibles.
3. Des mesures organisationnelles adaptées doivent assurer l'authenticité des modèles à partir desquels les comptes utilisateurs sont créés.
4. En cas d'utilisation d'un porte-clés matériel (carte à puce ou token matériel), ce dispositif assure la protection en confidentialité et en intégrité des clés et des certificats qu'il contient.

1.5 Recommandations sur les postes de travail

1. Le poste de travail sur lequel Stormshield Data Security est installé doit être sain. Il doit pour cela exister dans l'organisation une politique de sécurité du système d'information dont les exigences sont respectées sur les postes de travail. Cette politique doit notamment prévoir que les logiciels installés soient régulièrement mis à jour et que le système soit protégé contre les virus et autres logiciels espion ou malveillant (pare-feu correctement paramétré, antivirus à jour, etc).

2. La politique de sécurité doit également prévoir que les postes non équipés de Stormshield Data Security n'aient pas accès aux dossiers confidentiels partagés sur un serveur, afin qu'un utilisateur ne puisse pas provoquer un déni de service en altérant ou en supprimant, par inadvertance ou par malveillance, les fichiers protégés par le produit.
3. L'accès aux fonctions d'administration du système du poste est restreint aux seuls administrateurs système.
4. Le système d'exploitation doit gérer les journaux d'événements générés par le produit en conformité avec la politique de sécurité de l'organisation. Il doit par exemple restreindre l'accès en lecture à ces journaux aux seules personnes explicitement autorisées.
5. L'utilisateur doit veiller à ce qu'un attaquant potentiel ne puisse pas observer voire accéder au poste lorsque la session Stormshield Data Security est ouverte.

1.6 Recommandation sur le chiffrement des fichiers

L'algorithme de chiffrement des fichiers doit être l'AES.

1.7 Recommandations sur les intervenants

1. L'administrateur de la sécurité est considéré de confiance. Il définit la politique de sécurité de Stormshield Data Security en respectant l'état de l'art, et éventuellement crée les comptes des utilisateurs via l'application Stormshield Data Authority Manager.
2. L'administrateur système est également considéré de confiance. Il est en charge de l'installation et de la maintenance de l'application et du poste de travail (système d'exploitation, logiciels de protection, librairie *PKCS#11* d'interface avec une carte à puce, applications bureautiques et métier, etc). Il applique la politique de sécurité définie par l'administrateur de la sécurité.
3. L'utilisateur du produit doit respecter la politique de sécurité en vigueur dans son organisme.

1.8 Environnement de certification et de qualification

Les modules logiciels évalués dans le cadre de la certification Critères Communs EAL3+ et de la qualification de Stormshield Data Security sont :

1. Le composant "Chiffrement transparent" (Stormshield Data Team), qui assure la définition des règles de sécurité, le chiffrement des fichiers conformément à ces règles, et le chiffrement du fichier d'échange du système (mémoire paginée ou swap).
2. Le "noyau Stormshield Data Kernel", commun à tous les produits de la gamme, qui assure l'authentification de l'utilisateur, surveille l'inactivité du poste, gère un annuaire de certificats de confiance, et contrôle la non-révocation des certificats utilisés.
3. Le module cryptographique logiciel interne (Stormshield Data Crypto), qui gère les clés de l'utilisateur, qu'elles soient stockées dans un fichier (implémentation logicielle) ou dans une carte à puce.

En revanche, les modules suivants sont en dehors du périmètre de l'évaluation :

1. L'outil d'administration Stormshield Data Authority Manager.
2. L'éventuelle carte à puce et son middleware *PKCS#11*.

2. Installation de Stormshield Data Security

Cette section décrit comment installer et désinstaller Stormshield Data Security.

2.1 Configuration requise

Pour connaître la configuration requise sur les systèmes Microsoft Windows, reportez-vous à la section **Compatibilité** de la note de version de Stormshield Data Security 10.1.1.

> **NOTE**
> L'installation du produit en étant connecté à Windows avec un compte utilisateur du domaine est impossible pour un utilisateur du domaine si l'UAC (User Account Control) est activée car l'élévation de privilège ne fonctionne pas.

2.2 Comment télécharger Stormshield Data Security

Les produits Stormshield Data Security sont distribués via notre Espace client. Cet espace vous permet de consulter et télécharger :

- les différentes versions logicielles et correctives de la gamme Stormshield Data Security ;
- l'empreinte des paquets d'installation afin d'en vérifier l'authenticité.

Pour consulter la documentation du produit, rendez-vous sur le site de Documentation technique Stormshield.

2.3 Comment vérifier l'authenticité du logiciel Stormshield Data Security

Le logiciel Stormshield Data Security est disponible sous deux formats :

- un package Windows Installer (*.msi*) ;
- un package d'installation exécutable (*.exe*).

Pour vérifier l'authenticité de l'un de ces paquets :

- calculez son empreinte SHA-256 à l'aide d'un outil de votre choix ;
- vérifiez que cette empreinte est bien identique à celle publiée sur l'Espace Client.

Le fichier exécutable peut également être vérifié à l'aide de sa signature numérique :

1. Dans l'explorateur, effectuez un clic droit sur le fichier *.exe* et sélectionnez **Propriétés**.
2. Cliquez sur **Signatures Numériques** et sélectionnez la ligne **Stormshield**.
3. Cliquez ensuite sur **Détails**.

2.4 Comment installer Stormshield Data Security

Une clé de licence vous est communiquée en fonction des droits d'usage que vous avez acquis lors de la commande du produit. Cette clé de licence est demandée à l'installation.

L'installation de Stormshield Data Security nécessite d'être administrateur de la machine et peut se faire à partir d'un paquet *.exe* ou *.msi*. Pour installer à partir du paquet *.msi*, utilisez une fenêtre de ligne de commande. Pour plus d'informations, reportez-vous à la section suivante.

NOTE
L'installation de la version 10.1.1 de Stormshield Data Security ne doit pas être effectuée sur une version strictement inférieure à Security BOX 8.0.3. Dans ce cas, il faut d'abord désinstaller l'ancienne version avant de réinstaller cette version 10.1.1.

Avant d'installer le composant Stormshield Data Mail, veuillez installer ou mettre à jour la version de Microsoft Outlook choisie.

Pour mettre à jour la version 8.0.5 de Security BOX Suite vers la version 10.1.1 de Stormshield Data Security, il est indispensable de passer par une désinstallation complète de la version 8.0.5 via un script dédié avant d'installer la version 10.1.1. Ce script est disponible auprès du support Stormshield Data Security. Veuillez contacter le support Stormshield Data Security pour plus d'informations.

2.5 Fichiers de base de la procédure d'installation

La procédure d'installation de base comporte les fichiers ci-dessous disponibles sur l'espace client MyStormshield.

ASTUCE
x86 : package 32 bits
x64 : package 64 bits

SDS_Suite_10.0.000xx_FRA_Release_x86_setup SDS_Suite_10.0.000x_FRA_Release_x64_setup	Packages autonomes permettant d'installer la solution et ses prérequis.
SDS_Suite_10.0.000xx_FRA_Release_x86 SDS_Suite_10.0.000xx_FRA_Release_x64	Packages *msi* permettant d'installer la solution. Ces packages nécessitent le prérequis « SQL Server Compact Edition ».
SSCERuntime-FRA	Packages *msi* 32/64 bits du prérequis SQL Server Compact Edition 4.0.
VSTO Runtime 40 x86 Office 2010 VSTO Runtime 40 x64 Office 2010	Packages *exe* 32/64 bits du prérequis Visual Studio 2010 Tools pour Office Runtime. Ce package est uniquement nécessaire pour l'installation du composant Stormshield Data Mail Édition Outlook.

Deux modes d'installation sont disponibles pour chaque version 32 et 64 bits :

- Mode interactif : le mode autonome en utilisant le setup. Il suffit de cliquer sur le fichier *xxx setup.exe* pour lancer l'installation en interactif. C'est le mode d'installation par défaut de Stormshield Data Security 10.1.1.
  Après avoir saisi sa clé de licence, et avoir accepté le contrat de licence, la procédure d'installation propose l'installation de tous les composants de la suite autorisés par la clé de licence.

- Mode silencieux : il s'agit de l'installation sans interaction utilisateur. Ce mode utilise le package *msi*. L'installation préalable du package SSCE (SQL Server Compact Edition) et, pour le composant Stormshield Data Mail Édition Outlook, du package VSTO Runtime 4.0 Office 2010 est alors requise. Il est ensuite possible d'installer le package en tant qu'administrateur par les commandes traditionnelles de Windows Installer. Si l'installation n'est pas faite avec les droits d'administrateur, le produit ne s'installera pas (erreur 1925).

Par exemple :

```
msiexec /qn /i "<chemin>Stormshield Data Security 10.X" LICENCENUM=<numéro de licence>
```

où `<numéro de licence>` doit être indiqué sous la forme ABCDEFGHABCDEFGH (16 caractères attachés).

Le lancement de cette commande doit être fait dans une fenêtre de ligne commande ouverte en tant qu'administrateur.

Les variantes possibles sont :

- `/qn` installation sans aucun écran ;
- `/qn+` idem `/qn` avec un écran final de confirmation ;
- `/qb` installation avec un écran comportant une barre d'avancement et une durée estimée restante ;
- `/qb+` idem `/qb` avec un écran final de confirmation.

En mode silencieux, la procédure installe toutes les applications autorisées par la licence. Grâce à la propriété privée `REMOVE` (reportez-vous à la section Paramétrage de la présélection des applications), il est possible de limiter les applications installées.
Une fois l'installation terminée, Stormshield Data Security démarre automatiquement chaque fois que vous démarrez Windows.

NOTE
Le commutateur `/norestart` n'est pas supporté. Pour empêcher le redémarrage de la machine, il faut créer un *.mst* avec les options ad hoc.

2.6 Paramétrage de la présélection des applications

Grâce à la propriété `REMOVE`, il est possible de limiter les applications pouvant être installées par l'utilisateur, même si la clé de licence en autorise d'autres.

Une application pratique de cette propriété est la possibilité d'avoir différents profils d'installation tout en ayant qu'une seule clé de licence et un seul package d'installation.

Voici la liste des valeurs possibles :

Code	Produit supprimé
SBoxFile	Stormshield Data File
SBoxDisk	Stormshield Data Virtual Disk
SBoxShredder	Stormshield Data Shredder
SBoxMailOutlookAddIn	Stormshield Data Mail Édition Outlook

Code	Produit supprimé
SBoxMailNotes	Stormshield Data Mail Édition Notes
SBoxTeam	Stormshield Data Team
SBoxExtCarte	Stormshield Data Extension Carte
SBoxSign	Stormshield Data Sign
SBoxConnector	Stormshield Data Connector

Dans la définition de la valeur de la propriété `REMOVE`, les différents composants dont l'installation est interdite doivent être séparés par une virgule et il ne doit pas y avoir d'espace.

La clé de licence `<SBOXLICENCENUM>` permet l'installation de tous les composants de Stormshield Data Security, la ligne de commande suivante supprime Stormshield Data File et Stormshield Data Virtual Disk des applications pouvant être installées.

```
msiexec /i "<chemin>\ Stormshield Data Security 10.1.1"
LICENCENUM=<SBOXLICENCENUM> REMOVE=SBoxFile,SBoxDisk
```

NOTE
Le lancement de cette commande doit être effectué dans une fenêtre de ligne de commande ouverte en tant qu'administrateur.

2.7 Comment désinstaller Stormshield Data Security

1. Ouvrez le **Panneau de configuration**.
2. Ouvrez les **Programmes et fonctionnalités**.
3. Sélectionnez dans la liste la ligne correspondant à Stormshield Data Security.
4. Cliquez sur **Désinstaller**.
5. Suivez les indications à l'écran.

Vous pouvez également utiliser la commande Setup du package d'installation qui propose d'installer, désinstaller et modifier l'installation.

2.8 Application d'une version corrective

Une version corrective de Stormshield Data Security 10.1.1 se présente comme une version majeure du produit. Stormshield Data Security utilise le mécanisme de « mise à jour majeure » de Windows Installer. Par conséquent, l'installation d'une version corrective est identique à l'installation de la version de base.

Exemple de scénario :

1. Installation de la version 9.1xxxx Release

```
msiexec /i SSCERuntime_x64-FRA.msi /qn
msiexec /i "Stormshield Data Security 9.1xxxx FRA Release x64.msi" /qn
LICENCENUM=yyyyyyyyyyyyyyy
```

2. Installation de la version corrective 9.1yyyy

```
msiexec /i "Stormshield Data Security 9.1yyyy FRA Release x64.msi" /qn
LICENCENUM=yyyyyyyyyyyyyyy
```

2.9 A propos de Stormshield Data Security

Une fois l'installation de Stormshield Data Security terminée, vous pouvez visualiser les informations relatives à la version installée à partir de la fenêtre **A propos de Stormshield Data Security**.

Pour visualiser cette information, effectuez un clic droit sur l'icône Stormshield Data Security dans la barre des tâches et sélectionnez **A propos de Stormshield Data Security** dans le menu contextuel.

Utilisez la barre de défilement pour voir la liste complète des composants installés sur votre poste.

3. Mise en route de Stormshield Data Security

Cette section concerne les comptes utilisateurs protégés par un mot de passe. Si vous utilisez une carte à puce ou une clé USB pour vous identifier et vous connecter à Stormshield Data Security, reportez-vous à la section Installation et utilisation de l'extension pour carte (Cartes à puce et Clés USB).

3.1 Principes de Stormshield Data Security

Après avoir été installé, Stormshield Data Security démarre chaque fois que vous démarrez Windows.

Afin d'utiliser les composants de Stormshield Data Security, vous devez vous connecter à Stormshield Data Security. Pour cela, vous devez disposer d'un compte utilisateur correctement configuré.

Lors de votre connexion à Stormshield Data Security, votre compte utilisateur est ouvert, ce qui vous permet d'accéder à tous les composants de la suite, soit simultanément ou en alternance.

Le logiciel Stormshield Data Security est un logiciel multi-utilisateurs. Si plusieurs utilisateurs peuvent partager le même poste et maintenir des configurations personnalisées et sécurisées propres à leur environnement, un seul utilisateur à la fois peut être connecté et peut utiliser Stormshield Data Security.

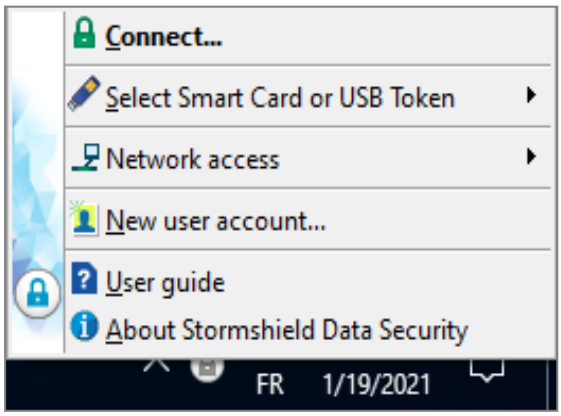
Si un utilisateur souhaite créer différents profils, il doit alors utiliser un compte utilisateur Stormshield Data Security différent pour chaque profil.

3.2 Menu Stormshield Data Security

Effectuez un clic droit sur l'icône Stormshield Data Security affichée à droite de la barre de tâches Windows pour faire apparaître le menu Stormshield Data Security :

Tant que vous n'êtes pas connecté, cette icône reste grise. Lorsque une session Stormshield Data Security est verrouillée, cette icône est rouge.

Effectuez un clic-droit sur cette icône pour ouvrir le menu **Stormshield Data Security**.



Ce menu peut prendre différentes formes en fonction du paramétrage du compte utilisateur et du mode de connexion/déconnexion ou de verrouillage/déverrouillage.

3.3 Vous possédez déjà un compte Stormshield Data Security

L'ensemble de la gamme des produits Stormshield Data Security partage les mêmes moteurs cryptographiques. Une seule connexion permet d'utiliser l'un ou l'autre des logiciels sans devoir changer de compte utilisateur.

Si vous possédez déjà un compte provenant d'un des logiciels de la suite Stormshield Data Security, il est inutile de créer un nouveau compte.

Si vous avez déjà créé un compte sous une version antérieure à la version 7.2, celui-ci est conservé.

Par contre, il faut déplacer le répertoire utilisateur :

C:\ProgramData\Arkoon\Security Box\Users.

L'emplacement exact dépend de la configuration de votre système d'exploitation.

En cas de migration à partir d'une version précédente, les comptes utilisateurs sont automatiquement migrés vers ces nouveaux répertoires. Cette migration se fait lors de la mise à jour du logiciel. Ajouter ultérieurement un compte ancien dans le nouveau répertoire devra se faire manuellement.

3.4 Création d'un compte

Pour créer un compte Stormshield Data Security, vous disposez de deux méthodes :

- la création ou génération d'une ou deux clés par Stormshield Data Security ;
- l'importation de clé PKCS#12.

Si vous créez un compte à deux clés, et en fonction des politiques de sécurité et de certification retenues par les administrateurs, vous pouvez utiliser l'une ou l'autre des deux méthodes pour la création de chaque clé.

3.4.1 Création d'une clé

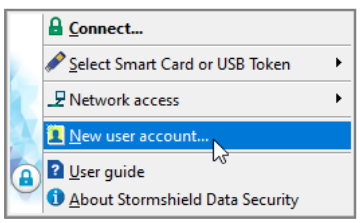
La création de votre compte par Stormshield Data Security passe par la création d'une clé que vous utiliserez par exemple pour la sécurisation de vos fichiers et messages. La clé créée est auto-certifiée pour être immédiatement utilisable par les logiciels de la suite. Cependant, cette clé ne sera pas automatiquement considérée comme étant de confiance par vos correspondants et pourra être ultérieurement certifiée par une autorité de confiance.

Vous pouvez créer deux clés distinctes, l'une pour le chiffrement et l'autre pour la signature. Dans ce cas, il faut exécuter deux fois la procédure ci-dessous.

Pour récupérer une clé de sécurité préalablement sauvegardée dans un fichier (au format *PKCS#12*, extensions *P12* ou *PFX*), reportez-vous à la section Importer une clé au format PKCS#12.

Pour créer une clé :

1. Ouvrez le menu **Stormshield Data Security** et sélectionnez **Nouvel utilisateur**.



2. Sélectionnez **Compte avec mot de passe**.
3. Déterminez le type de compte que vous souhaitez créer en choisissant entre :

- utiliser deux clés différentes pour chiffrer et signer (conseillé si vous utilisez un logiciel de la gamme Stormshield Data Security qui gère la signature électronique) ;
- utiliser une seule clé pour chiffrer et signer ;
- utiliser une seule clé pour chiffrer uniquement ;
- utiliser une seule clé pour signer uniquement.

Le reste de la procédure décrit comment créer un compte qui utilise une seule clé pour chiffrer et signer (clé personnelle).

Si vous souhaitez utiliser deux clés différentes, les actions décrites ci-dessous s'appliquent à la fois à la clé de chiffrement et à la clé de signature.

4. Cliquez sur **Créer un compte** et passez l'écran de bienvenue.
5. Entrez l'identifiant et le mot de passe de votre choix. Ils vous seront demandés pour vous connecter à Stormshield Data Security.

Le nombre de caractères gérés pour la création de l'identifiant est limité à 28.

Vous pouvez vérifier le mot de passe que vous avez saisi en cliquant sur l'œil situé à côté de **Mot de passe**.

5. Passez à l'écran suivant.
6. Choisissez l'option **Générer votre clé personnelle** (chiffrement ou signature) et sélectionnez le type et la longueur de votre clé.
7. Cliquez sur **Suivant**.
8. À partir de la fenêtre suivante, vous allez générer votre clé de sécurité à partir de nombres aléatoires. Pour cela, effectuez l'une des deux opérations suivantes :

- cliquez dans le cadre et déplacez la souris en effectuant des mouvements désordonnés ;
- tapez la touche F10 et tapez au hasard sur les touches de votre clavier.

Pour générer deux clés séparées pour le chiffrement et la signature, répétez les deux opérations précédentes (étape 6 et étape 8).

Une fois la capture terminée, passez à l'écran suivant.

9. Saisissez les informations constituant votre identité, telle qu'elle sera indiquée dans votre certificat auto-certifié.

Les champs suivis d'une astérisque sont obligatoires.

10. Passez à l'écran suivant.
11. Saisissez un mot de passe Security Officer (mot de passe de secours) qui sera demandé en cas d'oubli du mot de passe principal ou si vous bloquez votre compte en saisissant consécutivement trop de codes erronés (par défaut trois codes erronés). Pour plus de détails, lisez le paragraphe à la section Déblocage de votre compte.

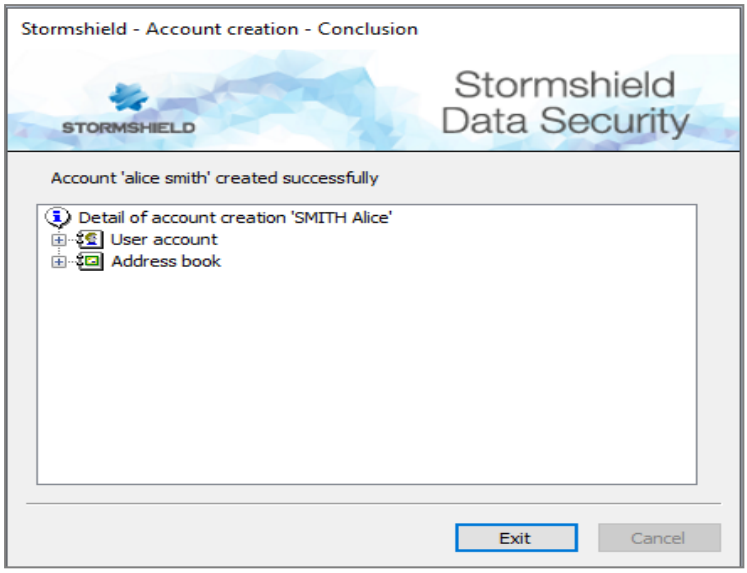
Passez ensuite à l'écran suivant en cliquant **Suivant**.

12. Vérifiez le récapitulatif de votre compte.

Revenez sur l'un des écrans précédents pour modifier une donnée erronée en cliquant sur **Précédent**.

13. Cliquez sur **Terminer**.

Stormshield Data Security génère votre (vos) clé(s) personnelle(s) et crée votre compte.



Votre compte est désormais utilisable.

NOTE
Votre compte est physiquement constitué d'un répertoire dont le nom est votre identifiant Stormshield Data Security (l'identifiant que vous avez donné à l'étape précédente (étape 4). Après la création de votre compte, ou après toute modification du compte, il est important de sauvegarder ce répertoire qui contient votre "keystore" (fichier contenant vos clés et paramètres de configuration) et votre annuaire de confiance.

Par défaut, les comptes utilisateurs sont situés à l'emplacement :

C:\ProgramData\Arkoon\Security BOX\Users

L'emplacement exact dépend de la configuration de votre système d'exploitation.

Votre compte comporte un certificat personnel auto-certifié. Ce certificat, produit par vous-même, peut éveiller la méfiance de certains de vos correspondants qui n'accordent leur confiance qu'aux certificats délivrés par une autorité reconnue. Si nécessaire, vous pouvez faire certifier votre clé par une autorité de certification (voir la section Certification de votre clé).

3.4.2 Importer une clé au format PKCS#12

Cette section explique comment créer votre compte en récupérant une clé de sécurité et un certificat sauvegardés dans un fichier au format *PKCS#12* (extensions *P12* ou *PFX*).

Cette fonction offre la possibilité d'utiliser une clé (et son certificat associé) générée par le passé ou encore d'utiliser une clé générée de façon centralisée par une PKI utilisant un puissant générateur de codes aléatoires. Enfin, cette fonction permet de sauvegarder des clés privées qui peuvent être utilisées pour des opérations de recouvrement.

1. Ouvrez le menu **Stormshield Data Security** et choisissez **Nouvel utilisateur**.
2. Sélectionnez **Compte avec mot de passe**.
3. Déterminez le type de compte que vous souhaitez créer en choisissant entre :

- utiliser deux clés différentes pour chiffrer et signer (conseillé si vous utilisez un logiciel de la gamme Stormshield Data Security qui gère la signature électronique) ;
- utiliser une seule clé pour chiffrer et signer ;

- utiliser une seule clé pour chiffrer uniquement ;
- utiliser une seule clé pour signer uniquement.

La suite de ce paragraphe décrit comment créer un compte qui utilise juste une seule clé (clé personnelle) pour le chiffrement et la signature.

Si vous souhaitez utiliser deux clés différentes pour le chiffrement et la signature, la procédure décrite ci-dessous s'applique aux deux types clés.

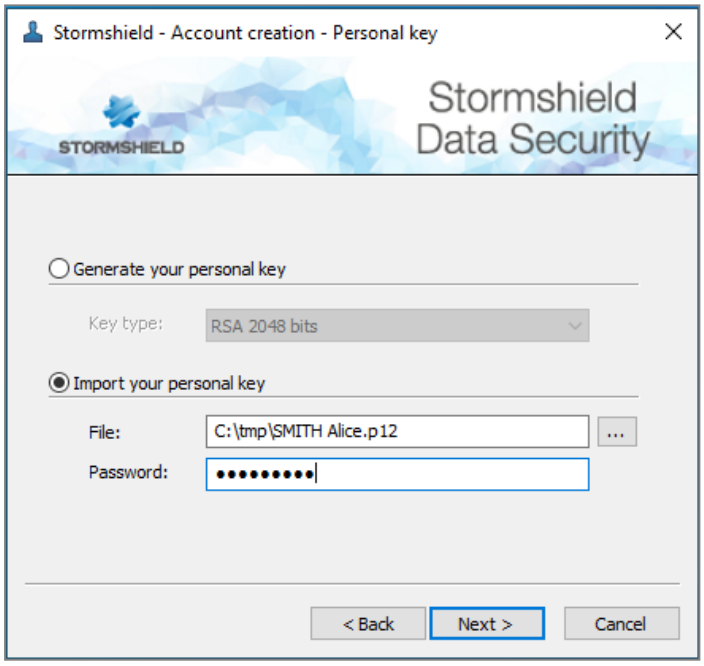
4. Cliquez sur **Créer un compte** et passez l'écran de bienvenue.
5. Entrez l'identifiant et le mot de passe de votre choix. Ils vous seront demandés pour vous connecter à Stormshield Data Security.

Vous pouvez vérifier le mot de passe que vous avez saisi en cliquant sur l'œil situé à côté de **Mot de passe**.

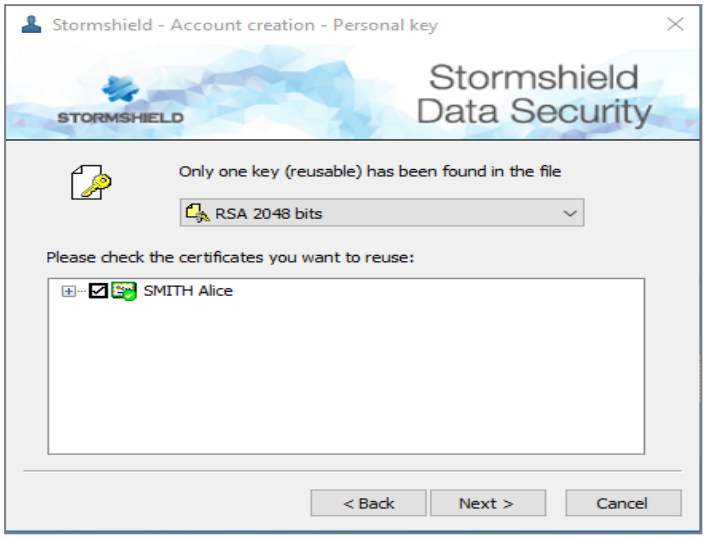
Passez à l'écran suivant.

6. Choisissez le bouton **Importer votre clé personnelle** et :

- sélectionnez le fichier. Le chemin complet vers le fichier contenant la clé et le certificat associé doit être indiqué (format *PKCS#12* avec l'extension *P12* ou *PFX*) ;
- le mot de passe qui protège la clé stockée dans ce fichier.



7. Passez à l'écran suivant.

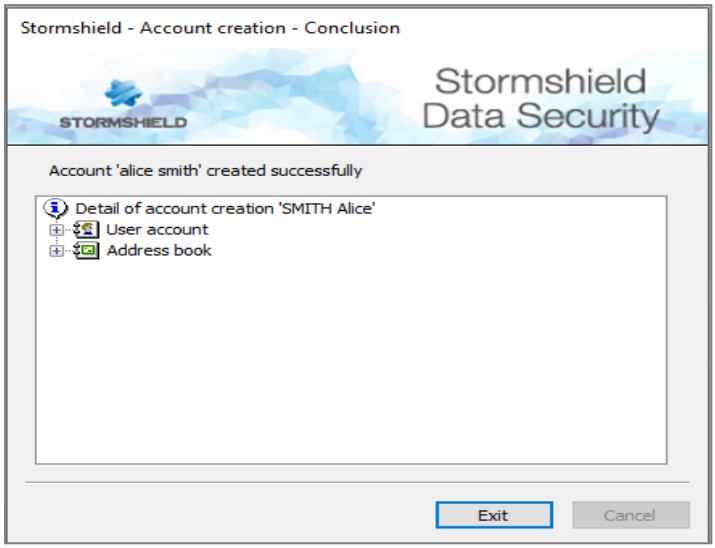


Si le fichier comporte plusieurs clés ou certificats, sélectionnez la clé à importer et cochez le certificat associé à cette clé.

- Pour afficher un certificat, cliquez dessus.
- Pour revenir à la liste des certificats contenus dans le fichier importé, cliquez sur le bouton : ;
- Si le fichier *PKCS#12* contient plusieurs clés, Stormshield Data Security les trie pour utiliser celle qui a un certificat compatible avec les usages demandés (chiffrement, signature ou les deux à la fois) et en fonction du type de compte à créer.
- Si plusieurs clés sont compatibles, Stormshield Data Security demande de choisir entre celles qui sont compatibles. Pour cela, l'utilisateur doit sélectionner successivement chacune des clés et visualiser le certificat associé jusqu'à ce qu'il ait trouvé la clé qu'il souhaite utiliser. Par défaut, Stormshield Data Security sélectionne la première clé dont le certificat est le plus longtemps valide.
- Si aucune clé n'est compatible, Stormshield Data Security vous en informe. Vous devez créer une nouvelle clé. Reportez-vous à la section Création d'une clé.

8. Cliquez sur **Suivant**.
9. Saisissez un mot de passe Security Officer (SO) ou mot de passe de secours qui vous sera demandé en cas d'oubli du mot de passe principal ou si vous bloquez votre compte en saisissant trop de codes faux consécutifs (par défaut trois codes erronés). Pour plus de détails, reportez-vous à la section Déblocage de votre compte.
10. Passez à l'écran suivant et vérifiez le récapitulatif de votre compte. Revenez sur l'un des écrans précédents pour modifier une donnée erronée en cliquant sur **Précédent**.
11. Cliquez sur **Terminer**.

Stormshield Data Security importe votre clé personnelle et crée votre compte. Votre compte est désormais utilisable.



IMPORTANT
Votre compte est physiquement constitué d'un répertoire dont le nom est votre identifiant Stormshield Data Security. Il est important de sauvegarder ce répertoire qui contient votre keystore (fichier contenant vos clés et paramètres de configuration) et votre annuaire, afin de prévenir toute perte d'information.

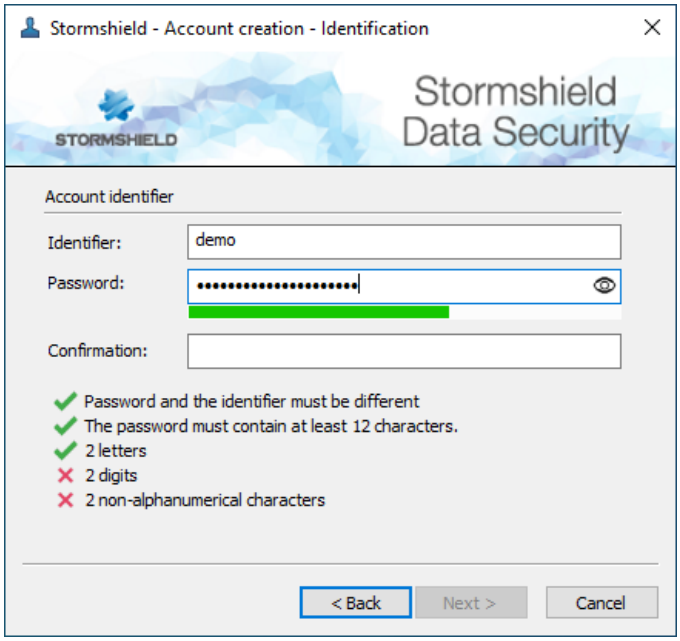
3.5 Informations sur votre mot de passe

Pour assurer la confidentialité de vos données, il est important de respecter un certain nombre de règles lors de la définition du mot de passe :

- il doit être suffisamment long ;
- il doit être constitué de caractères variés (caractères spéciaux et alphanumériques).

Ces règles sont définies dans Stormshield Data Authority Manager. Pour plus d'informations, reportez-vous à la section 12 *Personnalisation de l'installation* du guide de Stormshield Data Authority Manager.

Lors de la création de votre compte, Stormshield Data Security vous indique les règles à respecter :



3.6 Connexion à Stormshield Data Security

Lorsque vous vous connectez à Stormshield Data Security, votre identité est vérifiée et vos clés et paramètres sont accessibles.

En cas d'utilisation de plusieurs sessions Windows en parallèle, un seul utilisateur peut se connecter à Stormshield Data Security à un instant donné.

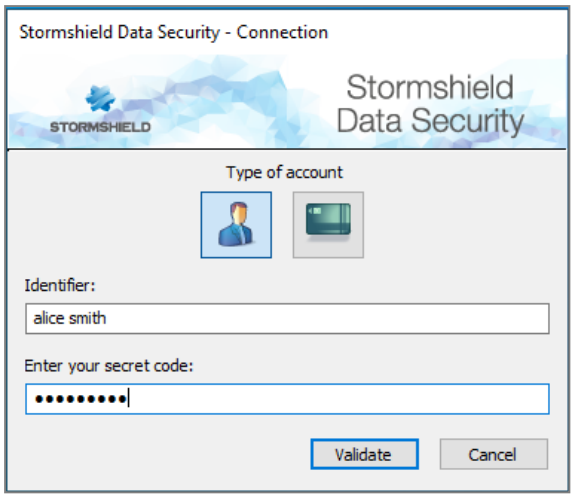
En mode carte, insérez simplement la carte pour ouvrir le menu Stormshield Data Security. La fenêtre de connexion (étape 2) s'ouvre directement si la carte est déjà insérée dans le lecteur. Si vous utilisez une carte à puce virtuelle, connectez-vous comme décrit ci-dessous.

Pour vous connecter à Stormshield Data Security :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Connecter**
3. Choisissez le **Type de compte** avec lequel vous souhaitez vous connecter.

Pour un compte mot de passe :

a. Saisissez votre identifiant et votre mot de passe :



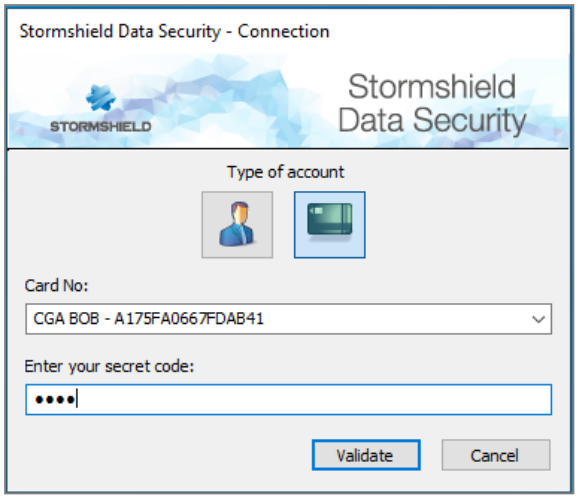
b. Cliquez sur **Valider**.

c. Si l'identifiant ne correspond pas à un compte existant, le champ pour entrer le mot de passe et le bouton **Valider** restent grisés. Dans ce cas, créez un compte Reportez-vous à la section Création d'un compte.

Par défaut, Stormshield Data Security propose l'identifiant du dernier utilisateur connecté.

Pour un compte carte :

a. Sélectionnez la carte ou le token et saisissez votre code confidentiel :



b. Cliquez sur **Valider**.

c. Si l'identifiant ne correspond pas à un compte existant, il est précédé de <NO SDS ACCOUNT>. Dans ce cas, créez un compte. Reportez-vous à la section Création d'un compte.

NOTE
Si vous saisissez consécutivement trop de codes erronés (par défaut : 3), votre compte se bloque. Pour le débloquer, reportez-vous à la section Déblocage de votre compte.

L'icône utilisateur à la gauche du champ identifiant utilisateur n'apparaît que lorsque Stormshield Data Security a trouvé le compte correspondant à l'identifiant.

Une fois votre connexion validée, l'icône Stormshield Data Security sur la barre de tâches devient verte : .

Vous venez d'ouvrir une session avec Stormshield Data Security. Tant que vous êtes connecté, vous pouvez accéder aux logiciels de la suite Stormshield Data Security installés sur votre poste de travail (File, Virtual Disk, Shredder, Sign, Mail).

Sur un poste, si aucun utilisateur ne s'est jamais connecté à Stormshield Data Security et si aucun compte Stormshield Data Security n'est disponible, Stormshield Data Security propose lors de sa première exécution une étape préalable pour la création d'un compte utilisateur.

En cas d'éloignement de votre poste de travail, il est conseillé de ne pas laisser votre session de travail ouverte. Pour cela, vous pouvez soit verrouiller votre session Stormshield Data Security (reportez-vous à la section Verrouillage), soit vous déconnecter (reportez-vous à la section Déconnexion).

3.7 Déconnexion

La déconnexion ne peut se faire que lorsque l'utilisateur est connecté (icône verte) ou verrouillé (icône rouge).

La déconnexion est la fermeture définitive de votre compte.

Il est possible de configurer Stormshield Data Security pour qu'il se déconnecte automatiquement. Reportez-vous à la section Paramétrage sur mise en veille et verrouillage Windows .

IMPORTANT
La déconnexion peut affecter le fonctionnement de certains des composants de Stormshield Data Security. Consultez la documentation de chaque composant pour plus d'informations.

NOTE
La procédure de déconnexion ci-dessous est la même pour le mode mot de passe ou le mode carte. Après déconnexion, si vous réinsérez la carte ou le token, vous accédez à l'écran de connexion.

Pour vous déconnecter :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Déconnecter**.
3. L'icône Stormshield Data Security dans la barre de tâches devient grise :  .

NOTE
La fermeture de la session Windows et l'arrêt du système entraînent la fermeture et l'arrêt de Stormshield Data Security.

3.8 Verrouillage

Le verrouillage interdit l'accès à vos clés.

Il est possible de configurer Stormshield Data Security pour verrouiller automatiquement votre session de travail. Reportez-vous à la section Paramétrage sur mise en veille et verrouillage Windows .

IMPORTANT
Verrouiller votre session peut affecter le fonctionnement de certains des composants de Stormshield Data Security. Par exemple, l'accès à des données contenues dans un fichier chiffré devient impossible. Consultez la documentation de chaque composant pour plus d'informations.

NOTE
La procédure de verrouillage ci-dessous est la même pour le mode mot de passe ou le mode carte. Le retrait de la carte du lecteur permet également le verrouillage de votre session. En réinsérant la carte ou le token, vous accédez directement à l'écran de déverrouillage.

Pour verrouiller votre session :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Verrouiller**.
3. L'icône Stormshield Data Security dans la barre de tâches devient rouge : 

L'accès à votre compte est devenu impossible.

3.9 Déverrouillage

> **NOTE**
> La procédure de déverrouillage ci-dessous est la même pour le mode mot de passe ou le mode carte. Réinsérez la carte dans le lecteur pour accéder à l'étape 2 de la procédure.

Pour déverrouiller votre session :

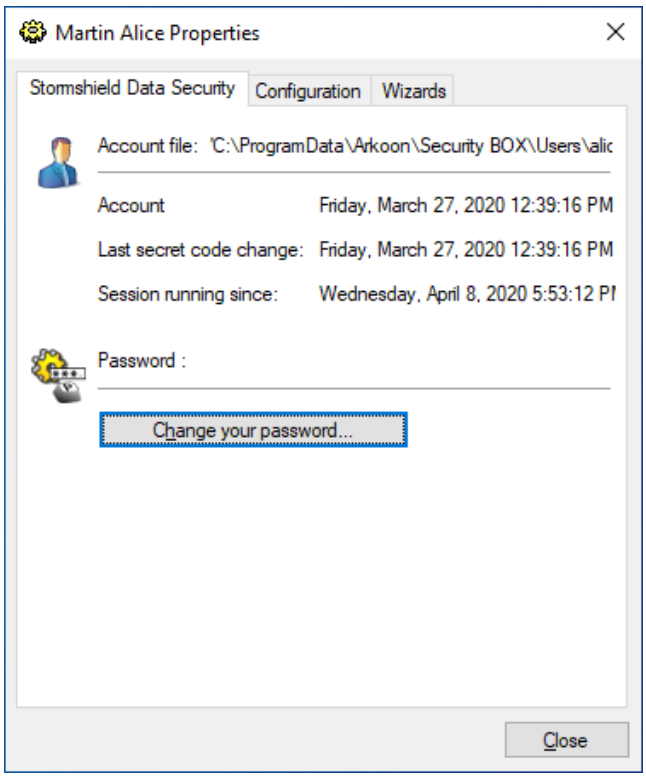
1. Double cliquez sur l'icône rouge pour ouvrir le menu **Stormshield Data Security**.
2. Saisissez votre mot de passe ou code confidentiel.
3. Cliquez sur **Déverrouiller**.
4. L'icône Stormshield Data Security redevient verte :  .

Si votre compte Stormshield Data Security est bloqué à la suite de tentatives infructueuses de saisie du mot de passe ou code confidentiel, une fenêtre vous informe que votre compte est bloqué. Vous devez d'abord vous déconnecter de votre compte avant d'essayer de le débloquer. Il n'est pas possible de déverrouiller un compte s'il est bloqué. Reportez-vous à la section Déblocage de votre compte.

3.10 Changement de votre mot de passe

Pour modifier manuellement votre mot de passe :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet **Stormshield Data Security** s'il n'est pas déjà ouvert :



4. Cliquez sur **Changer votre mot de passe**.
5. Saisissez votre mot de passe actuel puis deux fois votre nouveau mot de passe.

En cliquant sur l'œil situé dans le champ **Nouveau mot de passe**, vous visualisez votre mot de passe en clair. Celui-ci doit respecter les règles affichées en-dessous des champs.

NOTE
Stormshield Data Security différencie les majuscules des minuscules.
Par exemple, le mot de passe Dupont-1 est différent du mot de passe dupont-1.
Stormshield Data Security analyse le mot de passe et en indique la force. Reportez-vous à la section Informations sur votre mot de passe.

4. Installation et utilisation de l'extension pour carte (Cartes à puce et Clés USB)

L'authentification d'un utilisateur Stormshield Data Security se fait à l'aide d'un mot de passe ou d'un dispositif de sécurité de type carte à puce ou clé USB.

Pour installer et utiliser sur votre poste de travail un kit carte ou clé, vous devez installer l'extension carte de Stormshield Data Security.

Toutes les clés USB ne sont pas utilisables par Stormshield Data Security, notamment les clés USB de stockage d'information n'ont pas de fonction active de sécurité. Les clés utilisables comportent des mécanismes de sécurité identiques à ceux des cartes à puce. La terminologie clé USB utilisée dans ce document fait implicitement référence aux clés qui comprennent ces mécanismes.

Cette section décrit l'installation et l'utilisation de l'extension pour carte de Stormshield Data Security.

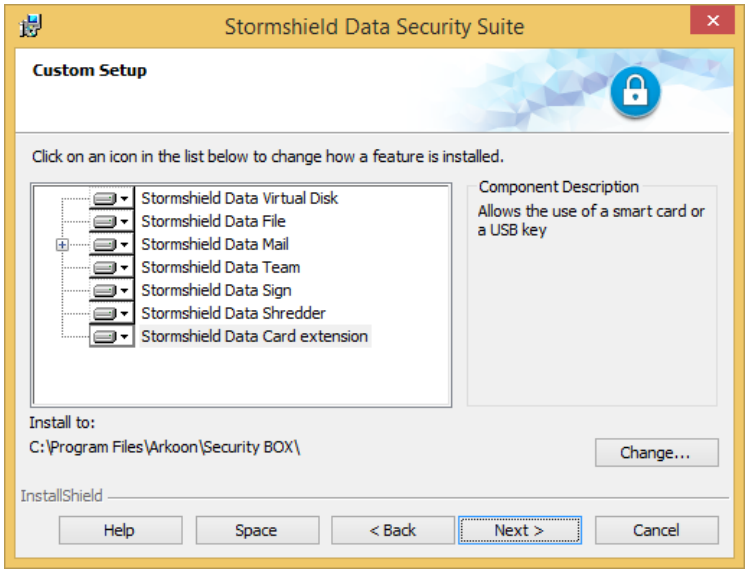
4.1 Comment installer l'extension pour carte

Le kit carte, le lecteur associé et le logiciel doivent être préalablement installés et configurés. Si cela n'est pas le cas, la détection automatique de la carte ne pourra être effectuée et celle-ci devra être lancée manuellement par la suite. Par défaut, le middleware Stormshield Data Security est installé et peut être utilisé avec les supports cryptographiques de technologie Plug-and-Play. Reportez-vous au *Guide d'administration* pour plus d'informations.

L'extension Stormshield Data Security pour carte et clé USB peut être installée en même temps que les autres composants. La procédure ci-dessous est à utiliser pour une installation ultérieure.

Pour installer l'extension Stormshield Data Security pour carte et clé USB :

1. Ouvrez le menu **Démarrer** de la barre de tâches.
2. Ouvrez le **Panneau de configuration** et choisissez la fonctionnalité **Ajout/Suppression de programmes**.
3. Sélectionnez dans la liste la ligne correspondant à Stormshield Data Security.
4. Cliquez sur **Changer**. Vous entrez en mode **Maintenance**.
5. Choisissez l'option **Modifier** puis passez les différents écrans.

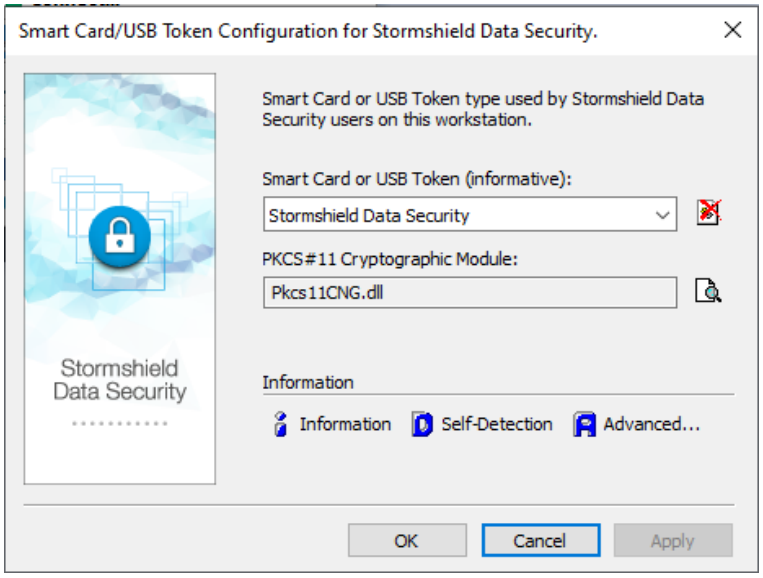


6. Sélectionnez l'élément Stormshield Data Security d'extension pour carte que vous voulez installer.

4.2 Configuration de l'extension pour carte

Vous pouvez indiquer à Stormshield Data Security le modèle précis de carte à puce ou de clé USB à utiliser. Pour cela :

1. Dans la barre de tâches de Windows, choisissez **Démarrer > Stormshield Data Security**.
2. Ouvrez le **Configurateur de l'extension carte**.
3. Cliquez sur le bouton **Auto-Détection** pour que Stormshield Data Security détecte automatiquement le bon module cryptographique puis sélectionnez le type de votre carte ou de votre clé USB parmi les valeurs pré-configurées :



4. Si vous ne trouvez pas le middleware associé à votre type de carte dans la liste proposée :

a. Saisissez le nom de votre carte dans la zone de saisie supérieure. En cliquant sur la flèche à droite, il est possible de voir la liste des lecteurs/cartes supportés et d'en sélectionner un.

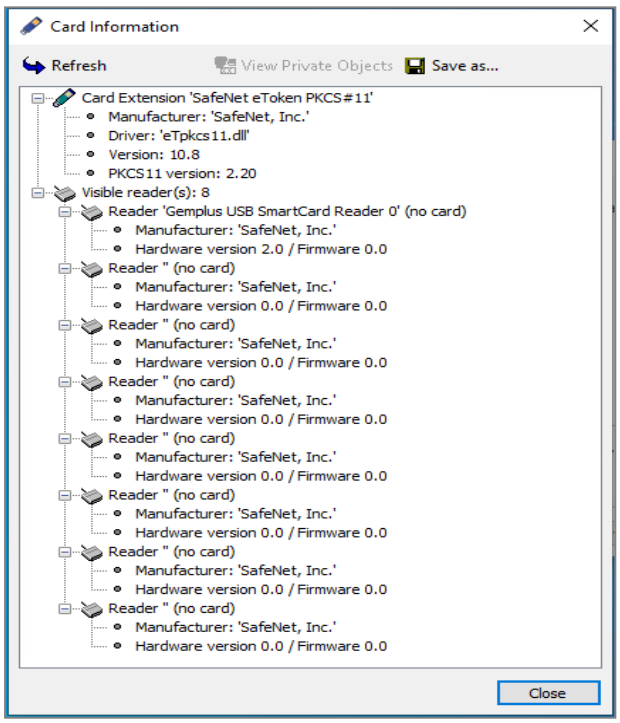
b. Renseignez le nom de la DLL du module d'interface cryptographique *PKCS#11* associé. Il faut que la DLL soit accessible de n'importe quelle application sur le système. Il faut donc que ce soit un chemin absolu ou que la DLL se trouve dans le répertoire system32 de Windows. Le nom de cette `DLL PKCS#11` dépend du logiciel (y compris son numéro de version) d'accès à la carte/clé. Consultez la documentation du fournisseur pour connaître ce nom.

Sinon, vous pouvez utiliser le middleware Stormshield Data Security proposé dans la liste avec tous les supports cryptographiques compatibles avec la technologie CNG de Microsoft (Plug-and-Play).

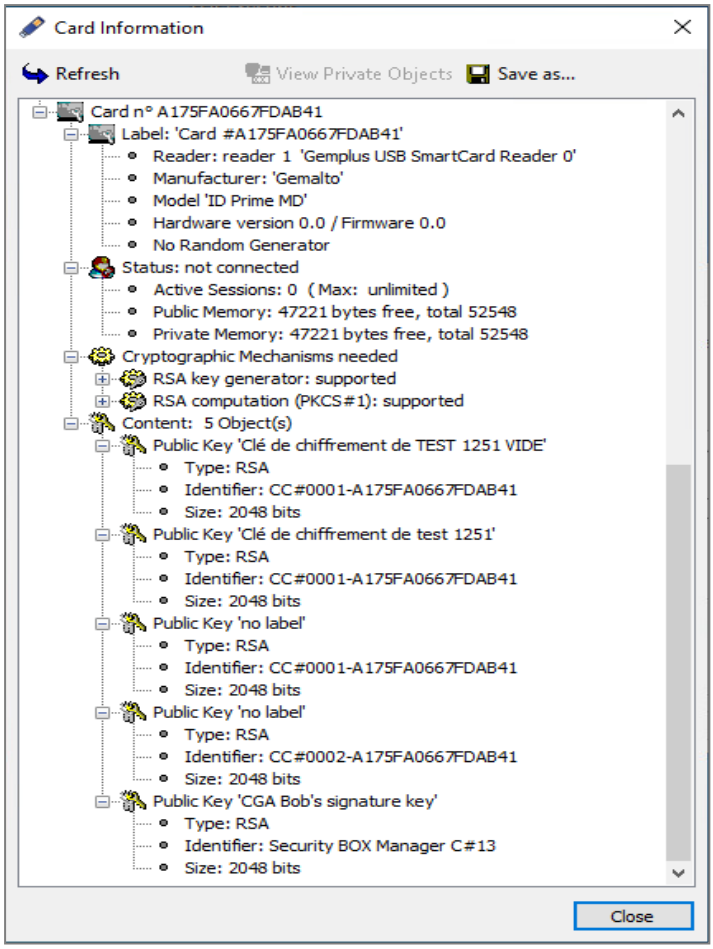
Pour la liste complète des cartes et clés supportées par Stormshield Data Security, contactez le service Support de Stormshield Data Security.

5. Cliquez sur **Informations** pour tester le module d'interface *PKCS#11* : le nombre de lecteurs visibles est indiqué. Si la DLL *PKCS#11* n'est pas accessible, un message d'erreur le signale ; il convient alors de vérifier le nom et le chemin de la DLL ainsi que de vérifier si les éléments pré-requis à cette DLL sont bien présents (notamment d'autres DLL).

- La copie d'écran suivante montre que l'extension carte est présente et configurée pour des cartes Gemalto. Il n'y a cependant pas de clés USB effectivement présentes ;



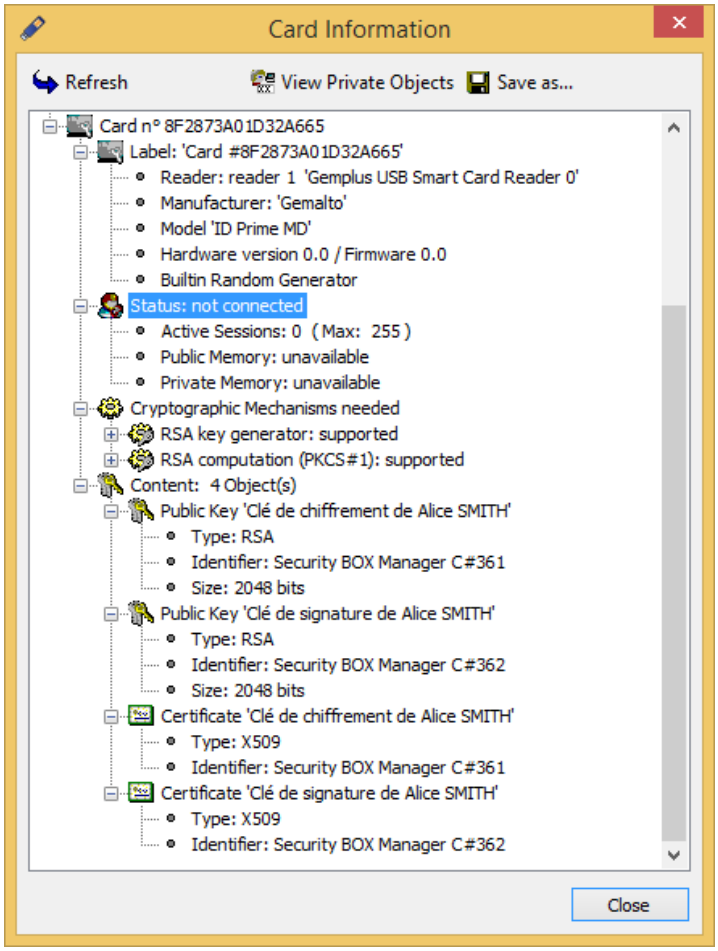
- La copie d'écran suivante montre qu'une clé USB est insérée et présente les caractéristiques de la clé USB ainsi que les objets publics (notamment les clés publiques et les certificats).



4.3 Consulter les objets privés

Il est possible de consulter les objets privés (essentiellement les clés privées) :

1. Cliquez sur **Information**.
2. Sélectionnez la ligne **Statut : non connecté** dans l'écran d'information.



3. Cliquez sur **Voir les objets privés**. Ce bouton n'est pas actif tant que la ligne précédente n'a pas été sélectionnée.
4. Saisissez le code PIN.

L'utilisation de la fenêtre **Information** permet d'analyser les problèmes d'accès aux cartes.

Le bouton **Enregistrer** permet d'enregistrer le contenu de la fenêtre dans un fichier. Le contenu de ce fichier est fréquemment demandé par le support en cas de problème d'accès à la carte/clé USB.

4.4 Création d'un compte en utilisant une carte à puce ou une clé USB

Avec une carte ou une clé USB :

- votre (vos) clé(s) de sécurité est (sont) stockée(s) dans la carte (clés privées et clés publiques) ;
- les calculs mettant en œuvre votre (vos) clé(s) privée(s) sont effectués par la carte (signature, déchiffrement).

La création d'un compte implique la création d'une ou plusieurs clés qui seront utilisées pour la sécurisation des volumes et des messages, et l'auto-certification de ces clés pour un usage immédiat.

Lors de la création d'un compte associé à une carte, Stormshield Data Security peut utiliser l'une des trois techniques suivantes :

- faire tirer à votre carte (clé) une nouvelle clé puis la faire certifier ;
- réutiliser une éventuelle clé et son certificat déjà présents dans la carte (clé) ;
- tirer une nouvelle clé et l'écrire dans la carte (clé) avec son certificat.

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Nouvel utilisateur**.
3. Choisissez un compte **carte à puce/clé USB**.
4. Sélectionnez la carte ou la clé USB que vous souhaitez utiliser.
5. Choisissez l'une des options suivantes dans le menu déroulant :

- utiliser deux clés différentes pour chiffrer et signer ;
- utiliser une seule clé pour chiffrer et signer ;
- utiliser une seule clé pour chiffrer uniquement ;
- utiliser une seule clé pour signer uniquement.

Reportez-vous à la section Création d'un compte pour plus d'informations.

5. Cliquez sur **Créer un compte**, puis passez l'écran de bienvenue.
6. Insérez votre carte, saisissez votre code confidentiel et cliquez sur **Connecter**.

Stormshield Data Security se connecte à la carte et affiche ce qu'elle contient : la carte peut être vide ou contenir les informations requises (clé publique, clé privée, certificat). Si la carte contient des données antérieures, vous pouvez choisir de les effacer.

Si vous choisissez d'effacer les clés existantes, seules les clés qui ne seront pas utilisées, seront effacées.

IMPORTANT
Dans le cas où la carte contient d'anciennes clés, il ne faut pas demander la suppression des objets non réutilisés : les anciennes clés seraient alors détruites.

7. Choisissez ensuite de générer une nouvelle clé ou de réutiliser une clé existante.

Pour la création d'un compte à deux clés, les étapes suivantes doivent être accomplies pour chaque clé.

- Pour générer une nouvelle clé, cliquez sur **Générer votre clé de chiffrement**. Sélectionnez le type et la longueur de votre clé puis validez.

Dans le cas d'un compte bi-clé, que la clé soit générée ou importée, il est possible de ne pas stocker les deux clés dans la carte mais d'en avoir une dans le compte Stormshield Data Security local. Pour cela, il faut désactiver l'option **Mettre votre clé de chiffrement dans la carte** (sélectionnée par défaut).

Il n'est pas possible de mettre les deux clés en local (sinon ce ne serait plus un compte carte). Cette case à cocher n'est par défaut pas active lorsqu'un objet de la carte est réutilisé.

Cliquez sur **Suivant** et allez à l'étape 8.

- L'option **Réutiliser une clé de la carte** est présente uniquement si une clé réutilisable a été trouvée dans la carte/clé USB. Si vous choisissez de réutiliser une clé existante, après avoir cliqué sur **Suivant**, la fenêtre suivante s'affiche :

Sélectionnez la clé à utiliser.

8. Votre clé de sécurité va être calculée à partir d'un nombre aléatoire. Pour obtenir ce nombre aléatoire, cliquez dans le cadre et déplacer la souris en effectuant des mouvements désordonnés.

La clé est générée localement sur le PC avant d'être importée sur la carte ou la clé USB. La génération d'une clé par la carte est possible pour certaines cartes. Reportez-vous au *Guide d'administration* pour plus d'informations.

Une fois la capture terminée, passez à l'écran suivant.

9. Si au moins une clé est générée localement, saisissez les informations constituant votre identité. Dans le cas d'un compte bi-clé, cette étape n'est effectuée qu'une seule fois.
10. Cliquez sur **Suivant**.
11. Sur l'écran suivant, il est possible de conserver une copie de vos clés dans votre fichier profil afin de pouvoir exporter cette clé par la suite ou de la sauvegarder tout de suite dans un fichier au format *PKCS#12*. Cette étape n'est proposée que si les clés (ou l'une d'entre elles) ont été générées localement.

NOTE
Le fait de garder une copie des clés dans le profil local (sous forme sécurisée) permet une

exportation de ces clés a posteriori (format *PKCS#12*) notamment dans le cas où la carte/clé USB ne permet pas l'exportation d'une clé privée.
La sauvegarde des clés dans un fichier *PKCS#12* permet d'avoir une copie des clés notamment dans le cas où la carte/clé USB ne permet pas l'exportation des clés privées.
L'intérêt de disposer d'une copie des clés privées (et des objets publics associés) est de permettre de recréer un compte Stormshield Data Security avec les mêmes clés/certificats et donc de pouvoir récupérer ses informations notamment en cas de perte/destruction de votre carte/clé USB.

12. Passez à l'écran suivant et vérifiez le récapitulatif de votre compte puis cliquez sur **Terminer**.

Stormshield Data Security génère, ou fait générer par la carte, vos clés personnelles et crée votre compte avec un récapitulatif de la clé ou des clés générées et de l'arborescence associée.

Le compte Stormshield Data Security créé en utilisant une carte à puce/clé USB est identifié par le numéro de série de la carte/clé USB.

Lorsque les clés (notamment la clé de signature) sont stockées dans la carte, il est recommandé de sauvegarder le compte Stormshield Data Security pour permettre la récupération de toutes les informations contenues.

4.5 Créer un compte en utilisant une carte à puce virtuelle

Pour créer un compte en utilisant une carte à puce virtuelle :

1. Déployez et peuplez la carte à puce virtuelle via des outils de gestion externes.
2. Ouvrez le menu **Stormshield Data Security**.
3. Choisissez **Nouvel utilisateur**.
4. Choisissez un compte **carte à puce/clé USB**.
5. Sélectionnez le middleware Stormshield Data Security dans le configurateur de carte.
6. Suivez les instructions décrites dans la section Création d'un compte en utilisant une carte à puce ou clé USB pour créer le compte.

4.6 Renouvellement des clés

Plusieurs méthodes sont envisageables pour le renouvellement des clés :

- génération de nouvelles clés directement sur le poste de l'utilisateur. Cette méthode est identique à celle des comptes mot de passe avec les spécificités des cartes/clés USB en ce qui concerne les possibilités d'exportation ; reportez-vous à la section Création d'une clé ;
- génération d'une clé en utilisant la carte. Cette méthode est identique à celle utilisée pour la génération de compte carte ; reportez-vous à la section Création d'un compte en utilisant une carte à puce ou une clé USB ;
- importation de nouvelles clés à partir de fichiers P12. Cette méthode est préférable car elle évite les phases de certification. La procédure est identique à celle des comptes mots de passe ; reportez-vous à la section Importer une clé au format PKCS#12.

IMPORTANT
Si vous avez changé votre clé en utilisant une carte à puce/clé USB, le déblocage de votre compte peut se révéler impossible. Vous devez impérativement conserver la clé de chiffrement antérieure dans la carte (ou la clé personnelle pour un compte n'utilisant qu'une seule clé) afin

de pouvoir accéder à votre compte Stormshield Data Security ultérieurement. La nouvelle clé de chiffrement sera automatiquement prise en compte lorsque le certificat de la clé en cours sera périmé.
Dans tous les cas, il est préférable de laisser les anciennes clés de chiffrement sur la carte afin de pouvoir déchiffrer les fichiers existants. Les clés de signature peuvent être supprimées immédiatement après le renouvellement car elles n'ont plus d'utilité.

4.7 Anciennes clés de chiffrement

Pour déchiffrer des fichiers chiffrés avec d'anciennes clés de chiffrement, vous pouvez sauvegarder, sur la nouvelle carte à puce/clé USB, ces anciennes clés et les certificats associés. Ces anciennes clés seront automatiquement utilisées pour le déchiffrement sans qu'il soit nécessaire de les importer en tant que clés de déchiffrement dans votre compte Stormshield Data Security. Il est toujours possible d'importer d'anciennes clés de chiffrement dans votre compte Stormshield Data Security.

IMPORTANT
Il est indispensable de stocker les certificats associés avec les anciennes clés pour que le déchiffrement soit possible – il serait autrement impossible de retrouver la clé à utiliser.

5. Certification de votre clé

L'utilisation de Stormshield Data Security requiert l'usage de clés certifiées. Cette section décrit comment certifier votre clé, demander un certificat et ajouter ou exporter un certificat.

5.1 Présentation des clés

Lorsque Stormshield Data Security génère une clé, il crée automatiquement un certificat auto-certifié (certificat signé directement avec sa propre clé privée). Les certificats ainsi produits n'étant pas émis par une autorité, ils ne sont pas automatiquement reconnus par d'éventuels correspondants.

La reconnaissance d'un certificat auto-certifié par un correspondant nécessite la transmission de ce certificat à ce correspondant avec une vérification de l'origine du certificat (par exemple, une remise en mains propres ou la vérification de l'empreinte du certificat. Dans le cadre d'échanges entre un grand nombre de correspondants, ce mécanisme d'échange est particulièrement fastidieux.

Pour qu'un utilisateur dispose d'un certificat automatiquement reconnu par un correspondant, il est nécessaire qu'il dispose d'un certificat émis par une autorité considérée comme étant de confiance par ce correspondant. Le manuel *Stormshield Data Authority Manager* décrit les moyens permettant la mise en place d'Infrastructures de Gestion de Clés, intégrant ou non une PKI ou un service externe. Il est également possible d'utiliser d'autres produits/services implémentant les fonctions de PKI sous réserve que ceux-ci gèrent des certificats conformes à la norme X.509 V3.

Dans le cadre d'une clé importée à partir d'un fichier *PKCS#12* ou présente dans une carte à puce, la phase de certification est rarement nécessaire car la carte est généralement directement fournie avec un certificat émis par une autorité de confiance.

La certification de vos clés comporte deux étapes :

- la soumission de la demande de certificat auprès de l'autorité ;
- l'ajout du certificat émis par l'autorité dans votre compte utilisateur.

Stormshield Data Security supporte toutes les autorités qui acceptent la demande de certificat au format *PKCS#10* et émettent des certificats binaires (*.cer*), des certificats PEM (*.crt*) ou des chaînes de certificats (*.p7b* ou *.p7c*).

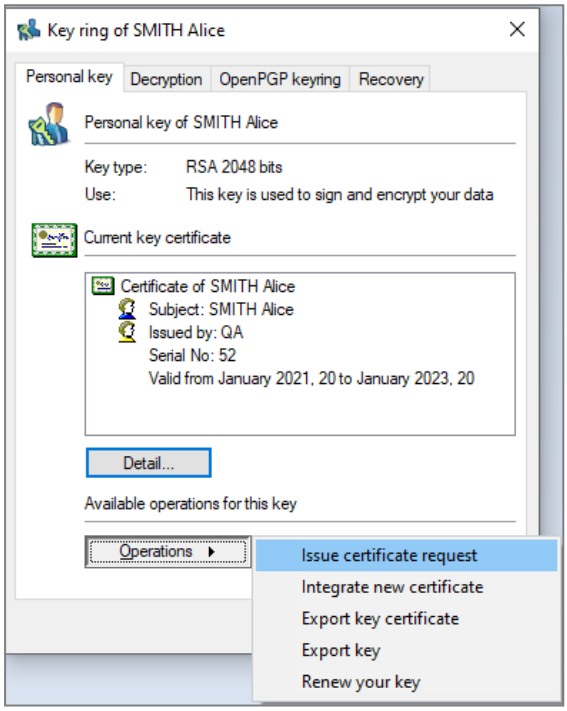
Stormshield Data Security ne gère pas les transferts de demandes de certificats ni les réponses. Ces transferts ne sont pas normalisés et varient selon l'autorité consultée : ils peuvent se faire via un support disque, le courrier électronique, ou encore une interface Web, etc. Contactez l'autorité en question pour connaître les détails de la procédure habituelle.

Notez qu'en utilisant l'extension de navigation Internet de Stormshield Data Security, il est possible de dialoguer avec une PKI via une interface Web. Ceci vous permet de soumettre les demandes de certificat auprès d'une PKI externe en utilisant les caractéristiques spécifiques de votre propre navigateur Internet, ce qui vous dispense de manipuler les requêtes au format *PKCS#10*. Les navigateurs supportés sont Microsoft Internet Explorer (via une interface CSP) et Netscape/Mozilla (via une interface *PKCS#11*).

5.2 Demande de certificat

Pour générer une demande de certificat :

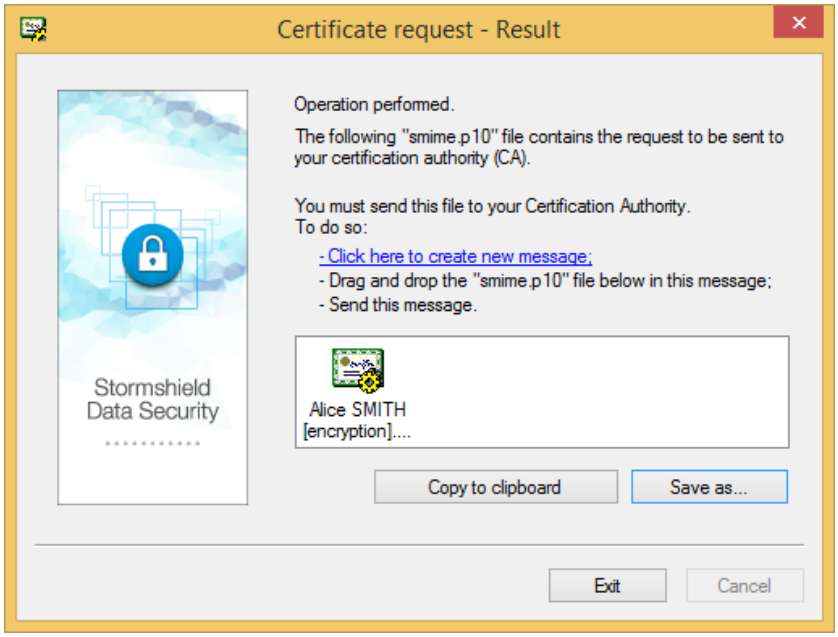
1. Ouvrez le menu **Stormshield Data Security** et choisissez **Propriétés**.
2. Cliquez sur l'onglet *Configuration*.
3. Choisissez l'icône **Porte-clés**.
4. Si vous possédez deux clés, choisissez l'onglet *Clé de chiffrement* ou *Clé de signature*. Sinon, choisissez *Clé personnelle*.
5. Cliquez sur **Opérations** et choisissez **Faire une demande de certificat**, puis passez l'écran d'introduction :



6. Saisissez tous les paramètres demandés. Ces paramètres font partie de votre identité et seront utilisés pour établir le certificat qui vous sera délivré. Votre autorité peut cependant modifier ces données.
7. Passez à l'écran suivant.
8. Vérifiez le récapitulatif de votre demande. Revenez sur l'écran précédent pour modifier une donnée erronée en cliquant sur **Précédent** si nécessaire. Passez à l'écran suivant.
9. L'écran affiche votre demande de certificat au format *PKCS#10*.

Pour la transmettre à votre autorité, vous pouvez :

- la copier en cliquant sur **Copier dans le presse-papier**. Vous pouvez alors coller la requête dans une fenêtre liée au PKI ;
- l'enregistrer dans un fichier en cliquant sur **Enregistrer sous**. Le fichier contenant la requête peut alors être envoyé à l'autorité de certification ;
- sélectionner le lien **Créez un nouveau message en cliquant ici**. Un message s'ouvre par défaut dans votre messagerie. Indiquez le destinataire (l'autorité de certification ou une autorité d'enregistrement en fonction de la PKI utilisée). Copiez la demande vers ce message (par exemple par un glisser-déposer) à partir de l'icône qui est dans la fenêtre et complétez le message en fonction des spécificités de l'autorité de certification.

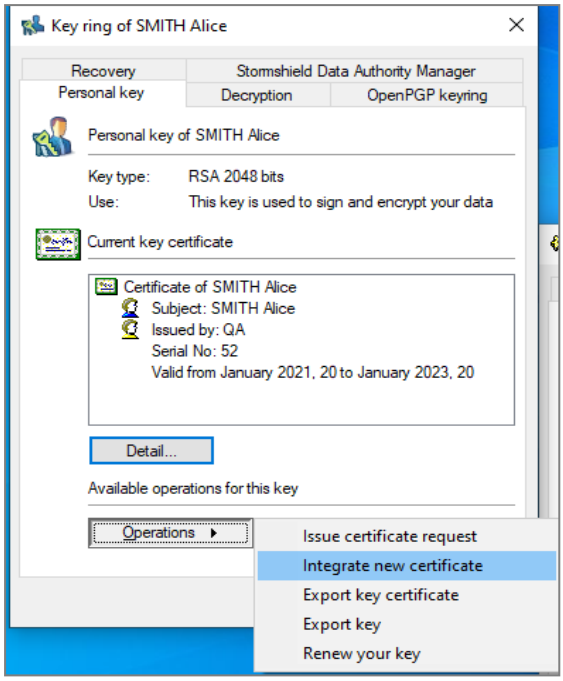


Lorsque la demande de certificat a été transférée à l'autorité ou sauvée dans un fichier, cliquez **Quitter**.

5.3 Intégration d'un certificat

Pour intégrer le certificat délivré par votre autorité :

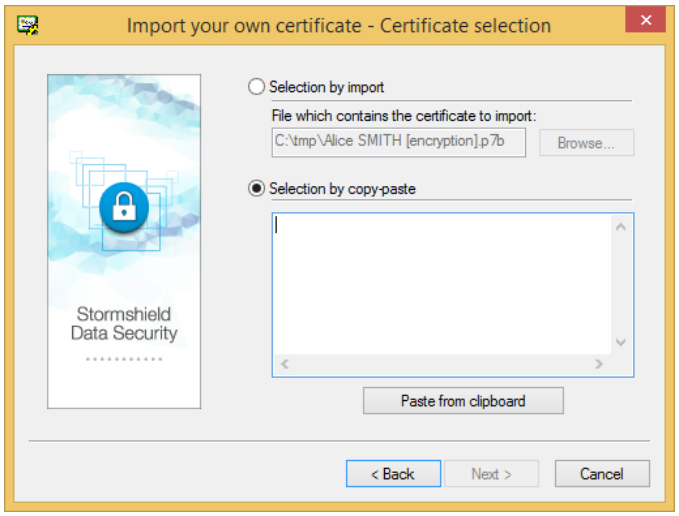
1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Porte-clés**.
5. Si vous possédez deux clés, choisissez l'onglet *Clé de chiffrement* ou *Clé de signature*. Si vous n'avez qu'une clé, choisissez l'onglet *Clé personnelle*.
6. Cliquez sur **Opérations** et choisissez **Intégrer un nouveau certificat** puis passez l'écran d'introduction.



7. Pour transférer votre certificat (au format X509), vous pouvez :

- l'importer (**Sélection par importation**) depuis un fichier (*.CER* (format binaire), *.CRT* (format PEM), *p7b/p7c* (chaîne de certificats)
- le copier (**Sélection par copier-coller**) s'il vous a été fourni codé en Base 64. Dans ce cas, il faut bien penser à mettre les balises :

====== BEGIN CERTIFICATE ==== et ===== END CERTIFICATE =====



8. Passez à l'écran suivant.
9. Si le fichier (format *p7b* ou *p7c*) comporte plusieurs certificats, cochez le certificat que vous souhaitez importer.

Les différents certificats sont présentés dans une structure arborescente qui reflète la hiérarchie. Les certificats des utilisateurs se situent à la base de l'arbre (à gauche) alors que les autorités sont placées vers la droite (un niveau à chaque nœud de l'arbre). Pour dérouler l'arborescence, il faut cliquer sur le symbole + qui est à gauche du nom du porteur du certificat.

Un certificat coché indique qu'il est sélectionné et qu'il sera importé. Le certificat de l'utilisateur courant est automatiquement sélectionné. Les certificats d'autorité et les certificats des autres utilisateurs ne sont, par défaut, pas sélectionnés.

Lorsque vous sélectionnez un certificat, un message de confirmation s'affiche. Les certificats externes sélectionnés (à l'exception du certificat de l'utilisateur courant) sont ajoutés à votre l'annuaire local et seront donc considérés comme étant de confiance parce qu'émis par une source reconnue et autorisée.

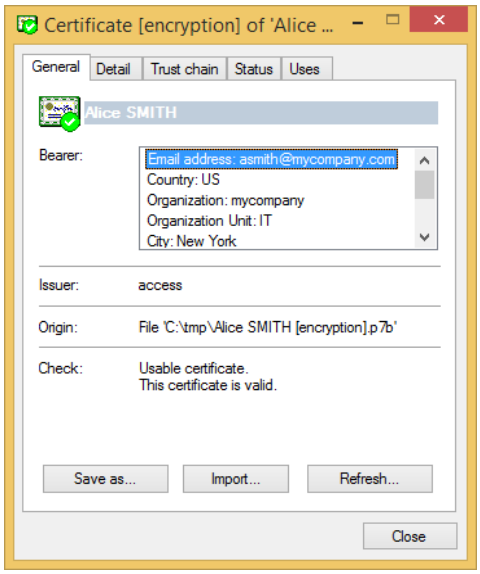
Pour revenir à la liste des certificats, cliquez sur le bouton **Fermer**.

10. Immédiatement à gauche du nom, il y a une icône indiquant le statut du certificat :

vert = OK, jaune = avertissement, rouge = erreur.

Pour connaître la raison de l'erreur ou de l'avertissement, il est nécessaire de visualiser le certificat.

Pour afficher un certificat, cliquez dessus :



La section **Contrôle** indique le statut.

Pour revenir à la liste de certificats, cliquez sur **Fermer**.

11. Passez à l'écran suivant et vérifiez le récapitulatif du certificat que vous allez intégrer à votre compte.
12. Cliquez sur **Terminer** et vérifiez le résultat de l'opération.

Vous devez désormais communiquer ce nouveau certificat à vos correspondants, par exemple en leur envoyant un message signé indiquant que vous leur communiquez votre nouveau certificat (lequel est inclus dans votre signature). Dans le cas où un annuaire LDAP est utilisé par la PKI et qu'il est partagé avec les correspondants, cet envoi n'est pas nécessaire car ceux-ci pourront le retrouver directement.

5.4 Exporter votre certificat

Vous pouvez exporter dans un fichier votre certificat, avec éventuellement sa parenté, afin de le fournir directement à vos correspondants ou de le déposer par exemple dans un annuaire (LDAP).

Le fichier contenant votre certificat est généré selon l'un des formats suivants :

- le certificat seul :

- format binaire (extension *.cer*) ;
- format binaire codé base 64 (extension *.crt*).
- le certificat avec sa parenté :
- format PKCS#7 (extensions *.p7c* ou *.p7b*).

Pour exporter le certificat auto-certifié ou délivré par votre autorité :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Porte-clés**.
5. Si vous possédez deux clés, choisissez l'onglet *Clé de chiffrement* ou *Clé de signature*. Si vous avez qu'une clé, choisissez l'onglet *Clé personnelle*.
6. Cliquez sur **Opérations** et choisissez **Exporter le certificat de votre clé**.

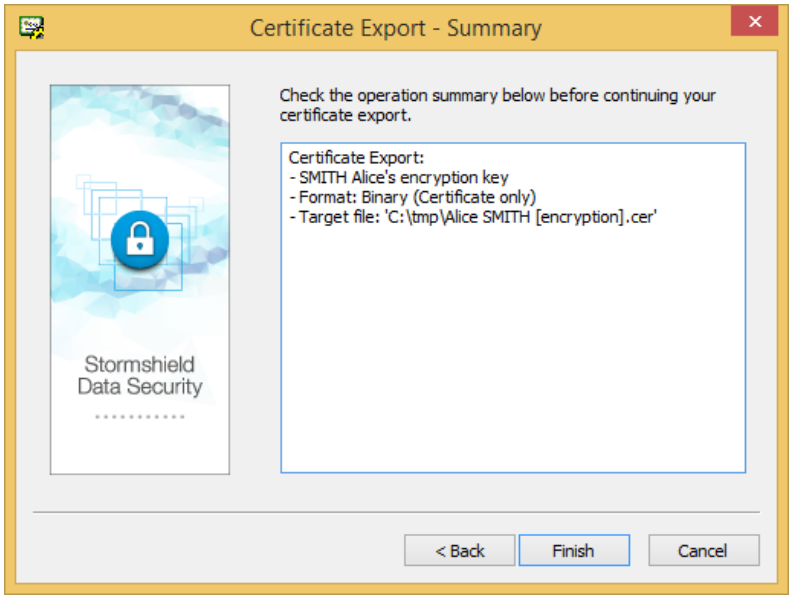
Passez l'écran d'introduction.

7. Choisissez entre **Exporter le certificat seul** ou **Exporter le certificat et sa parenté** puis passez à l'écran suivant pour indiquer le nom du fichier.
8. Saisissez le nom du fichier à créer et cliquez sur **Suivant**.

NOTE
L'appui sur **Enregistrer sous** sauvegarde le nom complet du fichier d'exportation mais n'exporte pas immédiatement le fichier.

Cliquez sur **Suivant**.

9. Vérifiez le récapitulatif, puis cliquez sur **Terminer**.



Votre certificat a été exporté dans le fichier indiqué.

6. Utilisation des certificats

Les certificats au format X509 contiennent notamment des données concernant la clé publique et son détenteur. La clé publique est utilisée pour véhiculer des informations confidentielles entre les correspondants, plus particulièrement pour transmettre les clés de chiffrement de données.

Cette section explique comment :

- mettre en œuvre un annuaire centralisé selon le protocole LDAP. ;
- consulter et gérer votre annuaire de confiance ;
- échanger des certificats par l'envoi de messages.

IMPORTANT
Les seuls certificats acceptés sont les certificats auto-signés présents dans l'annuaire de confiance de l'utilisateur et les certificats dont la parenté est dans l'annuaire de confiance.

6.1 Mise en œuvre d'annuaires LDAP

Si Stormshield Data Security ne trouve pas le certificat d'un correspondant dans votre annuaire de confiance, il peut systématiquement le rechercher sur un ou plusieurs serveurs LDAP. Les annuaires LDAP sont utilisés pour rechercher des certificats et les importer dans un annuaire de confiance, ou comme cible pour les contacts déclarés dans l'annuaire de confiance.

Contrairement aux certificats provenant de l'annuaire de confiance, les certificats reçus d'un annuaire LDAP ne sont pas automatiquement considérés comme étant de confiance. Cependant, avant d'être utilisés par les composants Stormshield Data Security, tous les certificats, quelle que soit leur provenance, sont entièrement analysés.

Si la parenté des certificats provenant de l'annuaire LDAP ne peut être vérifiée, une erreur est générée et le processus de sécurisation est bloqué. Dans le cas des certificats provenant de votre annuaire de confiance, seul un avertissement est généré et le processus de sécurisation peut arriver à son terme.

Pour mettre en œuvre un annuaire LDAP, vous devez configurer un moteur de recherche LDAP et déclarer un annuaire LDAP.

Il est possible de déclarer des annuaires LDAP qui sont utilisés uniquement pour des recherches manuelles (pour des importations par exemple).

NOTE
Les annuaires déclarés pour les recherches automatiques doivent être accessibles et/ou opérationnels en permanence. Attention aux serveurs dont l'accessibilité est masquée par un pare-feu : un pare-feu peut intercepter et faire échouer les demandes de connexions IP entre l'ordinateur et l'annuaire, et les requêtes Stormshield Data Security.

6.1.1 Configurer un moteur de recherche LDAP

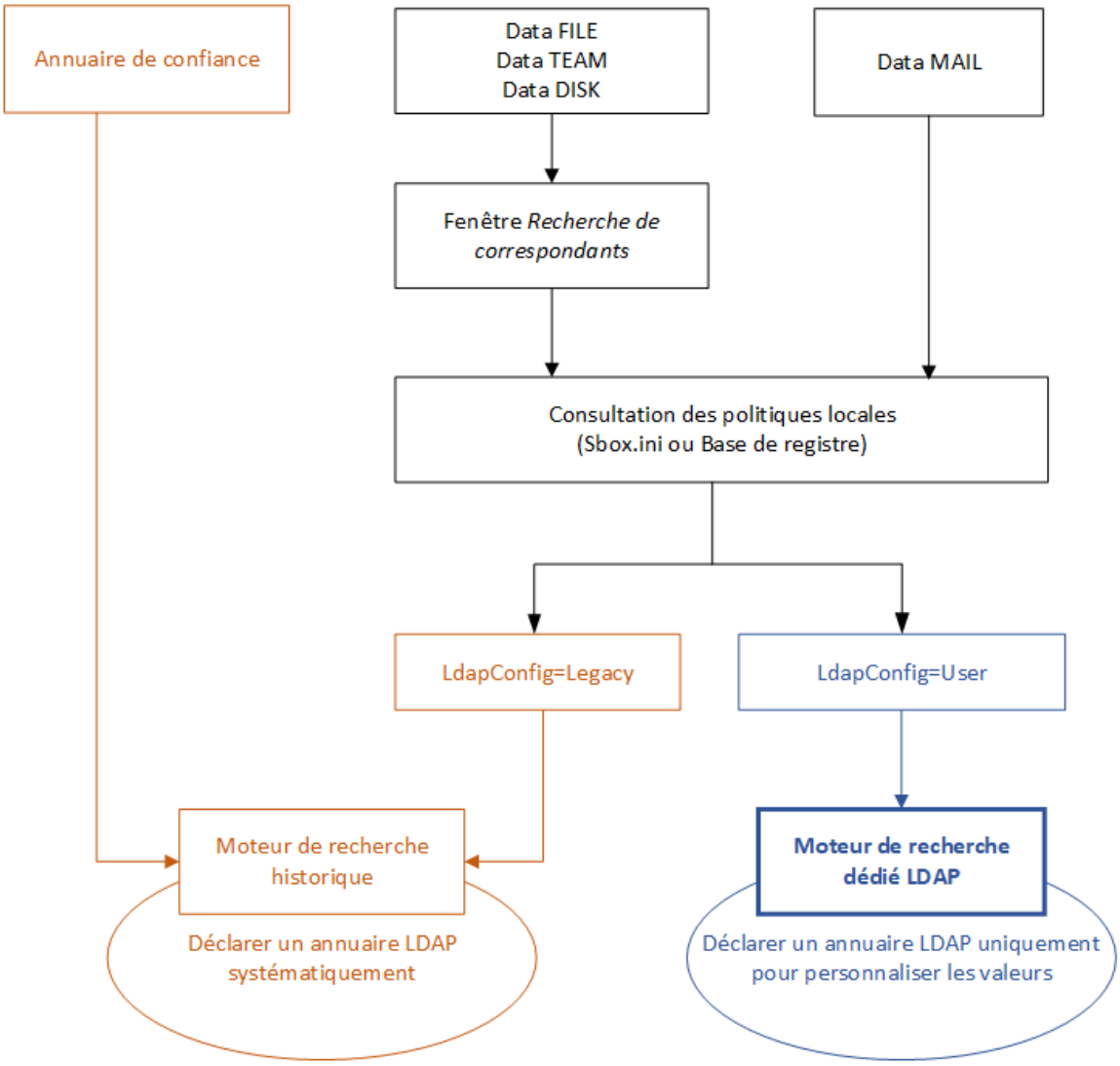
Deux moteurs de recherche sont disponibles pour rechercher des correspondants dans vos annuaires LDAP :

- Le moteur de recherche historique, qui peut être utilisé par l'ensemble des composants Stormshield Data Security et qui est obligatoirement utilisé par l'annuaire de confiance,
- Le moteur de recherche dédié LDAP, qui peut être utilisé par les composants Stormshield Data File, Disk, et Team via la fenêtre de sélection des collaborateurs, ainsi que par le composant Stormshield Data Mail. Ce moteur n'est pas utilisé par l'annuaire de confiance.

Le paramètre `LdapConfig` dans les politiques locales (fichier *Sbox.ini*) permet de choisir le moteur à utiliser. Les valeurs possibles sont :

- `LdapConfig=Legacy` : moteur de recherche historique (par défaut),
- `LdapConfig=User` : moteur de recherche dédié LDAP.

Le schéma ci-dessous décrit quel moteur de recherche est utilisé en fonction des composants dans lesquels la recherche LDAP est effectuée et de la personnalisation que vous souhaitez apporter.



Personnaliser le moteur de recherche dédié LDAP

Si vous souhaitez utiliser un autre serveur LDAP et/ou des attributs différents, personnalisez le moteur de recherche.

1. Dans la section [Directory] du fichier *SBox.ini*, appliquez la valeur *User* au paramètre `LdapConfig`. Pour plus d'informations, reportez-vous à la section Politiques locales du *Guide d'administration* Stormshield Data Security.
2. Déclarez un annuaire LDAP tel que décrit dans la section Déclarer un annuaire LDAP :
   a. Spécifiez le serveur LDAP à utiliser,
   b. Spécifiez les attributs que vous souhaitez utiliser.

Utiliser le moteur de recherche de l'annuaire de confiance

1. Dans la section [Directory] du fichier *SBox.ini*, appliquez la valeur *Legacy* au paramètre `LdapConfig`. Pour plus d'informations, reportez-vous à la section Politiques locales du *Guide d'administration* Stormshield Data Security.
2. Déclarez un annuaire LDAP tel que décrit dans la section Déclarer un annuaire LDAP.

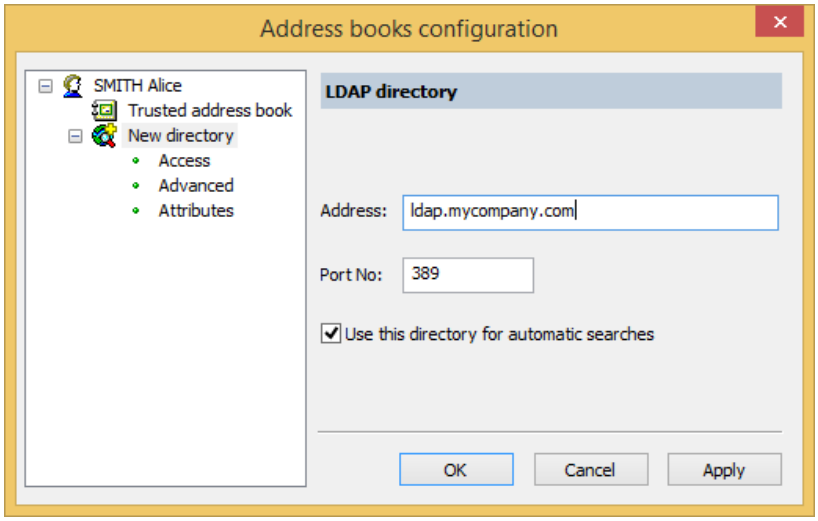
6.1.2 Déclarer un annuaire LDAP

Déclarez un annuaire LDAP pour pouvoir faire des recherches LDAP avec l'annuaire de confiance ou pour personnaliser le serveur et/ou les attributs LDAP dans Stormshield Data File, Disk, Team ou Mail.

1. Ouvrez le menu **Stormshield Data Security** et choisissez **Propriétés**.
2. Cliquez sur l'onglet *Configuration*.
3. Choisissez l'icône **Annuaire**.
4. Choisissez le menu **Fichier > Configuration**.
5. Développez votre racine, puis la catégorie **Annuaire LDAP**.

L'annuaire LDAP est le deuxième annuaire en dessous de votre annuaire de confiance. Si aucun annuaire LDAP n'est encore déclaré, il sera alors juste listé comme **Nouvel annuaire**.

6. Renseignez le nom du serveur et si besoin son numéro de port (dont la valeur usuelle est 389). Une connexion SSL est mise en œuvre si le port renseigné est le 636.

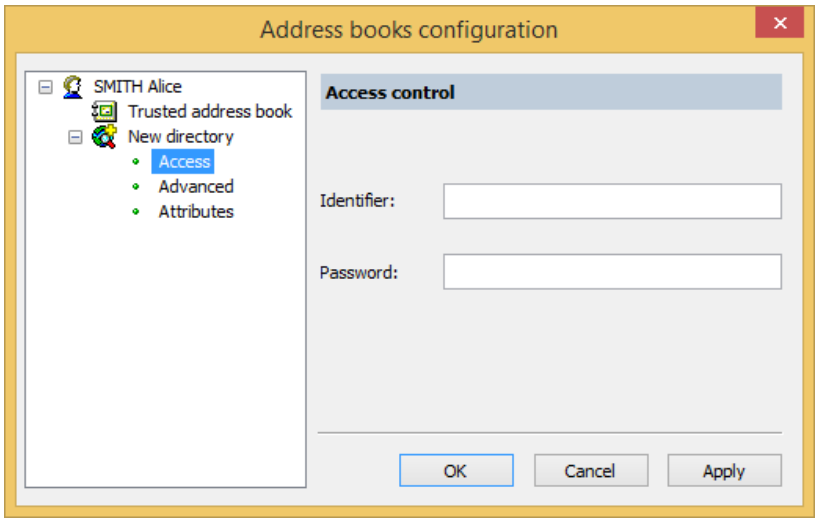


6.1.3 Rubrique Accès

L'accès à votre annuaire LDAP supporte deux modes d'authentification :

- NTLM (mécanisme d'identification Windows, l'identifiant et le mot de passe ne circulent pas sur le réseau).
  Pour mettre en œuvre l'authentification du domaine Windows, il suffit d'ajouter à la configuration le mot-clé `<MySelf>` dans **Identifiant** et **Mot de passe**.

- Simple (mécanisme d'identification universel, l'identifiant et le mot de passe sont envoyés en clair sur le réseau).
  Si le premier mode d'authentification échoue, Stormshield Data Security tente le second mode.
  Saisissez dans l'écran ci-dessous l'identifiant et le mot de passe d'accès qui ont été fournis par l'administrateur de l'annuaire LDAP.



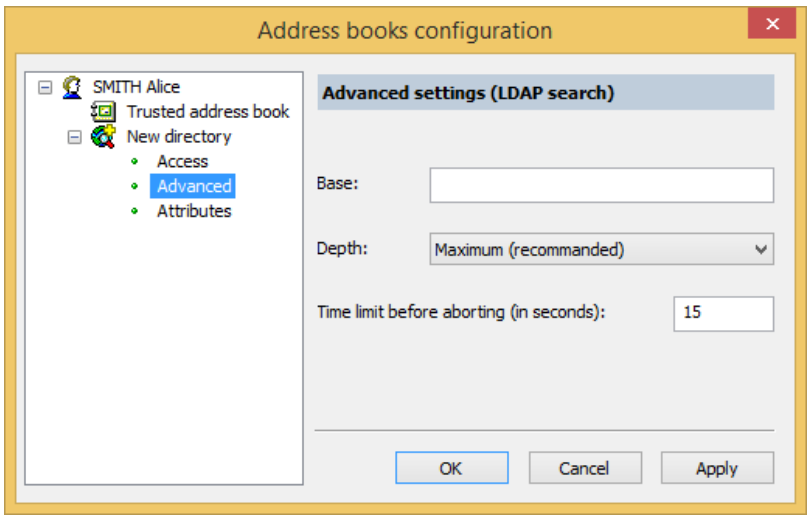
NOTE
L'authentification via Kerberos n'est pas supportée.

6.1.4 Recherche de l'annuaire LDAP

Vous pouvez configurer les recherches des annuaires LDAP avec les écrans qui suivent.

Rubrique des paramètres avancés

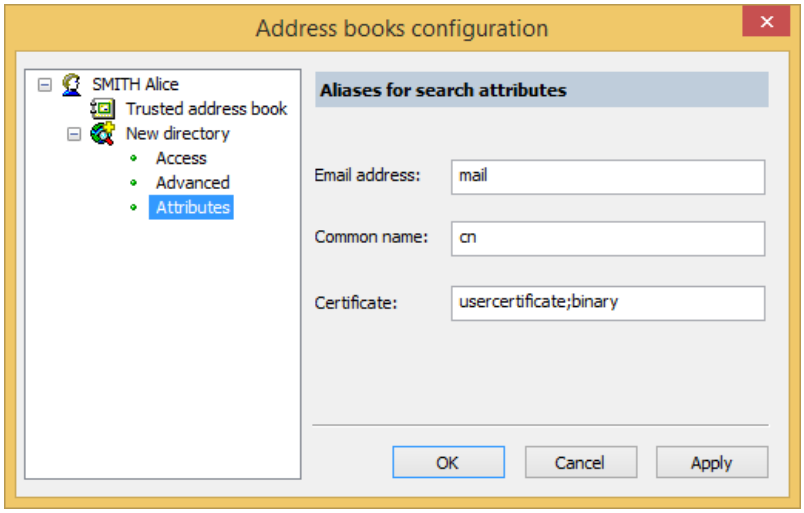
Cet écran vous permet d'affiner les recherches dans l'arborescence de l'annuaire.



- **Base** : indiquez la branche de l'arbre ("dn" pour Distinguished Name) à partir de laquelle Stormshield Data Security doit effectuer les recherches ;
- **Profondeur** : indiquez la profondeur de la recherche avec :
- **Minimum** si la recherche est directement faite sur la base de recherche spécifiée ;
- **Un niveau** si la recherche doit s'effectuer uniquement sur le niveau immédiatement en dessous de la base de recherche ;
- **Maximum** si la recherche doit s'effectuer sur tous les niveaux en dessous de la base de recherche.
- **Limite de temps avant abandon** : augmentez cette durée en fonction des performances de votre infrastructure technique pour l'accès à l'annuaire. Il ne faut toutefois pas mettre une valeur trop importante pour ne pas bloquer complètement les recherches en cas de non réponse d'un annuaire.

Rubrique des attributs de recherche

Une recherche LDAP effectuée par Stormshield Data Security porte sur les attributs : adresse e-mail, nom d'usage et certificat.

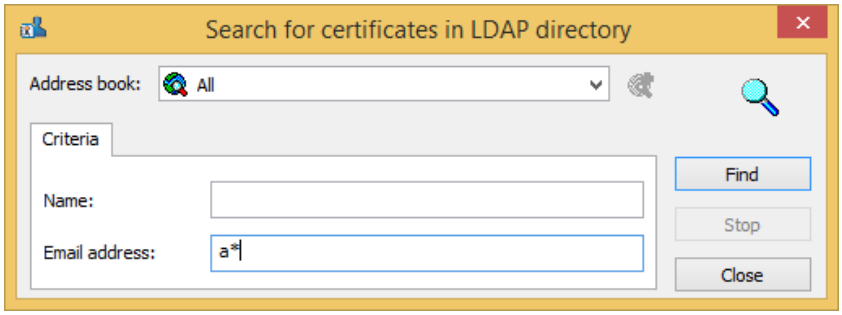


Cet écran permet de renseigner les noms de ces attributs si, dans votre annuaire LDAP, ils sont différents des noms usuels : respectivement **mail**, **cn** et **usercertificate;binary**.

6.1.5 Importer un certificat publié à partir d'un annuaire LDAP

Stormshield Data Security permet d'importer dans votre annuaire de confiance le certificat d'un correspondant publié à partir un annuaire LDAP quelconque.

1. Pour cela, ouvrez le menu **Stormshield Data Security** et choisissez **Propriétés**.
2. Cliquez sur l'onglet *Configuration*.
3. Choisissez l'icône **Annuaire**.
4. Choisissez le menu **Édition / Rechercher**.



5. Renseignez l'adresse du serveur LDAP à interroger et les critères de recherche : nom et/ou adresse e-mail. Vous pouvez inclure dans vos critères des caractères génériques tels que "*" ou "?" si l'annuaire interrogé les accepte.
6. Cliquez sur **Rechercher** pour lancer la recherche ; la fenêtre affiche le résultat de la recherche. Stormshield Data Security n'affiche dans cette fenêtre que les certificats, c'est-à-dire les certificats présents dans l'annuaire, valides (par rapport à leur période de validité) et utilisables pour le chiffrement et/ou la signature électronique.
7. Pour afficher le détail d'un certificat, sélectionnez-le et cliquez sur **Aperçu**.
8. Pour importer dans votre annuaire un ou plusieurs certificats, sélectionnez-les et cliquez sur **Importer**.

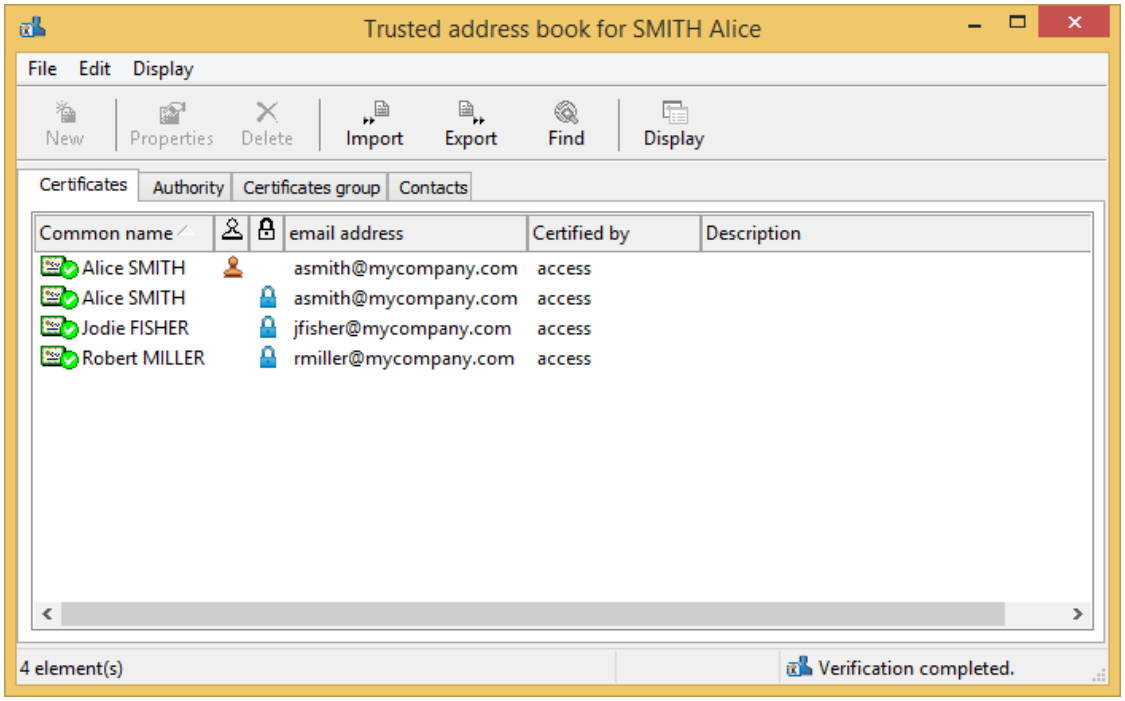
6.2 Gérer votre annuaire de confiance

Votre annuaire de confiance permet de conserver et d'utiliser les certificats de vos correspondants (et autorités). Cet annuaire est protégé, il ne peut être modifié que par vous-même. Il est dit de « confiance » c'est-à-dire que tous les certificats que vous y avez intégrés sont considérés comme valides par Stormshield Data Security.

6.2.1 Consulter l'annuaire de confiance

Pour consulter votre annuaire de confiance :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Annuaire**.



L'onglet *Certificat* affiche les certificats personnels de vos correspondants, c'est-à-dire les certificats qui ne sont pas des certificats d'autorité.

L'onglet *Autorité* affiche les certificats d'autorité, c'est-à-dire les certificats avec l'extension X.509 émis par une autorité reconnue (voir la note dessous).

L'onglet *Groupes de certificats* affiche les certificats qui regroupent plusieurs certificats en un seul. Par exemple, le chiffrement se fait pour plusieurs personnes avec un seul certificat.

L'onglet *Contacts* permet de créer des raccourcis vers des certificats hébergés dans un annuaire LDAP.

La validité d'un certificat est indiquée par l'icône située à gauche de sa ligne. Les différentes icônes possibles sont indiquées dans le tableau suivant.

	valide	périmé ou non encore valide	contrôlé en erreur
certificat utilisateur			
certificat d'autorité			

Pour un certificat qui n'est pas un certificat d'autorité, deux colonnes indiquent si ce certificat est autorisé à signer et/ou à chiffrer :

- : le certificat est autorisé à chiffrer.
- : le certificat est autorisé à signer.

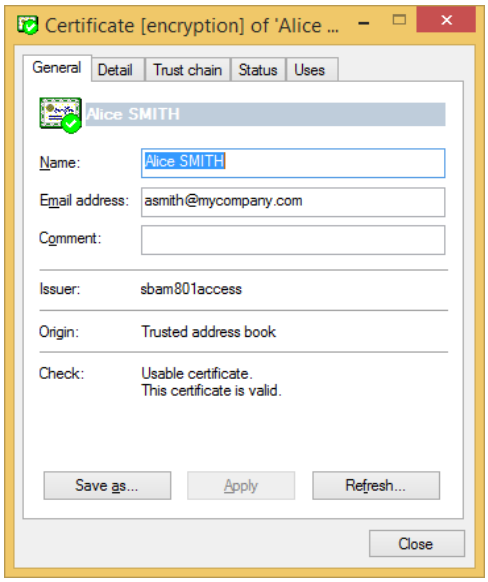
Pour modifier l'affichage des certificats, cliquez sur le bouton **Affichage** ou ouvrez le menu **Affichage>Présentation**.

NOTE

- Un certificat X.509 v3 est un certificat d'autorité s'il possède une extension particulière ("BasicConstraint"). Cette extension peut comporter la longueur maximale d'une chaîne de certification issue de ce certificat.
- Certaines autorités utilisent des certificats racines X.509 v1, version qui ne supporte pas l'extension précitée. Stormshield Data Security considère tout certificat X.509 v1 auto-certifié comme un certificat d'autorité. Ces certificats peuvent être utilisés dans les différents composants de Stormshield Data Security pour signer et chiffrer. Il n'y a pas moyen de connaître les usages et le fait que ce sont explicitement des certificats d'autorité. Il est cependant recommandé de ne pas utiliser de certificats de ce type.
- Stormshield Data Security ne prend pas en compte les certificats X.509 version 2.

6.2.2 Afficher un certificat

Pour afficher un certificat, double-cliquez dessus ou sélectionnez-le dans la liste et cliquez sur **Propriétés**.



L'onglet **Général** affiche un résumé du contenu du certificat :

- le nom usuel et l'adresse e-mail du titulaire ;
- un commentaire que vous renseignez librement (celui-ci ne fait pas partie du certificat) ;
- le nom usuel de l'autorité de certification ;
- la provenance du certificat (annuaire de confiance, annuaire LDAP, e-mail) ;
- l'état après vérification ; un message d'erreur s'affiche, si besoin.

De cet onglet, vous pouvez aussi exporter le certificat, en cliquant **Enregistrer sous**.

L'onglet Détail affiche la totalité du contenu du certificat.

Des informations complémentaires sur les différents champs peuvent être obtenues en consultant la norme X.509 V3 ou la RFC3280.

En cas d'erreur ou d'avertissement, le message d'explication est répété dans cette fenêtre immédiatement après la première ligne.

L'onglet **Parenté** reconstitue et affiche la chaîne de certification et indique le résultat des contrôles effectués sur cette chaîne.

NOTE
Les certificats participant à la chaîne de parenté sont uniquement recherchés dans l'annuaire de confiance. Aucune recherche LDAP n'est effectuée pour rechercher cette chaîne.

En cliquant sur un des certificats de la chaîne, il est possible d'en visualiser le contenu.

6.2.3 Importer des certificats

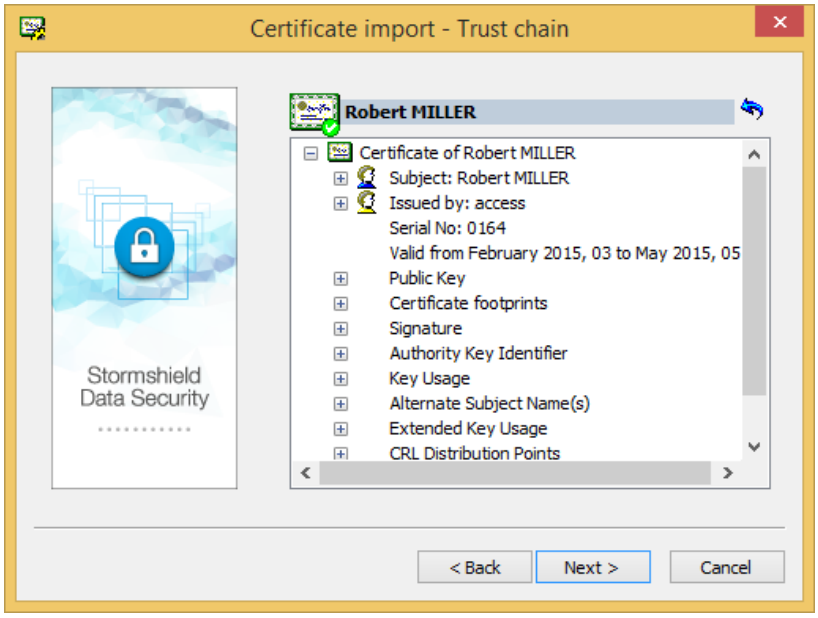
Vous pouvez importer dans votre annuaire de confiance :

- des certificats seuls, chaque certificat étant stocké dans un fichier au format binaire (extension *.cer*) ou base 64 (extension *.crt*) ;
- des listes de certificats, chaque liste provenant d'un fichier au format PKCS#7 (extension *.p7b* ou *.p7c*) ;
- une sauvegarde complète de l'annuaire (extension *.p7z*).

NOTE
En cas d'import d'un certificat avec une personnalisation alors que le certificat personnalisé est déjà dans votre annuaire de confiance, il y aura alors dans votre annuaire de confiance une entrée pour le certificat sans personnalisation, ainsi qu'une entrée pour le certificat personnalisé.

Pour les importer, vous pouvez utiliser l'assistant ou le glisser-déposer.

1. Pour cela, dans la fenêtre principale de l'annuaire de confiance, cliquez sur le bouton **Importer** ou glissez-déposez un certificat ou une liste de certificats depuis le Bureau ou un dossier de l'Explorateur Windows.
2. Saisissez le nom du fichier contenant le ou les certificats à importer et passez à l'écran suivant. Stormshield Data Security affiche tous les certificats qu'il contient.
3. Pour visualiser un certificat, cliquez dessus :



Les fichiers sont vérifiés pendant l'importation. Le résultat est indiqué avec un signe de validation vert, jaune, ou rouge, sur l'icône du certificat. Quel que soit le statut valide ou non valide, le certificat est importé.

4. Pour revenir à la liste des certificats, cliquez sur le bouton : .
5. Pour vérifier qu'un certificat est bien celui de votre correspondant, contactez-le et vérifiez l'empreinte affichée.
6. Pour importer un ou plusieurs certificats de la liste, cochez-les et cliquez sur **Suivant** pour vérifier le récapitulatif, puis cliquez sur **Terminer**.

6.2.4 Exporter des certificats ou l'annuaire de confiance

Si vous détenez dans votre annuaire de confiance des certificats que certains de vos correspondants ne possèdent pas, vous pouvez les leur fournir en exportant ces certificats.

Pour les exporter, il est possible d'utiliser l'assistant ou le glisser-déposer.

Pour exporter des groupes de certificats, reportez-vous à la section Exporter un groupe de certificats.

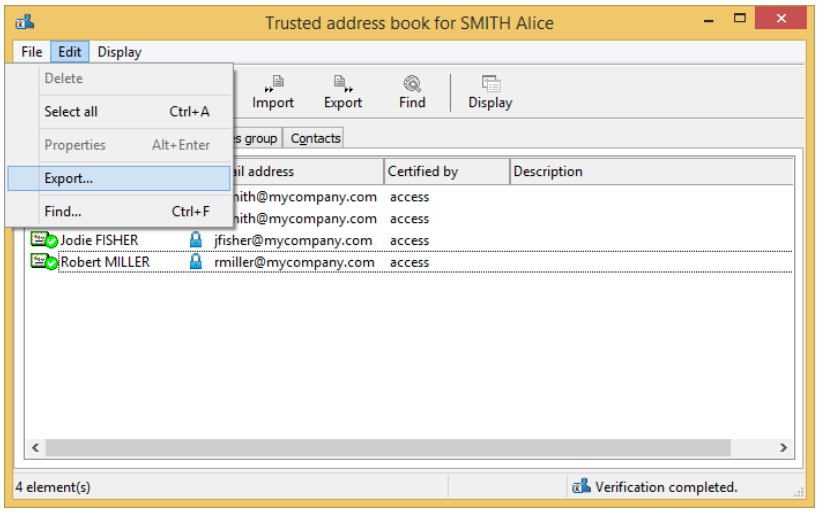
Vous pouvez également exporter la totalité de votre annuaire de confiance dans un fichier propre à Stormshield Data Security, portant l'extension *.p7z*.

Ce fichier contiendra l'ensemble des certificats de votre annuaire, leurs personnalisations éventuelles, les groupes de certificats ainsi que les certificats des contacts.

Par l'assistant

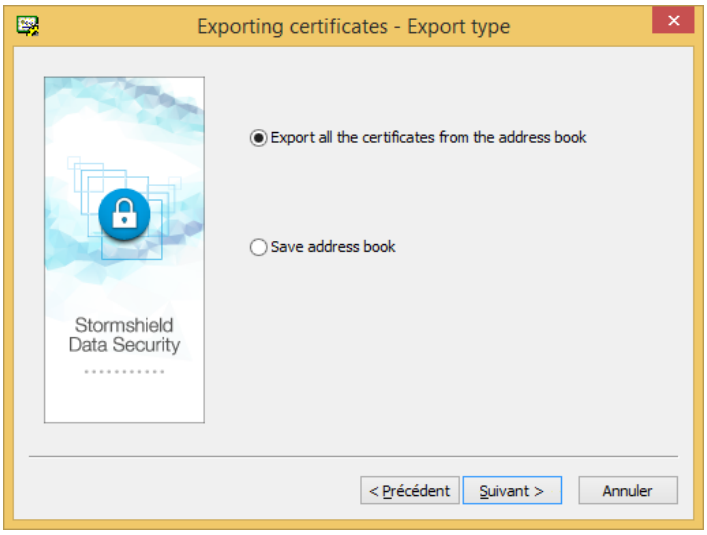
Pour exporter un ou plusieurs certificats de votre annuaire de confiance :

1. Sélectionnez-les dans votre annuaire de confiance.
2. Cliquez sur le bouton **Exporter** ou choisissez le menu **Edition > Exporter**.



Passez l'écran d'introduction.

3. Sélectionnez le type d'export.



L'intitulé de la première option diffère en fonction des éléments que vous avez sélectionnés dans l'annuaire :

- **Exporter tous les certificats de l'annuaire** : ce choix est proposé lorsqu'aucun certificat n'a été sélectionné dans l'annuaire. Dans ce cas tous les certificats seront exportés dans un fichier de type *.p7b* ou *.p7c*.
- **Exporter les certificats sélectionnés** : ce choix est proposé lorsque plusieurs certificats ou groupes ont été sélectionnés dans l'annuaire. Dans ce cas seuls les certificats sélectionnés seront exportés dans un fichier de type *.p7b* ou *.p7c*.
- **Exporter le certificat sélectionné** : ce choix est proposé lorsque vous n'avez sélectionné qu'un seul certificat dans l'annuaire. Dans ce cas le certificat sélectionné sera exporté dans un fichier de type *.cer* ou *.crt*.

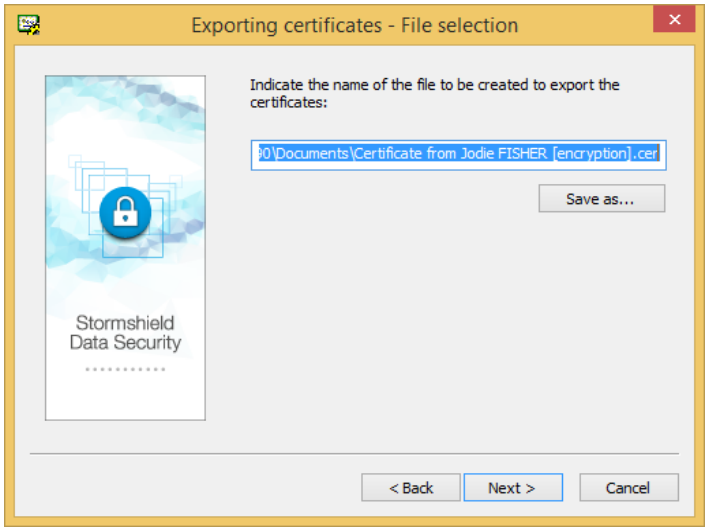
L'option **Sauvegarder l'annuaire** propose dans tous les cas de sauvegarder tous les certificats de l'annuaire avec les informations personnalisées qui leur sont associées.

4. Si vous avez sélectionné la première option de la fenêtre **Type d'export** et dans ce cas seulement, la fenêtre **Options** s'ouvre et propose d'ajouter des éléments supplémentaires au fichier d'export :
   - **Inclure la parenté** : permet d'exporter la parenté du certificat. Dans ce cas, les certificats d'autorités qui sont partagés ne sont pas dupliqués.
   - **Inclure les groupes et les contacts**: permet d'inclure dans le fichier d'export les groupes et les certificats des contacts. Pour plus d'informations sur l'export de groupes, reportez-vous à la section Exporter un groupe de certificats.

   Cette dernière case est cochée par défaut lorsque des groupes ont été sélectionnés dans l'annuaire. Elle est également grisée pour éviter de la décocher au risque de générer un fichier d'export vide.

> **NOTE**
> Si vous cochez cette option alors qu'aucun groupe n'est sélectionné dans l'annuaire, tous les groupes seront exportés.

5. Indiquez un nom et un emplacement pour le fichier d'export. L'assistant propose un nom par défaut, adapté au type d'export à effectuer. Sinon, entrez les informations directement dans la zone d'édition ou en utilisant le bouton **Enregistrer sous**.



> **NOTE**
> L'assistant corrige automatiquement l'extension du fichier si elle ne correspond pas au type de fichier d'export qui va être généré.

6. Un récapitulatif vous permet de vérifier les informations avant de commencer l'exportation.
7. Les certificats que vous avez sélectionnés ont été exportés dans le fichier indiqué. Vous pouvez maintenant envoyer le fichier en utilisant un e-mail, une clé USB, un fichier partagé, etc., ou bien l'utiliser pour restaurer le contenu de votre propre annuaire si le fichier exporté porte l'extension *.p7z*.

Par glisser-déposer

Il est possible d'exporter des certificats en effectuant un glisser-déposer à partir de l'annuaire de confiance.

1. Sélectionnez un ou plusieurs certificats dans l'annuaire de confiance.
2. Faites un glisser-déposer vers le Bureau, vers un dossier dans l'Explorateur Windows ou vers une autre application Windows susceptible de recevoir un fichier.

Si un seul certificat est exporté, le fichier résultant s'appelle *<CommonName>.cer*. Il n'est pas possible de choisir un autre nom ou un autre format. Il n'y a pas de distinction entre les certificats de signature et de chiffrement au niveau du nom.

Si plusieurs certificats sont exportés, le fichier résultant s'appelle *Certificate List.p7b*. Il n'est pas possible de choisir un autre nom ou un autre format.

6.2.5 Supprimer un certificat

Sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.

Pour supprimer plusieurs fichiers, sélectionnez-les à l'aide de la touche CTRL.

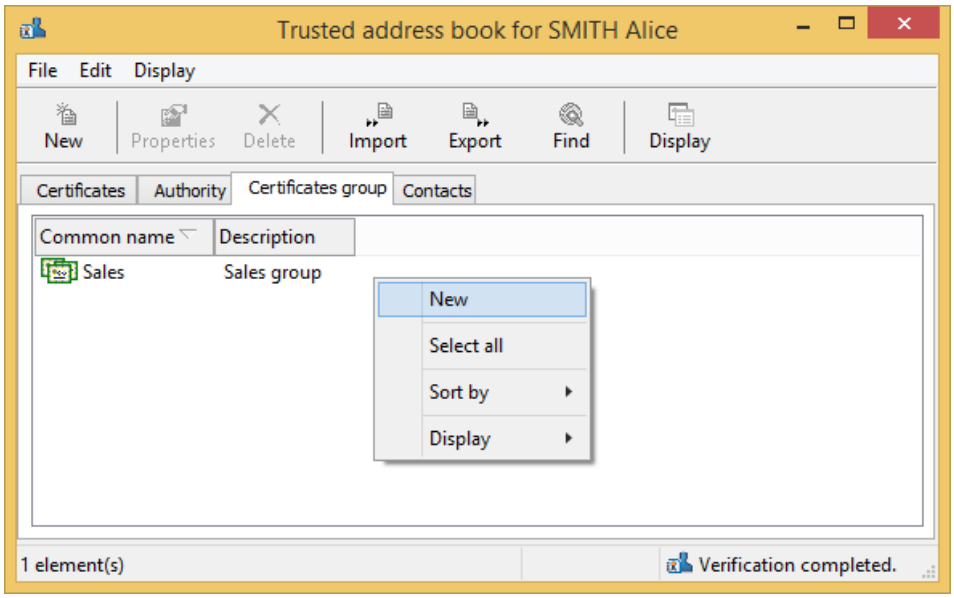
6.2.6 Créer un groupe de certificats

Créer un groupe de certificats simplifie le chiffrement de fichiers à destination de groupes de destinataires fixes. Au lieu de sélectionner chaque destinataire, vous sélectionnez un groupe prédéterminé. Dans ce cas, le ou les documents sont chiffrés pour chaque destinataire ayant un certificat valide.

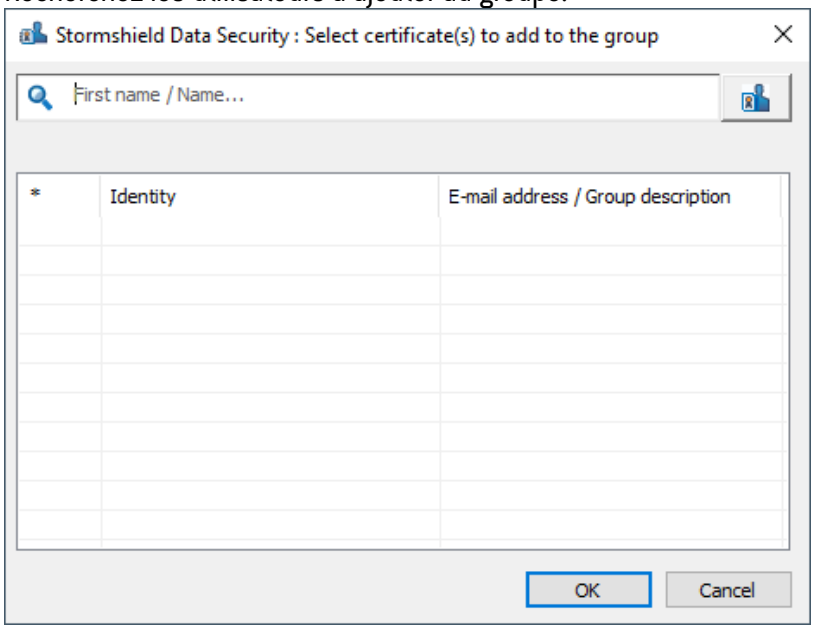
Seuls les groupes sauvegardés dans votre annuaire de confiance sont acceptés par Stormshield Data Security. Vous ne pouvez pas importer ou utiliser de groupes provenant d'annuaires LDAP.

1. Pour créer un groupe de certificats, choisissez l'onglet *Groupes de certificats* dans votre annuaire de confiance.
2. Faites un clic droit dans la fenêtre et choisissez **Nouveau**.

Si vous cliquez sur un groupe existant, le menu sera différent.



3. Entrez les informations sur le groupe et cliquez sur le bouton **Ajouter** pour ajouter des certificats.
4. Recherchez les utilisateurs à ajouter au groupe.

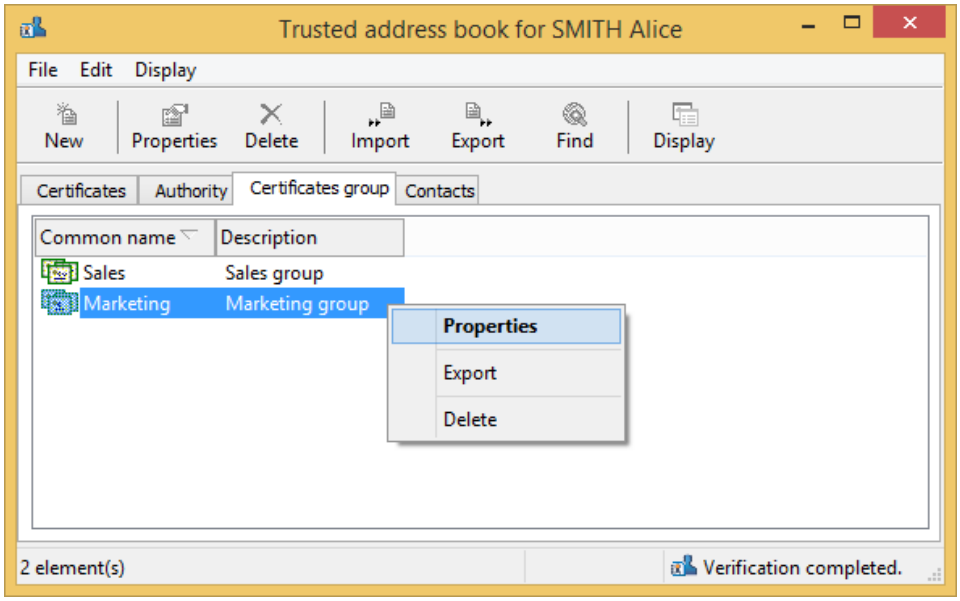


5. Cliquez sur **OK** lorsque vous avez fini.
6. Cliquez sur **OK** pour fermer la fenêtre du groupe.

6.2.7 Modifier un groupe de certificats

Pour modifier un groupe de certificats :

1. Choisissez l'onglet *Groupes de certificats* dans votre annuaire de confiance.
2. Faites un clic droit sur le groupe de certificats à modifier et choisissez **Propriétés**.



3. Ajoutez ou retirez les certificats.

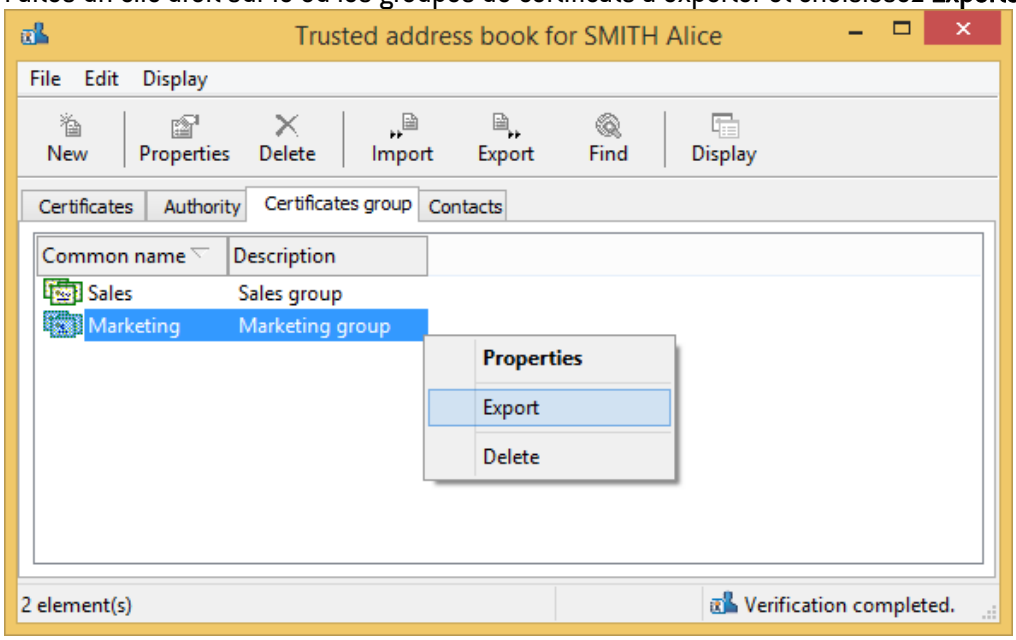
Vous pouvez aussi modifier le nom du groupe et la description.

4. Cliquez **OK** pour confirmer vos modifications.

6.2.8 Exporter un groupe de certificats

Pour exporter un groupe de certificats :

1. Faites un clic droit sur le ou les groupes de certificats à exporter et choisissez **Exporter**.



Il est possible de sélectionner plusieurs groupes avant de demander l'exportation. Dans ce cas, tous les certificats présents dans les groupes seront placés dans le fichier d'export (avec suppression des éventuels doublons).

2. Les étapes suivantes sont les mêmes que pour l'exportation des certificats. Référez-vous à la section Exporter des certificats ou l'annuaire de confiance.

Dans le cas de l'export de groupe(s) de certificats, la case **Exporter les groupes et les contacts** de la fenêtre **Options** de l'assistant et cochée par défaut et grisée.

6.2.9 Supprimer un groupe de certificats

1. Sélectionnez-le dans la liste de groupes de votre annuaire de confiance.
2. Effectuez un clic droit sur le groupe à supprimer et cliquez sur le bouton **Supprimer**.

Pour sélectionner plusieurs groupes, utilisez les touches habituelles de Windows (shift et CTRL).

Pour supprimer tous les groupes, effectuez un clic droit sans sélectionner un seul groupe et cliquez sur **Sélectionner tout** puis cliquez sur **Supprimer**.

6.3 Echange de certificats à l'aide de Stormshield Data Mail

Les échanges de certificats entre utilisateurs sont assez rares dans la pratique. Les annuaires LDAP sont en général utilisés pour le partage des certificats entre les correspondants. Les échanges manuels ne sont donc utilisés que pour des échanges ponctuels entre correspondants d'entreprises différentes ou pour des tests/expérimentations.

La procédure d'échange de certificats est différente si vous avez Stormshield Data Mail. Si vous n'avez pas Stormshield Data Mail, vous devez utilisez les procédures d'exportation et importation décrites section Gérer votre annuaire de confiance puis expédier votre fichier de certificats par un moyen approprié.

6.3.1 Communiquer votre certificat à vos correspondants

La technique la plus simple pour communiquer son certificat à un correspondant consiste à lui envoyer un message signé à l'aide de Stormshield Data Mail. Si vous possédez ce logiciel, reportez-vous au chapitre correspondant de son manuel.

Avec la messagerie sécurisée au standard S/MIME V3, les messages transmis ou reçus contiennent en général la signature de l'émetteur qui contient le certificat de signature de l'émetteur. Avec Stormshield Data Mail, tout envoi de message sécurisé (signé) permet de communiquer un certificat de signature à un correspondant.

Avant d'envoyer un message chiffré à votre correspondant, vous, en tant qu'émetteur, devez préalablement avoir intégré le certificat de ce correspondant dans votre annuaire. Dans le cas contraire, ce certificat doit être disponible dans un annuaire LDAP.

L'intégration se fait manuellement suite à la lecture d'un message signé par votre correspondant. Vous devez prendre connaissance des informations communiquées dans le certificat pour accorder votre confiance au certificat qui va être intégré dans votre annuaire. Une fois le certificat manuellement ajouté dans votre annuaire de confiance, l'accès aux certificats pour les échanges chiffrés/signés est automatisé.

Par défaut, Stormshield Data Mail transmet les certificats de signature et de chiffrement avec un message signé. Si vous avez Stormshield Data Mail, référez-vous au guide d'utilisation pour plus de détails.

Si vous n'avez pas Stormshield Data Mail, reportez-vous à la section Exporter des certificats.

6.3.2 Importer le certificat d'un correspondant à l'aide de Stormshield Data Mail

Les messages électroniques signés et chiffrés contiennent généralement les certificats des expéditeurs. Ces certificats incluent les certificats de signature et de chiffrement ainsi que les certificats de l'autorité.

Pour importer le certificat d'un correspondant, vous avez deux possibilités :

- si vous possédez Stormshield Data Mail, veuillez vous référer à la documentation Stormshield Data Mail , section Échange de certificats ;
- si vous ne possédez pas Stormshield Data Mail, vous devez utiliser votre outil de messagerie pour extraire le certificat au format *PKCS#7*. Utilisez la procédure d'importation des certificats décrite dans la section Importer des certificats.

6.4 Travail en ligne / hors connexion

Stormshield Data Security contrôle la connexion physique à votre réseau local d'entreprise.

Lorsque vous êtes connecté à votre réseau (travail en ligne), chaque fois que vous recherchez un certificat sur votre annuaire LDAP, le ou les certificats trouvés sont enregistrés dans un fichier temporaire local (cache).

Lorsque vous êtes déconnecté de votre réseau (travail hors connexion), Stormshield Data Security détecte la déconnexion : les recherches de certificats sont alors redirigées vers le cache local qui a été alimenté lors de votre connexion.

Ce mécanisme permet de chiffrer vos fichiers et mails adressés à des collaborateurs même lorsque vous n'êtes pas connecté à votre réseau d'entreprise : vous devez simplement avoir préalablement utilisé au moins une fois le certificat de chaque collaborateur.

Il en est de même des listes de révocation : elles sont téléchargées en ligne, enregistrées dans un fichier local consultable quand vous travaillez hors connexion.

Vous pouvez forcer le fonctionnement en mode hors connexion (par exemple si votre réseau local rencontre des problèmes). Pour cela :

1. Effectuez un clic-droit sur l'icône de Stormshield Data Security dans la barre des tâches.
2. Sélectionnez **Accès réseau > Travailler hors connexion**.
3. Désélectionnez **Accès réseau > Rétablir la connexion**.
4. En sélectionnant à nouveau **Rétablir la connexion automatiquement**, Stormshield Data Security détecte automatiquement la connexion au réseau d'entreprise et repasse automatiquement en fonctionnement en ligne.

7. Contrôle de révocation

Le contrôle de révocation est un élément fondamental, puisqu'il constitue le seul moyen de signaler qu'un certificat ne doit plus être utilisé (ex : son titulaire ne fait plus partie d'un groupe, il suspecte que sa clé a été compromise, ou en a obtenu une autre, etc.).

Il s'opère au moyen de listes de révocation de certificats (CRL) ou au moyen du protocole OCSP dans le cas où une adresse URL d'un répondeur OCSP est indiquée dans le certificat.

Cette section présente les listes de contrôle de révocation et comment Stormshield Data Security les utilise.

7.1 Contrôle de révocation

Le contrôle d'un certificat porte sur trois aspects :

- contrôle des données propres du certificat : format, dates de validité, signature, extension… ;
- contrôle de la chaîne de parenté. Il faut être capable d'établir une chaîne complète de certificats jusqu'à un certificat d'autorité de confiance. Chaque certificat de cette chaîne subit le même niveau de contrôle que le certificat à contrôler initialement. Lorsqu'un certificat d'une chaîne ne peut être validé, une autre chaîne est vérifiée (tant qu'une chaîne valide n'a pas été trouvée) ;
- contrôle de la révocation. Ce contrôle est effectué en regardant si le certificat est bien absent de la liste de révocation émise par son autorité de délivrance (ou par un tiers ayant délégation pour la produire). Les listes de révocation étant elles-mêmes signées avec des certificats, le mécanisme de contrôle de certificats s'applique également aux certificats mis en œuvre au niveau des listes de révocation.

La validation complète d'un certificat nécessite donc l'accès à plusieurs listes de révocation. Dans la suite du chapitre, l'abréviation CRL est utilisée pour désigner les listes de révocation.

7.2 Listes de révocation

Le mécanisme de vérification d'une CRL est décrit dans les normes définissant les certificats et les CRL (norme X.509, RFC 3280 et RFC 5280). Tous les certificats qui sont utilisés par Stormshield Data Security sont entièrement contrôlés avant leur utilisation sauf si le contrôle de révocation est désactivé ou si c'est son propre certificat.

Les CRLs devant être téléchargées pour vérifier des certificats sont obtenues de deux façons :

- à partir des certificats, en utilisant l'extension des points de distribution ;
- à partir de la configuration du contrôleur de révocation qui indique, éventuellement, des points de distribution pour chaque autorité définie dans le contrôleur.

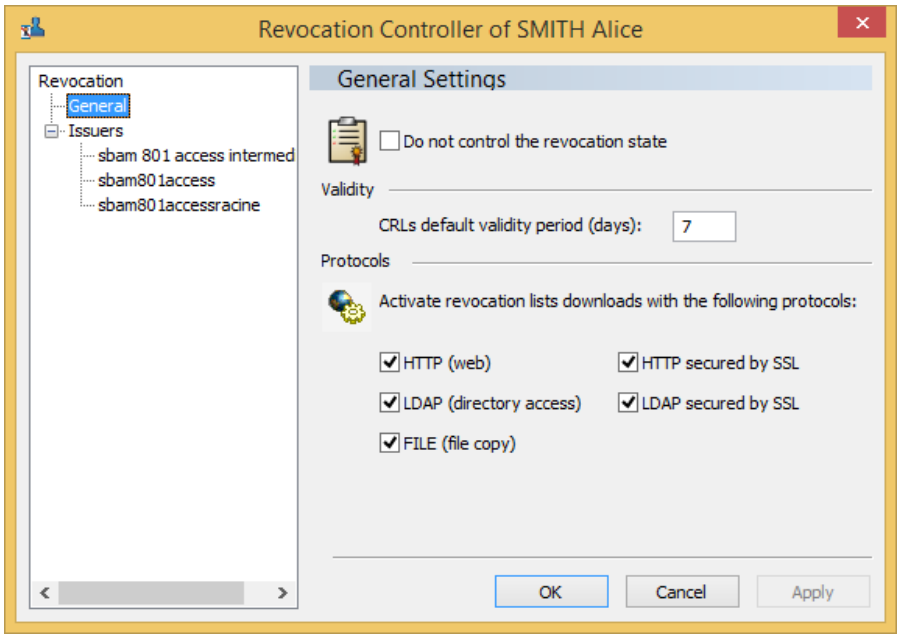
Stormshield Data Security intègre un contrôle complet des certificats utilisés, avec si besoin, un téléchargement (configurable) automatisé des listes de révocation (CRLs), au moyen des protocoles FILE, HTTP, LDAP, HTTPS (HTTP avec SSL2), LDAPS (LDAP avec SSL2). Les points de distribution des CRLs, indiqués éventuellement dans les certificats, sont gérés et il y a également la possibilité de définir des points de distribution personnalisés.

Vous pouvez configurer les critères de téléchargement pour chaque émetteur de certificat (autorité de certification). Les listes de révocation reçues sont conservées localement dans une base sécurisée.

Vous pouvez demander explicitement à “ne pas contrôler la révocation des certificats” ou de limiter leur validité à un nombre de jours paramétrable. Vous disposez d’un choix de protocole pour charger les listes de révocation.

7.3 Configuration générale

A partir de la fenêtre **Contrôleur de révocation**, vous pouvez configurer la manière dont Stormshield Data Security va traiter les contrôles de révocation :



- Cocher **Ne pas contrôler la révocation des certificats** permet que la révocation des certificats ne soit plus vérifiée et que des certificats explicitement déclarés comme corrompus soient utilisés. Cette option ne doit être sélectionnée que lorsque les réseaux d’accès aux CRL sont indisponibles et bloquent le fonctionnement de Stormshield Data Security.
- Dans la section **Validité**, vous pouvez limiter la validité des CRLs à un nombre de jours paramétrable. Les CRLs contiennent une date de prochaine génération qui est généralement très supérieure à la date de prochaine publication. Cette option permet d’invalider « rapidement » une CRL et donc de télécharger plus fréquemment les CRL ou de ne plus utiliser une CRL ancienne. Cette date correspond à la date de génération de la CRL augmentée de la validité paramétrée.

En ce qui concerne la période de validité des CRLs, la donnée est recopiée au niveau de chaque autorité connue lors de la création de celle-ci. La période utilisée au niveau de chaque autorité est celle qui a été copiée initialement. Même en changeant la valeur dans la configuration générale, il n’est plus possible de mettre à jour la valeur copiée dans l’autorité.

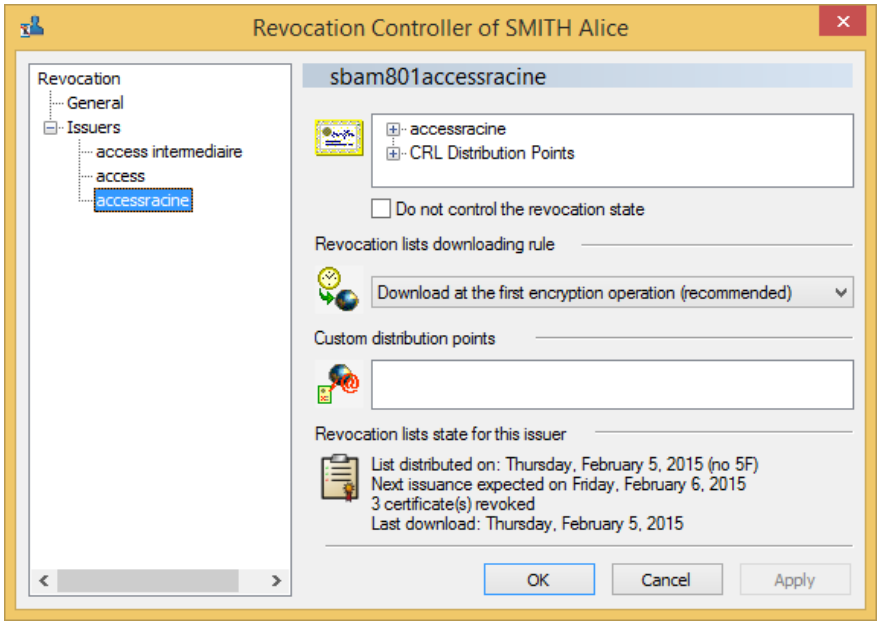
Le téléchargement d’une CRL à l’issue de cette période ne réinitialise pas l’attente : la CRL sera rechargée dès que nécessaire. La valeur 0 pour ce paramètre invalide la fonctionnalité.

- Sélectionner les protocoles pour charger les listes de révocation. Seuls les protocoles indiqués seront utilisés. Les points de distribution présents dans les certificats et utilisant un protocole non autorisé sont ignorés.

7.4 Prise en compte d'une autorité

Lorsqu'un certificat est correctement configuré et qu'il contient des points de distribution valides, l'autorité est automatiquement créée dans le contrôleur de révocation et le point de distribution issu du certificat est pris en compte. L'autorité est listée sous **Émetteurs** dans la fenêtre **Contrôleur de révocation**.

Le nom (dans l'arborescence de gauche) correspond au `<CommonName>` de l'autorité.



Pour connaître l'identité complète de l'autorité, cliquez sur le symbole + à gauche du nom (dans la liste en haut à droite).

Pour afficher la liste des points de distributions d'un certificat, cliquez sur le symbole + à gauche de **Points de téléchargement personnalisés**. Cette liste correspond à l'URL à utiliser pour la recherche de la plus récente CRL. Cette liste est filtrée à l'exécution en n'utilisant que les protocoles autorisés (à l'affichage, toutes les URL sont présentes).

NOTE
Les points de téléchargement pour les CRLs de l'autorité ne sont pas présents dans le certificat de l'autorité mais dans les certificats qu'elle produit. Les points de téléchargement présents dans le certificat de l'autorité sont ceux permettant de télécharger les CRLs de son autorité mère.

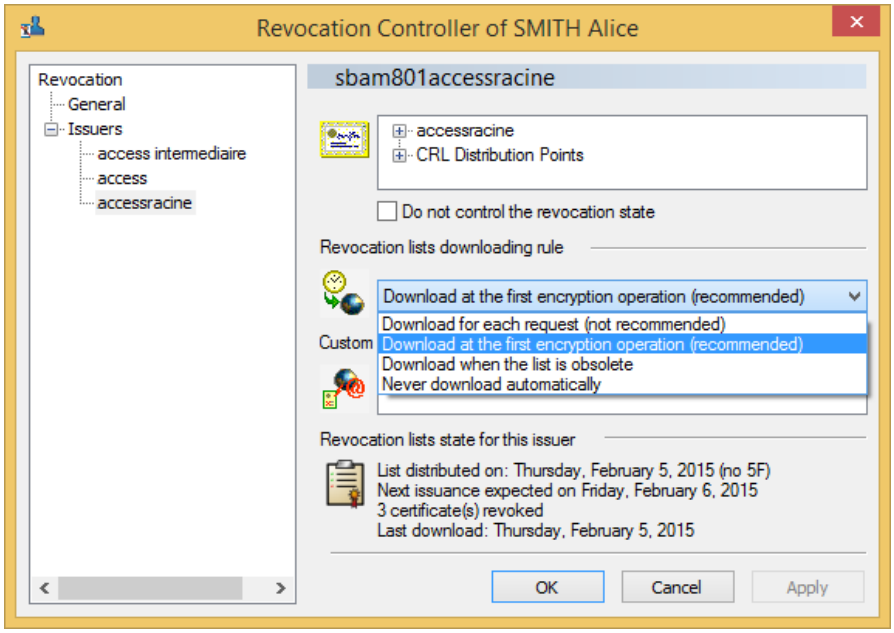
7.4.1 Désactivation

Pour cesser le contrôle de révocation des certificats émis par une autorité, il faut cocher l'option correspondante.

Il est recommandé de n'utiliser cette option qu'en cas d'indisponibilité du réseau pour accéder aux CRLs, ce qui pourrait entraîner des perturbations dans le fonctionnement du logiciel.

7.4.2 Politiques de téléchargement

Vous pouvez modifier la politique de téléchargement des CRL pour chaque autorité :



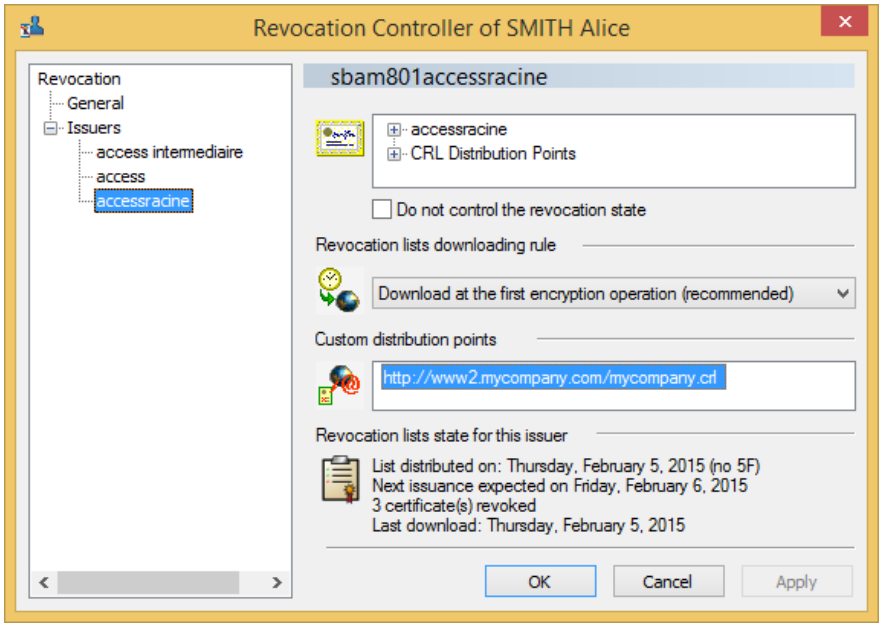
NOTE
Quelle que soit la politique sélectionnée, un téléchargement est effectué lorsque la date de prochaine génération d'une CRL est atteinte.

- **Télécharger systématiquement (non recommandé)**. Il est déconseillé d'utiliser cette option, Stormshield Data Security ayant souvent recours aux CRLs. Cette option ne doit être utilisée que dans les environnements à forte sécurité dans lesquels Stormshield Data Security est utilisé pour des chiffrements occasionnels.
- **Télécharger une première fois après la connexion (recommandé)**. La CRL sera chargée lors de sa première utilisation après la connexion de l'utilisateur à Stormshield Data Security.
- **Télécharger lorsque la liste est périmée**. La liste est téléchargée lorsqu'elle devient obsolète (c'est-à-dire que sa date de génération augmentée de la période de validité configurée est atteinte). Lorsqu'on utilise ce paramètre, vérifiez que la CRL téléchargée est plus récente que la CRL courante. Dans le cas contraire, la CRL est téléchargée à chaque fois qu'elle est utilisée.
- **Ne jamais télécharger automatiquement**. La CRL est téléchargée manuellement. Cette option est à réserver à des utilisateurs avancés qui n'ont besoin de télécharger les CRLs qu'occasionnellement.

7.4.3 Points de téléchargement

Outre les points de téléchargement obtenus automatiquement à partir des certificats (et présents dans la liste du haut), il est possible de définir manuellement des points supplémentaires. Cela sert notamment lorsqu'une autorité n'a pas défini ses points de téléchargement dans les certificats, que ceux-ci ont changé ou ne sont pas accessibles dans certains environnements.

1. Dans la liste des points de distributions personnalisés, placez-vous sur la ligne qui suit le dernier point personnalisé défini (ou sur la première ligne s'il n'y en a pas encore) et appuyez sur la touche F2.



2. Entrez l'URL de téléchargement de la CRL en spécifiant bien le protocole à utiliser.
3. Appuyer sur la touche entrée pour sortir du mode édition du point de distribution.

Il est possible de modifier un point déjà défini en le sélectionnant et en appuyant sur la touche F2 pour les éditer.

NOTE
Concernant le protocole LDAP, une connexion SSL est mise en œuvre si le protocole indiqué est ldaps:// ou si le port renseigné dans l'URL est le port 636.

7.4.4 Information sur les CRLs

Pour chaque autorité répertoriée dans le contrôleur de révocation, les données relatives à l'état de dernier téléchargement de CRL sont disponibles en bas à droite et contiennent :

- la date de génération de la CRL courante ;
- la date prévue de la prochaine génération de la CRL (souvent appelée date d'expiration de la CRL) ;
- le nombre de certificats révoqués qu'elle contient ;
- la date du dernier téléchargement de cette CRL. Une même CRL peut voir cette date évoluer car elle est potentiellement chargée chaque fois que vous vous connectez et l'utilisez (si la configuration recommandée est utilisée).

7.5 Téléchargement manuel

Pour télécharger manuellement une CRL, effectuez un clic-droit sur le nom de l'autorité puis **Télécharger** .

NOTE
Le téléchargement manuel est à réserver à des cas particuliers notamment pour des utilisateurs itinérants qui n'ont que très rarement accès au réseau de l'entreprise.

7.6 Suppression d'une autorité

Il est possible de supprimer une autorité du contrôleur de révocation.

Sélectionnez l'autorité dans la liste et cliquez sur Supprimer.

Cette action n'a aucun effet sur les performances du produit et sert uniquement à nettoyer la liste des autorités prises en compte.

8. Fonctions avancées

Cette section décrit les fonctions avancées que vous utiliserez de manière exceptionnelle.

8.1 Gestion de votre connexion Stormshield Data Security

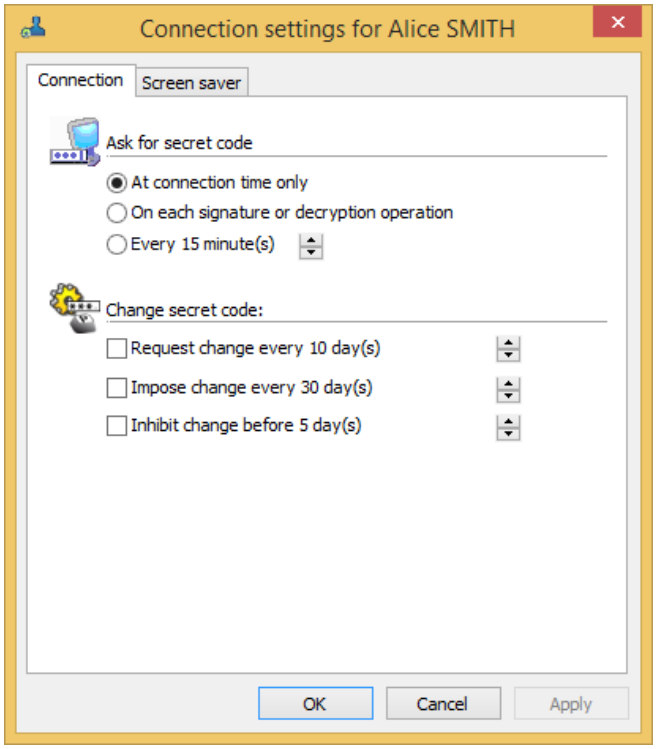
Pour modifier les règles de gestion de votre connexion Stormshield Data Security :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Connexion**.

8.1.1 Paramétrage de la gestion du code confidentiel

> **NOTE**
> Cette section s'applique aux comptes cartes et aux comptes mot de passe.

Demander le code confidentiel



À la connexion uniquement

Vous pouvez demander à ce que le mot de passe ou code confidentiel ne soit pas systématiquement exigé, mais ne soit demandé qu'une seule une fois après chaque lancement de Stormshield Data Security.

Cette option est recommandée dans la plupart des cas.

IMPORTANT
Prenez alors soin de vous déconnecter de Stormshield Data Security, ou de verrouiller votre compte, avant de vous éloigner de votre poste. Une autre personne pourrait, sans cela, venir sur votre poste et signer des messages avec votre clé ou déchiffrer des messages confidentiels qui vous ont été adressés.

Pour se prémunir du risque d'utilisation frauduleuse du produit, il convient de fixer un verrouillage ou une déconnexion automatique sur inactivité du poste (reportez-vous à la section Paramétrage sur mise en veille et verrouillage Windows).

À chaque opération

Afin de garantir une plus grande sécurité, vous pouvez demander que le mot de passe ou code confidentiel soit systématiquement exigé à chaque opération mettant en œuvre votre clé privée (signature, décryptage).

Cette option est à réserver à une utilisation très ponctuelle du produit.

Toutes les « x » minutes

Vous pouvez demander que le mot de passe ou code confidentiel soit demandé de façon cyclique, toutes les "x" minutes.

Si vous activez cette option, votre session sera maintenue ouverte pendant le temps indiqué. Au-delà de ce délai, votre code sera demandé si vous effectuez une opération. Cette option est un bon compromis entre la saisie au lancement uniquement et la saisie systématique du mot de passe ou du code confidentiel.

8.1.2 Changement du mot de passe

NOTE
Cette section s'applique seulement au compte mot de passe. Si vous utilisez une authentification physique (carte à puce ou clé), reportez-vous à la section Création d'un compte en utilisant une carte à puce ou une clé USB.

Le changement régulier permet de se prémunir contre une compromission non détectée du mot de passe de l'utilisateur.

Sélectionnez votre option, et utilisez les flèches pour indiquer la période de temps.

- **Demander le changement tous les « x » jours**

Cette fonction permet de garantir une confidentialité maximale de votre mot de passe. En le changeant régulièrement, tous les X jours, vous limitez les risques qu'il soit connu d'une tierce personne.

- **Imposer le changement tous les « x » jours**

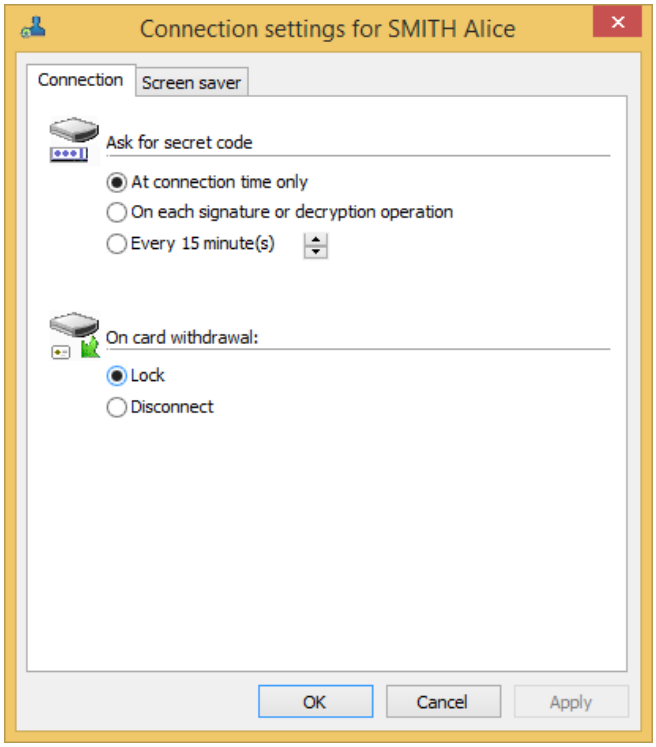
Contrairement à la fonction précédente qui propose le changement, celle-ci oblige l'utilisateur à changer son mot de passe.

- **Interdire le changement avant « x » jours**

Cette fonction empêche de changer le mot de passe avant un certain délai. Ceci permet d'éviter que l'utilisateur modifie son mot de passe une première fois, puis le modifie de nouveau afin de réutiliser son mot de passe d'origine. Ces changements successifs permettraient aux utilisateurs d'utiliser toujours les mêmes mots de passe ce qui entraînerait une sécurité amoindrie.

8.1.3 Retrait de la carte ou du token

Si vous utilisez une carte à puce ou un token USB, vous pouvez configurer le comportement de Stormshield Data Security lors du retrait de la carte :



Sélectionnez soit :

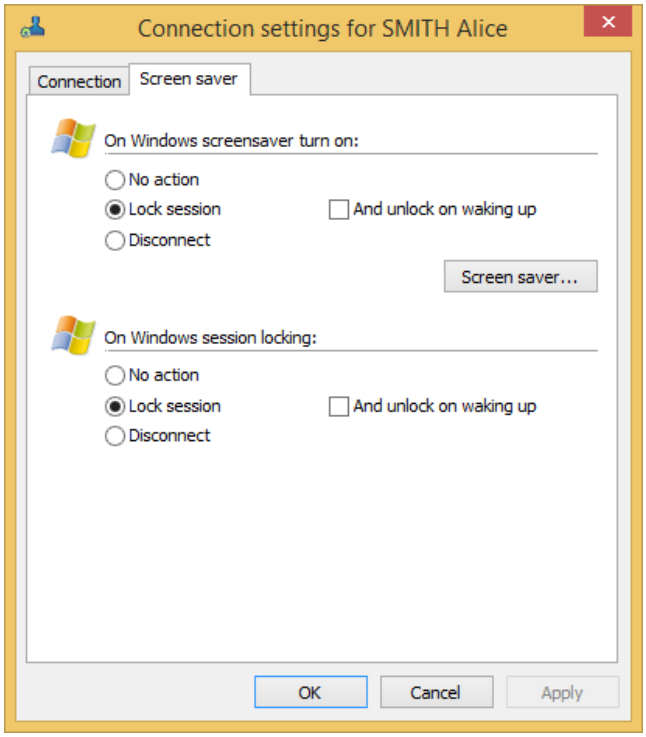
- **Verrouiller** : la session est automatiquement verrouillée ;
- **Déverrouiller** : la session est déconnectée.

Lorsqu'on verrouille une session Stormshield Data Security, les clés privées et la configuration de l'utilisateur deviennent inaccessibles mais certains des composants le restent. Par exemple, les volumes sécurisés de l'utilisateur restent montés mais ne sont pas accessibles. Naturellement, il n'est pas possible d'ouvrir des ressources protégées. Par ailleurs, lorsqu'une session est verrouillée, il n'est pas possible pour un autre utilisateur de se connecter sans déconnecter l'utilisateur courant.

Dans le cas d'une déconnexion, toutes les ressources sont fermées et inaccessibles.

8.1.4 Paramétrage sur mise en veille et verrouillage Windows

Sur l'onglet **Écran de veille**, vous pouvez paramétrer l'action de Stormshield Data Security lorsque l'écran de mise en veille est activé ou lorsque Windows est verrouillé.



Aucune action

Vous pouvez demander que la mise en veille de votre système n'ait aucun impact sur votre session Stormshield Data Security.

IMPORTANT
Cette option n'est pas recommandée pour des raisons de sécurité.

Verrouiller la session

Vous pouvez demander que la mise en veille de votre système verrouille votre session Stormshield Data Security.

- Si vous cochez la case **Et déverrouiller au réveil** : votre mot de passe ou code confidentiel sera demandé au réveil du système, c'est-à-dire dès que vous ferez bouger la souris ou que vous enfoncerez une touche de votre clavier ;
- Si vous ne cochez pas cette case : votre mot de passe ou code confidentiel sera demandé à la première opération de cryptographie suivant le réveil de votre système.

Le verrouillage est effectif cinq secondes après la mise en veille.

Déconnecter

Vous pouvez demander que la mise en veille de votre système vous déconnecte de Stormshield Data Security.

La déconnexion est effective cinq secondes après la mise en veille.

L'usage des fonctions **Verrouiller la session** ou **Déconnecter** peut avoir des effets indésirables si vous utilisez Stormshield Data Virtual Disk avec des données en cours d'utilisation au moment de la mise en veille ou du verrouillage.

8.2 Clé de déchiffrement

Cette section décrit comment configurer et utiliser les clés de déchiffrement, qu'il s'agisse d'une clé antérieure ou de la clé d'un collaborateur (clé de délégation).

8.2.1 Présentation

Stormshield Data Security permet avec les clés de déchiffrement de déchiffrer des documents (fichiers/messages) de manière transparente alors qu'ils sont chiffrés avec une clé différente de votre clé de chiffrement courante.

Stormshield Data Security gère deux types de clés de déchiffrement :

- les anciennes clés personnelles. Si vous effectuez le renouvellement de votre clé de chiffrement (ou de la clé personnelle), votre ancienne clé est automatiquement déplacée dans les clés de déchiffrement que vous possédez déjà ;
- les clés de délégation. Il s'agit des clés de chiffrement que des collaborateurs peuvent vous confier afin de vous permettre de déchiffrer des documents (fichiers/messages) chiffrés à leur attention.

Alors qu'une clé de délégation ne permet que de déchiffrer, une ancienne clé permet non seulement de déchiffrer mais également de transchiffrer, notamment vers votre nouvelle clé dans le cas d'un renouvellement.

Une clé de délégation permet d'autoriser l'un de vos collaborateurs à déchiffrer à votre place les messages qui vous sont destinés (par exemple, pendant vos vacances). A cette fin, vous devez lui confier votre clé personnelle (si vous n'utilisez qu'une seule clé pour la signature et le chiffrement) ou vos deux clés (si vous utilisez deux clés différentes pour la signature et le chiffrement).

Muni de votre clé de chiffrement, votre collaborateur ne pourra que déchiffrer vos messages. Afin d'être certain que votre collaborateur ne puisse signer en votre nom, vous devez utiliser des clés de chiffrement et de signature séparées. Dans ce cas, à partir de votre compte de sécurité, vous exporterez votre clé de chiffrement utilisée, qui sera ensuite importée dans le compte de sécurité des collaborateurs à qui vous avez décidé de confier cette clé de chiffrement.

> **NOTE**
> Les clés de chiffrement ainsi importées dans un compte ne peuvent pas être exportées. La personne qui a reçu la délégation ne peut donc pas la transmettre à son tour.

Pour exporter votre clé de sécurité, reportez-vous à la section Exporter votre clé de sécurité. Vous obtenez un fichier *p12* ou *.pfx* contenant votre clé protégée par un mot de passe. Ce fichier peut servir pour la fonction d'import dans un autre compte.

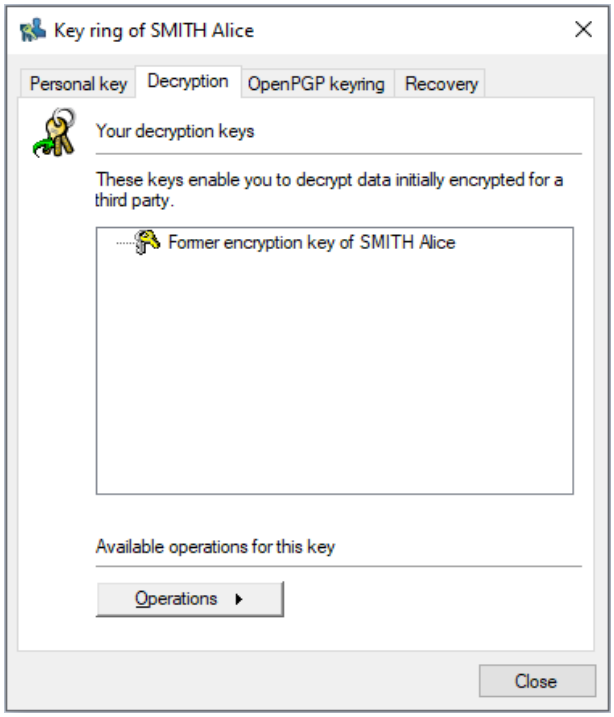
Si vous souhaitez déléguer le déchiffrement de vos messages/informations, il est recommandé d'utiliser deux clés distinctes pour la signature et le chiffrement.

8.2.2 Importer une clé de déchiffrement

Pour importer une clé de déchiffrement :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.

4. Choisissez l'icône **Porte-clés**.
5. Cliquez sur l'onglet *Déchiffrement*.



6. Cliquez sur **Opérations** et choisissez **Importer une clé**. Passez l'écran d'introduction.
7. Renseignez le nom du fichier contenant la clé à importer et saisissez son mot de passe.

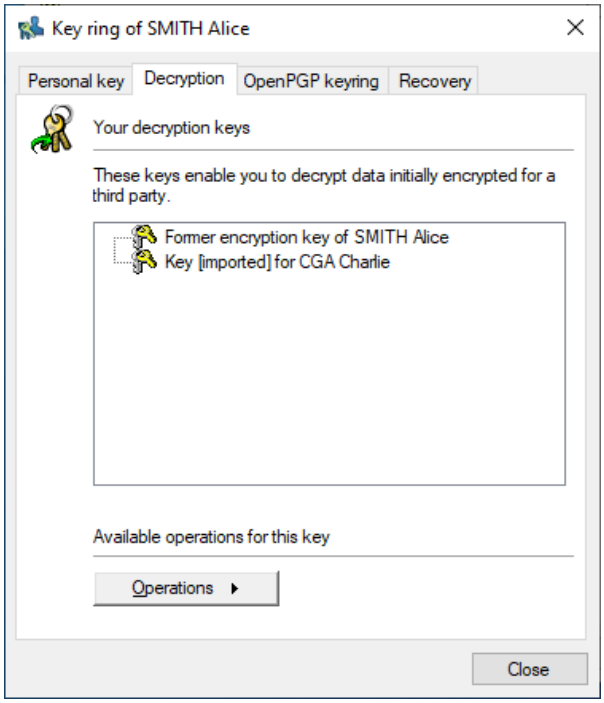
Stormshield Data Security affiche la liste des certificats présents dans le fichier, c'est-à-dire le certificat associé à la clé contenue dans le fichier, avec éventuellement sa parenté.

8. Pour visualiser un certificat de la liste, cliquez dessus.

Pour revenir à la liste des certificats, cliquez sur le bouton **Fermer**.

9. Cochez les certificats parents si vous souhaitez les importer dans votre annuaire de confiance puis passez à l'écran suivant.
10. Sélectionnez le type de clé à importer (délégation ou ancienne clé), puis passez à l'écran suivant.
11. Vérifiez le récapitulatif, cliquez sur **Terminer** et vérifiez le résultat de l'opération.

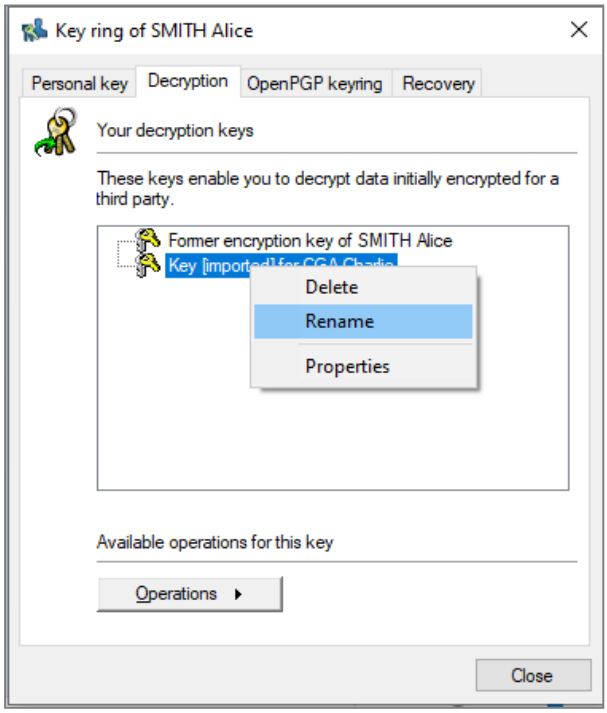
La clé importée apparaît alors dans la liste :



8.2.3 Renommer une clé de déchiffrement

Pour modifier le libellé créé automatiquement par Stormshield Data Security :

1. Allez dans l'onglet *Déchiffrement*.
2. Effectuez un clic-droit sur la clé dont vous souhaitez changer le libellé et sélectionnez **Renommer**.



Il est également possible de sélectionner la clé concernée et d'utiliser le bouton **Opérations**.

3. Tapez le nouveau libellé (le libellé est devenu modifiable).
4. Validez la modification avec la touche Entrée.

La touche Echap permet d'annuler la modification.

8.2.4 Afficher les informations sur une clé

Pour afficher les informations sur une clé déchiffrement :

1. Allez dans l'onglet *Déchiffrement*.
2. Effectuez un clic-droit sur la clé concernée et sélectionnez **Propriétés**. Il est également possible de sélectionner la clé concernée et d'utiliser le bouton **Opérations**.

Le certificat associé à la clé est alors affiché.

8.2.5 Suppression d'une clé

Lorsqu'une clé de déchiffrement n'est plus utilisée, par exemple en fin de délégation, vous pouvez la supprimer du compte. Pour cela, il faut :

1. Allez dans l'onglet *Déchiffrement*.
2. Effectuez un clic-droit sur la clé concernée et sélectionnez **Effacer**. Il est également possible de sélectionner la clé concernée et d'utiliser le bouton **Opérations**.
3. Confirmez la demande de suppression.

8.3 Clé de recouvrement

Cette section décrit comment utiliser une clé de recouvrement.

8.3.1 Principes

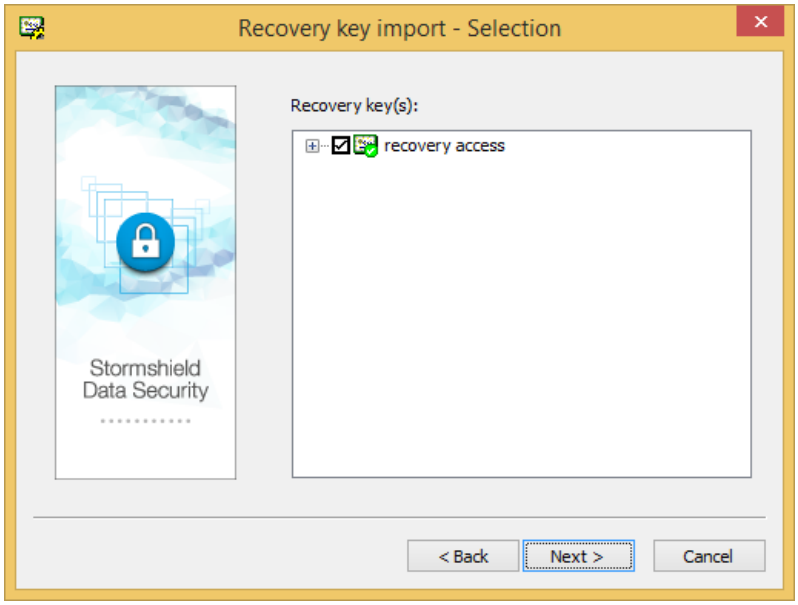
La clé de recouvrement permet de sécuriser l'utilisation d'un logiciel de chiffrement fort. Si un utilisateur perd son compte et n'a pas sauvegardé sa clé de chiffrement, la clé de recouvrement, si elle a été définie, permettra de déchiffrer toutes les données de l'utilisateur. Par exemple, si un collaborateur quitte une société sans déchiffrer la totalité de ses données, celles-ci pourront être retrouvées en clair.

La clé de recouvrement peut provenir d'un autre compte Stormshield Data Security duquel on aura exporté le certificat public de chiffrement. En raison de l'usage qui peut être fait de la clé de recouvrement, il est primordial de bien protéger le compte de recouvrement.

8.3.2 Importer une clé de recouvrement

Pour importer une clé de recouvrement :

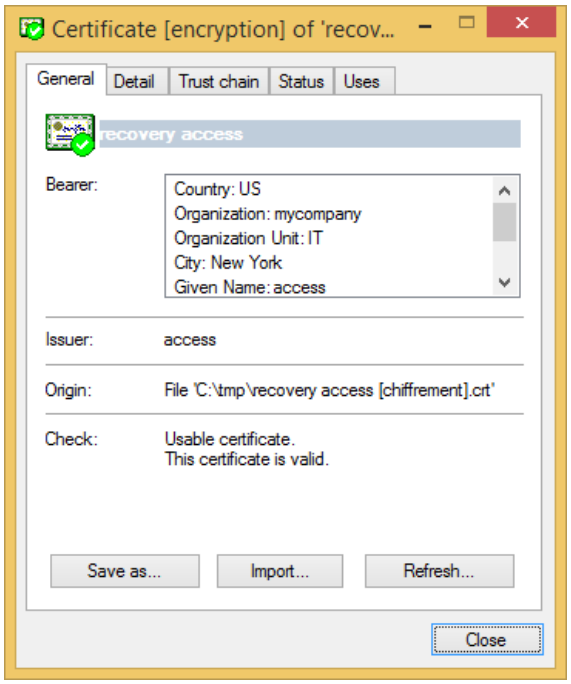
1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet **Configuration**.
4. Choisissez l'icône **Porte-clés**.
5. Cliquez sur l'onglet **Recouvrement**.
6. Cliquez sur **Opérations** et choisissez **Importer une clé**, puis passez l'écran d'introduction.
7. Renseignez le nom du fichier *.p7b* ou*.p7c* contenant les clés à importer ou le nom du certificat *.cer* ou *.crt* contenant une seule clé. Stormshield Data Security affiche la liste des certificats présents dans le fichier, c'est-à-dire le certificat associé à la clé contenue dans le fichier, avec éventuellement sa parenté.



Le certificat sélectionné doit avoir les usages de chiffrement.

NOTE
Il peut arriver que le certificat de recouvrement devant être utilisé ne soit pas indiqué comme étant de confiance (petite coche verte) notamment dans le cas où il a été généré dans un environnement tiers (volontairement distinct du reste).

8. Il est possible de créer plusieurs niveaux de certificats de recouvrement chacun des niveaux pouvant représenter un niveau de l'organisation de l'entreprise (pour permettre un recouvrement à un niveau branche par exemple).
9. Pour visualiser un certificat de la liste, cliquez dessus.



Pour revenir à la liste des certificats, cliquez sur le bouton **Fermer**.

10. Passez à l'écran suivant et sélectionnez les produits pour lesquels la clé de recouvrement sera utilisée.
11. Vérifiez le récapitulatif, cliquez sur **Terminer** et vérifiez le résultat de l'opération. La clé importée apparaît alors dans la liste.

8.3.3 Utiliser une clé de recouvrement

Il est possible d'utiliser des clés de recouvrement provenant d'un compte Stormshield Data Security ou d'une source extérieure.

- Si la clé de recouvrement est issue d'un compte Stormshield Data Security, utilisez ce compte pour déchiffrer les données.
- Si la clé de recouvrement provient d'une autre source, exportez de cette autre source, la clé privée (et son certificat) au format *PKCS#12* (*.P12*), ou obtenez cette clé à ce format par tout moyen standard.

Il faut ensuite créer un compte Stormshield Data Security en utilisant ce fichier *.P12* et son mot de passe associé (reportez-vous à la section Importer une clé au format PKCS#12), puis utiliser ce compte Stormshield Data Security pour déchiffrer les données.

Vous pouvez créer un compte avec seulement la fonction de déchiffrement.

Vous devriez être en mesure de déchiffrer toutes les données de l'utilisateur, chiffrées par lui-même, ou par ses collaborateurs à son intention si ceux-ci utilisent la même clé de recouvrement. Néanmoins, il vous sera impossible de déchiffrer les données provenant de l'extérieur (par exemple les e-mails reçus).

8.3.4 Renommer une clé

Pour modifier le libellé créé automatiquement par Stormshield Data Security :

1. Allez dans l'onglet *Recouvrement*.
2. Effectuez un clic-droit sur le certificat dont on veut changer le libellé et sélectionner **Renommer**.

Il est également possible de sélectionner la clé concernée et d'utiliser le bouton **Opérations**.

3. Saisissez le nouveau libellé (le libellé est devenu modifiable).
4. Validez la modification avec la touche Entrée.

La touche Echap permet d'annuler la modification.

8.3.5 Afficher les informations d'une clé

Pour afficher les informations d'une clé de recouvrement :

1. Allez dans l'onglet *Recouvrement*.
2. Effectuez un clic-droit sur la clé concernée et sélectionnez **Propriétés**.

Il est également possible de sélectionner le certificat concerné et d'utiliser le bouton **Opérations**.

Le certificat est alors affiché.

8.3.6 Suppression d'une clé

Vous pouvez supprimer une clé de recouvrement du compte :

1. Allez dans l'onglet *Recouvrement*.
2. Effectuez un clic-droit sur la clé concernée et sélectionnez **Effacer**.

Il est également possible de sélectionner la clé concernée et d'utiliser le bouton **Opérations**.

3. Confirmez la demande de suppression.

8.4 Exporter votre compte Stormshield Data Security

Vous pouvez exporter votre compte utilisateur dans un fichier Windows Installer qui contiendra toutes les informations et les fichiers de votre compte.

Une fois votre compte exporté sur ce fichier Windows Installer, vous pourrez le conserver pour le sauvegarder, ou le transporter sur un autre poste utilisant Stormshield Data Security pour y installer votre compte utilisateur.

Pour exporter votre compte :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Assistants*.
4. Cliquez sur **Exporter votre compte**.
5. Passez l'écran d'introduction.

L'icône à droite du champ de saisie permet d'ouvrir une fenêtre standard de sélection de fichiers.

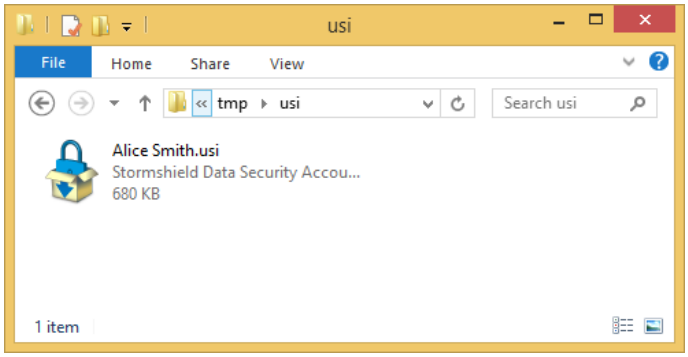
6. Saisissez le nom du fichier à créer et passez à l'écran suivant.
7. Vérifiez le récapitulatif puis cliquez sur **Terminer**.

Stormshield Data Security crée alors le fichier *.usi* à l'endroit indiqué et affiche un compte rendu.

8.5 Installer votre compte utilisateur

Vous devez avoir préalablement exporté ou créé votre compte utilisateur avec Stormshield Data Authority Manager.

1. Double-cliquez sur le fichier *.usi* qui contient votre compte :



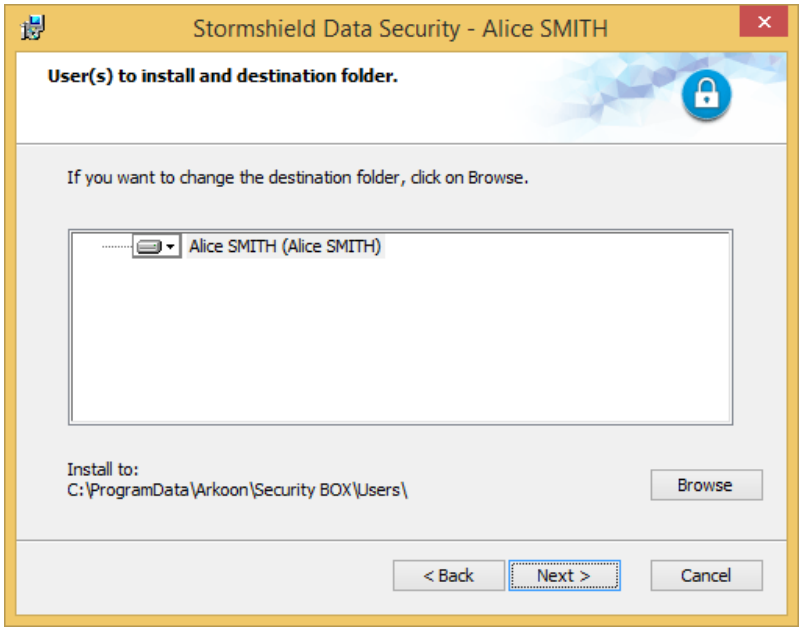
2. Le processus d'installation du compte démarre, et permet de :

a. choisir le compte que vous voulez installer. Pour un export, seuls les comptes qui peuvent être exportés sont affichés.

b. choisir l'emplacement exact où vous souhaitez l'installer (bouton **Modifier**).

NOTE
Nous recommandons de garder l'emplacement indiqué par défaut, sinon vous ne pourrez pas utiliser le compte directement. Vous aurez à entrer l'adresse complète du compte dans la fenêtre de connexion, ou modifier le compte (reportez-vous au *Guide d'administration*).

3. Cliquez sur **Suivant** pour effectuer l'installation du compte.



Une fois votre compte installé, si vous n'avez pas modifié l'emplacement d'installation par défaut, vous pouvez vous connecter directement à votre compte utilisateur.

8.6 Exporter votre clé de sécurité

Vous pouvez exporter dans un fichier votre clé de sécurité (clé publique et clé privée), avec son certificat et son éventuelle parenté.

Si vous avez un compte à deux clés, vous pouvez importer les clés individuellement.

En sauvegardant ce fichier, vous pourrez :

- recréer un nouveau compte à partir de votre clé actuelle ;
- utiliser cette clé dans toute application capable d'importer une clé de sécurité.

Cela sera utile pour les clés de déchiffrement dans les cas de déchiffrement par délégation (reportez-vous à la section Clé de déchiffrement). Cela peut être utilisé également pour déchiffrer les documents antérieurement chiffrés avec cette clé).

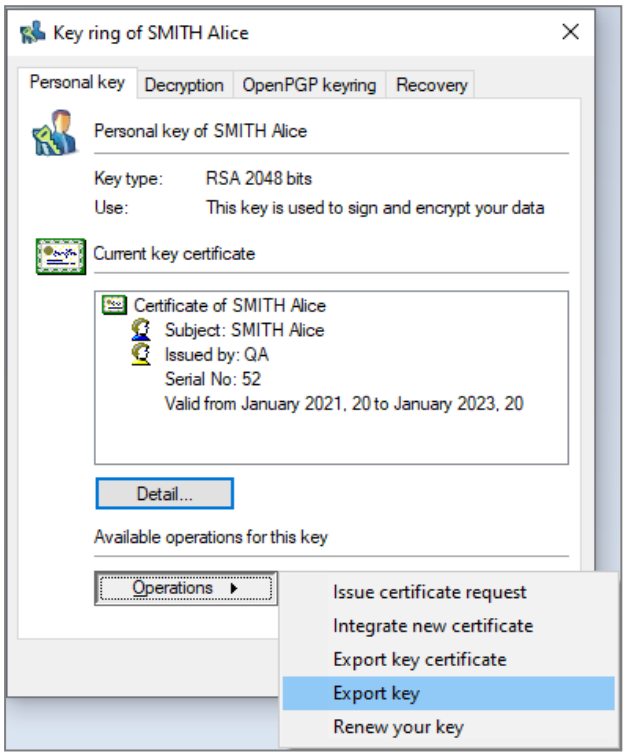
Le fichier contenant votre clé est généré au format *PKCS#12* (extensions *.p12* ou *.pfx*). Si vous avez deux clés, chacune sera exportée dans un fichier séparé.

Pour exporter votre clé :

1. Ouvrez le menu Stormshield Data Security.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Porte-clé**.

- Si vous possédez deux clés, choisissez l'onglet *Clé de chiffrement* ou *Clé de signature*.
- Si vous ne possédez qu'une seule clé, choisissez l'onglet *Clé personnelle*.

5. Cliquez sur **Opérations** et choisissez **Exporter votre clé** puis passez l'écran d'introduction.



6. Cochez l'une des deux options suivantes. Vous pouvez cochez les deux options.

- l'option **Fournir la parenté de votre certificat** pour associer à votre clé le certificat de/des autorités qui ont certifié votre clé.

Seuls les certificats dans votre annuaire de confiance seront affichés. Aucune recherche ne sera faite sur l'annuaire LDAP.

- l'option **Fournir les anciens certificats de votre clé** si vous avez effectué un ou plusieurs renouvellements de certificats mais que vous souhaitez pouvoir déchiffrer des documents chiffrés avec d'anciens certificats.

Passez ensuite à l'écran suivant.

7. Saisissez le nom du fichier à créer et passez à l'écran suivant.

Le bouton **Enregistrer sous** permet de modifier le nom du fichier, mais les clés ne sont pas exportées.

8. Saisissez le mot de passe de protection du fichier qui va permettre de chiffrer votre clé dans le fichier généré.

NOTE
Le mot de passe saisi doit faire au moins huit caractères de long et contenir soit un chiffre, soit une marque de ponctuation. Si ce n'est pas le cas, l'exportation est refusée.

9. Passez à l'écran suivant, vérifiez le récapitulatif, puis cliquez sur **Terminer**.

Votre clé a été exportée dans le fichier indiqué.

8.7 Renouvellement des clés

Vous pouvez renouveler vos clés afin de changer vos clés de chiffrement ou de signature.

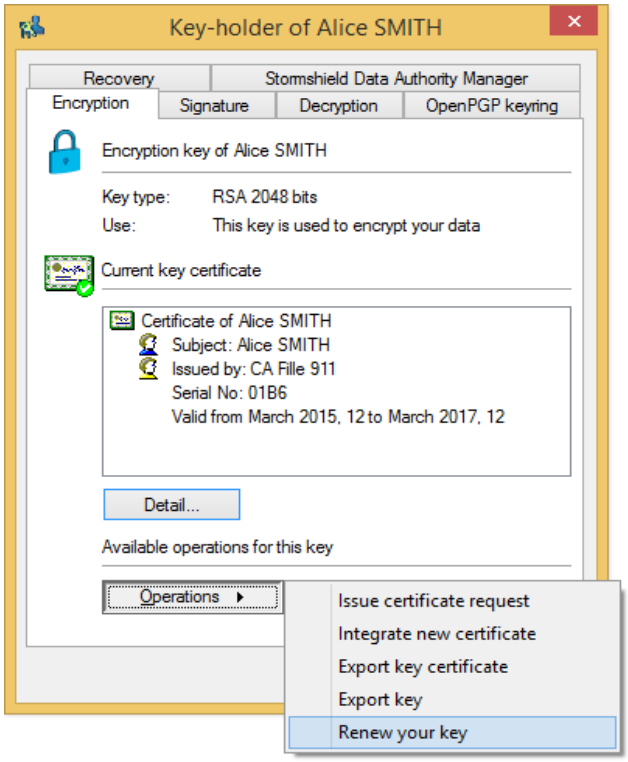
Pour renouveler votre clé :

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Porte-clés**.

Si vous possédez deux clés, choisissez l'onglet *Chiffrement* ou *Signature*.

Si vous n'avez qu'une clé, choisissez l'onglet *Clé personnelle*.

5. Cliquez sur **Opérations** et choisissez **Renouveler votre clé** puis passez l'écran d'introduction.



6. Indiquez comment vous souhaitez créer la clé de chiffrement :

- Pour créer une nouvelle clé, choisissez l'option **Générer votre clé personnelle** et sélectionnez le type et la longueur de votre clé.

Pour la suite de la procédure, voir la section étape 8 dans la Création d'une clé.

- Pour importer une clé existante, choisissez **Importer votre clé**.

Pour la suite de la procédure, voir la section étape 5 dans la Importer une clé au format PKCS#12.

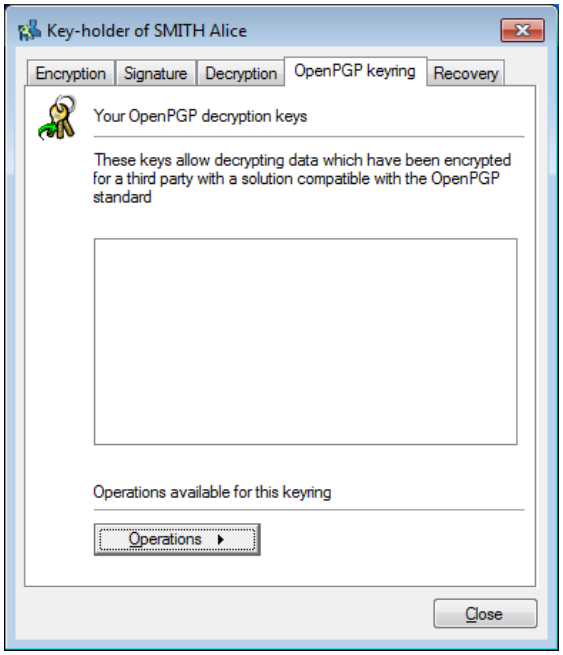
7. Cliquez sur **Terminer**.

Stormshield Data Security génère ou importe votre clé personnelle et déplace votre ancienne clé en tant que clé de déchiffrement afin que vous puissiez déchiffrer tous vos anciens documents. Les clés de signature ne sont pas gardées.

8.8 Clés de déchiffrement OpenPGP

Stormshield Data Security gère les clés de déchiffrement de messages au format OpenPGP. Ces clés sont utilisées par l'add-in Stormshield Data Mail Édition Outlook pour lire des messages sécurisés par les applications PGP, GnuPGP ou toute application compatible avec le format OpenPGP.

Lorsque l'add-in Stormshield Data Mail Édition Outlook est installé sur la machine, l'onglet *Porte-clés OpenPGP* dans les propriétés du compte de l'utilisateur, permet de gérer ces clés.



8.8.1 Importer un porte-clés OpenPGP

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Porte-clés**.
5. Sélectionnez l'onglet *Porte-clés OpenPGP*.
6. Cliquez sur **Opérations** puis **Importer un porte-clés**.
7. Sélectionnez un fichier au format OpenPGP (*.gpg*, *.pgp*ou *.asc*). Le fichier peut contenir plusieurs clés.
8. Saisissez le mot de passe protégeant le fichier.

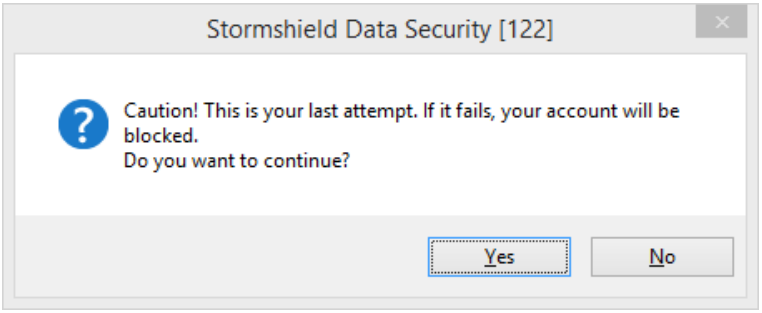
8.9 Déblocage de votre compte

Si vous avez oublié votre mot de passe ou votre code confidentiel, ou si votre compte est bloqué suite à la saisie consécutive d'un trop grand nombre de codes erronés, vous pouvez débloquer votre compte de deux façons distinctes :

- à l'aide du mot de passe de secours saisi lors de la création de votre compte.
- si vous ne connaissez pas le mot de passe de secours : en contactant votre administrateur pour lui fournir la suite de caractères nécessaires au déblocage.

Le nombre de tentatives de mot de passe ou de code confidentiel est limité à trois mais peut être modifié. Consultez le *Guide d'administration*.

Avant que la dernière tentative de mot de passe ou de code confidentiel ne soit effectuée, la fenêtre suivante est affichée. Si vous cliquez sur **Non**, la tentative n'est pas effectuée : vous pouvez chercher à retaper soigneusement le mot de passe ou code confidentiel (tout en vérifiant que les touches MAJ et NUM LOCK ne sont pas activées).



Lorsque le compte est bloqué, la fenêtre suivante s'affiche lors d'une saisie de mot de passe ou de code confidentiel. Cette fenêtre s'affiche au moment du blocage (dernier essai infructueux) et lors des saisies suivantes, que le mot de passe ou code confidentiel soit correct ou non :

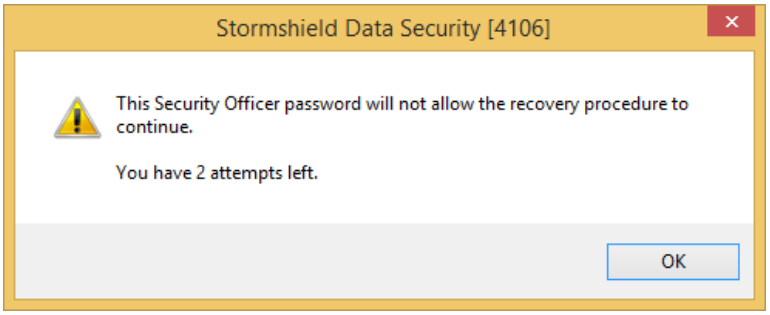
8.9.1 Pour débloquer le compte si vous connaissez le mot de passe Security Officer :

1. Dans la fenêtre de connexion sélectionnez **Déverrouiller** pour démarrer l'outil de déverrouillage.
2. Passez la page d'introduction en cliquant sur **Suivant**.

> **NOTE**
> Selon la configuration de votre compte, la procédure se poursuit étape 3) ou étape 4).

3. Sélectionnez **Vous connaissez le mot de passe de secours**.
4. Saisissez le mot de passe Security Officer puis cliquez sur **Suivant**.

En cas d'erreur de la saisie du mot de passe Security Officer, le message suivant s'affiche :



IMPORTANT
En cas de blocage du mot de passe de secours, il n'est plus possible de débloquer le compte.

5. Saisissez un nouveau mot de passe en respectant les critères affichés puis confirmez-le.
6. Cliquez sur **Terminer**.

Le compte est à nouveau opérationnel avec votre nouveau mot de passe. Vous devez vous connecter à Stormshield Data Security en utilisant le nouveau mot de passe.

8.9.2 Pour débloquer le compte si vous ne connaissez PAS le mot de passe Security Officer :

1. Dans la fenêtre de connexion sélectionnez **Déverrouiller** pour démarrer l'outil de déverrouillage.
2. Passez la page d'introduction en cliquant sur **Suivant**.

NOTE
Selon la configuration de votre compte, la procédure se poursuit étape 3) ou étape 4).

3. Sélectionnez **Vous ne connaissez pas le mot de passe de secours** et cliquez sur **Suivant**.
4. Fournissez à votre administrateur les caractères affichés à l'écran en utilisant la fonction **Copier dans le presse-papier**.

La longueur de la suite de caractères à fournir varie selon le mode de création de votre compte et peut atteindre 126 caractères :

IMPORTANT
Veillez à ne pas fermer la fenêtre de récupération de mot de passe avant que votre administrateur vous contacte.

5. Saisissez les caractères fournis par votre administrateur puis cliquez sur **Suivant** : votre compte est débloqué.
6. Saisissez un nouveau mot de passe en respectant les critères affichés puis confirmez-le.
7. Cliquez sur **Terminer**.

Le compte est à nouveau opérationnel avec votre nouveau mot de passe. Vous devez vous connecter à Stormshield Data Security en utilisant le nouveau mot de passe.

9. Cas d'erreurs fonctionnelles

Ce chapitre liste les cas d'erreurs fonctionnelles rencontrés lors de l'utilisation de Stormshield Data Security Enterprise.

NOTE
Dans les tableaux suivants, le terme **Journalisation** signifie qu'un événement a été enregistré dans l'observateur d'événements de Microsoft Windows.

Le PIN saisi est erroné.	
Circonstance	Vous saisissez un PIN incorrect dans l'assistant de création du compte.
Effet	Affichage du message d'erreur “Code confidentiel incorrect. Veuillez le saisir à nouveau.” Invitation à en saisir un nouveau.
Journalisation	Oui

La carte est bloquée.	
Circonstance	La carte insérée est bloquée.
Effet	Affichage du message : “Votre carte est bloquée.”
Journalisation	Oui

Vous n'avez pas les autorisations ad'hoc sur le dossier de stockage des comptes.	
Circonstance	Vous n'avez pas les autorisations sur le dossier dans lequel les comptes utilisateurs sont créés.
Effet	Dans ce cas, le noyau Stormshield Data Security refuse de se lancer et affiche le message : “Les valeurs des paramètres DefaultyPath1 et/ou DefaultPath2 présents dans *SBox.ini* ne sont pas valides. Stormshield Data Security ne peut pas démarrer. Veuillez contacter votre administrateur.”
Journalisation	Oui

Le contenu de la carte ne permet pas de créer le compte.	
Circonstance	Le contenu de la carte/du token (nombre et type de clés) n’est pas en accord avec la politique de création automatique définie dans le fichier *SBox.ini*.
Effet	Affichage du message : “Le contenu de votre carte ne permet pas d'utiliser la création de compte automatique.” Le compte n’est pas créé.
Journalisation	Oui

Le modèle est bloqué.	
Circonstance	Le modèle utilisé pour la création de compte est protégé par mot de passe : il est bloqué suite à un trop grand nombre d'essais infructueux.
Effet	Affichage du message : "Le modèle est bloqué (nombre d'essais trop important)." Le compte n'est pas créé.
Journalisation	Oui

Le compte modèle est inaccessible	
Circonstance	Le modèle est introuvable, non accessible ou ne correspond pas au type de compte désiré (mauvais paramétrage du *SB0X.ini* ou des permissions sur le fichier modèle).
Effet	Affichage du message : "Échec de la copie des modèles". Le compte n'est pas créé.
Journalisation	Oui

La liste des certificats de confiance est inaccessible.	
Circonstance	La liste des certificats est introuvable ou non accessible suite à un mauvais paramétrage du *SB0X.ini* ou des permissions sur le(s) fichier(s) certificats).
Effet	Affichage du message : "Echec de la copie des modèles". Le compte n'est pas créé.
Journalisation	Oui

Un utilisateur est déjà connecté à Stormshield Data Security dans une autre session Windows.	
Circonstance	Vous n'êtes pas connecté à Stormshield Data Security dans une session Windows, ouvrez une seconde session Windows, et essayez de vous connecter à Stormshield Data Security dans cette seconde session.
Effet	Connexion refusée avec le message "Un utilisateur est déjà connecté."
Journalisation	Oui

Le code secret saisi est incorrect.	
Circonstance	Vous avez saisi un mot de passe ou un PIN qui n'est pas le bon.
Effet	Affichage du message "Le code secret est incorrect". Affichage de nombre d'essais restant. Invitation à ressaisir le mot de passe ou le PIN.
Journalisation	Oui

L'identifiant saisi ou la carte insérée ne correspondent à aucun compte Stormshield Data Security.	
Circonstance	Vous avez saisi un identifiant pour lequel il n'existe pas de compte Stormshield Data Security. Vous avez inséré une carte pour laquelle il n'existe pas de compte Stormshield Data Security.
Effet	Affichage du message : "Cet utilisateur n'existe pas." Invitation à ressaisir un nouvel identifiant.
Journalisation	Oui

Annexe A. Crédits

Le logiciel Stormshield Data Security utilise le composant logiciel libre BouncyCastle.Net, dont voici la licence :

Copyright (c) 2000 - 2015 The Legion of the Bouncy Castle Inc. (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2023. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.