GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA SIGN

Signature électronique

Version 10.1

Dernière mise à jour du document : 29 mars 2022

Référence : sds-fr-sd_sign-guide_d_utilisation-v10

Table des matières

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

Préface

Ce document fournit les informations essentielles à l'utilisation de Stormshield Data Sign. Il décrit les fonctions de Stormshield Data Sign dans sa configuration par défaut. Vous pouvez personnaliser l'installation de ce composant à l'aide de Stormshield Data Authority Manager. Les options de personnalisation les plus importantes sont données dans ce guide. Ce guide s'adresse :

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

1. Introduction

Cette section présente les fonctions et caractéristiques de Stormshield Data Sign.

1.1 Authenticité et intégrité des données

Stormshield Data Sign est un logiciel de sécurité informatique qui permet de signer électroniquement des documents électroniques. Les signatures électroniques sont basées sur l'infrastructure à clé publique – en anglais : public key infrastructure (PKI). Elles résultent d'une opération cryptographique.

Stormshield Data Sign permet donc à votre entreprise ou organisation de garantir pour quelque type de document que ce soit, l'authenticité de ses signataires et l'intégrité de son contenu.

En outre, signer un document avec Stormshield Data Sign peut être considéré comme un engagement au même titre qu'une signature manuscrite peut le faire.

Lorsque vous signez un document avec Stormshield Data Sign :

- L'empreinte unique du document est créée à l'aide d'un algorithme mathématique.
- L'empreinte du document est signée avec votre clé privée puis est combinée avec votre clé publique et votre certificat pour créer une signature électronique unique qui sera ajoutée à votre document.

Stormshield Data Sign place le document signé dans un nouveau fichier qui porte le même nom de fichier que le fichier original mais a une extension différente. Le document signé est scellé et tout changement apporté au document après la signature invalide la signature. C'est une façon de protéger le document contre toute falsification des données et de signature.

Lorsque vous vérifiez un document signé avec Stormshield Data Sign :

- La signature de l'expéditeur est vérifiée à l'aide de la clé publique de l'expéditeur et l'empreinte du document original est extraite. Stormshield Data Sign calcule à son tour l'empreinte du document signé et compare le résultat à l'empreinte originale extraite. Si les empreintes sont identiques, l'authenticité du document est validée.
- L'authenticité et la validité de la signature sont vérifiées à l'aide de la liste de révocation.

1.2 Caractéristiques clés de Stormshield Data Sign

Cette section présente les caractéristiques et avantages les plus importants de Stormshield Data Sign.

1.2.1 Différents types de signatures

Stormshield Data Sign permet d'apposer différents types de signatures sur un document. Il est possible de :

- **co-signer** un document en ajoutant votre propre signature à un document déjà signé, indépendamment des autres signatures déjà présentes.
  Par exemple, un contrat entre deux parties requiert la signature des deux parties pour être valide. Stormshield Data Sign permet à chaque partie de signer le document indépendamment l'une de l'autre et, ce, dans n'importe quel ordre.

- **contre-signer** un document signé en ajoutant votre propre signature sur une autre signature.
  Par exemple, pour être payée, une facture doit être d'abord signée par le commanditaire qui valide la facture, puis contre-signée par le comptable. Le paiement nécessite les deux signatures : le comptable doit attendre la validation du commanditaire et contre-signe en fait cette validation.
- **sur-signer** un document en apposant votre signature sur l'enveloppe qui contient le document signé.
  Par exemple, un transporteur garantit l'intégrité du document qui lui est confié en le mettant sous enveloppe et en signant cette enveloppe. Aucune co- ou contre-signature ne peut alors être ajoutée ou retirée du document transporté.

1.2.2 Analyse des documents

Outre le support de multiples signatures, Stormshield Data Sign peut analyser le contenu de documents de type PDF ou Microsoft Word afin d'y détecter la présence de macros et de champs dynamiques (par exemple, la date) qui peuvent éventuellement modifier l'apparence ou le contenu d'un document après qu'il ait été signé. Stormshield Data Sign vous avertit, le cas échéant, de la présence de macros et champs dynamiques, ainsi que des risques potentiels encourus. Cependant, Stormshield Data Sign vous laisse le choix de la décision finale s'agissant de la signature du document.

Lorsque Stormshield Data Sign détecte des éléments dynamiques dans un document pendant le processus de signature, un message d'erreur et une icône d'avertissement s'affichent dans la fenêtre de résumé final.

Lorsque Stormshield Data Sign détecte des éléments dynamiques dans un document pendant le processus de vérification de signature, la signature est alors considérée comme suspecte et une icône d'avertissement s'affiche. Pour plus d'informations, voir la section Vérifier un fichier signé.

NOTE
La détection de contenu dynamique requiert l'utilisation de Microsoft Word et n'est disponible que pour les documents de type *.doc*. Les documents de types *.docx* et *.docm* ne peuvent être traités.

1.2.3 Conformité

Stormshield Data Sign implémente la norme RFC 2630 – CMS Standard : Cryptographic Message Syntax.

1.2.4 Compatibilité

Stormshield Data Sign permet la sauvegarde des documents signés dans deux types de fichiers distincts, à savoir des fichiers de type *.p7f* ou *.p7m*.

Les fichiers de type *.p7m* peuvent être expédiés vers et validés par des correspondants qui n'utilisent pas Stormshield Data Sign, mais utilisent un autre logiciel conforme à la norme RFC 2630, qui spécifie les règles de format de la signature électronique.

1.2.5 Facilité d'utilisation

Stormshield Data Sign est complètement intégré dans l'environnement Windows, ce qui permet de signer des documents à partir un simple clic droit.

La manière dont s'utilise Stormshield Data Sign est très semblable à la manière dont nous utilisons un parapheur. En premier lieu, vous placez les documents à signer dans le parapheur Stormshield Data Sign. En second lieu, vous signez les documents. En outre, Stormshield Data Sign offre la possibilité de vérifier les signatures apposées sur les documents et d'extraire le contenu des documents signés.

1.3 Connexion sécurisée

L'accès à vos clés est protégé : pour les utiliser, vous devez vous connecter à Stormshield Data Security. Ce processus consiste à vous authentifier et vérifier que vous êtes bien le propriétaire des clés.

Stormshield Data Security propose deux méthodes d'authentification :

- par mot de passe : vous saisissez un identifiant et un mot de passe,
- par carte à puce ou clé USB : vous saisissez le code secret de la carte (en anglais, “PIN” Personal Identification Number).

Le stockage des clés sera défini en fonction du niveau de sécurité requis pour les signatures. Les signatures exigeant un haut niveau de sécurité requièrent l'utilisation d'équipements très sécurisés telles que les cartes à puces et clés USB. Ces équipements offrent une gestion renforcée des moyens d'authentification des utilisateurs en générant et stockant les données confidentielles (clés privées, mots de passe et certificats électroniques) à l'intérieur de l'environnement protégé de la puce. Les clés privées des utilisateurs ne peuvent pas être perdues, lues ou utilisées par une tierce partie. Toutefois, pour des signatures plus formelles, un mot de passe peut être suffisant.

La gestion des comptes utilisateurs est décrite dans le *Guide d'installation et de mise en œuvre*.

2. Installation de Stormshield Data Sign

2.1 Configuration requise

Pour connaître la configuration requise sur les systèmes d'exploitation Microsoft, reportez-vous à la section **Compatibilité** de la note de version de Stormshield Data Security 10.1.

200 Mo d'espace disque sont requis pour l'installation de tous les composants de Stormshield Data Security.

IMPORTANT
Stormshield Data Security n'est pas compatible avec la fonction **Changement Rapide d'Utilisateur**.

2.2 Installation de Stormshield Data Sign

Stormshield Data Sign est un composant de Stormshield Data Security Enterprise.

Une clé de licence 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.

La procédure d'installation est détaillée dans le *Guide d'installation et de mise en œuvre*.

3. Comment dialoguer avec Stormshield Data Sign

Cette section présente les différentes matières de dialoguer avec Stormshield Data Sign a partir de l'Explorateur Windows et du Parapheur Stormshield Data Sign.

Stormshield Data Sign s'intègre parfaitement dans l'interface Windows et l'Explorateur Windows. Les fonctions peuvent être lancées à partir :

- du bouton droit de la souris après la sélection d'un objet dans l'Explorateur Windows.
- du glisser-déposer vers la fenêtre du Parapheur Stormshield Data Sign
- de la barre de menus, après démarrage de l'application.

Lorsque la fenêtre du Parapheur Stormshield Data Sign est ouverte, les fonctions peuvent être lancées à partir de la barre de menus.

NOTE
Dans le reste du guide, le terme *Parapheur* désigne le Parapheur Stormshield Data Sign.

3.1 Le clic droit

A partir de l'Explorateur Windows ou de la fenêtre du Parapheur, cliquez sur le bouton droit de la souris après avoir sélectionné un fichier pour accéder au menu contextuel.

Dans les chapitres suivants, l'utilisation du clic droit est préconisée.

3.2 Le glisser-déposer

Lorsque le Parapheur est lancé, il est possible de sélectionner un fichier puis, en maintenant le bouton gauche de la souris enfoncé, de le déplacer vers la fenêtre du Parapheur. A partir de cette fenêtre, les différentes fonctions peuvent être lancées à partir du menu contextuel ou de la barre de menu.

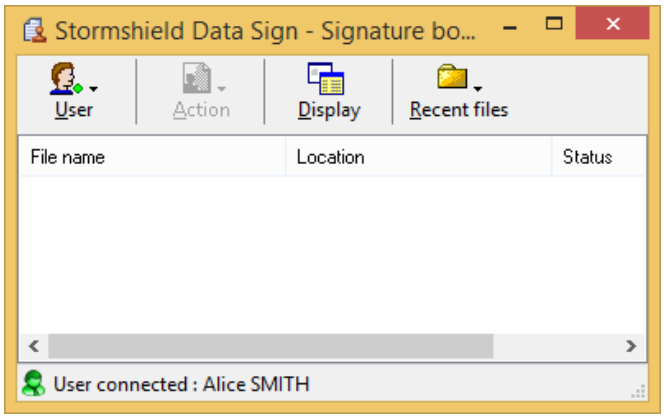
3.3 La barre de menus

Cette section décrit comment lancer les fonctions de Stormshield Data Sign à partir de la barre de menus du Parapheur.

Ouvrez la fenêtre du Parapheur Stormshield Data Sign en sélectionnant **Tous les programmes** > **Stormshield Data Security** > **Stormshield Data Sign** à partir du menu **Démarrer**.

NOTE

Le Parapheur peut également être lancé à partir de la fenêtre de configuration **Général** en cliquant sur **Démarrer le Parapheur Stormshield Data Sign**.



Quatre menus, décrits ci-dessous, sont disponibles à partir du Parapheur.

A partir du menu **Utilisateur**, il est possible de :

- Verrouiller ou déverrouiller une session Stormshield Data Security
- Se connecter à ou déconnecter de Stormshield Data Security
- Créer un nouvel utilisateur Stormshield Data Security
- Quitter la fenêtre Stormshield Data Sign Parapheur

Le menu **Actions** propose les mêmes options que celles disponibles à partir du menu contextuel après avoir sélectionné un fichier. Si aucun fichier n'est sélectionné, le menu **Actions** n'est pas accessible. Les choix du menu sont :

- **Retirer** pour retirer le fichier sélectionné de la liste. Le fichier n'est pas effacé du disque.
- **Extraire** pour extraire le contenu d'un fichier sélectionné après avoir ôté un niveau de signature (référez-vous à la section Extraire le fichier d'origine pour plus d'informations)
- **Lire** pour lancer l'opération associée par défaut au type du fichier sélectionné. Généralement l'application associée par défaut avec le fichier sélectionné est démarrée.
- **Signer** pour signer le fichier sélectionné
- **Signatures** pour afficher les signatures contenues dans le fichier sélectionné et vérifier les certificats associés.
- **Propriétés** pour afficher les propriétés du fichier sélectionné.

Le menu **Afficher** permet de modifier le type d'affichage du fichier.

Les types d'affichage disponibles sont :

- Grandes icônes
- Petites icônes
- Liste
- Détail

Les types d'affichage sont similaires à ceux de l'Explorateur Windows.

Sélectionner **Fichiers récents** permet d'accéder à la liste des derniers fichiers utilisés par le Parapheur. La sélection d'un de ces fichiers dans la liste provoque son ajout au Parapheur.

4. Configuration des options

Cette section décrit comment configurer les options générales et plus avancées de Stormshield Data Sign.

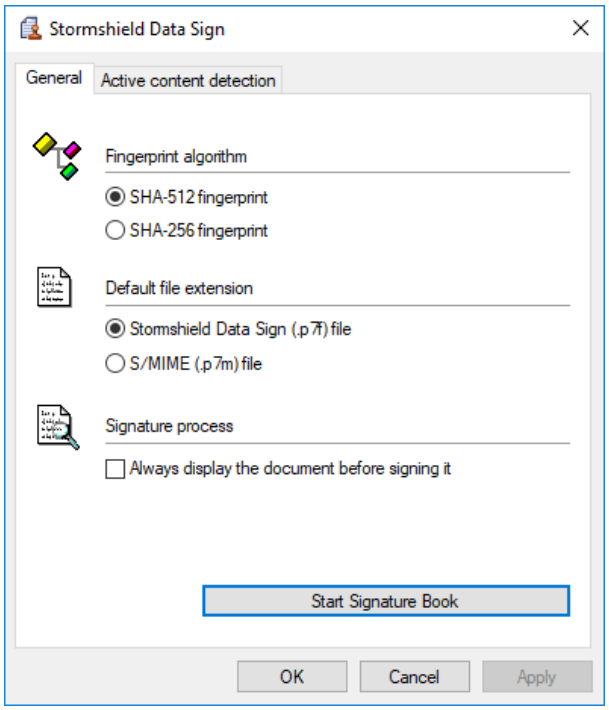
4.1 Accéder à la fenêtre de configuration

Pour afficher la fenêtre de configuration :

1. A partir de l'Explorateur Windows, effectuez un clic droit sur l'icône Stormshield Data Security et sélectionnez **Propriétés**. Allez sur l'onglet *Configuration* et double-cliquez sur l'icône Sign. La fenêtre de configuration s'affiche.
2. Sélectionnez **Général** ou **Détection de contenu actif**.

4.2 Options générales

Les options générales sont affichées ci-dessous :



A partir de cette fenêtre de configuration, vous pouvez :

- Choisir l'algorithme que Stormshield Data Sign utilisera pour calculer l'empreinte utilisée dans la signature électronique :
- SHA-512,
- SHA-256.
- Choisir l'extension qui sera utilisée pour identifier le nouveau fichier lors du processus de signature d'un fichier. Le nom du fichier source est conservé. Seule l'extension diffère. Sélectionnez l'une des deux possibles extensions :
  - **Stormshield Data Sign (*.p7f*) file**
  - **S/MIME (*.p7m*) file**

NOTE

Il est recommandé de sélectionner l'extension *.p7f* afin d'éviter tout conflit avec d'autres outils utilisant des fichiers de type *.p7m*.

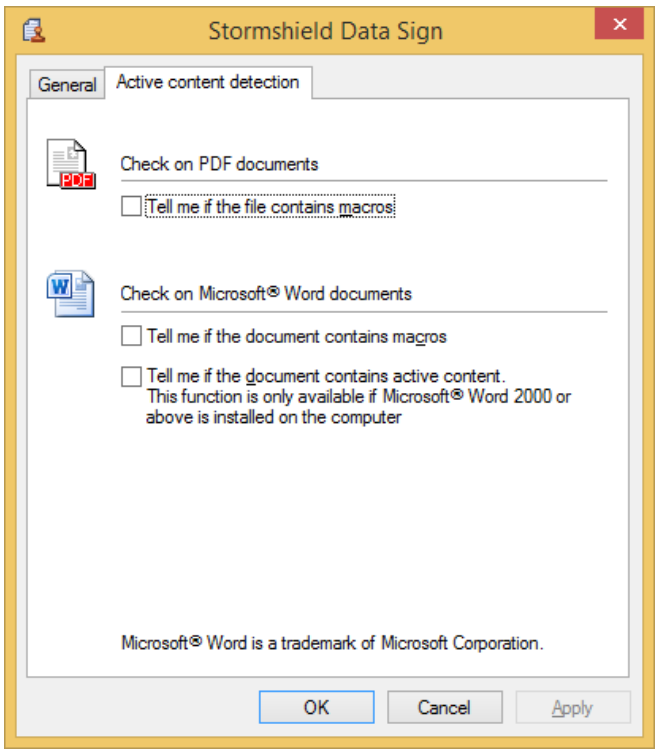
Lorsque vous choisissez l'extension *.p7f* :

- Le pictogramme est ajouté en bas à droite de l'icône d'origine du fichier, visible dans l'Explorateur Windows.
- Le fichier ne peut être lu par une tierce partie utilisant un autre outil de signature électronique.
- Vous pouvez demander la visualisation systématique du document avant de le signer. Dans ce cas, vous devrez obligatoirement afficher le document avant de le signer.
- Vous pouvez démarrer le Parapheur en cliquant sur **Lancer le parapheur Stormshield Data Sign**. Le Parapheur peut également être lancé en sélectionnant **Tous les programmes** > **Stormshield Data Security** > **Stormshield Data Sign** à partir du menu **Démarrer**.

4.3 Activer l'analyse des documents PDF et Word

Un document Adobe PDF ou Microsoft Word peut contenir des macros et des champs dynamiques qui peuvent modifier son apparence sans votre intervention. Si vous signez un tel document, le contenu ou la structure du document peut être ultérieurement modifié, ce qui peut entraîner des problèmes d'intégrité.

Avant de signer un document, Stormshield Data Sign peut procéder à une vérification du document afin de détecter la présence de macros et champs dynamique dans son contenu. Pour activer cette fonction, sélectionnez les options adéquates :



5. Utilisation de Stormshield Data Sign

Cette section décrit les différentes tâches que vous pouvez accomplir avec Stormshield Data Sign.

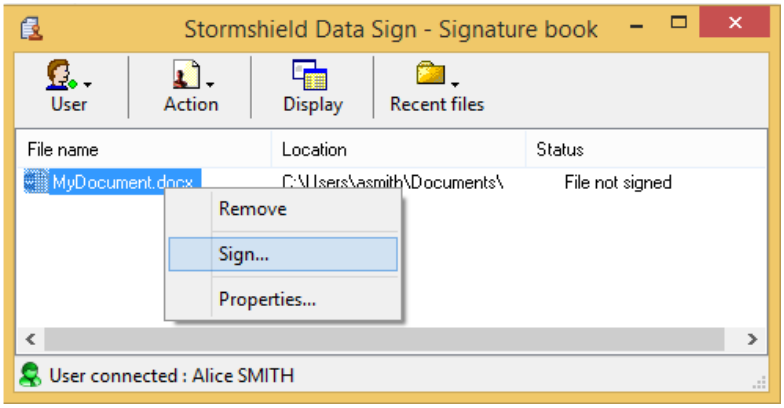
5.1 Signer un fichier

Pour signer un fichier :

1. Dans l'Explorateur Windows, sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Envoyer vers > Stormshield Data Sign**à partir du menu contextuel : le fichier est alors déposé dans le Parapheur.

   NOTE
   Si le Parapheur est déjà ouvert, sélectionnez le fichier désiré pour le déplacer et le déposer dans le Parapheur

2. Dans le Parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Signer**.



3. Suivez les instructions de l'assistant, qui demande systématiquement votre code confidentiel ou votre mot de passe.

Si vous êtes sur le point de signer un document Microsoft Word, ou un document PDF, Stormshield Data Sign peut l'analyser et informer de la présence de macros ou de contenu actif pouvant modifier dynamiquement l'apparence du document lors de son affichage. Ces contrôles sont activables dans la configuration de Stormshield Data Sign (voir la section Activer l'analyse des documents PDF et Word). Il vous appartient ensuite de signer ou non le document.

L'affichage du document avant de le signer est optionnel à moins que l'option **Toujours afficher le document avant de le signer** ne soit sélectionnée (voir la section Options générales). Dans ce cas, vous devez obligatoirement afficher le document avant de pouvoir continuer.

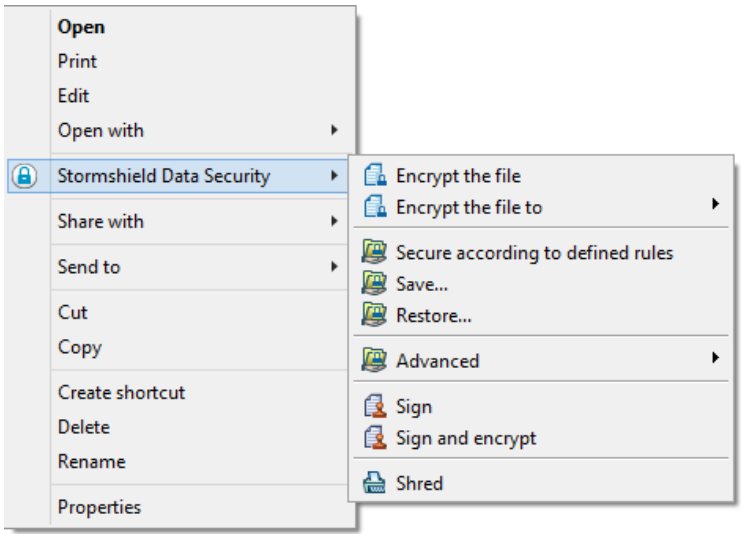
NOTE
Lorsque vous cliquez sur **Afficher**, le programme qui ouvre par défaut le document est automatiquement démarré.

Après avoir signé un document avec succès, Stormshield Data Sign ne modifie pas le fichier original. Il génère un nouveau fichier portant le même nom mais avec une extension différente, basée sur les options configurées antérieurement (voir la section Options générales).

5.1.1 Signer un fichier ou signer et chiffrer un fichier depuis le menu contextuel

Pour signer un fichier depuis le menu contextuel :

1. Sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Stormshield Data Sign > Signer** à partir du menu contextuel :



2. Suivez ensuite les instructions de l'assistant, qui demande systématiquement votre code confidentiel ou votre mot de passe, puis cliquez sur **Quitter** pour terminer la procédure.

Pour signer et chiffrer un fichier depuis le menu contextuel :

1. Sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Stormshield Data Sign > Signer et chiffrer** à partir du menu contextuel.

> **NOTE**
> Ce menu n'est présent que si le module Stormshield Data Sign est installé.

2. Suivez ensuite les instructions de l'assistant, qui demande systématiquement votre code confidentiel ou votre mot de passe, puis cliquez sur **Quitter**.
3. A l'ouverture de la fenêtre **Choix de vos correspondants**, sélectionnez les correspondants pour lesquels vous voulez effectuer le chiffrement puis cliquez sur **OK**.

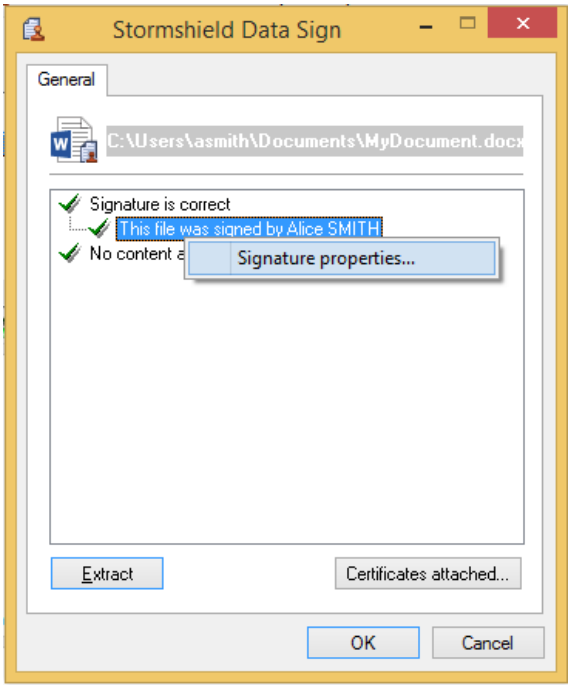
5.2 Vérifier un fichier signé

Utilisez la procédure ci-dessous pour vérifier un fichier signé. Ce dernier doit être un fichier avec une extension de type *.p7f* ou *.p7m*.

1. Dans l'Explorateur Windows, double-cliquez sur le fichier ou faites un clic droit pour sélectionner à partir du menu contextuel **Envoyer vers > Stormshield Data Sign** ; la fenêtre du Parapheur s'ouvre et le fichier y est déposé.

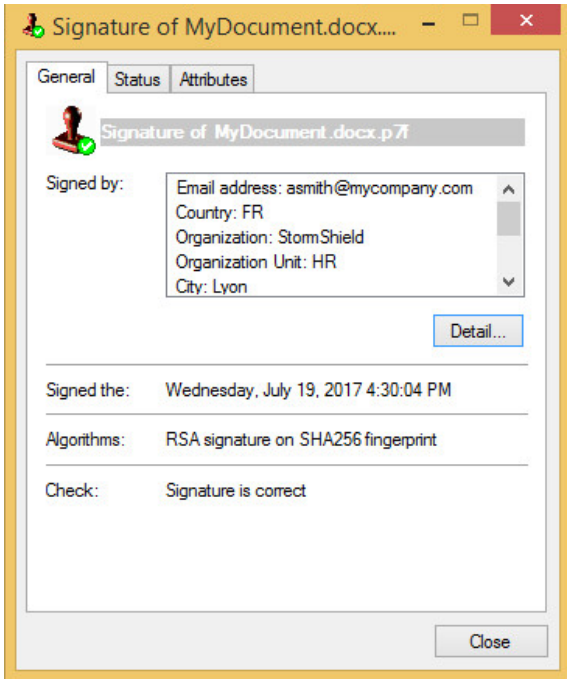
> **NOTE**
> Si la fenêtre du Parapheur est déjà ouverte, vous pouvez utiliser le glisser-déposer pour y placer le fichier.

2. A l'intérieur du Parapheur, effectuez un clic droit sur le fichier et sélectionnez **Signatures**. Le certificat du signataire s'affiche (voir ci-dessous). Seul le premier niveau de signatures est affiché. Il inclue la signature, puis les éventuelles co-signatures et contre-signatures. Le second niveau de signature correspondant à la sur-signature n'est pas montré.

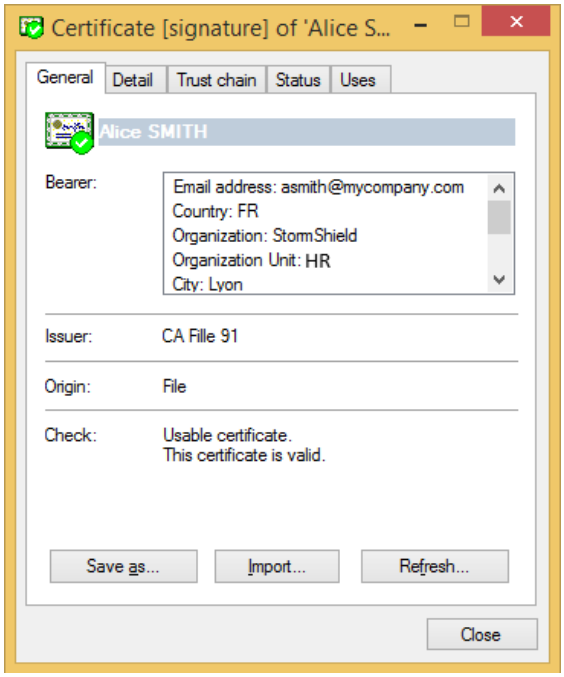


Si vous cliquez sur **Certificats joints**, Stormshield Data Sign affiche les certificats joints au fichier lors de la signature. Ces certificats ne peuvent cependant pas être considérés comme valides tant qu'ils n'ont pas été vérifiés à l'aide de votre annuaire de confiance.

3. Cliquez sur la signature avec le bouton droit de votre souris et choisissez **Propriété de la signature**. La fenêtre suivante s'affiche :



4. Cliquez sur **Détail** pour afficher le certificat du signataire :



Stormshield Data Sign vérifie :

- L'authenticité du contenu du document et de la signature : Stormshield Data Sign vérifie la signature et obtient l'empreinte originale du document. Puis Stormshield Data Sign calcule l'empreinte du document signé pour la comparer à l'empreinte originale. Si les empreintes sont identiques, cela signifie que le document n'a pas été modifié et Stormshield Data Sign en garantit l'authenticité.
- La validité du certificat de la signature : Stormshield Data Sign vérifie la validité du certificat pour garantir l'authenticité du signataire. En cas de signatures multiples, chaque signature est vérifiée : tous les certificats requis pour valider la signature numérique sont vérifiés.

Pour valider un certificat, Stormshield Data Sign consulte la liste de révocation. Cette liste étant régulièrement mise à jour, les résultats sont susceptibles d'être différents à chaque demande de vérification.

Cliquez sur **Importer** pour importer le certificat du signataire dans votre annuaire de confiance.

Cliquez sur **Rafraîchir** pour dynamiquement mettre à jour les données de la signature avec le ou les nouveaux certificats ou les informations de la liste de révocation.

Une fois la vérification achevée, Stormshield Data Sign affiche une icône résumant le résultat des vérifications effectuées :

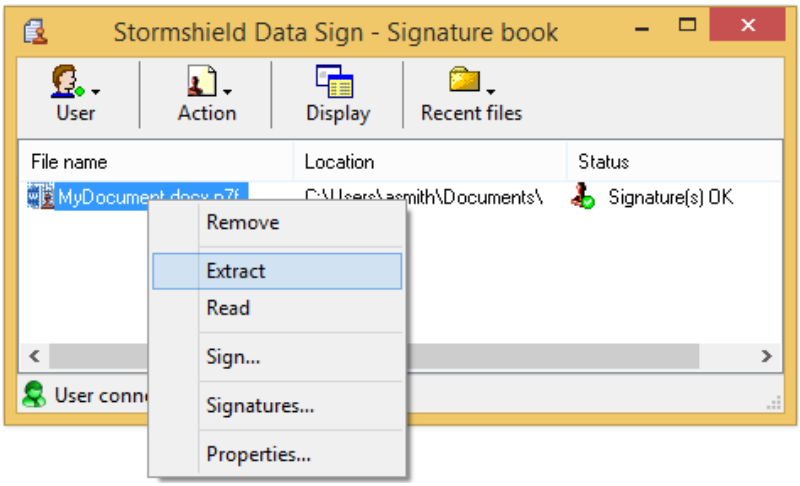
La signature est correcte et le certificat du signataire est valide.
Une anomalie a été détectée.
Une erreur grave a été détectée.

5.3 Extraire le fichier d'origine

Utilisez la procédure ci-dessous pour extraire d'un fichier signé le fichier d'origine et le sauvegarder dans un nouveau fichier :

1. Effectuez l'une des deux actions possibles :

- A partir du Parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Extraire** :



- A partir de la fenêtre affichant la signature d'un fichier, cliquez sur **Extraire**.

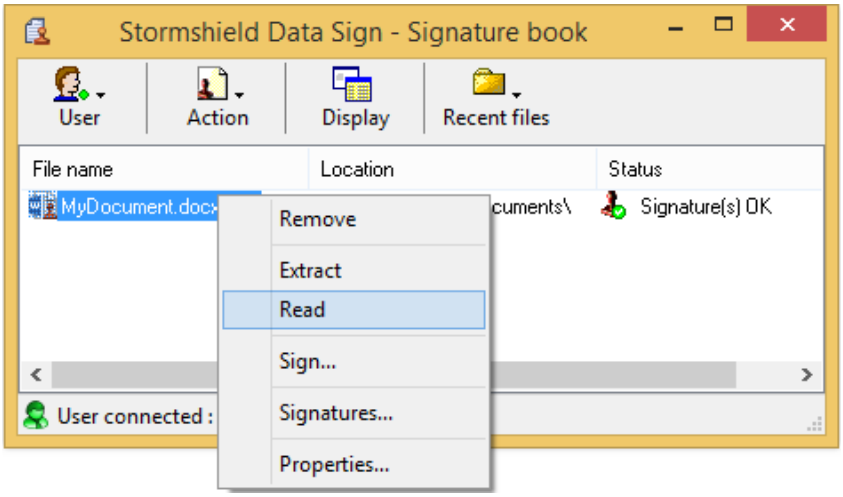
2. Saisissez le nom du fichier sous lequel le fichier d'origine va être enregistré.

> **NOTE**
> Si vous extrayez le contenu d'un fichier sur-signé, le résultat de l'extraction contient le premier niveau de signature mais ne contient aucune sur-signature.

5.4 Lire le contenu d'un fichier signé

Pour lire le contenu d'un fichier signé avec l'application associée sans pour autant extraire le fichier d'origine :

1. Dans le Parapheur, cliquez sur le fichier signé avec le bouton droit de votre souris et choisissez **Lire** :



2. Attendez que le compte rendu de la signature s'affiche.
3. Cliquez sur **Lire**. L'action associée par défaut en fonction du type du fichier s'exécute. Généralement le fichier est ouvert dans l'application appropriée.

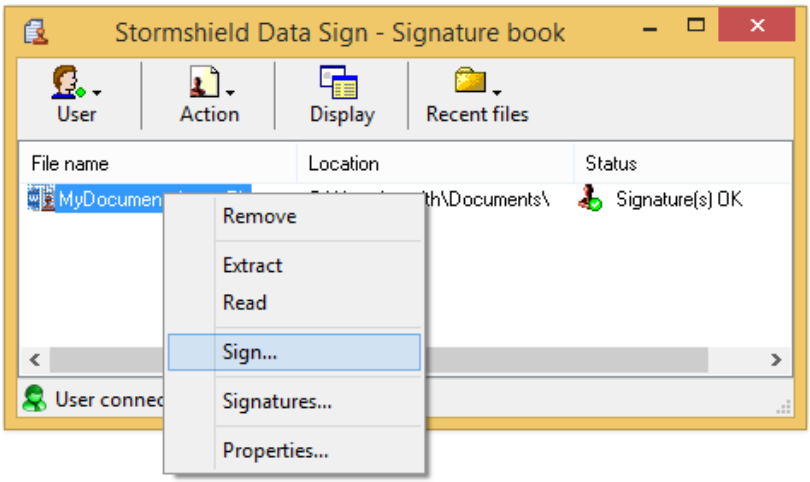
5.5 Signer un fichier déjà signé

Pour signer un fichier déjà signé :

1. Dans l'Explorateur Windows, sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Envoyer vers > Stormshield Data Sign** à partir du menu contextuel : le fichier est alors déposé dans le Parapheur.

- Si le Parapheur est déjà ouvert, y déplacer et déposer le fichier sélectionné.
- Vous pouvez également double-cliquer sur un fichier *.p7f*. Le Parapheur s'ouvre alors automatiquement et le fichier y est déposé.

2. Dans le Parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Signer**.



3. Suivez les instructions de l'assistant, qui vous demande systématiquement votre code confidentiel ou votre mot de passe. La fenêtre **Choix de l'opération** s'affiche :

4. Sélectionnez l'une des options en fonction de ce que vous souhaitez faire :

- **Co-signer** pour ajouter votre propre signature au fichier, indépendamment des autres signatures déjà présentes, qu'elles soient correctes ou non.
- **Contre-signer** pour ajouter signature et contre-signer toutes les autres signatures déjà présentes (y compris les contre-signatures). Cette opération n'est disponible que si toutes les signatures ont déjà été vérifiées et validées.

> **NOTE**
> Vous pouvez contre-signer :
> - toutes les signatures (comme décrit ci-dessous)
> - une seule signature (voir la section Contre-signer une signature précise)

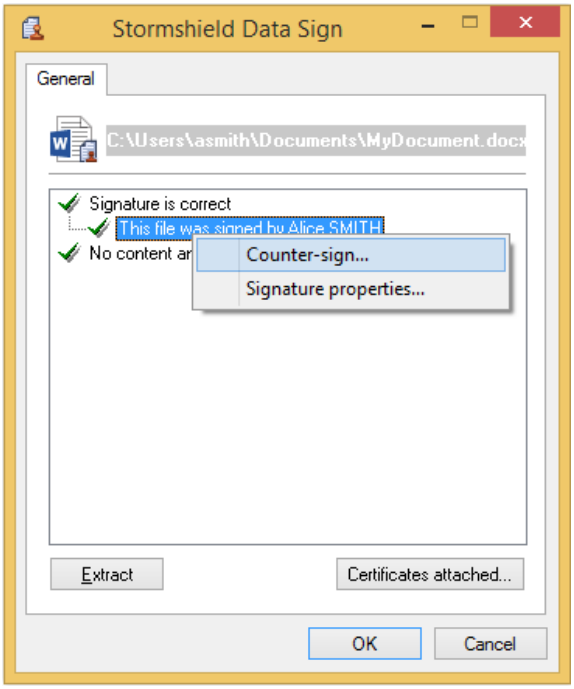
- **Sur-signer**. Lorsque vous sur-signez un document, le fichier signé d'origine n'est pas modifié : l'assistant propose de générer un nouveau fichier portant par défaut le même nom auquel est ajoutée l'extension *.p7f*.

> **NOTE**
> Chaque fois qu'un fichier est sur-signé, l'extension *.p7f* est ajoutée au nouveau fichier généré. Il est donc possible de rencontrer des fichiers avec de multiples extensions *.p7f*.

5.6 Contre-signer une signature précise

Pour contre-signer une signature précise dans un fichier déjà signé :

1. Dans l'Explorateur Windows, sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Envoyer vers > Stormshield Data Sign** à partir du menu contextuel : le fichier est alors déposé dans le Parapheur.
2. Dans le Parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Signatures**. Stormshield Data Sign affiche sous forme arborescente les signatures et contre-signatures éventuelles contenues dans le fichier.
3. Cliquez sur la signature concernée avec le bouton droit de votre souris, choisissez **Contre-signer** et saisissez votre code confidentiel ou mot de passe.



Votre contre-signature est ajoutée au fichier signé d'origine. Cette modification sera effective lors de la fermeture de la fenêtre.

5.7 Notifier par e-mail

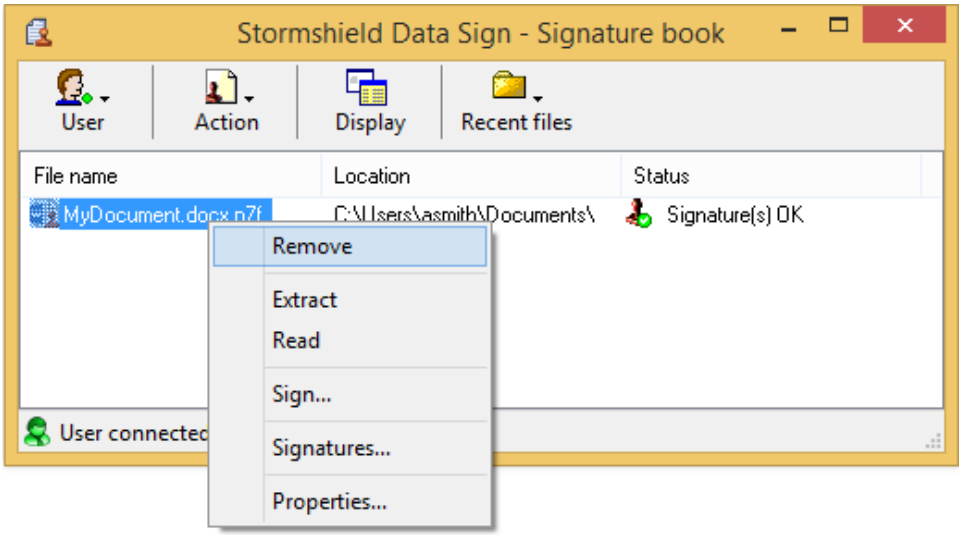
Sur la dernière fenêtre de l'assistant, deux options de notification par e-mail sont proposées :

- **Notifier les collaborateurs par e-mail** : Stormshield Data Security prépare un courrier électronique à destination de collaborateurs afin que ceux-ci soient avertis de la signature du document. Si le document avait été précédemment signé, la liste des destinataires est pré-remplie avec les adresses e-mail des co-signataires ;
- **Demander une signature par e-mail** : Stormshield Data Security prépare un courrier électronique à destination des collaborateurs afin que ceux-ci apposent également leur signature sur le document.

Ces cases peuvent être pré-cochées. Reportez-vous au *Guide d'administration de Stormshield Data Security* pour plus d'informations sur les paramètres `MailToNotifyCoWorkers` et `MailToAskForSignature` dans la section [Sign] du fichier de configuration *Sbox.ini*.

5.8 Enlever un fichier du Parapheur

1. Pour enlever un fichier du Parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Enlever** :



2. Confirmez votre choix.

Le fichier est retiré de la liste du Parapheur mais n'est pas physiquement supprimé.

NOTE
Une façon plus rapide de retirer un fichier de la liste consiste à sélectionner le fichier et appuyer sur la touche **Effacer** du clavier.

documentation@stormshield.eu