GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA MAIL ÉDITION NOTES

Messagerie sécurisée

Version 10.1

Dernière mise à jour du document : 29 mars 2022

Référence : sds-fr-sd_mail_notes-guide_d_utilisation-v10

Table des matières

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

Préface

Stormshield Data Mail Édition Notes faisant partie de Stormshield Data Security, il est possible d'utiliser le même compte utilisateur pour accéder aux différents composants de la suite installés sur votre poste et d'utiliser les clés et certificats antérieurement disponibles.

Pour plus d'informations, reportez-vous au *Guide d'installation et de mise en œuvre*.

Il existe deux versions de Stormshield Data Mail :

- Stormshield Data Mail Édition Notes,
- Stormshield Data Mail Édition Outlook, pour Microsoft Outlook 2019 et 365 Professional.

1. Introduction

Cette section décrit les caractéristiques et fonctionnalités de Stormshield Data Mail Édition Notes.

1.1 Présentation

1.1.1 Généralités

Stormshield Data Mail est un logiciel de sécurité informatique. Il ajoute aux messages que vous échangez tous les jours sur Internet ou sur votre Intranet les services de sécurité suivants :

- **la confidentialité** du message : seul(s) le ou les destinataires pourront lire le message transmis ;
- **l'intégrité** du message, qui ne peut être modifié en cours de transfert sans que cela ne soit détecté ;
- **l'authentification de l'émetteur** : le destinataire du message est certain de l'identité de l'émetteur.

La confidentialité est assurée par le chiffrement (cryptage) du message.

L'intégrité du message et l'authentification de l'émetteur sont garanties par une signature électronique.

Stormshield Data Mail implémente la norme S/MIME V3 : vous pouvez échanger des messages sécurisés avec tout correspondant dès lors qu'il possède un logiciel de messagerie supportant la norme S/MIME V2 ou V3.

NOTE
Si vous essayez de sécuriser un message avec les fonctions de sécurité natives de votre client de messagerie, puis avec Stormshield Data Mail, ce message doublement sécurisé ne pourra être lu par son destinataire.

1.1.2 Intégration au client de messagerie

Stormshield Data Mail ne se substitue pas à votre client de messagerie habituel : il le complète et se charge de la sécurité de vos messages.

Stormshield Data Mail utilise le mode « intégré » pour sécuriser vos messages. C'est une extension qui s'intègre dans votre client de messagerie. Elle sécurise (chiffre et/ou signe) et dé-sécurise (déchiffre) vos messages au fur et à mesure tout en les conservant sous leur forme sécurisée dans votre base de messages.

Stormshield Data Mail est disponible sous forme d'add-in pour les clients de messagerie suivants :

- Microsoft Outlook 2019 et 365
- Lotus Notes 8.x et 9.x

1.1.3 Ce qui est sécurisé

La norme S/Mime V3 permet de sécuriser un message, c'est-à-dire **son texte et ses pièces jointes**.

L'enveloppe du message (en-tête rfc822), qui contient notamment le nom de l'émetteur, la liste des destinataires, la date d'émission et surtout l'objet du message, n'est quant à elle pas sécurisée.

Ainsi, même si un message est sécurisé, son objet peut être lu ou modifié lors de son acheminement sur le réseau. C'est pourquoi la prudence est de mise lorsque vous écrivez ou lisez une information dans l'objet d'un message sécurisé.

1.2 Sécurisation de vos messages

1.2.1 Cryptographie à clé publique

Stormshield Data Mail met en œuvre des moyens de cryptographie dits « à clé publique ».

Chaque correspondant possède un (ou plusieurs) couple(s) de clés : une clé privée et une clé publique. La **clé privée** doit être conservée de façon confidentielle par son propriétaire. En revanche, la **clé publique** est destinée à être distribuée.

Stormshield Data Mail peut mettre en œuvre :

- un couple de clés unique pour le chiffrement et la signature ;
- deux couples de clés différents, l'un pour le chiffrement, l'autre pour la signature.

1.2.2 Chiffrement

Le chiffrement est une technique utilisant des propriétés mathématiques (cryptographie) pour transformer un message intelligible (en clair) en un message (chiffré) que seuls les destinataires désignés peuvent décoder et lire.

L'émetteur chiffre un message avec un processus mettant en œuvre la clé publique du destinataire ; ce dernier utilise un processus mettant en œuvre sa clé privée pour déchiffrer le message. Le destinataire étant le seul à posséder cette clé privée, l'émetteur est assuré que le message ne peut pas être lu par un tiers.

1.2.3 Signature électronique

Une signature électronique est un «sceau» numérique appliqué sur le message : elle garantit l'intégrité du message et l'identité du signataire.

Le signataire signe un message au moyen de sa clé privée ; le destinataire vérifie la signature au moyen de la clé publique du signataire. Le signataire étant le seul à posséder la clé privée ayant signé le message, le destinataire est assuré que le message a bien été émis par le signataire et qu'il n'a pas été falsifié au cours de son transfert.

1.2.4 Certificats

Pour envoyer des messages chiffrés à des correspondants, vous devez connaître la clé publique de chiffrement de vos correspondants.

Les clés publiques sont distribuées sous forme de certificat. Un certificat est un document électronique qui associe une clé publique à son propriétaire. Stormshield Data Security supporte le format de certificat X.509 V3.

NOTE
En cas de renouvellement de la clé de chiffrement ou de certificats, les certificats (ainsi que la

clé associée) utilisés pour le chiffrement antérieur de données doivent être conservés afin de pouvoir déchiffrer ultérieurement ces données.

Pour plus d'informations sur l'export et l'import de certificats, consultez le *Guide d'installation et de mise en œuvre*.

1.2.5 Confiance

Un certificat établit un lien entre une clé publique et une identité. Vous ne pouvez utiliser un certificat que si vous faites confiance à ce lien.

En effet, si par exemple vous voulez envoyer un fichier chiffré à Alice, vous devez être certain que le certificat supposé d'Alice est effectivement bien le sien ; sinon vous prenez le risque que votre fichier soit chiffré non pas avec la véritable clé d'Alice, mais avec la clé d'un imposteur qui pourra déchiffrer votre fichier destiné à Alice.

Deux techniques permettent d'accorder sa confiance à un certificat :

- la confiance par héritage adopte le principe que si vous faites confiance à une autorité dans son rôle de certification, vous faites implicitement confiance aux certificats qu'elle délivre.
- la confiance explicite impose que vous vérifiez vous-même l'origine du certificat. Une technique usuelle consiste à en vérifier l'empreinte à partir d'une source parallèle d'information (téléphone, publication, courrier, site web, etc.).

1.2.6 Annuaires de confiance

La gestion des annuaires de confiance et des certificats est décrite dans le *Guide d'installation et de mise en œuvre*.

Stormshield Data Mail Édition Notes permet de gérer un annuaire de confiance : vous y insérez les certificats des correspondants et des autorités auxquels vous faites confiance.

Si vous souhaitez chiffrer un message pour un ou des destinataires absents de votre annuaire de confiance et que vous avez déclaré un annuaire LDAP, celui-ci est automatiquement interrogé.

Dans ce cas, si le paramètre `SilentImportTrustedLdapCert` du fichier de configuration *SBox.ini* vaut 1, les certificats obtenus à partir de l'annuaire LDAP sont automatiquement importés dans l'annuaire de confiance tant que leur statut n'est pas en erreur (non révoqués, non périmés).

Pour plus d'informations sur ce paramétrage, reportez-vous à la Section [Mail] du *Guide d'administration*.

1.2.7 Contrôle de révocation

Le contrôle de révocation vérifie, avant son utilisation, qu'un certificat est bien valide, c'est-à-dire qu'il n'a pas été révoqué. Les listes de révocation (CRL) sont fournies par les autorités de certification.

Stormshield Data Security assure automatiquement le téléchargement des listes de révocation à partir des points de distribution déclarés dans les certificats ou ceux configurés dans le composant Contrôleur de révocation.

L'utilisateur peut configurer les critères de téléchargement pour chaque autorité de certification. Les listes de révocation reçues sont conservées localement dans une base sécurisée.

Pour plus de détails sur les listes de révocation, reportez-vous au *Guide d'installation et de mise en œuvre*.

1.3 Connexion sécurisée

L'accès à vos clés est protégé : pour pouvoir les utiliser, vous devez vous connecter à Stormshield Data Security, processus qui consiste à vous authentifier et à 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 cryptographique : vous saisissez le code secret de la carte (en anglais, “PIN” Personal Identification Number).

Stormshield Data Security supporte différents types de cartes à puces et de clés USB.

Pour plus d'informations, reportez-vous au *Guide d'installation et de mise en œuvre*.

2. Installation de Stormshield Data Mail Édition Notes

Cette section présente la configuration requise et l'installation de l'application.

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 Stormshield Data Security 10.1.

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

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

2.2 Installation de Stormshield Data Mail Édition Notes

Stormshield Data Mail Édition Notes 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*.

Après l'installation de l'add-in Stormshield Data Mail Édition Notes, la première ouverture de votre client de messagerie peut prendre plusieurs dizaines de secondes.

NOTE
Le cumul d'autres add-ins S/MIME, tels que Microsoft MAPI S/MIME AME processor n'est pas supporté.

2.3 Echange de certificats

Emettre un message chiffré nécessite que l'émetteur connaisse la clé publique du destinataire, laquelle est contenue dans son certificat.

Il existe plusieurs moyens pour s'échanger des certificats :

- mettre en œuvre un annuaire LDAP ;
- s'échanger son certificat par envoi de message ;
- consulter et gérer son annuaire de confiance.

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

3. Mise en route de Stormshield Data Mail Édition Notes

Stormshield Data Security se lance automatiquement au démarrage de votre système.

Pour pouvoir signer et chiffrer des messages, recevoir et vérifier du courrier sécurisé, vous devez avoir installé Stormshield Data Mail Édition Notes et vous connecter à Stormshield Data Security.

Pour vous connecter à Stormshield Data Security, vous devez posséder un « compte ». La procédure de création et de gestion des comptes utilisateurs est décrite dans le manuel détaillant les fonctions communes.

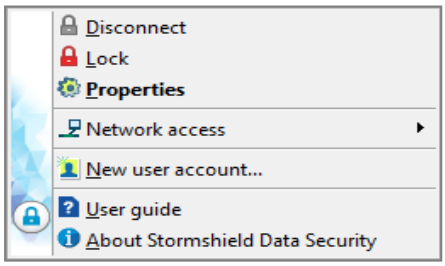
Cette section décrit uniquement les comptes protégés par un mot de passe. Si vous disposez d'un dispositif matériel d'authentification (carte à puce, …), reportez-vous au *Guide d'installation et de mise en œuvre* qui décrit les fonctions communes aux logiciels de la suite Stormshield Data Security.

3.1 Menu Stormshield Data Security

Tout ce qui concerne votre connexion à Stormshield Data Security s'effectue par un clic droit sur l'icône Stormshield Data Security affichée à droite de votre barre de tâches Windows.

Cette icône est grisée tant que vous n'êtes pas connecté, rouge quand votre session est verrouillée et verte lorsque vous êtes connecté.

Un clic droit sur cette icône ouvre un menu, nommé Menu Stormshield Data Security dans la suite de ce guide.

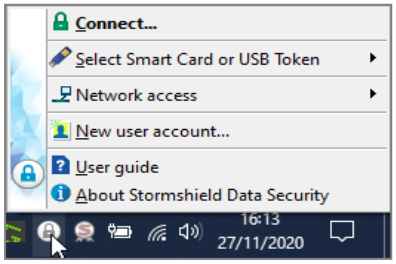


Les rubriques du menu Stormshield Data Security affichées dépendent de la façon dont ont été configurées les actions de connexion/déconnexion, verrouillage/déverrouillage, etc.

3.2 Connexion à Stormshield Data Security

L'opération de connexion permet à Stormshield Data Security de vous authentifier et de retrouver vos paramètres de configuration.

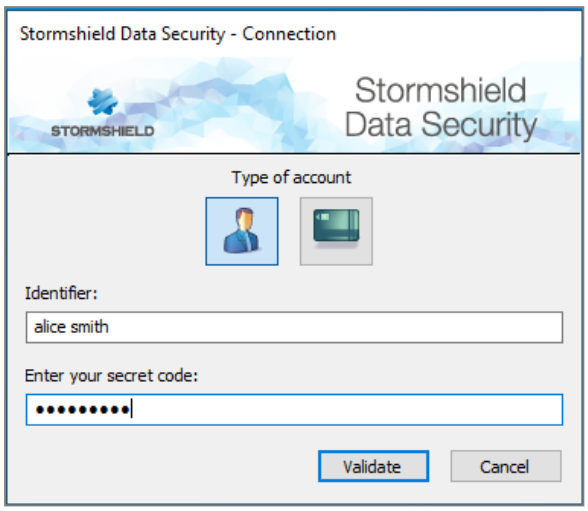
1. Pour vous connecter à Stormshield Data Security, ouvrez le menu Stormshield Data Security (clic droit sur l'icône dans la barre des tâches Windows) et choisissez **Connecter** :



2. 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 :

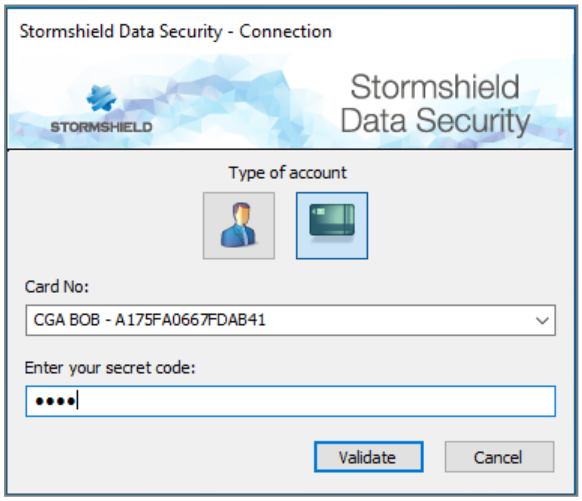


b. Cliquez sur **Valider**.

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** dans le *Guide d'installation*.

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** dans le *Guide d'installation*.

Par défaut, Stormshield Data Security pré-remplit ces champs avec les informations du dernier utilisateur à s'être connecté avec succès sur ce poste.

NOTE
Si vous saisissez un code erroné plusieurs fois de suite (3 par défaut), votre compte se bloque.

L'image à la gauche du champ de l'identifiant utilisateur ne s'affiche qu'une fois que Stormshield Data Security reconnaît le compte.

Une fois votre connexion validée, l'icône Stormshield Data Security devient verte : .

Vous venez d'ouvrir une session Stormshield Data Security. Tant que vous restez connecté, vous pouvez accéder aux composants installés de Stormshield Data Security (tels que Stormshield Data File, Stormshield Data Virtual Disk, Stormshield Data Shredder, Stormshield Data Mail) depuis votre bureau.

3.3 Présélections des options de sécurité

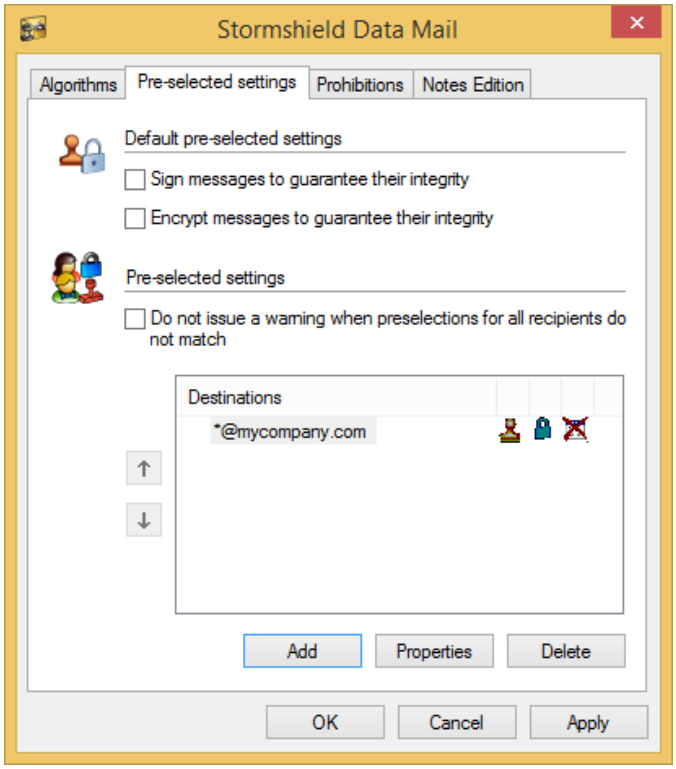
Les options de sécurité sont présélectionnées pour l'ensemble des éditions Stormshield Data Mail Édition Notes utilisées.

Vous pouvez configurer la sécurité

- soit globalement pour tous les messages que vous envoyez ;
- soit selon les destinataires d'un message.

Pour cela :

1. Ouvrez le menu Stormshield Data Security.
2. Choisissez **Propriétés**.
3. Sélectionnez l'onglet *Configuration*.
4. Effectuez un double clic sur l'icône Stormshield Data Mail.
5. Sélectionnez l'onglet *Présélections*.



3.3.1 Présélections selon les destinataires

Vous pouvez configurer Stormshield Data Mail Édition Notes de manière à ce qu'il présélectionne les options de sécurité d'un message en fonction de ses destinataires. Vous pouvez même demander l'application automatique de ces options, sans confirmation de votre part.

Par exemple, vous pouvez :

- signer et chiffrer automatiquement les messages destinés à votre siège social ;
- signer automatiquement les messages destinés à certains de vos fournisseurs ;
- ni chiffrer, ni signer par défaut les messages adressés à vos correspondants privés, en vous laissant la possibilité d'intervenir pour modifier ces deux options.

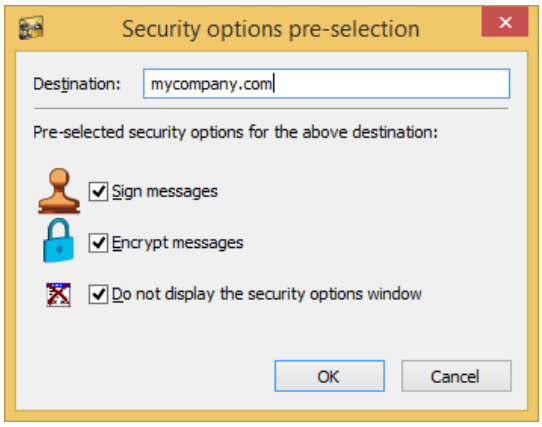
Vous présélectionnez les options de sécurité à l'aide d'un champ **Destination**. Une destination est un filtre d'adresse électronique : une présélection est appliquée à un destinataire si son adresse électronique satisfait au filtre de la destination concernée. Vous pouvez utiliser les caractères '*' qui signifie toute série de caractères et '?' qui signifie tout caractère (un seul).

Par exemple, si les adresses électroniques de votre siège social se terminent toutes par @siege.companie.fr, vous pouvez définir la destination *@siege.companie.fr et lui appliquer les options **Signer** et **Chiffrer**.

Une destination peut ainsi être un nom de domaine au lieu d'une adresse électronique complète.

Pour définir une présélection :

1. Sélectionnez l'onglet *Présélections*.
2. Cliquez sur **Ajouter** dans la liste des présélections ; la fenêtre suivante s'affiche :



3. Renseignez la destination (suffixe d'adresse électronique, adresse complète ou utilisation de * ou ?) dans le champ **Destination**.
4. Sélectionnez les options de sécurité à appliquer à cette destination :
   - **Signer les messages**
   - **Chiffrer les messages**

Vous pouvez sélectionner une des options ou les deux.

5. Cochez la case **Ne pas afficher la fenêtre de choix des options de sécurité** si vous souhaitez que ces options de sécurité soient automatiquement appliquées à un message adressé à cette destination, sans confirmation de votre part.

Décochez cette case si vous souhaitez au contraire pouvoir modifier ces options avant l'envoi du message.

6. Cliquez sur **OK** pour valider.

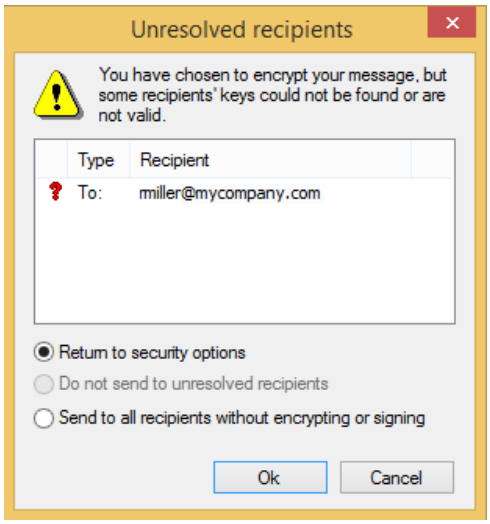
C'est la première destination trouvée dans la liste qui est appliquée à un destinataire. Pour déplacer une destination dans la liste, utilisez les flèches à droite de liste.

3.3.2 Règles de gestion

Une option (signer ou chiffrer) est présélectionnée (cochée) si elle est demandée pour au moins un destinataire.

La fenêtre de saisie des options de sécurité est affichée si elle est demandée pour au moins un destinataire.

Si le traitement aboutit à un échec avec les présélections (notamment si vous avez demandé de chiffrer alors que vous ne détenez par les certificats de certains destinataires). La fenêtre suivante s'affiche :



Choisissez alors entre :

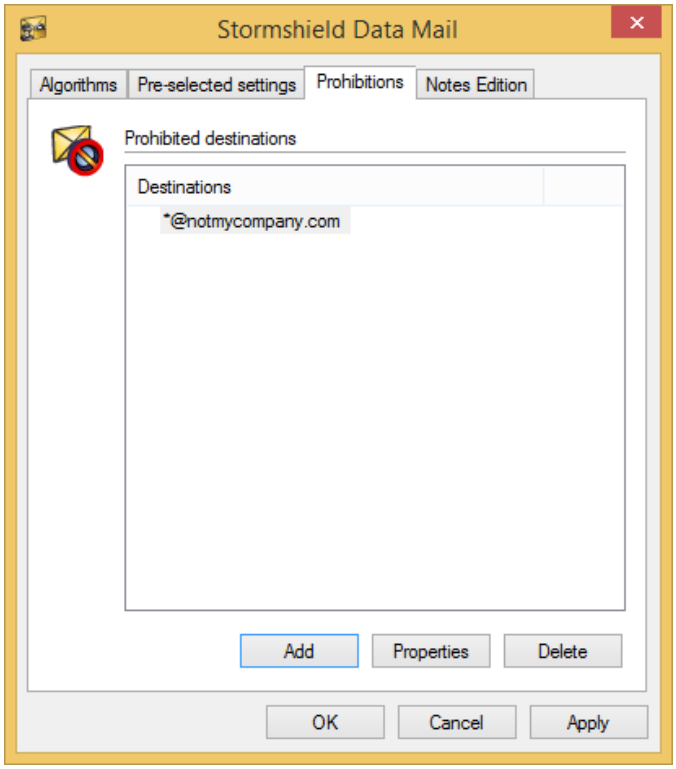
- **Retour au choix des options de sécurité**.
- **Ne pas émettre vers les destinataires non résolus** : vous émettez uniquement vers les destinataires dont le certificat est valide correct.
- **Émettre non chiffré, mais signé, vers tous les destinataires** : vous émettez non chiffré, mais signé, vers TOUS les destinataires.

3.4 Destinations interdites

Vous pouvez vous interdire d'émettre des messages vers certaines destinations ou adresses électroniques (pour la définition stricte d'une destination, reportez-vous à la section Présélections selon les destinataires). Les destinations interdites sont communes à toutes les éditions de Stormshield Data Mail Édition Notes.

Pour interdire une destination :

1. Ouvrez le menu Stormshield Data Security.
2. Choisissez **Propriétés**.
3. Choisissez l'onglet *Configuration*
4. Effectuez un double clic sur l'icône Stormshield Data Mail.
5. Choisissez l'onglet *Interdictions* :

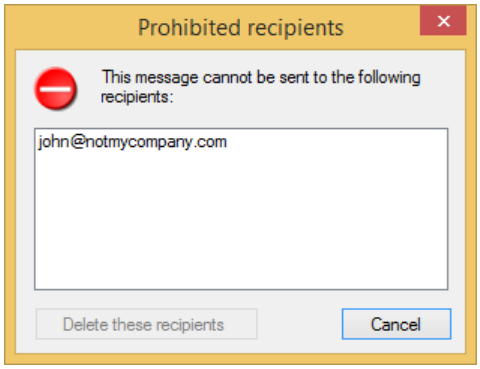


6. Cliquez sur **Ajouter**.
7. Saisissez l'adresse électronique dans le champ **Destination** de la boîte de dialogue suivante :

Vous pouvez utiliser le caractère * pour représenter une série de caractères et ? pour représenter un seul caractère. Comme pour les règles de présélection, vous pouvez spécifier seulement un nom de domaine.

NOTE
Les règles d'interdiction l'emportent sur celles de présélection. Ceci veut dire que si un destinataire est touché à la fois par une règle d'interdiction et une règle de présélection, l'envoi du courrier sera interdit.

Si vous adressez un message à une destination interdite, Stormshield Data Mail Édition Notes affiche la fenêtre d'erreur suivante :



Pour envoyer le message aux destinataires autorisés seulement, cliquez sur **Supprimer ces destinataires**.

3.5 Paramétrage d'affichage de demande de connexion

Il est possible de paramétrer séparément les comportements d'affichage de la demande de connexion lors de l'émission d'un message en clair en mode **Utilisateur déconnecté** et **Utilisateur verrouillé**. Ces paramétrages s'effectuent dans le fichier *SBox.ini* (section `[Mail]`) :

- Mode **Utilisateur déconnecté** : `DisplayComlogWindow`
  - 0 : Affichage de la fenêtre de connexion uniquement si l'utilisateur coche les boutons **Signer** ou **Chiffrer** lors de la composition du message.
  - 1 : Affichage systématique de la fenêtre de connexion à Stormshield Data Security (par défaut).
- Mode **Utilisateur verrouillé** : `DisplayComlogWindowUserLocked`
  - 0 : Affichage de la fenêtre de connexion uniquement si l'utilisateur coche les boutons **Signer** ou **Chiffrer** lors de la composition du message.
  - 1 : Affichage systématique de la fenêtre de connexion à Stormshield Data Security (par défaut).

4. Emettre un message sécurisé

Cette section vous explique comment émettre un message sécurisé.

4.1 Saisie des options de sécurité

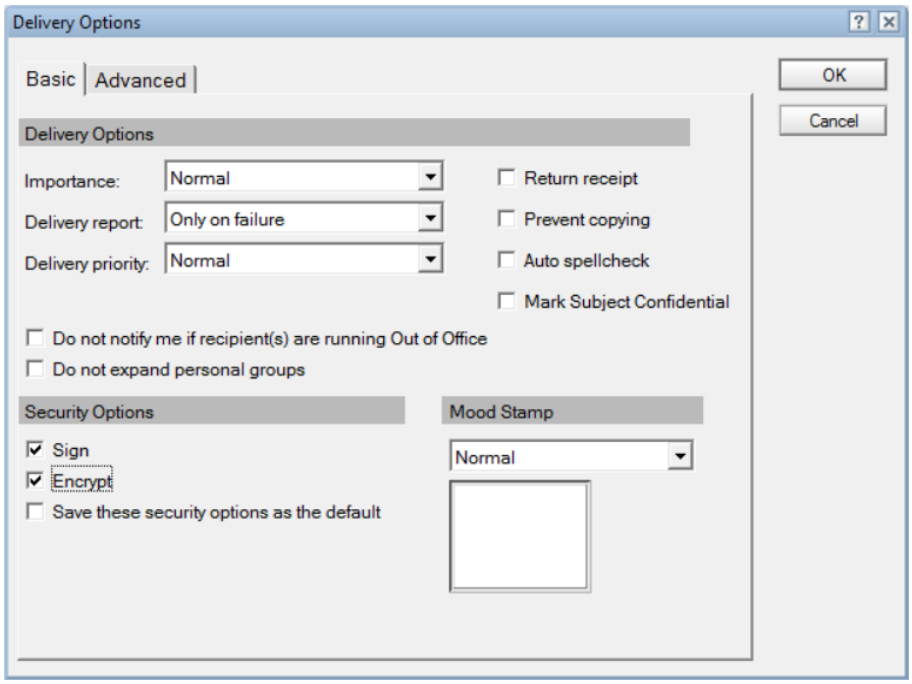
Ce paragraphe suppose que vous êtes déjà connecté à Stormshield Data Security avant d'émettre votre message. Si tel n'est pas le cas, reportez-vous à la Section 4.3, « Vous n'êtes pas connecté à Stormshield Data Security ou votre session est verrouillée » ci-après.

Pour émettre un message :

1. Ouvrez et écrivez le message comme vous le faites d'habitude avec votre mailer.

NOTE
Si vous sauvegardez votre message avant de l'envoyer, c'est-à-dire si vous l'enregistrez comme “brouillon”, votre message n'est pas sécurisé : il ne l'est qu'à l'envoi.

2. Pour renseigner les options de sécurité de votre message, cliquez sur le bouton **Options de distribution** de la barre d'action de Lotus Notes. La fenêtre suivante s'affiche.



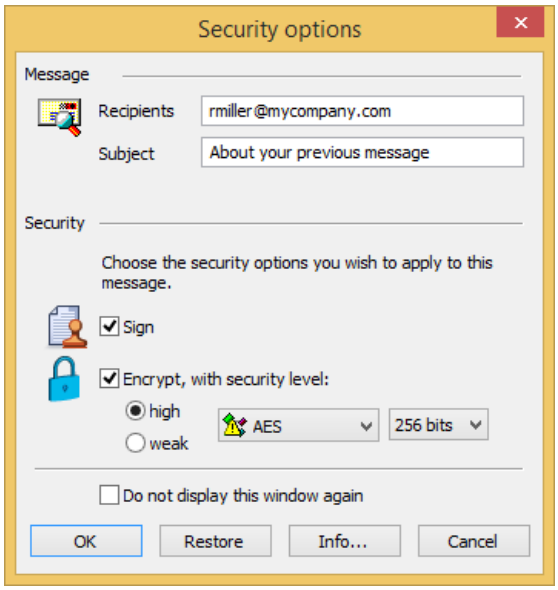
3. Dans l'onglet *Paramètres de base* cochez les options de sécurité que vous souhaitez appliquer à votre message : **Signer** et/ou **Chiffrer**.

Par défaut, Stormshield Data Mail Édition Notes remplace la sécurité native de Notes mais conserve l'interface de Notes pour le pilotage des options de sécurité. Il est possible de paramétrer Stormshield Data Security pour faire cohabiter les deux sécurités (Notes et Stormshield Data Security) ; les informations nécessaires se trouvent dans le *Guide d'administration de Stormshield Data Security*.

En sélectionnant l'une ou l'autre de ces options, la fenêtre **Options de sécurité** de Stormshield Data Security sera pré-remplie en fonction de votre choix (cases **Signer** et **Chiffrer** cochées ou pas).

S'il est précisé par configuration que la fenêtre **Options de sécurité** de Stormshield Data Security ne doit pas s'afficher, c'est la fenêtre précédente **Options de distribution** de Notes qui permet la sélection des options de sécurité à appliquer au message et à ses pièces jointes.

4. Cliquez sur **OK** pour valider les options. Stormshield Data Mail Édition Notes affiche alors la fenêtre suivante :



5. Si vous devez modifier les options de sécurité à appliquer au message :
   - Si vous chiffrez le message, Stormshield Data Mail Édition Notes propose par défaut un algorithme fort. Si certains de vos correspondants ne disposent pas d'un mailer sécurisé par cryptographie forte, sélectionnez l'option faible afin qu'ils puissent le déchiffrer. Votre message est alors plus vulnérable.
   - Pour choisir un autre algorithme proposé par Stormshield Data Mail Édition Notes, utilisez la liste déroulante.
     Pour modifier les paramètres des algorithmes fort et faible, reportez-vous à la section Lire un message sécurisé.
   - Pour ne plus voir s'afficher cette fenêtre, cochez la case **Ne plus afficher cette fenêtre**.
6. Pour confirmer votre sélection et envoyer le message, cliquez sur **OK**.

Le message émis est placé dans le dossier approprié (**Items envoyés** par défaut), sécurisé avec les options sélectionnées. Si vous avez choisi le chiffrement, le message est automatiquement chiffré avec votre clé publique. Il sera déchiffré quand vous l'ouvrirez (reportez-vous à la section Paramètres Édition Notes).

4.2 Certificat non trouvé ou non valide

Si vous chiffrez votre message, Stormshield Data Mail Édition Notes recherche dans votre annuaire de confiance et éventuellement sur votre (vos) annuaire(s) LDAP le certificat de chaque destinataire. Il vérifie aussi que chaque certificat est valide, permet le chiffrement, ne présente aucune extension critique non supportée (s'il en comporte une, la règle oblige à rejeter le certificat).

Si au moins un certificat est absent ou invalide, Stormshield Data Security indique les destinataires incriminés.

1. Sélectionnez l'action à exécuter :

- **Retour au choix des options de sécurité**.
- **Ne pas émettre vers les destinataires non résolus** : le courrier ne sera envoyé qu'aux destinataires dont le certificat est valide.
- **Émettre non chiffré, mais signé, vers tous les destinataires** : le courrier sera envoyé en clair à tous les destinataires.

2. Cliquez au choix

- sur **OK** : l'action est exécutée ;
- sur **Annuler** : le message est annulé.

Le message sera placé dans le dossier approprié (**Éléments envoyés**, par défaut) bien qu'il n'ait pas été envoyé.

4.3 Vous n'êtes pas connecté à Stormshield Data Security ou votre session est verrouillée

Si vous émettez un message alors que vous n'êtes pas connecté à Stormshield Data Security ou que votre session est verrouillée, alors la fenêtre suivante s'affiche :

Si vous cliquez sur **Connecter** (respectivement **Déverrouiller**), Stormshield Data Mail Édition Notes affiche (respectivement déverrouille) la fenêtre de connexion, puis vous demande les options de sécurité à appliquer au message.

Si vous cliquez sur **Annuler**, l'émission est annulée. Pour le réémettre ultérieurement, vous devrez retourner dans votre client de messagerie et redemander l'envoi.

Si vous cliquez sur **Emettre en clair**, le message indiqué est émis sans sécurité.

5. Lire un message sécurisé

L'information suivante sur la lecture d'un message sécurisé s'applique quand vous essayez d'ouvrir un message sécurisé, mais aussi quand vous sélectionnez un message et que le volet de lecture est activé (en fait, que le message est ouvert).

5.1 Ouverture d'un message sécurisé

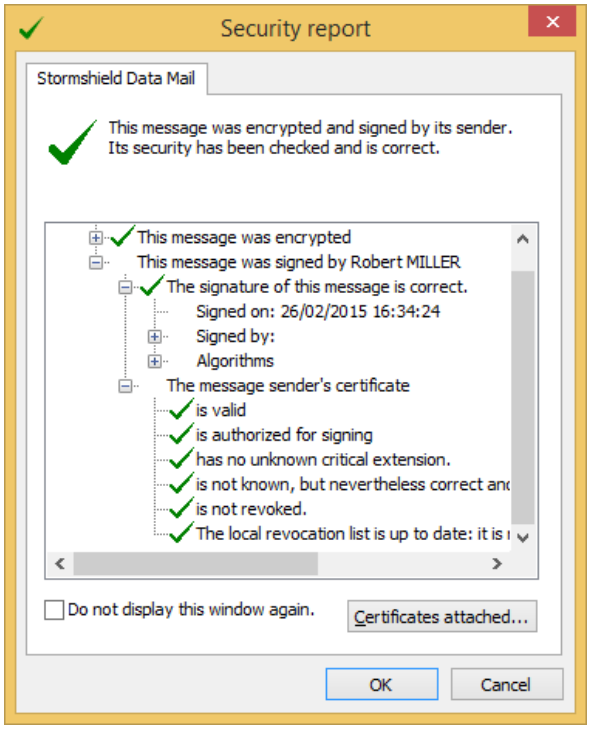
Vous recevez et lisez vos messages comme vous avez l'habitude de le faire avec votre mailer : Stormshield Data Mail Édition Notes se charge de "dé-sécuriser" au moment où vous l'ouvrez tout message sécurisé par son émetteur.

Si vous n'êtes pas connecté à Stormshield Data Security ou si votre session Stormshield Data Security est verrouillée, une boîte de dialogue s'affiche:

Si vous cliquez sur **Connecter** (ou **Déverrouiller**), Stormshield Data Mail Édition Notes affiche la fenêtre de connexion, puis entame la dé-sécurisation du message.

Stormshield Data Mail Édition Notes affiche ensuite le “compte-rendu de sécurité” du message.

Cliquez sur un ⊞ pour déplier une branche de l'arbre :



Ce compte-rendu comprend le détail des algorithmes mis en œuvre pour le chiffrement et la signature.

En cas de signature, il comprend en outre :

- l'identité de l'émetteur qui a signé le message ;
- le résultat de la vérification cryptographique de la signature (vérifiée avec la clé publique contenue dans le certificat de l'émetteur) : signature correcte ou incorrecte ;
- le résultat des contrôles effectués sur le certificat de l'émetteur ; Stormshield Data Mail Édition Notes vérifie que le certificat est valide, est autorisé à signer, ne présente aucune extension critique non supportée (s'il en comporte une, la règle oblige à rejeter le certificat)

;

- un indicateur de confiance à accorder au certificat de l'émetteur.

Par défaut, Stormshield Data Mail Édition Notes affiche le compte-rendu de sécurité à l'ouverture d'un message sécurisé. Si vous souhaitez que ce compte-rendu ne s'affiche plus à l'ouverture d'un message, cochez la case **Ne plus afficher cette fenêtre**. Cependant la fenêtre ne s'affichera effectivement plus que si tous les contrôles sont corrects ; si un seul contrôle n'est pas correct, alors cette fenêtre s'affichera à l'ouverture du message pour vous avertir du problème détecté.

5.2 Suppression de la sécurité d'un message

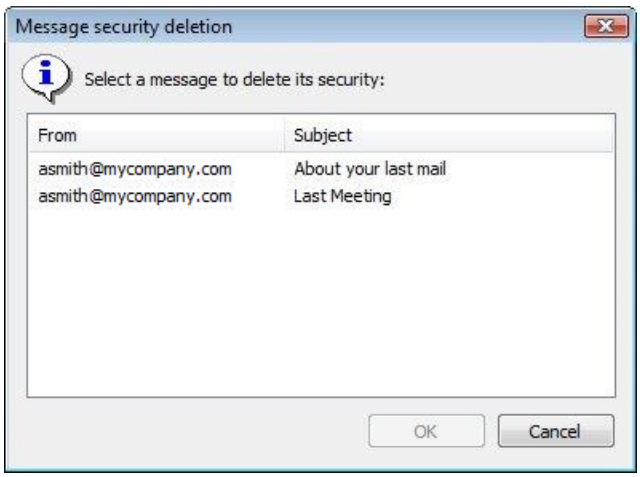
Par défaut, les messages sécurisés reçus sont conservés sécurisés dans la base de messages du client de messagerie.

Il peut arriver que vous ne souhaitiez pas conserver sécurisé un message reçu sécurisé, par exemple si vous voulez le déposer dans un dossier public.

5.2.1 Suppression manuelle de la sécurité d'un message

Pour supprimer la sécurité d'un message donné, choisissez le menu **Action > Supprimer la sécurité**.

Si plusieurs messages sécurisés sont ouverts en même temps, sélectionnez celui dont vous souhaitez supprimer la sécurité :



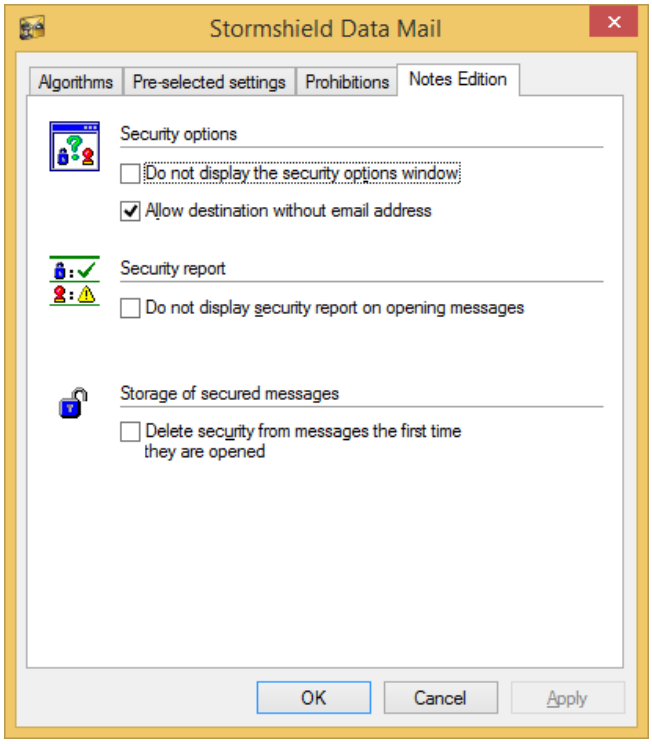
IMPORTANT
Si vous confirmez la suppression de sa sécurité, le message sera désormais conservé "en clair" dans la base de messages de Notes, sans aucune sécurité.

5.2.2 Suppression automatique de la sécurité d'un message

Stormshield Data Mail Édition Notes peut automatiquement supprimer la sécurité des messages que vous recevez. La sécurité d'un message sera réellement supprimée au moment où vous ouvrirez le message.

Pour cela :

1. Ouvrez le menu Stormshield Data Security.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Effectuez un double clic sur l'icône Stormshield Data Mail.
5. Cliquez sur l'onglet *Edition Notes* :



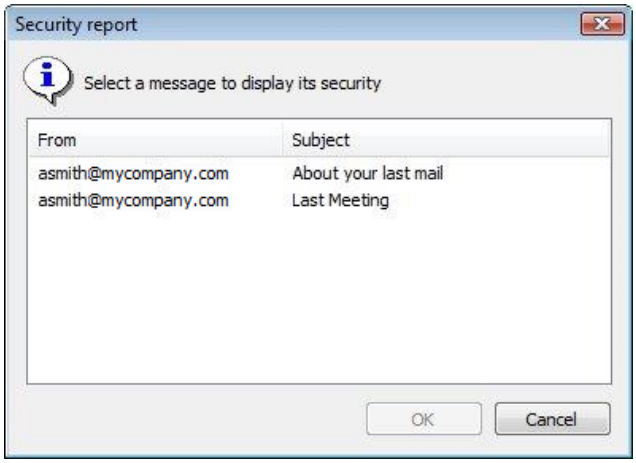
6. Cochez la case **Supprimer la sécurité d'un message à sa première ouverture**.

IMPORTANT
Les informations concernant la sécurité du message reçu (algorithmes, compte-rendu de vérification de la signature, ...) ne seront disponibles qu'au moment de la première ouverture du message. Elles seront perdues ensuite.

5.3 Consultation du compte-rendu de sécurité

Une fois que votre message est ouvert, vous pouvez re-consulter le compte-rendu de sécurité de votre message en sélectionnant le menu **Action > Afficher le compte-rendu de sécurité**.

Si plusieurs messages sécurisés sont ouverts en même temps, sélectionnez celui dont vous souhaitez afficher le compte-rendu :


Security report
Select a message to display its security
From
Subject
asmith@mycompany.com
About your last mail
asmith@mycompany.com
Last Meeting
OK
Cancel

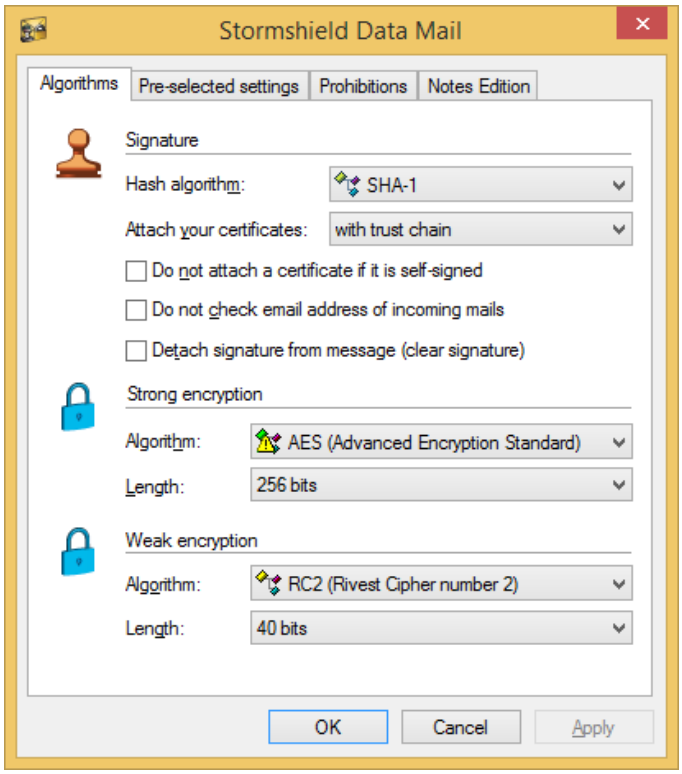
6. Fonctions avancées

Cette section traite des fonctions avancées de Stormshield Data Mail Édition Notes et s'adresse aux utilisateurs avertis.

6.1 Gestion de vos algorithmes

Pour modifier vos algorithmes Stormshield Data Mail Édition Notes :

1. Ouvrez le menu Stormshield Data Security.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Effectuez un double clic sur l'icône Stormshield Data Mail.
5. Cliquez sur l'onglet *Algorithmes* :



6.1.1 Signature

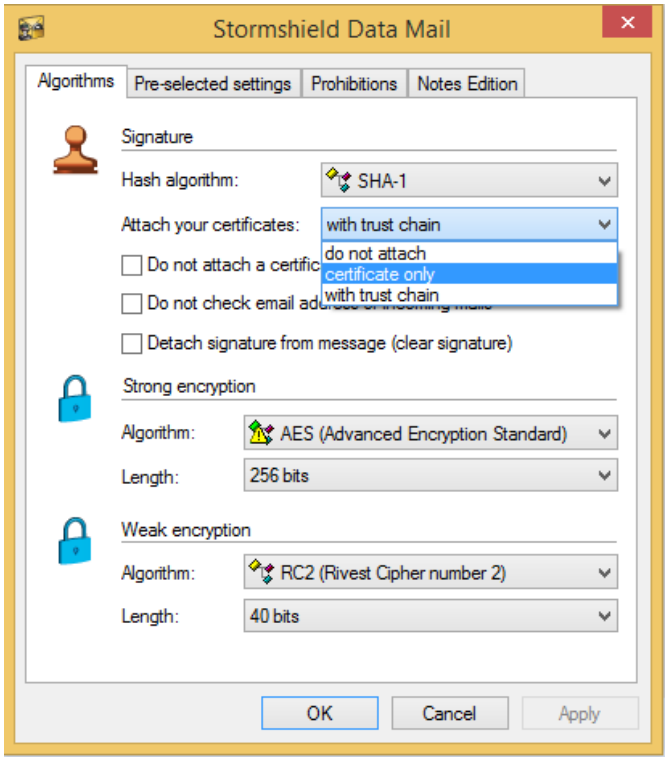
Les paragraphes suivants décrivent les options de l'onglet *Algorithmes*.

Algorithme d'empreinte

Cette liste déroulante permet de choisir l'algorithme d'empreinte à utiliser lors de la signature d'un message. Stormshield Data Security propose SHA-1 (conseillé) et MD5.

Joindre vos certificats

Cette liste permet de choisir la manière de communiquer vos certificats à vos correspondants :



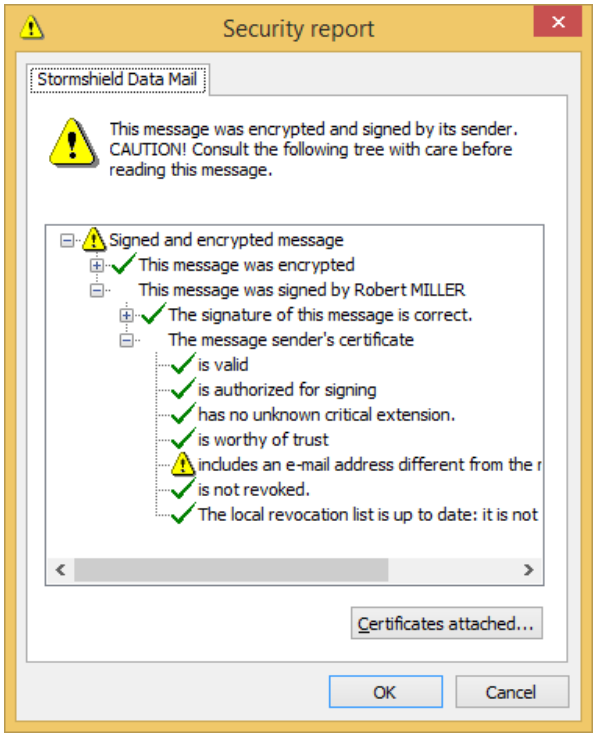
- **Ne pas joindre**. Vous devrez alors les lui communiquer autrement que par un message signé.
- Joindre le **certificat seul**. Le certificat est envoyé sans parenté. Le destinataire doit avoir les certificats de la chaîne dans son annuaire de confiance pour valider la parenté. Le destinataire n'a pas la possibilité d'importer les certificats pour avoir la parenté complète (avec le certificat parent comme source de confiance) quand les messages suivants sont envoyés.
- Joindre **avec sa parenté** (conseillé). Le certificat est envoyé avec toute sa parenté. Le destinataire doit avoir le certificat parent dans son annuaire de confiance pour valider le certificat.

Ne pas joindre un certificat s'il est auto-signé

Cochez cette case si vous êtes en attente de certificats de votre autorité. Ceci évite la propagation de certificats inutiles, par exemple si le destinataire importe le certificat sans prendre en compte qu'il est temporaire.

Ne pas vérifier l'adresse e-mail des courriers entrant

Cochez cette case pour supprimer le message d'erreur "**Le certificat comporte une adresse e-mail différente de l'adresse de l'émetteur du message**".



NOTE
Sélectionner cette possibilité est risqué car les utilisateurs font généralement confiance aux informations de leur client de messagerie. Dans ce cas ils supposeront que l'expéditeur est celui indiqué, ce qui pourrait créer des problèmes de sécurité.

Détacher la signature du message (signature en clair)

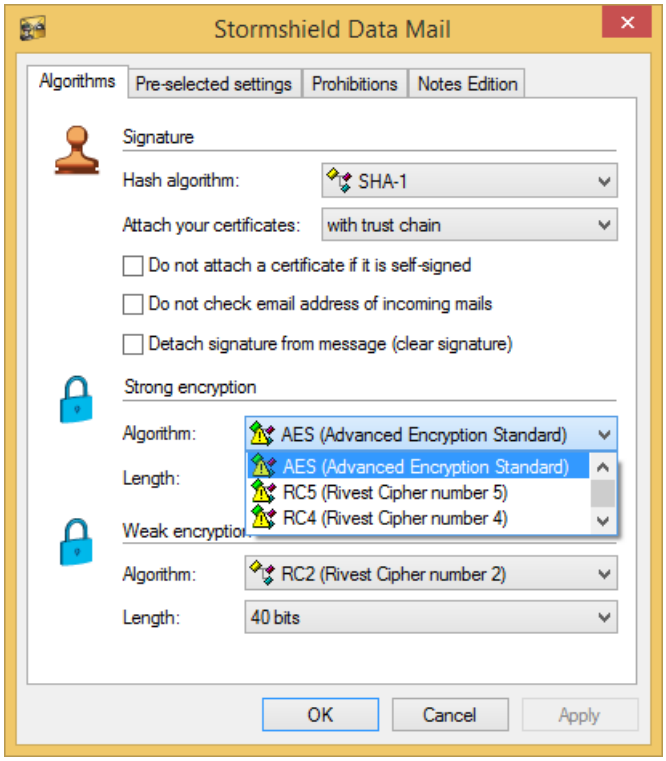
Cochez cette case si vous souhaitez signer en clair.

Autoriser une signature en clair assure que les destinataires peuvent lire le message même si leur client de messagerie ne prend pas en compte le format S/MIME ou refuse d'afficher les messages avec des signatures qui ne peuvent être validées (par exemple si les certificats et les CRL ne sont pas disponibles).

Cependant, une signature en texte clair est plus exposée à des modifications pendant l'émission du message. Normalement, les serveurs ne modifient pas les messages, mais il est possible que des balises soient ajoutées, des lignes blanches ajoutées ou enlevées, etc.

6.1.2 Chiffrement fort et chiffrement faible

Dans les rubriques **Chiffrement fort** et **Chiffrement faible**, présélectionnez les algorithmes de chiffrement et leur longueur de clé proposée par Stormshield Data Mail Édition Notes lors de la saisie des options de sécurité.



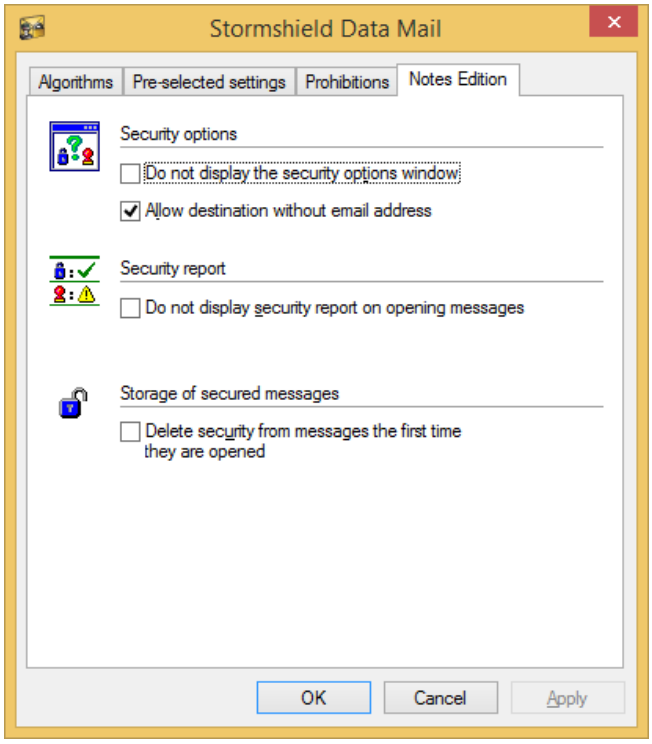
Par défaut, c'est l'algorithme de chiffrement fort (et sa longueur de clé) qui est proposé pour le chiffrement des messages.

NOTE
Quand les règles de sécurité conduisent au chiffrement automatique d'un message, le chiffrement utilise l'algorithme fort sélectionné ci-avant.

En général, le chiffrement fort est AES-256 et le faible est Triple DES-128. Le chiffrement fort peut être utilisé avec Stormshield Data Mail Édition Notes et les systèmes de messagerie les plus récents, alors que le chiffrement faible est utilisé avec les systèmes plus anciens.

6.2 Paramètres Édition Notes

1. Ouvrez le menu Stormshield Data Security.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Effectuez un double clic sur l'icône Stormshield Data Mail.
5. Cliquez sur l'onglet *Édition Notes* :



6.2.1 Saisie des options de sécurité

Ne pas afficher la fenêtre de choix des options de sécurité

Si vous cochez cette case, les options de sécurité que vous avez choisies en cours d'édition de votre message (et éventuellement renforcées en fonction des destinataires) seront appliquées sans confirmation de votre part.

Si vous décochez cette case, vous devrez confirmer ces options pour que ce message soit émis, à moins que tous les destinataires soient concernés par des présélections qui empêchent l'affichage de cette fenêtre.

Autoriser un destinataire sans adresse e-mail

Cette option vous permet d'envoyer des messages à des destinataires qui n'ont pas d'adresse électronique standard telle que nom@domain.com.

Utilisez cette option si vous avez défini des correspondants sans adresse Internet (mais avec adresse Notes). Cependant, ceci est plus rare.

6.2.2 Compte-rendu de sécurité

Ne pas afficher la fenêtre de compte-rendu de sécurité à l'ouverture d'un message

Si vous décochez cette case, la fenêtre de compte-rendu de sécurité sera systématiquement affichée à l'ouverture d'un message sécurisé.

Si vous cochez cette case, la fenêtre de compte-rendu de sécurité sera affichée à l'ouverture d'un message si au moins un contrôle n'est pas correct.

6.2.3 Stockage des messages sécurisés

Supprimer la sécurité d'un message à sa première ouverture

Si vous décochez cette case, vos messages seront conservés sécurisés dans vos dossiers Notes.

Si vous cochez cette case, la sécurité d'un message sera supprimée au moment où vous ouvrirez la première fois le message. Dans ce cas, les informations concernant la sécurité du message (algorithmes, compte-rendu de vérification de la signature, ...) ne seront disponibles qu'au moment de la première ouverture du message. Elles seront perdues ensuite.

6.3 Délégation de déchiffrement

La délégation de déchiffrement consiste à permettre à une autre personne (par exemple votre secrétaire) de déchiffrer vos messages en votre absence. Il faut pour cela lui confier votre clé personnelle (si vous ne possédez qu'une seule bi-clé de signature et de chiffrement) ou votre bi-clé de chiffrement (si vous possédez deux bi-clés différentes pour les fonctions de signature et de chiffrement).

Il faut bien noter qu'avec la clé que vous allez lui confier, la personne ne pourra que déchiffrer vos messages : elle ne pourra pas signer en votre nom.

La technique consiste à effectuer un export de la clé utilisée pour le chiffrement, à partir de votre compte de sécurité, pour permettre un import sur la machine et dans le compte de sécurité de la personne à qui vous la confiez.

Pour exporter votre clé de sécurité ou l'importer dans un compte comme clé de déchiffrement, reportez-vous au *Guide d'installation et de mise en œuvre*.

documentation@stormshield.eu