GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA AUTHORITY MANAGER

Version 10.1

Dernière mise à jour du document : 29 mars 2022

Référence : sds-fr-sd_authority_manager-guide_d_utilisation-v10

Table des matières

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

Préface

A propos de Stormshield Data Security Enterprise

Stormshield Data Security Enterprise est une suite logicielle qui comprend :

- Stormshield Data Security ;
- Stormshield Data Authority Manager.

NOTE
Il faut installer Stormshield Data Security pour utiliser Stormshield Data Authority Manager.

Applicabilité

La documentation décrit les fonctionnalités de Stormshield Data Authority Manager.

Stormshield Data Authority Manager :

- est client/serveur ;
- s'installe sur des systèmes d'exploitation serveur ;
- gère des utilisateurs avec des droits pour chacun d'eux ;
- permet l'utilisation de HSM (Hardware Security Module) ;
- permet d'utiliser des SGBD lourds (SQL Server).

Audience

Ce guide s'adresse à l'administrateur de la sécurité qui définit la politique de sécurité et qui éventuellement crée les comptes des utilisateurs.

Ce guide doit être utilisé avec le *Guide d'administration de Stormshield Data Security*.

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 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.

1.3 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.

1.4 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 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.

1.7 Recommandations sur le chiffrement des fichiers

1. L'algorithme de chiffrement des fichiers doit être l'AES.
2. Il est recommandé de transchiffrer les fichiers lors de la suppression de collaborateurs (module Stormshield Data Team).

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. Introduction

Cette section présente l'outil Stormshield Data Authority Manager en relation avec les composants de Stormshield Data Security, et décrit son architecture logicielle.

2.1 Présentation

La suite logicielle Stormshield Data Security est un produit de sécurité pour poste de travail sous Windows. Elle assure :

- le chiffrement de fichiers ;
- l'effacement irréversible ;
- la signature électronique ;
- la confidentialité et l'intégrité des échanges par messagerie ou sur réseau.

Stormshield Data Authority Manager est un outil d'administration dont le but principal est de créer et d'administrer les comptes des utilisateurs de Stormshield Data Security. Il assure à ce titre :

- le tirage des clés et la création des comptes ;
- la définition et la diffusion des politiques de sécurité ;
- la certification de clés.

Il peut ainsi certifier la clé d'un utilisateur de Stormshield Data Security ou toute autre clé, par exemple la clé d'un serveur SSL ou d'une autre autorité de certification.

Cette gestion de certificats inclut les fonctions classiques d'une infrastructure à clé publique (PKI) :

- dépôt d'une demande de certificat ;
- validation / rejet d'une demande ;
- publication sur un serveur LDAP des certificats délivrés ;
- révocation de certificat et publication de CRL.

2.2 Architecture

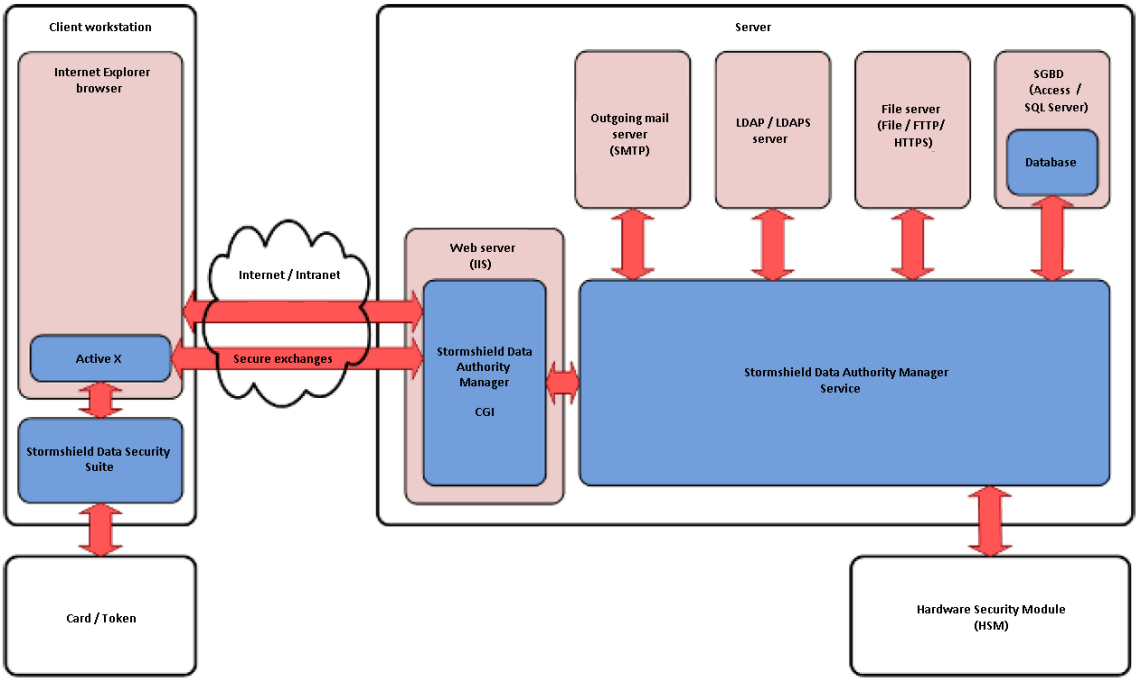
Stormshield Data Authority Manager s'installe sur une plateforme Windows Server et se pilote via un serveur HTTP (IIS). Plusieurs administrateurs peuvent avoir des droits différents. Le produit Stormshield Data Security 10.1 doit être installé sur le poste de chaque administrateur afin d'assurer son authentification forte. Cette authentification peut éventuellement mettre en œuvre une carte à puce ou un token USB.

La clé de l'autorité de certification est tirée et stockée par :

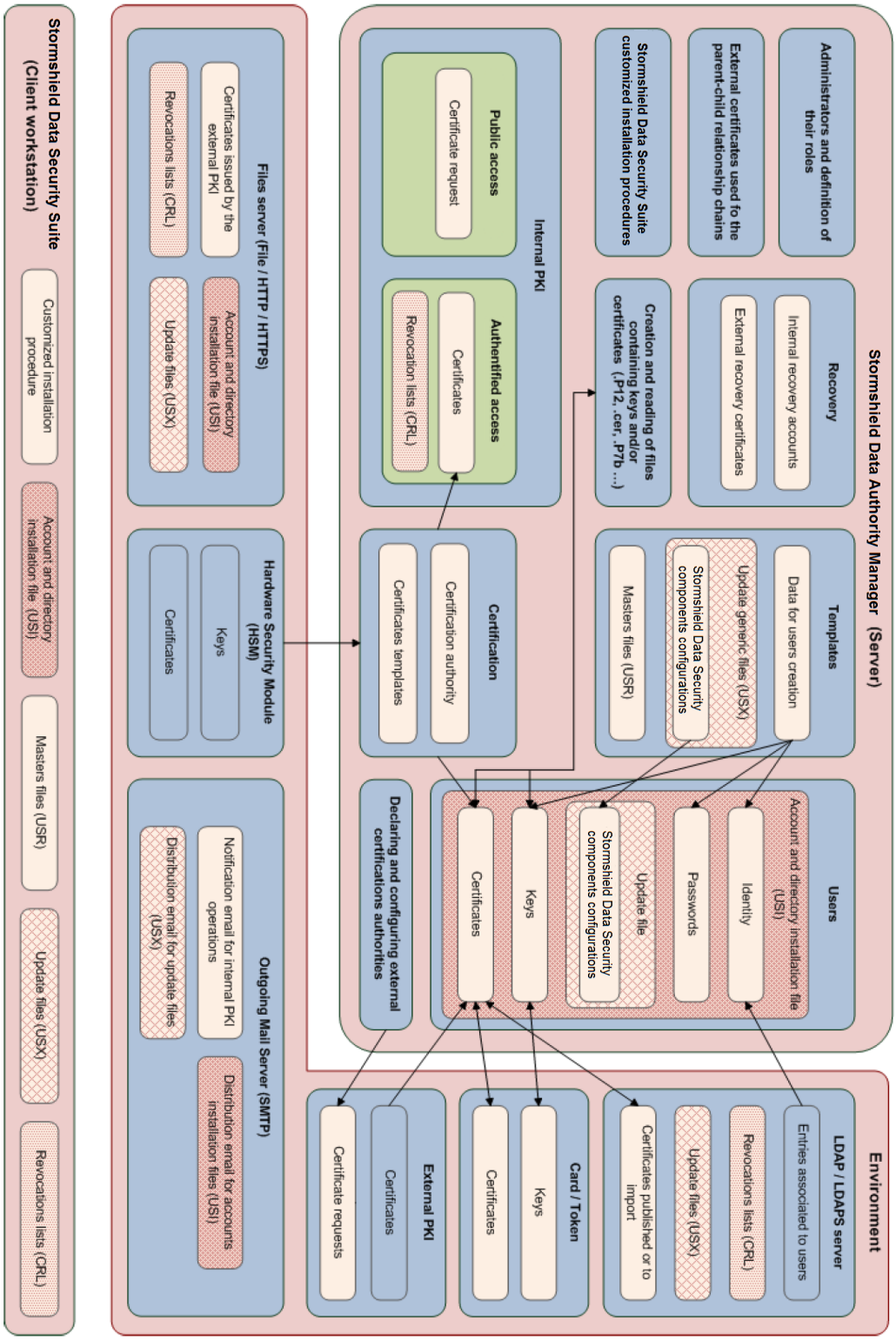
- soit le module cryptographique logiciel Stormshield Data Crypto ;
- soit un module cryptographique matériel (Hardware Security Module).

Les comptes des utilisateurs sont stockés dans une base de données et les certificats générés sont publiés sur un serveur LDAP. Des notifications sont transmises à l'utilisateur final par messagerie.

NOTE
Les logiciels serveur annexes (HTTP, LDAP, SMTP) ne sont pas fournis avec Stormshield Data Authority Manager.



Stormshield Data Authority Manager – Objects managed by the product and exchanged with its environment



3. Démarche d'administration

Cette section contient des informations conceptuelles sur ce que peut être une politique de sécurité et comment la mettre en œuvre grâce à Stormshield Data Authority Manager, en suivant la procédure générale donnée sous forme d'organigramme.

3.1 Définition d'une politique de sécurité

Mettre en place des systèmes de sécurité logique en entreprise nécessite une démarche construite à partir d'une politique de sécurité. Avant de procéder à une mise en place ou à un déploiement, le responsable de sécurité doit :

- inventorier les risques pour l'entreprise, leur impact par rapport à l'organisation ;
- définir une classification des informations et des traitements ;
- préciser les rôles et les droits des utilisateurs ou groupes d'utilisateurs vis à vis des accès aux informations et aux applications.

Avant d'aborder les aspects techniques, il est donc nécessaire de disposer d'une vue globale qui permette la recherche de moyens pour satisfaire de façon cohérente les exigences de sécurité.

La démarche qui consiste à déployer des produits Stormshield Data Security découle d'un choix de moyens. La mise en place de ces produits à clés publiques nécessite :

- une réflexion sur l'usage des certificats numériques, leur autorité, leur durée de vie et leur diffusion ;
- leur mise à disposition pour les utilisateurs et les composants ;
- la protection des clés et leur diffusion dans des équipements matériels (cartes ou tokens).

La politique de sécurité doit donc fixer les règles de production et de gestion des certificats numériques (PKI), mais aussi les règles d'application et de mise en œuvre de cette politique de sécurité sur les postes de travail.

Stormshield Data Authority Manager est un outil d'administration de Stormshield Data Security qui facilite son déploiement en entreprise, permet l'application de la politique de sécurité de l'entreprise et la mise en place d'une infrastructure basée sur la confiance.

3.2 Justification d'une autorité de certification

L'autorité de certification a pour but de contrôler les demandes de certification et de produire les certificats, nécessaires au fonctionnement des produits de sécurité, conformément à la politique de sécurité définie pour l'entreprise.

Le déploiement en entreprise peut selon les besoins être satisfait par :

- l'usage de certificats auto-certifiés pour chaque utilisateur, ceux-ci étant créés et diffusés par les propriétaires ou centralisés et mis à disposition dans un annuaire ;
- la création d'une autorité interne à l'entreprise avec ou sans sous-autorités ;
- l'utilisation d'une autorité externe qui produit et diffuse les certificats et / ou les cartes à puce.

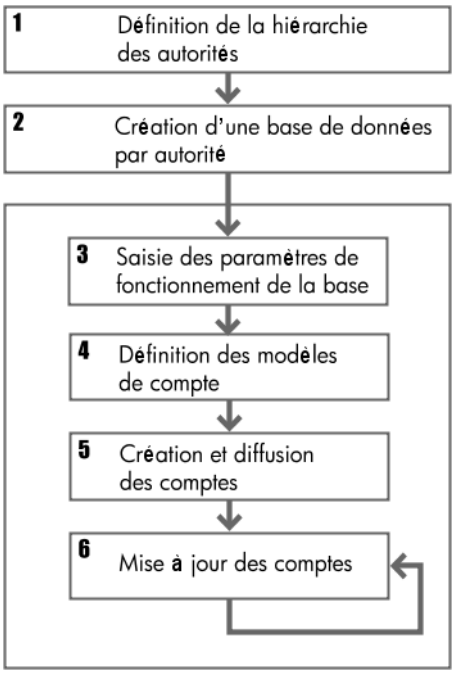
Pour créer une autorité interne à l'entreprise, et donc produire et gérer des certificats, il est possible d'utiliser :

- soit un logiciel de PKI du marché
- soit Stormshield Data Authority Manager, qui offre les fonctions nécessaires au déploiement de Stormshield Data Security.

3.3 Phases d'un déploiement

Avant de se lancer dans la création de comptes utilisateurs, l'administrateur de la sécurité doit établir sa démarche de déploiement. Outre le déploiement du logiciel proprement dit et de ses futures mises à jour, cette démarche consiste à définir les autorités, classer les utilisateurs par modèle, et définir les paramètres de chaque modèle.

L'administrateur qui souhaite déployer des composants Stormshield Data Security doit effectuer dans l'ordre les tâches illustrées par le diagramme ci-dessous.



4. Installation et mise en route

Cette section décrit comment installer Stormshield Data Authority Manager (configuration requise, installation et configuration du serveur, et configuration d'un éventuel HSM [Hardware Security Module]).

Une méthodologie d'installation et de déploiement de Stormshield Data Authority Manager est fournie en annexe (voir Annexe A, Méthodologie de déploiement).

4.1 Configuration requise

4.1.1 Serveur

Pour connaître la configuration requise, reportez-vous à la section **Compatibilité** de la note de version de Stormshield Data Security 10.1.

4.1.2 Client

Stormshield Data Authority Manager nécessite sur le poste client :

- Microsoft Internet Explorer 32 bits version 11 (en utilisant l'affichage de compatibilité) pour les pages en accès authentifié.
- Google Chrome 41 ou inférieur ou bien Mozilla Firefox 36 ou inférieur ou Internet Explorer 11 ou inférieur pour les pages en accès public.

> **NOTE**
> Pour utiliser l'affichage de compatibilité sur Internet Explorer 11, sélectionnez **Outils** puis **Paramètres d'affichage de compatibilité**. Ajoutez le site web correspondant à Stormshield Data Authority Manager à la liste d'Affichage de compatibilité.

- Stormshield Data Security 10.1 pour le profil administrateur (en accès authentifié) ; Security BOX Suite 8.0.x, 9.0.x, Stormshield Data Security 9.3.x ou 10.0 pour le profil utilisateur (en accès public).
- Un utilisateur de type Utilisateur avec pouvoir ou Administrateur, pour l'installation des contrôles ActiveX. Une fois que les contrôles ActiveX sont installés, un utilisateur standard peut se connecter.

4.2 Installation et paramétrage du serveur Web IIS

Pour installer le serveur Web IIS :

1. Ouvrez le **Gestionnaire de serveur**.
2. Ouvrez le menu **Gérer** puis cliquez sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'assistant **Ajout de rôles**, passez la première page et laissez cochée l'option **Installation basée sur un rôle ou une fonctionnalité**. Passez à la fenêtre suivante.
4. Sélectionnez le serveur sur lequel installer le rôle.
5. Cochez **Serveur WEB (IIS)** puis cochez **Outils de gestion** si besoin et cliquez sur **Ajouter les fonctionnalités**, puis **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

7. Sur la page **Services de rôle**, sélectionnez les branches suivantes :
   - **Développement d'application** puis cochez respectivement : **Extensions ISAPI, ASP** et **CGI**.
   - **Fonctionnalités HTTP communes** puis cochez **Contenu statique**.
   - **Sécurité** puis cochez **Filtrage des demandes**.
8. Cliquez sur **Suivant** puis **Installer**.
9. Fermez l'assistant puis le **Gestionnaire de serveur** une fois l'installation terminée.

4.3 Installation de Stormshield Data Authority Manager

L'installation se fait de manière standard avec le fichier *.msi* de *Stormshield Data Authority Manager* en entrant dans une invite de commande en mode administrateur la ligne de commande suivante : `msiexec /i <chemin complet du fichier msi>`.

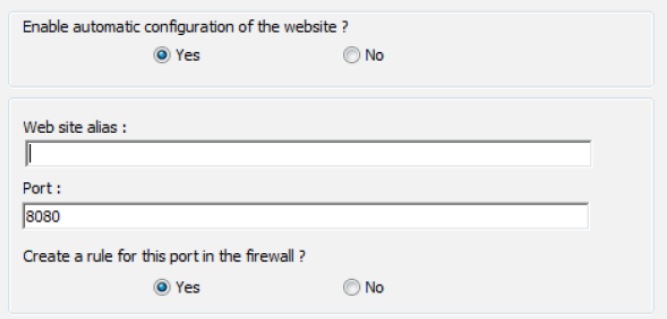
Le programme d'installation demande :

- la clé de licence, fournie avec le produit. Pour obtenir une licence de test, veuillez contacter le service commercial de Stormshield (sales@stormshield.eu).
- le dossier d'installation.
- le dossier où seront stockées les bases de données.

A l'issue de l'installation le service sbasrv est créé et démarré.

La configuration peut se faire automatiquement lors de l'installation :

1. Sélectionnez **Oui** pour le champ **Activer la configuration automatique du site Web ?**.



2. Renseignez l'alias du site Web ainsi que le port (ou laissez les valeurs pré-remplies).
3. Sélectionnez **Oui** pour le champ **Créer une règle pour ce port dans le firewall ?**.

La configuration automatique du serveur Web IIS n'est pas compatible avec les ports assignés à des protocoles. Pour utiliser ces ports (par exemple, le port sécurisé 443), la configuration de IIS se fera totalement manuellement (reportez-vous à la Section A.1, « Configuration du serveur Web IIS » et à la Section J.1, « Activation du protocole HTTPS sur Stormshield Data Authority Manager ») ou après une configuration automatique sur un port non assigné (reportez-vous à la Section J.1, « Activation du protocole HTTPS sur Stormshield Data Authority Manager »).

4.4 Arborescence créée lors de l'installation

La procédure d'installation propose par défaut :

```
<sdam_install_dir> = C:\Program Files\Arkoon\Security BOX Authority
Manager
```

```
<sdam_data_install_dir> = C:\
```

Ces deux chemins sont modifiables lors de l'installation.

Si vous souhaitez utiliser le SGBD Microsoft Access, le répertoire `<sdam_data_install_dir>` ne doit pas être une ressource réseau.

L'arborescence suivante est créée lors de l'installation de Stormshield Data Authority Manager :

- le dossier d'installation :

```
<sdam_install_dir>
\ActiveX
 \Bin
 \Database
 \Htdocs
 \Html
 \MailTemplates
 \Shared
 \Tools
```

- le dossier de données :

```
<sdam_data_install_dir>
\SBMData
  \Databases
  \tmp
```

4.5 URL d'accès au serveur

L'URL racine d'accès au serveur web IIS est :

```
http://hostname/bin/manager.exe
```

Où `<hostname>` est soit le nom de la machine hébergeant le serveur soit `<adresseIP>:<port>`.

Dans la suite du document, cette URL est nommée `<manager_root_url>`.

Ainsi, depuis le poste de l'administrateur, vous accédez au serveur Stormshield Data Authority Manager à l'aide de l'URL `<manager_root_url>/OpenSession`.

4.6 Configuration du poste administrateur

Stormshield Data Security 10.1 doit être installé sur le poste de l'administrateur.

Certaines opérations effectuées par Stormshield Data Authority Manager nécessitent l'exécution de composants ActiveX sur le poste de l'administrateur.

Vous devez donc :

- ajouter votre serveur aux sites de confiance,
- et autoriser l'exécution des ActiveX non marqués comme sécurisés sur ces sites de confiance.

Pour cela :

1. Dans le menu **Outils** de Internet Explorer, sélectionnez **Options Internet**.
2. Choisissez l'onglet **Sécurité**, la zone **Sites de confiance** et cliquez sur **Sites**.
3. Saisissez `<manager_root_url>`, où `<manager_root_url>` est l'adresse du serveur web hébergeant Stormshield Data Authority Manager.
4. Cliquez sur **Ajouter**, puis **OK**.
5. Cliquez ensuite sur **Personnaliser le niveau** dans les **Contrôles ActiveX et plug-ins**.

6. Modifiez **Contrôles d'initialisation et de scripts ActiveX non marqués comme sécurisés** en sélectionnant **Activer**.
7. Validez deux fois par **OK**.

Pour pouvoir télécharger et installer les ActiveX, l'administrateur doit être un utilisateur de type utilisateur avec pouvoir ou Administrateur.

Une fois que les ActiveX sont installés, un utilisateur standard peut utiliser le poste client pour se connecter à Stormshield Data Authority Manager.

4.7 Configuration du fichier *manager.ini*

Le fichier de configuration *manager.ini* placé dans le dossier d'installation `<sdam_install_dir>` de Stormshield Data Authority Manager contient des paramètres indépendants de toute base.

La prise en compte des modifications de certains paramètres nécessite de redémarrer le service Stormshield Data Authority Manager. Procédez de l'une des deux façons suivantes :

- Dans une fenêtre de commande, tapez `net stop sbasrv` puis `net start sbasrv`.
- Dans la fenêtre des services Windows, cliquez avec le bouton droit sur **Stormshield Data Authority Manager Service** et choisissez **Redémarrer**.

4.7.1 Serveur Web

Vous devez paramétrer dans la section `[WebServer]` les différents chemins dépendant de la configuration de votre serveur Web.

Si par la suite vous modifiez la configuration de votre serveur Web, n'oubliez pas de modifier ces paramètres pour que Stormshield Data Authority Manager continue à fonctionner correctement.

[WebServer]	
ManagerRootUrl	URL racine `<manager_root_url>` d'accès au serveur Stormshield Data Authority Manager, comme définie section URL d'accès au serveur . Cette URL est utilisée pour construire les liens dans les e-mails de notification. Valeur par défaut : déterminée automatiquement. Pour des raisons techniques, cette résolution automatique ne pouvant être parfaitement fiable, il est absolument nécessaire de renseigner ce paramètre.
ManagerCgiUrl	URL ajoutée comme préfixe aux noms des actions associées aux liens présents dans les pages de Stormshield Data Authority Manager. A spécifier pour utiliser des liens absolus. Valeur par défaut : vide, donc les liens sont relatifs.
ManagerDocUrl	URL préfixée aux liens vers les ressources (images, ActiveX…) dans les pages. Si vous utilisez le serveur Web IIS et le paramétrage proposé dans l'Annexe B, Configuration de Windows Server, la valeur de ce paramètre est "/". Valeur par défaut : vide, donc les liens sont relatifs.

4.7.2 Module cryptographique matériel

Si vous mettez en œuvre un module cryptographique matériel (HSM, Hardware Security Module), vous devez le déclarer dans la section `[HSM]`.

Définissez ensuite un ou plusieurs "containers". Ce terme générique permet de désigner un élément physique du module : un slot ou un token en fonction du type de module.

[HSM]	
Name	Nom informatif du module.
DllName	Chemin complet de la DLL *PKCS#11* associée au module.
ContainerIdentification	A ne spécifier que dans le cas où le HSM gère plusieurs "containers". Moyen de différencier les "containers". Les valeurs possibles sont : • `TokenSerialNumber` : le "container" est un token identifié par un numéro de série ; • `TokenLabel` : le "container" est un token identifié par un label ; • `SlotId` : le "container" est un slot identifié par son identifiant.

Si votre HSM ne gère qu'un seul "container", ajoutez une section `[ContainerIfUnique]` avec une clé Login.

[ContainerIfUnique]	
Login	Moyen de vous connecter au "container". Les valeurs possibles pour cette clé sont : • `none` : aucun login n'est demandé ; • `null` : un pointeur nul est transmis ; • `empty` : une chaîne vide est transmise ; • `gui` : un code secret est demandé à l'utilisateur lors de l'activation du container (voir la section Utilisation d'un module cryptographique matériel) ; • toute autre chaîne. Par défaut : `gui`

Si votre HSM gère plusieurs "containers", pour chaque "container" que vous voulez utiliser, ajoutez une section `[Container_XXX]`. Ces noms de sections doivent être uniques ; ils sont utilisés comme identifiants des tokens ou des slots (voir la section Activation/Désactivation d'un container).

[Container_XXX]	
Name	Nom informatif du "container".
TokenSerialNumber, TokenLabel ou SlotId	Valeur permettant d'identifier le "container".

[Container_XXX]	
Login	Moyen de vous connecter au "container". Les valeurs possibles pour cette clé sont : • `none` : aucun login n'est demandé ; • `null` : un pointeur nul est transmis ; • `empty` : une chaîne vide est transmise ; • `gui` : un code secret est demandé à l'utilisateur lors de l'activation du container (voir la section Utilisation d'un module cryptographique matériel) ; • toute autre chaîne. Par défaut : `gui`

Exemples

Pour un HSM avec un "container" unique

```
[HSM]
Name = "My HSM"
DllName = "X:\xxx\P11.dll"

[ContainerIfUnique]
Login = gui
```

Pour un HSM avec plusieurs "containers"

```
[HSM]
Name = "My HSM"
DllName = "X:\xxx\P11.dll"
ContainerIdentification = TokenSerialNumber

[Container_1]
Name = first
TokenSerialNumber = 03150177
Login = gui

[Container_2]
Name = second
TokenSerialNumber = 04152158
Login = gui
```

4.7.3 Accès à internet

La fonctionnalité de demande de certificat à un serveur Stormshield Data Authority Manager distant (section Demande de certificat à un serveur Stormshield Data Authority Manager distant) nécessite que Stormshield Data Authority Manager envoie une requête HTTP au serveur distant. Si les serveurs distants ne sont pas situés sur l'Intranet local mais sur Internet, selon la configuration de votre réseau, il est possible que les requêtes HTTP doivent transiter par un proxy.

Pour que les requêtes HTTP soient envoyées via un tel proxy, spécifiez ce proxy dans la section `[Internet]`. S'il n'est pas spécifié, les requêtes sont envoyées directement aux serveurs distants.

[Internet]	
ProxyName	Nom ou adresse de la machine proxy et son port, séparés par ":".

[Internet]	
ProxyBypass	Adresses pour lesquelles le proxy ne sera pas utilisé, séparées par ";"

4.7.4 Session

Pour utiliser Stormshield Data Authority Manager, tout administrateur doit préalablement ouvrir une session sur la base de données concernée.

La section `[Ctx]` concerne la gestion de ces sessions de travail.

[Ctx]	
LifeTime	Durée au-delà de laquelle une session inutilisée est fermée, en secondes. Valeur par défaut : 900 secondes (15 minutes)
ScanTime	Intervalle de scrutation des sessions, en secondes. Toutes les ScanTime secondes, le logiciel va vérifier que les sessions ne sont pas périmées. Valeur par défaut : 60 secondes.

4.7.5 Traitements automatiques

Stormshield Data Authority Manager vous permet d'effectuer certains traitements par lot : créations d'utilisateurs, demandes de certificats, exportation de certificats, etc.

Pour ces traitements dits "automatiques", une page HTML affiche le résultat de la dernière opération effectuée et lance l'opération suivante.

[Auto]	
ProcessPeriod	Le paramètre ProcessPeriod est la temporisation entre l'affichage de cette page et le lancement de l'opération suivante (submit), en millisecondes. Valeur par défaut : 200 millisecondes. Sur un serveur lent, il est recommandé d'augmenter cette valeur.

4.7.6 Algorithmes

La section `[Algo]` définit les différents algorithmes utilisés par Stormshield Data Authority Manager.

[Algo]	
HashStartKey CryptStartKey	Algorithmes de dérivation et de chiffrement du mot de passe de démarrage. Valeur par défaut : AES 256 bits / SHA-1
KeyGenSecretKey	Algorithme de génération de la clé secrète de chiffrement. Valeur par défaut : AES 256 bits
CryptBase	Algorithme de chiffrement des données sensibles dans la base de données. Valeur par défaut : AES 256 bits

[Algo]	
IterationCountKeystore HashKeystore CryptKeystore	Algorithmes de dérivation et de chiffrement pour la protection des clés des autorités quand elles sont stockées dans un fichier keystore. Valeur par défaut : 10000 / SHA-256 / SHA-1 / AES 256 bits
GroupDH HashDH CryptDH	Groupe Diffie-Hellman et algorithmes de hash et de chiffrement intervenant dans la protection des échanges entre le poste de l'administrateur et le serveur. Valeur par défaut : 14 / SHA-256 / AES 256 bits

Les valeurs pour les algorithmes de chiffrement sont :

DES Simple 64 bits, DES Triple 128 bits, DES Triple 192 bits, AES 128 bits, AES 192 bits, AES 256 bits, RC5 40 bits, RC5 64 bits, RC5 128 bits, RC5 256 bits, RC4 40 bits, RC4 64 bits, RC4 128 bits, RC4 256 bits, RC2 40 bits, RC2 64 bits, RC2 128 bits et RC2 256 bits.

Les valeurs pour les algorithmes de hash sont : SHA-256, SHA-1, MD5 et MD2.

Les valeurs pour le groupe Diffie-Hellman sont 5, 14, 15, 16, 17 et 18.

4.7.7 Désactivation d'attributs PKCS#11

Certains HSM peuvent ne pas supporter des attributs `PKCS#11` utilisés par Stormshield Data Authority Manager.

Si un tel cas se produit, il est possible de désactiver l'utilisation d'attributs `PKCS#11` lors de la création de certains objets.

Pour désactiver un attribut `PKCS#11` :

1. Déclarez une section portant le nom de l'objet pour lequel vous voulez désactiver cet attribut
2. Ajoutez la clé ayant pour nom l'attribut à désactiver (parmi la liste ci-dessous) et pour valeur zéro.

Section	Objet *PKCS#11* concerné
[CA_Public_Key_HSM	Clé publique de certification tirée par le HSM
[CA_Private_Key_HSM]	Clé privée de certification tirée par le HSM
[CA_Public_Key_P12]	Clé publique de certification importée d'un fichier PKCS#12
[CA_Private_Key_P12]	Clé privée de certification importée d'un fichier PKCS#12
[WK_Public_Key_HSM]	Clé publique de chiffrement tirée par le HSM
[WK_Private_Key_HSM]	Clé privée de chiffrement tirée par le HSM
[WK_Public_Key_P12]	Clé publique de chiffrement importée d'un fichier PKCS#12
[WK_Private_Key_P12]	Clé privée de chiffrement importée d'un fichier PKCS#12

Les attributs que vous pouvez désactiver sont :

Attributs	
CKA_CLASS	CKA_EXPONENT_1
CKA_KEY_TYPE	CKA_EXPONENT_2
CKA_TOKEN	CKA_COEFFICIENT
CKA_PRIVATE	CKA_EXTRACTABLE
CKA_MODIFIABLE	CKA_SENSITIVE
CKA_ID	CKA_WRAP
CKA_LABEL	CKA_VERIFY
CKA_MODULUS	CKA_ENCRYPT
CKA_MODULUS_BITS	CKA_VERIFY_RECOVER
CKA_PUBLIC_EXPONENT	CKA_UNWRAP
CKA_PRIVATE_EXPONENT	CKA_SIGN
CKA_PRIME_1	CKA_DECRYPT
CKA_PRIME_2	CKA_SIGN_RECOVER

Exemple

```
[WK_Public_Key_HSM]
CKA_LABEL = 0
```

L'attribut `PKCS#11 CKA_LABEL` ne sera pas déclaré lors du tirage de la clé publique de chiffrement par le HSM.

4.7.8 Attributs des clés privées dans les keystores des utilisateurs

Pour chaque utilisateur, Stormshield Data Authority Manager crée un fichier keystore qui est un véritable token *PKCS#11*.

A ce titre, chaque objet créé dans ce token possède des attributs `PKCS#11`.

Les sections ci-dessous permettent de définir la valeur de deux attributs sensibles relatifs aux clés privées de l'utilisateur :

Section	Type d'opération
[SBox.NewUserWizardExKS1]	Compte mot de passe avec une seule clé
[SBox.NewUserWizardExKS2]	Compte mot de passe avec deux clés
[SBox.NewUserWizardExGP1]	Compte carte avec une seule clé
[SBox.NewUserWizardExGP2]	Compte carte avec deux clés

[SBox.NewUserWizardExXXX]	
NoExtractableK	La clé privée peut être exportée : 0 : Oui 1 : Non Par défaut : 0
KModifiable	Indique si les clés sont modifiables, c'est-à-dire si elles possèdent l'attribut `PKCS#11 CKA_MODIFIABLE` positionné. 0 : les clés ne sont pas modifiables 1 : les clés sont modifiables. Par défaut : 0

Exemple

```
[SBox.NewUserWizardExKS1]
NoExtractableK = 1
```

La clé du compte mot de passe ne pourra pas être exportée par l'utilisateur.

4.7.9 Dossier des fichiers temporaires

Stormshield Data Authority Manager crée puis supprime des fichiers temporaires. Ce paramètre permet de spécifier le dossier dans lequel ces fichiers temporaires sont créés. L'installation du produit affecte à ce paramètre la valeur `<sdam_data_install_dir>\SBMData\tmp`.

Si vous modifiez cette valeur, veillez à sélectionner un dossier existant, et à octroyer à l'utilisateur réseau le droit de modification sur ce dossier (voir la section Droits NTFS requis pour l'utilisateur réseau).

Il est préférable que ce paramètre soit renseigné.

[Path]	
TempPath	Dossier dans lequel Stormshield Data Authority Manager crée puis supprime des fichiers temporaires. Valeur par défaut : `<sdam_data_install_dir>\SBMData\tmp`

4.8 Utilisation d'un module cryptographique matériel

Pour rappel, la clé de l'autorité de certification est générée et stockée par :

- un module cryptographique logiciel Stormshield Data Crypto ;
- un module cryptographique matériel (HSM).

Cette section explique comment utiliser un HSM.

4.8.1 Paramétrage du module cryptographique matériel

Pour utiliser un module cryptographique matériel, vous devez préalablement le déclarer et définir ses éventuels "containers" (token ou slot) dans le fichier *manager.ini* (section Module cryptographique matériel).

4.8.2 Activation/Désactivation d'un container

L'activation d'un "container" (un token ou un slot) consiste à connecter (login) Stormshield Data Authority Manager à ce container. La désactivation consiste à le déconnecter (logout).

Sur votre serveur, plusieurs autorités peuvent stocker leurs clés dans le même container. Dans ce cas, ce container doit être activé une seule fois : toutes les autorités pourront dès lors utiliser leurs clés.

Ces opérations d'activation et de désactivation s'effectuent à l'aide de l'outil en ligne de commande SBMHSM.EXE installé dans le dossier Tools du dossier d'installation `<sdam_install_dir>` de Stormshield Data Authority Manager.

Vous pouvez ouvrir directement une console sur ce dossier à partir du menu **Démarrer**, en sélectionnant **Tous les programmes**, **Stormshield Data Authority Manager**, puis **Ouvrir une console shell**.

Pour activer un token ou un slot :

```
SBMHSM /A [-c <identifiant>] [-p <mot de passe>] [-s]
```

-c : identifiant du token ou du slot ;

-p : mot de passe (voir la section Gestion du mot de passe de l'HSM) ;

-s : mode silencieux : aucun message n'est affiché.

Pour désactiver un token ou un slot :

```
SBMHSM /D [-c <identifiant>] [-s]
```

-c : identifiant du token ou du slot ;

-s : mode silencieux : aucun message n'est affiché.

Pour afficher l'état des tokens ou des slots définis dans le fichier *manager.ini* :

```
SBMHSM /L
```

4.8.3 Gestion du mot de passe de l'HSM

Stormshield Data Security peut fonctionner avec différents HSM qui possèdent des configurations matérielles différentes en fonction du niveau de sécurité et de confiance qu'ils apportent.

Dans le cas d'un HSM composé d'une base sécurisée, d'un Token de sécurité et d'un clavier spécifique (« Pin pad »), l'initialisation du HSM peut être effectuée en utilisant le « Pin pad », directement relié sur l'équipement de base, pour la saisie du mot de passe d'accès au Token.

Cette saisie du PIN est activée par l'appel à une fonction standard de Login.

Pour d'autres équipements, et en fonction de l'implémentation du middleware *PKCS#11* fourni par le constructeur de l'HSM, vous devez préciser dans le fichier *manager.ini* (section Module cryptographique matériel) la nature du PIN passé en paramètre de cette fonction Login. Ce paramètre "login" peut prendre les valeurs :

- none : la fonction Login n'est pas appelée (le Login a été effectué au démarrage du serveur et il est valable pour tous les produits tournant sur le serveur) ;
- `null` : un pointeur nul est transmis ;
- `empty` : une chaîne vide est transmise ;
- `gui` : un code secret est nécessaire pour valider la mise en service (valeur par défaut).

Dans ce cas, ce code secret est :

- Soit passé en ligne de commande de l'outil SBMHSM.EXE (voir la section Activation/Désactivation d'un container) ;
- Soit demandé interactivement par ce même outil ;
- toute autre chaîne, qui peut par exemple être un mot clé identifiant un profil de login.

5. Création et paramétrage d'une base de données

Cette section présente les liens entre une CA (autorité de certification) et une base de données, et décrit toutes les étapes nécessaires pour créer, initialiser et démarrer une base et ouvrir une session.

5.1 Introduction

5.1.1 Liens entre Autorité de Certification et base de données

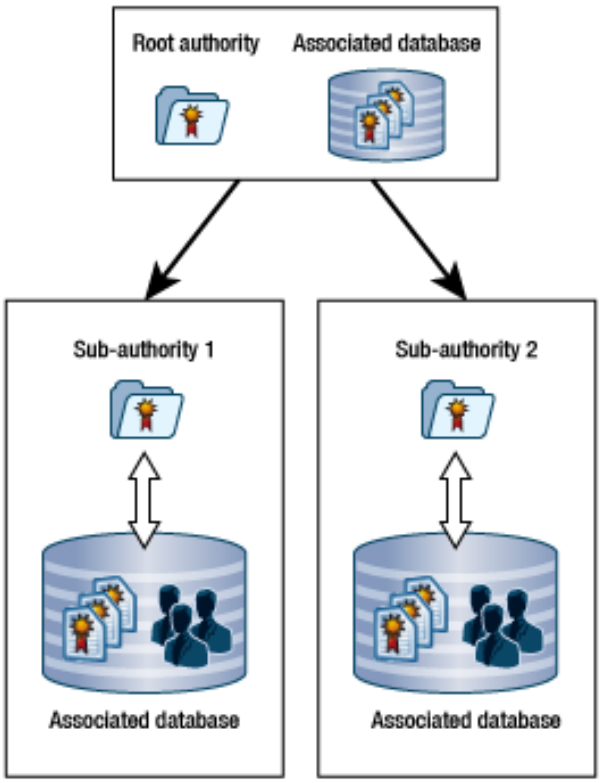
Chaque Autorité de Certification (ou sous-autorité) gère sa propre base de données qui contient :

- les comptes des utilisateurs qu'elle gère ;
- et/ou les certificats qu'elle génère.

L'Infrastructure de Gestion de Clés à mettre en place dépend de contraintes techniques et organisationnelles d'une entreprise selon qu'elle souhaite une gestion des certificats centralisée/décentralisée ou une gestion des utilisateurs par entité.

Après avoir défini la liste des autorités de votre infrastructure, leurs rôles respectifs et leur hiérarchie, vous devez donc créer une base de données pour chaque autorité. Ces deux opérations correspondent aux étapes 1 et 2 de la procédure de déploiement, et elles sont groupées en une seule procédure.

Le schéma suivant illustre une hiérarchie simplifiée à deux niveaux comportant une autorité racine et deux sous-autorités :



5.1.2 Clés d'une autorité de certification

Le fonctionnement d'une Autorité de Certification met en œuvre deux clés :

- La clé de "l'autorité de certification" proprement dite est utilisée pour signer les certificats générés par cette autorité. Le certificat de cette clé identifie publiquement l'autorité.
- La clé de "chiffrement" permet de chiffrer les données confidentielles des utilisateurs gérés dans la base de données (leurs clés privées, mot de passe, etc…). Cette clé est interne à Stormshield Data Authority Manager.

Ces deux clés sont de même type (ce sont des bi-clés RSA), et sont stockées dans le même module cryptographique :

- Soit le module interne de Stormshield Data Authority Manager (qui est un keystore fichier) ;
- Soit dans un module matériel (HSM).

Il est important de noter qu'aucun mécanisme de recouvrement de la base de données n'est mis en œuvre. C'est pourquoi il est fondamental de sauvegarder ces deux clés :

- Si le module interne est utilisé : en sauvegardant le keystore fichier et la base de données après la procédure d'initialisation décrite ci-après ;
- Si un HSM est utilisé : en utilisant les mécanismes de duplication de token qu'il propose.

5.1.3 Administrateur principal et autres administrateurs

Une base de données peut être gérée/administrée par plusieurs administrateurs physiques, chaque administrateur pouvant avoir des rôles différents (voir la sectionDéfinition des administrateurs et de leurs rôles).

Un tel administrateur est authentifié automatiquement et de manière forte à l'aide de son compte Stormshield Data Security (compte mot de passe ou compte carte à puce / clé USB).

L'administrateur dit principal se distingue des administrateurs physiques :

- Il s'authentifie à l'aide d'un simple mot de passe (sans mécanisme fort mettant en oeuvre un compte Stormshield Data Security) ;
- Son rôle est défini dans le fichier *bases.ini* placé dans le dossier d'installation `<sdam_install_dir>` de Stormshield Data Authority Manager. L'administrateur principal peut avoir :
- Tous les droits ;
- Uniquement le droit de gérer les administrateurs ;
- Aucun droit (ce qui équivaut à désactiver cet administrateur principal).

Reportez-vous à la section Fichier bases.ini pour définir précisément le rôle de l'administrateur principal.

5.1.4 Mise en route d'une autorité et d'une base associée

L'ordre des opérations à effectuer pour préparer une autorité ou une base de données est le suivant :

1. Créez physiquement votre base (voir la section Création d'une base de données). Elle sera le support physique pour la gestion de l'autorité et des comptes utilisateurs.
2. Initialisez cette base, opération qui consiste principalement à tirer les clés de certification et de chiffrement de l'autorité (section Initialisation d'une base de données).

Votre base est alors opérationnelle.

Pour pouvoir exploiter cette base, il faut :

3. La démarrer (section Démarrage/Arrêt d'une base de données) ; l'autorité associée à la base de données peut dès lors :

- Recevoir les demandes de certificats ;
- Automatiquement et périodiquement mettre à jour la liste de révocation (CRL).

4. Ouvrir une session sur cette base (section Ouverture/Fermeture de session sur une base), soit avec le mot de passe "administrateur principal", soit avec votre compte Stormshield Data Security. Vous accédez alors aux fonctions qui vous sont autorisées.

Notez que si vous utilisiez une précédente version de Stormshield Data Authority Manager, vous devez importer les données de votre ancienne base de données.

5.1.5 Mot de passe de démarrage

Le démarrage ainsi que l'arrêt d'une base nécessite la présentation d'un mot de passe spécifique.

Ce mot de passe de démarrage peut être confié à un exploitant : il ne permet pas d'utiliser les services de Stormshield Data Authority Manager.

La procédure pour définir le mot de passe de démarrage se trouve à la section Saisie du mot de passe de démarrage .

5.2 Création d'une base de données

Stormshield Data Authority Manager supporte deux SGBD : Microsoft Access et Microsoft SQL Server.

L'outil de création de base de données permet de :

- créer et peupler une base de données, si l'administrateur choisit de travailler avec Microsoft Access ;
- prendre en compte une base existante peuplée, si l'administrateur choisit de travailler avec Microsoft SQL Server.

NOTE
Pour les bases Microsoft SQL Server, avant d'utiliser l'outil de création, vous devez :

- créer les bases : une base Microsoft SQL Server par base Stormshield Data Authority Manager souhaitée ;
- peupler ces bases à l'aide du script `create_database_SqlServer.sql` fourni dans le dossier `<sdam_install_dir>\DataBase`.

Vous pouvez obtenir des informations supplémentaires en consultant la procédure décrite dans l'Migration de Microsoft Access vers Microsoft SQL Server.

5.2.1 Assistant de création

1. Lancez l'outil SBMCB.EXE en sélectionnant dans le menu **Démarrer** de Windows : **Tous les programmes**, **Stormshield Data Authority Manager**, **Créer une nouvelle base**.

NOTE
L'outil doit être lancé avec les droits d'administration pour éviter que le processus de création de base ne s'interrompe par manque de privilèges.

2. Dans la première page, saisissez :

- l'identifiant de la base, en utilisant uniquement des lettres minuscules sans accent et des chiffres. Cet identifiant est essentiellement utilisé en interne par Stormshield Data Authority Manager ;
- le libellé de la base. Ce libellé est utilisé dans toutes les pages de Stormshield Data Authority Manager pour faire référence à la base d'utilisateurs.

3. La deuxième page permet de sélectionner le type de base de données :

Si Microsoft Access est sélectionné, la base est créée, et on accède directement à la page des droits de l'administrateur principal.

Si Microsoft SQL Server est sélectionné, on accède à une page de saisie des paramètres de connexion à une base Microsoft SQL Server existante :

Si l'option de **demande de saisie d'un mot de passe à la connexion** n'est pas cochée, le mot de passe doit être saisi dans cette page. Il est possible de contrôler les paramètres saisis en testant la connexion à la base à l'aide du bouton **Tester**.

4. Dans la page des droits de l'administrateur principal, sélectionnez les autorisations (section Autorisations) qui seront accordées à l'administrateur principal. Choisissez entre :

- lui accorder **tous les droits** ;
- lui accorder le droit de gérer les administrateurs (**Administrateur des autorisations**) ;
- désactiver l'administrateur principal (**aucun droit**). Dans ce cas, seule l'ouverture d'une session par authentification forte (section Ouverture de session sur une base) sera possible après l'initialisation de la base (section Initialisation d'une base de données). Vous devez donc obligatoirement créer au moins un administrateur des autorisations immédiatement après l'initialisation de la base (voir Définition des administrateurs et de leurs rôles).

5. Dans la dernière page, validez le traitement de la base d'utilisateurs en appuyant sur le bouton **Terminer**.

Le lien avec une base physique est désormais établi : vous devez désormais l'initialiser comme cela est décrit à la section Initialisation d'une base de données.

5.2.2 Fichier *bases.ini*

Le fichier *bases.ini*, placé dans le dossier d'installation `<sdam_install_dir>` de Stormshield Data Authority Manager, comporte une section par base de données.

Cette section, qui a le même identifiant que la base associée, est automatiquement créée et renseignée par l'assistant de création de base SBMCB.EXE.

Chaque section comprend les données suivantes :

[<BaseId>]	
BaseName	Nom usuel de la base

[<BaseId>]	

ConnectionString	Chaîne de connexion au SGBD. Par exemple :
	Pour Microsoft Access :
	`Provider=Microsoft.Jet.OLEDB.4.0;Data Source=<sdam_data_install_dir>\SBMData\DataBases\<baseid>.sba`
	Pour Microsoft SQL Server :
	`Provider=SQLOLEDB;Data Source=<server name>;DataBase=<database name>;User Id=<user ID>;Password=<password>`

AskSqlPwd	Demande de saisie d'un mot de passe lors de la connexion à la base : • 0 : le mot de passe n'est pas demandé à l'utilisateur lors de la connexion à la base. Si vous n'utilisez pas Microsoft Access, vous devez vérifier que ce mot de passe est bien renseigné dans la chaîne de connexion `ConnectionString`. **IMPORTANT** Cela signifie que le mot de passe est « en clair » dans le fichier *bases.ini*. • 1 : le mot de passe est demandé à l'utilisateur lors de la connexion à la base. Il est ajouté à la chaîne de connexion. Vous devez donc vérifier que le champ Password n'est pas renseigné dans la chaîne `ConnectionString (Password=` doit être présent à la fin de la chaîne, mais pas sa valeur `<password>`). Si vous utilisez Microsoft Access, cette donnée doit être égale à 0.
KSPath	Chemin complet du fichier keystore contenant les clés de l'autorité. Ce champ est sans objet quand les clés sont stockées dans un HSM. Par défaut : `<sdam_data_install_dir>\DataBases\<baseid>.mng`
MainAdmin	Droits accordés à l' "administrateur principal" : `All` : Tous les droits `Admin` : Uniquement le droit de gérer les administrateurs de la base `None` : Aucun droit (ce qui signifie que l'authentification par un simple mot de passe est désactivée)

5.3 Initialisation d'une base de données

L'initialisation d'une base de données consiste à :

- tirer les clés de l'autorité (clé de certification, clé de chiffrement) ;
- définir ses mots de passe de protection ;
- et éventuellement à faire certifier sa clé de certification auprès d'une autre autorité.

NOTE
Une base dont l'initialisation n'a pas été achevée, est inutilisable. Et une initialisation interrompue ne peut pas être reprise. Une session inutilisée ayant une durée de vie limitée, il est préférable d'effectuer l'initialisation d'une base sans marquer d'arrêt significatif.

5.3.1 Sélection de la base à initialiser

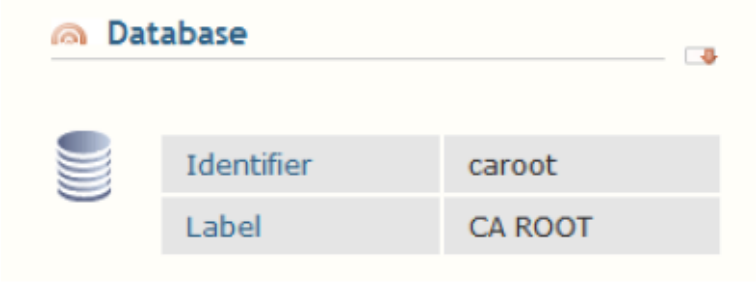
1. Accédez à la page d'initialisation en saisissant l'URL `<manager_root_url>/InitBase` où `<manager_root_url>` est l'URL racine définie dans la section URL d'accès au serveur .

Elle propose la liste des bases existantes qui ne sont pas démarrées.

2. Lancez l'initialisation de la base sélectionnée, en appuyant sur le bouton **Initialiser**.

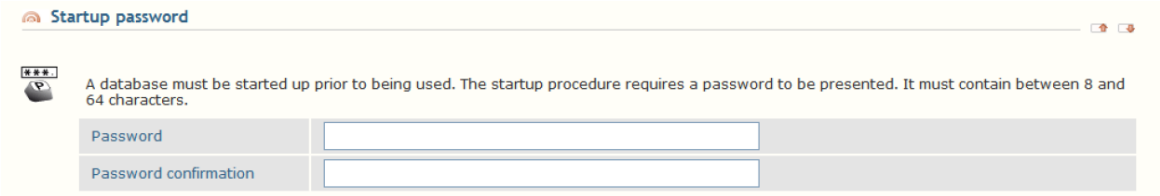
5.3.2 Saisie du mot de passe de démarrage

La première partie de la page affiche l'identifiant et le libellé de la base saisis lors de sa création (section Assistant de création).



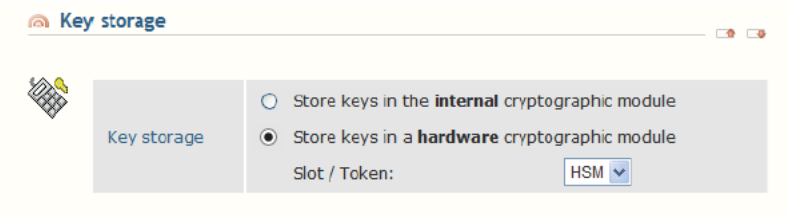
Un lien dans le bandeau en haut de la page permet de revenir à la page de sélection de la base à initialiser.

Saisissez le mot de passe de démarrage de la base qui sera utilisé ultérieurement pour démarrer et arrêter la base (section Démarrage/Arrêt d'une base de données).



5.3.3 Sélection du module cryptographique

Sélectionnez le module cryptographique dans lequel la clé de chiffrement et la clé de l'autorité de certification seront stockées. Elles peuvent être stockées dans le module cryptographique interne ou bien dans un module cryptographique matériel (HSM). Le module cryptographique matériel est déclaré dans le fichier *manager.ini* (section Module cryptographique matériel). Seuls les containers activés (section Activation/Désactivation d'un container) sont proposés.

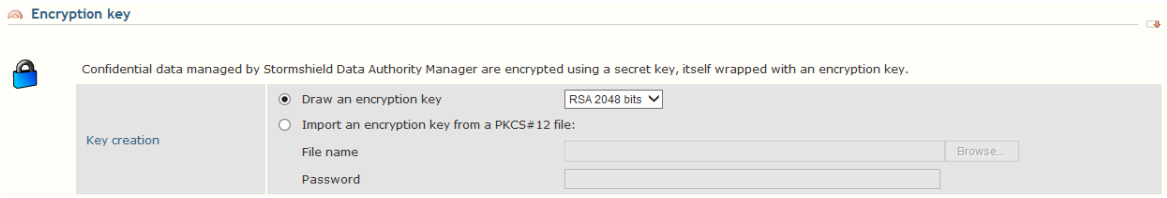


5.3.4 Création de la clé de chiffrement

Pour créer la clé de chiffrement, vous pouvez :

- faire tirer la clé au module cryptographique. Si vous utilisez le module cryptographique interne, vous pouvez créer une clé RSA de 1024, 2048 ou 4096 bits. Certaines de ces tailles de clé, bien qu'elles soient systématiquement proposées, peuvent ne pas être supportées par un module cryptographique matériel ;
- importer dans le module cryptographique une clé présente dans un fichier *PKCS#12*.

Sélectionnez le chemin complet du fichier ainsi que son mot de passe.



Dans tous les cas, vous pouvez choisir de créer une clé exportable, c'est-à-dire une clé qui pourra ultérieurement être "sortie" de son module de sécurité.

Pour créer une clé exportable, Stormshield Data Authority Manager positionne, pour la clé privée, l'attribut CKA_EXTRACTABLE à TRUE, et l'attribut CKA_SENSITIVE à FALSE. Pour une clé non exportable, il positionne l'attribut CKA_EXTRACTABLE à FALSE, et l'attribut CKA_SENSITIVE à TRUE.

NOTE
La propriété d'exportation peut ne pas être supportée par un module cryptographique matériel.

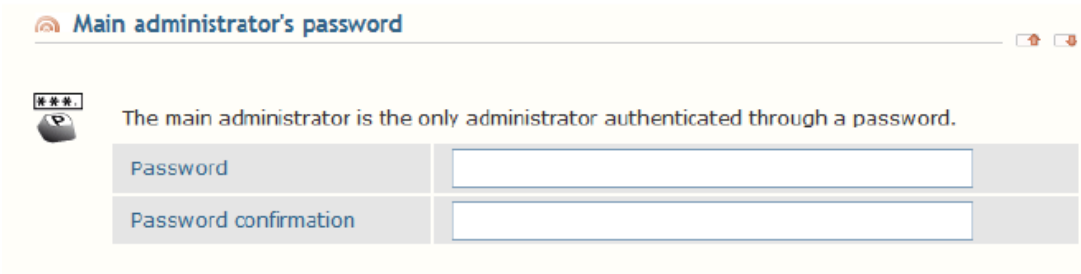
Si vous utilisez un module cryptographique matériel qui ne supporte pas la totalité du standard *PKCS#11*, vous pouvez désactiver dans le fichier *manager.ini* certains attributs *PKCS#11* (section Désactivation d'attributs *PKCS#11*).

Dans le cas de l'importation de la clé, vous accédez ensuite à une page de présentation du contenu du fichier *PKCS#12*, dans laquelle vous validez l'importation.

5.3.5 Saisie du mot de passe de l'administrateur principal

La première partie de cette page affiche un compte rendu de l'opération de création de la clé de chiffrement.

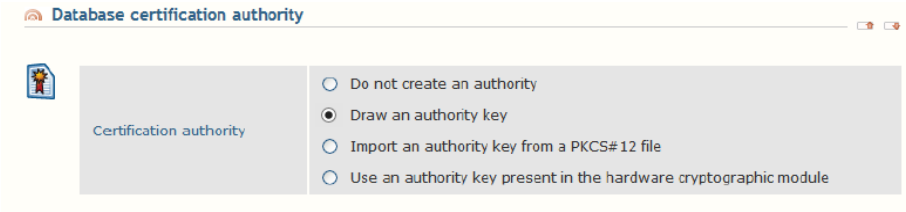
Saisissez le mot de passe de l'administrateur principal (section Modification du mot de passe de l'administrateur principal). Ce mot de passe vous sera demandé lors de l'ouverture par mot de passe d'une session sur la base.



5.3.6 Création de la clé de signature de l'autorité de certification

Sélectionnez ensuite le mode de création de la clé de signature de l'autorité de certification :

- Ne pas créer d'autorité de certification dans la base. L'initialisation de la base est alors achevée. Vous accédez directement à la page de compte rendu de l'initialisation de la base (section Compte-rendu de l'initialisation) ;
- Faire tirer au module cryptographique une nouvelle clé (voir la section Génération de la clé de l'autorité de certification) ;
- Importer une clé présente dans un fichier *PKCS#12* (voir la section Importation de la clé de l'autorité de certification) ;
- Utiliser une clé déjà présente dans le module cryptographique matériel (voir la section Utilisation d'une clé déjà présente dans le module cryptographique matériel).



Génération de la clé de l'autorité de certification

Génération de la clé de l'autorité de certification

Dans cette page, choisissez la taille de la clé RSA que le module cryptographique doit générer. Si vous utilisez le module cryptographique interne, vous pouvez créer une clé RSA de 1024, 2048 ou 4096 bits. Certaines de ces tailles de clé, bien qu'elles soient systématiquement proposées, peuvent ne pas être supportées par un module cryptographique matériel.

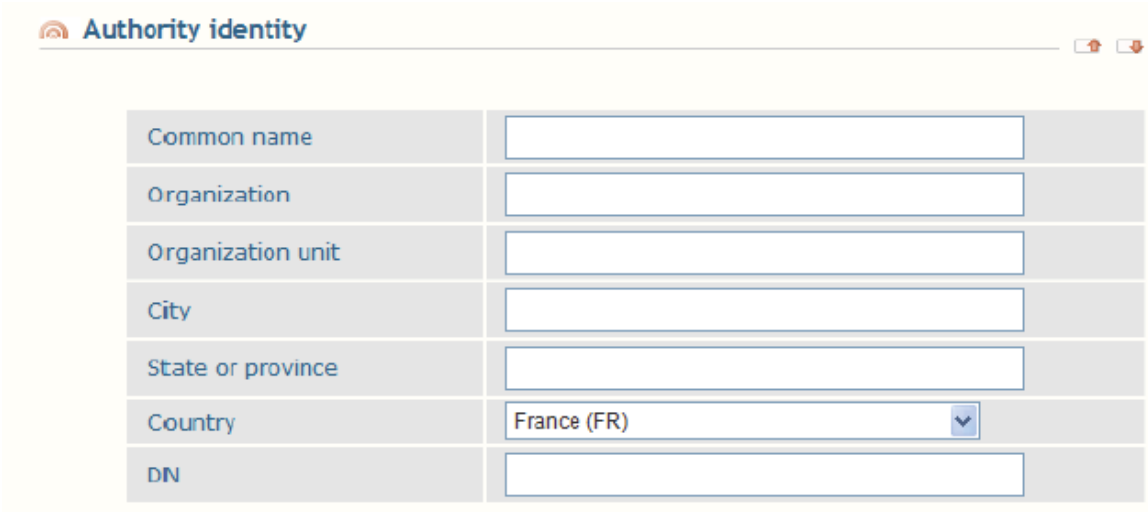
Vous pouvez choisir de créer une clé exportable. Mais cette propriété peut ne pas être supportée par un module cryptographique matériel.

Si vous utilisez un module cryptographique matériel, vous pouvez choisir dans le fichier *manager.ini* de ne pas positionner certains attributs *PKCS#11* (section Désactivation d'attributs *PKCS#11*) lors de la génération de la clé.

Génération du certificat de la clé

La première partie de cette page affiche un compte rendu de l'opération de génération de la clé.

1. Saisissez l'identité de l'autorité de certification :

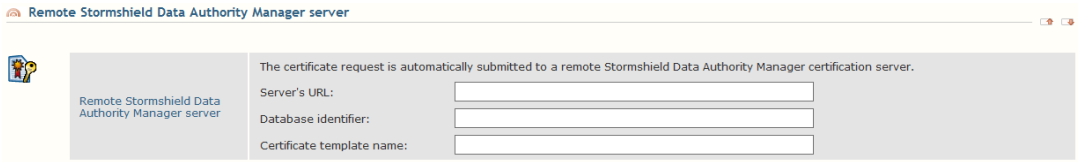


2. Pour générer le certificat de la clé de l'autorité de certification, vous pouvez choisir de :

- faire certifier la clé par une autorité de certification externe. Vous accédez alors à la page de demande de certificat qui vous propose plusieurs moyens pour effectuer votre demande (voir la section Création de demande).

Si vous choisissez d'effectuer une demande de certificat à un Stormshield Data Authority Manager distant, vous devez saisir :

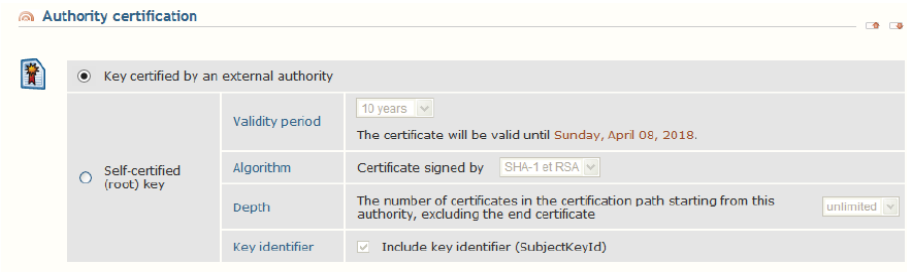
- l'URL racine `<manager_root_url>` du serveur Stormshield Data Authority Manager distant, comme définie à la section URL d'accès au serveur ;
- l'identifiant de la base présente sur ce serveur, qui contient l'autorité de certification à utiliser ;
- le libellé du modèle de certificat présent dans cette base, qui doit être utilisé pour générer le certificat.



Après la confirmation de la demande, la page de compte-rendu de l'initialisation de la base est affichée (voir la section Compte-rendu de l'initialisation).

NOTE
Le certificat généré par l'autorité externe devra être importé ultérieurement (section Importation d'un nouveau certificat). Tant que cette importation n'a pas été effectuée, l'autorité de certification ne peut pas générer de certificat.

- faire certifier par elle-même la clé de l'autorité de certification. L'autorité est alors une autorité racine auto-certifiée. Vous accédez directement à la page de compte rendu de l'initialisation de la base (section Compte-rendu de l'initialisation).



Importation de la clé de l'autorité de certification

Dans cette page, sélectionnez le chemin complet du fichier *PKCS#12* ainsi que son mot de passe.

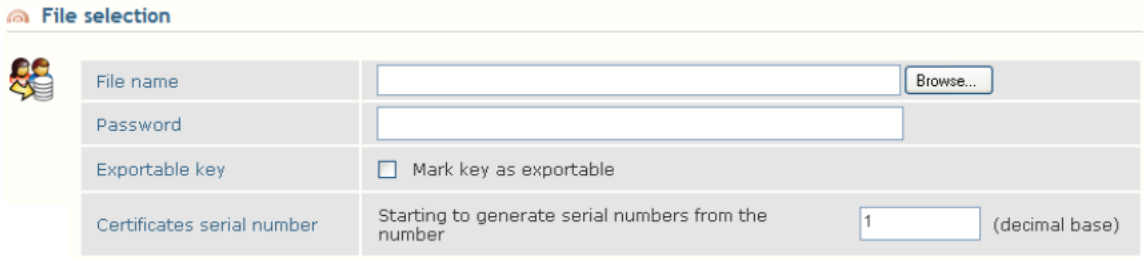
Vous pouvez choisir de créer une clé exportable. Mais cette propriété peut ne pas être supportée par un module cryptographique matériel.

Vous pouvez saisir le premier numéro de série des certificats qui seront générés par l'autorité de certification. Par défaut, la numérotation débute à 1. Mais il peut être nécessaire de tenir compte des numéros de série de certificats déjà émis par cette autorité de certification dans le cadre d'une autre PKI, dans la mesure où la génération des numéros de série était aussi incrémentielle.

Si vous utilisez un module cryptographique matériel, vous pouvez choisir dans le fichier *manager.ini* de ne pas positionner certains attributs *PKCS#11* (section **Désactivation d'attributs *PKCS#11***) lors de l'importation de la clé.

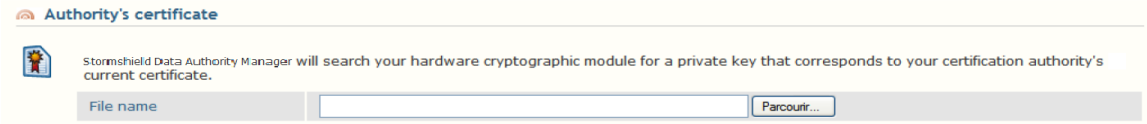
Vous accédez ensuite à une page de présentation du contenu du fichier PKCS#12, dans laquelle vous validez l'importation en appuyant sur le bouton Terminer. Vous accédez alors à la page de compte-rendu de l'initialisation de la base (section **Compte-rendu de l'initialisation**).

Lors de cette opération, le certificat de la clé est aussi importé à partir du fichier *PKCS#12*.



Utilisation d'une clé déjà présente dans le module cryptographique matériel

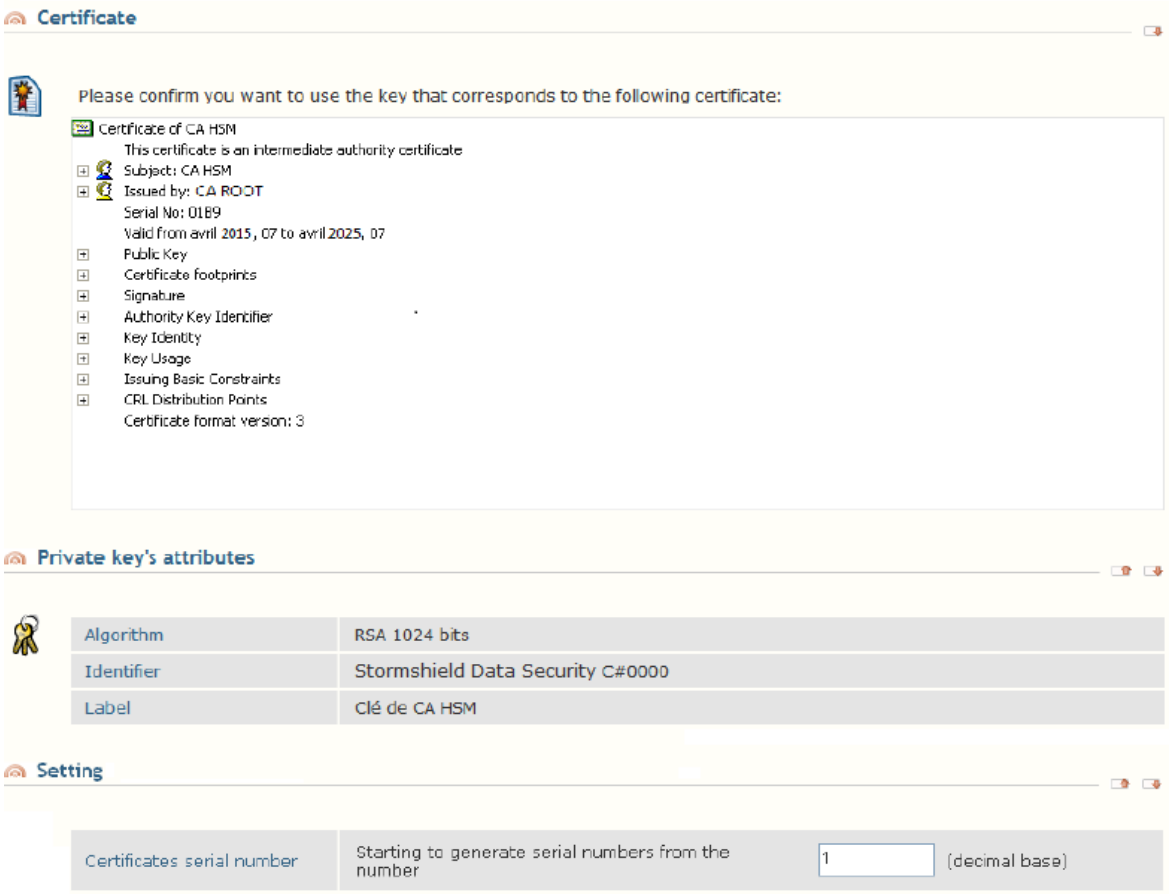
Pour l'autorité de certification, vous pouvez ré-utiliser une clé déjà présente dans le module cryptographique matériel. Fournissez le chemin complet d'un fichier contenant le certificat de la clé à rechercher dans le module cryptographique.



Vous accédez ensuite à une page de présentation du contenu du certificat et des attributs de la clé trouvée dans le module cryptographique.

Vous pouvez saisir le premier numéro de série des certificats qui seront générés par l'autorité de certification. Par défaut, la numérotation débute à 1. Mais il peut être nécessaire de tenir

compte des numéros de série de certificats déjà émis par cette autorité de certification dans le cadre d'une autre PKI, dans la mesure où la génération des numéros de série était aussi incrémentielle.

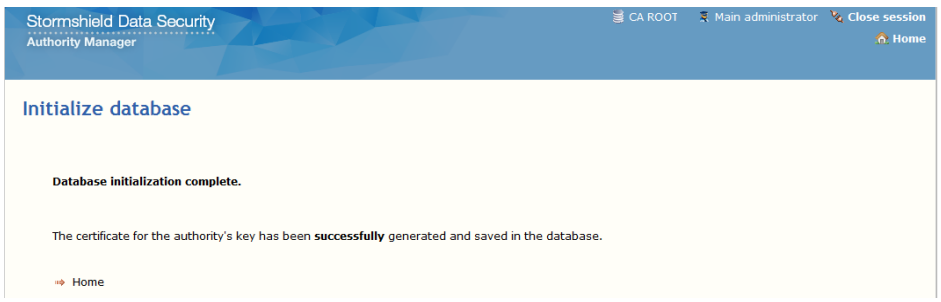


Dans la page, vous validez l'association en appuyant sur le bouton **Terminer**. Vous accédez alors à la page de compte-rendu de l'initialisation de la base (section Compte-rendu de l'initialisation).

Lors de cette opération, le certificat est importé.

5.3.7 Compte-rendu de l'initialisation

Cette page affiche l'identifiant et le libellé de la base, ainsi que le compte-rendu de la dernière opération effectuée.



Un lien permet d'accéder à la page d'accueil de Stormshield Data Authority Manager (section Page d'accueil).

5.3.8 Arborescence créée lors de l'initialisation

Lors de l'initialisation de la base, les dossiers suivants sont créés sous

```
<sdam_data_install_dir>\SBMData\<base_id>
```

où `<sdam_data_install_dir>` est le dossier de données (section Arborescence créée lors de l'installation) et `<base_id>` l'identifiant de la base.

Dossier	Contient
`\Certs`	certificats provenant d'une autre PKI afin d'être importés par lots
`\CertsPublished`	certificats générés par Stormshield Data Authority Manager quand ils sont publiés "par fichier"
`\Crl`	dernière CRL émise : <base_id>.crl
`\CrlHistory`	historique des CRL, sous la forme : <AAAAMMJJ – CrlNbHexa>.crl
`\Log`	journal du manager : <base_id>.txt journal de l'outil de migration de base : BaseUpgrade.txt
`\MailTemplates`	fichiers de définition des mails émis
`\MSITarget`	cible de la personnalisation de la procédure d'installation
`\Users`	comptes utilisateurs
`\UsersFiles`	fichiers liste de Stormshield Data File et Shredder

5.4 Démarrage/Arrêt d'une base de données

Pour démarrer et arrêter une base de données, utilisez l'outil *SBMSTART.EXE* contenu dans le dossier **Outils** du dossier d'installation de Stormshield Data Authority Manager.

Vous pouvez ouvrir directement une console sur ce dossier à partir du menu **Démarrer**, en sélectionnant **Tous les programmes**, **Stormshield Data Authority Manager**, puis **Ouvrir une console shell**.

25 bases peuvent être démarrées simultanément.

- Pour démarrer une base :

```
SBMSTART /O [-b <identifiant>] [-p <mot de passe>] [-s]
```

b : identifiant de la base saisi lors de sa création (voir la section Assistant de création). Si cet identifiant est absent ou incorrect, la liste des bases non démarrées est affichée ;

-p : mot de passe de démarrage de la base saisi lors de son initialisation (section Saisie du mot de passe de démarrage) ;

-s : mode silencieux : aucun message n'est affiché.

- Pour arrêter une base :

```
SBMSTART /C [-b <identifiant>] [-p <mot de passe>] [-s]
```

-b : identifiant de la base saisi lors de sa création (voir la section Assistant de création). Si cet identifiant est absent ou incorrect, la liste des bases démarrées est affichée ;

-p : mot de passe de démarrage de la base saisi lors de son initialisation (section Saisie du mot de passe de démarrage) ;

-s : mode silencieux : aucun message n'est affiché.

Pour afficher l'état des bases définies dans le fichier *bases.ini* :

```
SBMSTART /L
```

- Si le mot de passe de démarrage contient des caractères non ASCII (caractères accentués par exemple), l'outil *SBMSTART.EXE* ne peut pas fonctionner. Pour contourner ce comportement, vous pouvez exécuter la commande de démarrage de la base dans un script PowerShell. Pour plus d'informations, reportez-vous à la section Démarrage d'une base de données avec PowerShell.

5.5 Mise à jour de Stormshield Data Authority Manager

5.5.1 Sur la même machine

Le logiciel Stormshield Data Authority Manager est directement mis à jour avec la version 10.1 sur la même machine, il y a donc conservation du dossier d'installation et du dossier de données.

1. Installez directement la nouvelle version de Stormshield Data Authority Manager version 10.1 sur la version précédente. Arrêtez le service Security BOX Authority Manager ou Stormshield Data Authority Manager selon le numéro de version installée, lors de la demande pendant l'installation.

Si vous choisissez un dossier d'installation différent de celui de la version précédente, vous pouvez activer la configuration automatique du site Web lors de la nouvelle installation.

Si vous choisissez le même dossier d'installation :

- Si lors de la première installation vous aviez choisi la configuration automatique de votre serveur Web, vous devez de nouveau activer la configuration automatique.

IMPORTANT
Toutes les personnalisations effectuées dans IIS sur le site de Stormshield Data Authority Manager, seront perdues.

- Si vous aviez effectué la configuration manuellement, vous ne devez pas activer la configuration automatique.

Vous devez sélectionner le même dossier de données que la version précédente.

2. Démarrez chaque base définie dans le fichier *bases.ini* (voir la section Démarrage/Arrêt d'une base de données).
3. Lancez l'outil **Mise à jour de base** sur chaque base (voir la section Outil de mise à jour de base de données).

   Lorsque la base est déjà à jour, seule la fonctionnalité de peuplement est proposée.
4. Dans IIS, renommez le site par un clic droit sur le nom du site > **Renommer** en Stormshield Data Authority Manager.

5.5.2 Sur une nouvelle machine, sans copie de l'arborescence

Stormshield Data Authority Manager version 10.1 est installé sur une nouvelle machine, sans volonté de conserver les anciennes arborescences des bases.

1. Installez Stormshield Data Authority Manager version 10.1 sur la nouvelle machine.
2. Copiez dans le dossier `<sdam_data_install_dir>/SBMData/Databases` les fichiers des bases des versions précédentes <base_id>.sba et les fichiers keystores associés *<base_id>.mng*.
3. Remplacez le nouveau fichier *bases.ini* par l'ancien fichier *bases.ini*.
4. Démarrez chaque base définie dans le fichier *bases.ini* (voir la section Démarrage/Arrêt d'une base de données).
5. Lancez l'outil de Mise à jour de base sur chaque base (voir la section Outil de mise à jour de base de données).

Lorsque la base est déjà à jour, seule la fonctionnalité de peuplement est proposée.

Pour chaque base il y a création d'une arborescence dans le dossier `<sdam_data_install_dir>/SBMData` et mise à jour des chemins dans les paramètres généraux.

5.5.3 Sur une nouvelle machine, avec copie de l'arborescence

Stormshield Data Authority Manager version 10.1 est installé sur une nouvelle machine, avec conservation des anciennes arborescences des bases.

1. Installez Stormshield Data Authority Manager version 10.1 sur la nouvelle machine en effectuant la configuration automatique du site Web.
2. Copiez dans le dossier `<sdam_data_install_dir>/SBMData/Databases` les fichiers des bases des versions précédentes *<base_id>.sba* et les fichiers keystores associés *<base_id>.mng*.
3. Effectuez l'une des opérations suivantes :

- étape 4
- ou étape 5

4. Si le dossier de données `<sdam_data_install_dir>` est le même que celui de la machine précédente :

- Pour chaque base, copiez l'ancienne arborescence de la base `<sdam_data_install_dir>/SBMData/<base_id>` sur la nouvelle machine dans le même dossier `<sdam_data_install_dir>/SBMData/<base_id>`.
- Remplacez le nouveau fichier *bases.ini* par l'ancien fichier *bases.ini*.
- Démarrez chaque base définie dans le fichier *bases.ini* (voir la section Démarrage/Arrêt d'une base de données).
- Lancez l'outil de Mise à jour de base sur chaque base (voir la section Outil de mise à jour de base de données).

  Lorsque la base est déjà à jour, seule la fonctionnalité de peuplement est proposée.

IMPORTANT
L'outil effectue une réinitialisation des paramètres généraux en utilisant l'arborescence `<sdam_data_install_dir>/SBMData/<base_id>`. Ainsi, si vous aviez modifié des paramètres généraux comportant l'arborescence initiale, ces modifications ont été perdues.

5. Si le dossier de données `<sdam_data_install_dir>` est différent de celui de la machine précédente :

- Copiez l'ancienne arborescence de la base `<sdam_data_install_dir_former_version>/SBMData/<base_id>` sur la nouvelle machine dans le nouveau dossier `<sdam_data_install_dir>/SBMData/<base_id>`.
- Remplacez le nouveau fichier *bases.ini* par l'ancien fichier *bases.ini*, en mettant à jour les chemins définis dans les données `BasePath` et `KSPath` en utilisant `<sdam_data_install_dir>`.
- Démarrez chaque base définie dans le fichier *bases.ini* (voir la section Démarrage/Arrêt d'une base de données).
- Lancez l'outil de **Mise à jour de base** sur chaque base (voir la section Outil de mise à jour de base de données). L'outil effectue une réinitialisation des paramètres généraux en utilisant l'arborescence `<sdam_data_install_dir>/SBMData/<base_id>`.
  Lorsque la base est déjà à jour, seule la fonctionnalité de peuplement est proposée.

5.5.4 Outil de mise à jour de base de données

Lorsque la base est déjà à jour, seule la fonctionnalité de peuplement est proposée.

1. Démarrez la base version précédente.
2. Lancez l'outil de mise à jour de base de données *SbmUpBa.exe* en sélectionnant **Tous les programmes**, **Stormshield Data Authority Manager** , puis **Mettre à jour une base**, à partir du menu **Démarrer**.
3. Sur la première page :

- Sélectionnez l'identifiant de la base Stormshield Data Authority Manager de la version précédente à mettre à jour à partir des identifiants de bases démarrées.
- Saisissez le mot de passe de l'administrateur principal de la base à mettre à jour.

4. La page suivante demande de confirmer la mise à jour de la base.
5. La dernière page affiche un compte rendu détaillé des opérations effectuées et permet d'éditer celles-ci dans un fichier de journalisation.

Si la base est une base Microsoft Access, un compactage est effectué après la migration afin de réduire sa taille et d'améliorer les performances. La base doit être redémarrée après cette opération.

NOTE
Pour une base Microsoft Access, si une erreur survient lors de la migration d'une base volumineuse (par exemple une base contenant plus de 40000 certificats, ou faisant au moins 300 Mo), vous pouvez effectuer à nouveau l'opération de migration en modifiant au préalable une valeur dans la base de registre :

1. Dans le menu **Démarrer** de Windows, choisissez **Exécuter**, puis saisissez **regedit**.
2. Déplacez-vous sur la clé :
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Jet\4.0\Engines\Jet 4.0
3. Modifiez la valeur de `MaxLocksPerFile` : sauvegardez l'ancienne valeur (par défaut 9500 en décimal), et saisissez 250000 en décimal.

Après la migration de la base, vous devez repositionner l'ancienne valeur (par défaut 9500 en décimal).

Attention, cette valeur sera utilisée pour toutes les connexions sur une base de données effectuées par Jet, par toutes les applications de votre serveur utilisant Jet.

5.6 Peuplement d'une base 10.1

5.6.1 Présentation

Cette fonctionnalité permet d'importer dans une base version 10.1 les utilisateurs d'une autre base version 10.1. Elle permet entre autre de récupérer le contenu d'une base ayant une autorité racine périmée.

Si vous souhaitez importer les données d'une base de version antérieure à 10.1 , il est recommandé d'effectuer d'abord une mise à jour de la base (voir la section Outil de mise à jour de base de données).

Exhaustivement, cette fonctionnalité permet d'importer :

- les utilisateurs standards ;

Lors de l'importation, le statut « administrateur interne » (voir la section Ajout d'un administrateur interne à la base).

NOTE
Après l'importation d'utilisateurs dans la base destination, il est pertinent d'importer dans la liste des certificats externes (voir la section Autres certificats externes) de cette base le certificat de l'autorité de certification qui a certifié les clés des utilisateurs importés (l'autorité de certification de la base source par exemple). Cela permettra de diffuser à partir de la base destination des comptes possédant la parenté des certificats.

- les modèles ;

Lors de l'importation, si l'importation d'un modèle échoue parce qu'un modèle possédant le même identifiant est déjà présent, les utilisateurs importés dérivant de ce modèle dériveront du modèle présent dans la base.

- les comptes de recouvrement ;
- le signataire de politiques de sécurité ;

Cette importation échoue si la base destination en contient déjà un.

- les modèles de certificat (voir la section Modèles de certificats) et les autorités de certification externes (voir la section Autorités de certification externes) utilisés par les utilisateurs importés ;
- des compteurs internes.

L'importation "complète" dans une base 10.1 Microsoft SQL Server du contenu d'une base 10.1 Microsoft Access est décrite dans l'Annexe C, Migration Microsoft Access vers Microsoft SQL Server.

5.6.2 Utilisation

Pour peupler la base, lancez l'outil de mise à jour de base *SbmUpBa.exe* à partir du menu **Démarrer** en sélectionnant **Tous les programmes, Stormshield Data Authority Manager**, puis **Mettre à jour une base**.

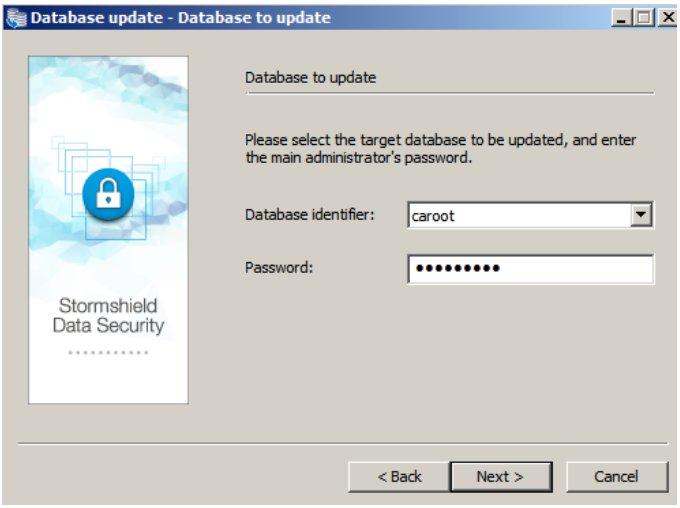
1. Dans la première page :

- Sélectionnez l'identifiant de la base version 10.1 à mettre à jour parmi les identifiants de bases démarrées.

La base à mettre à jour doit impérativement avoir été initialisée (voir la section Initialisation d'une base de données).

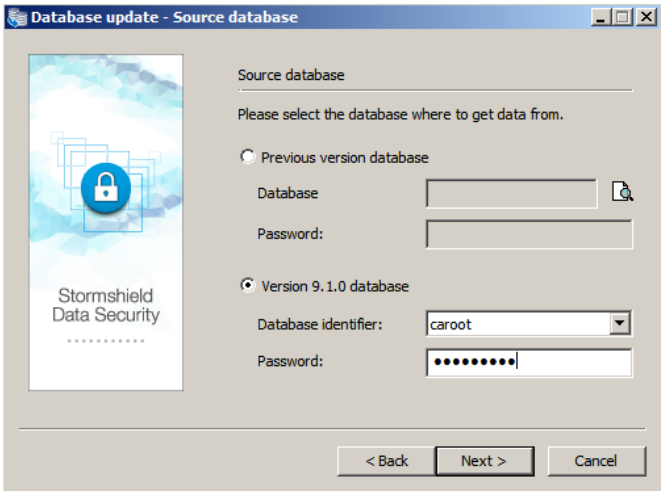
- Saisissez le mot de passe de l'administrateur principal de la base à mettre à jour.

Si vous ne voyez pas l'identifiant de la base que vous souhaitez mettre à jour, vérifiez qu'elle est bien démarrée.



2. Dans la deuxième page :

- Sélectionnez la puce **Base version 10.1** ;
- Sélectionnez la base de version 10.1 à partir de laquelle vous souhaitez importer les utilisateurs. Si vous ne voyez pas l'identifiant de la base que vous souhaitez utiliser, vérifiez qu'elle est bien démarrée ;
- Saisissez le mot de passe de l'administrateur principal de la base source.



3. La page suivante permet de choisir quels utilisateurs et modèles vous souhaitez importer.

Si vous sélectionnez la case à cocher **Importer les utilisateurs**, les sous-options de choix des utilisateurs deviennent disponibles. Choisissez d'importer :

- **tous les utilisateurs de la base source**. Si parmi les utilisateurs certains dérivent de modèles, ceux-ci sont aussi importés ;

- **les utilisateurs dérivés d'un modèle donné**. Si ce choix est sélectionné, alors le choix du modèle parmi tous les modèles présents dans la base source devient disponible. Ce modèle est aussi importé.

Vous pouvez aussi choisir d'importer tous les modèles de la base.

4. La page suivante permet de choisir les utilisateurs spéciaux à importer, à savoir :

- les comptes de recouvrement ;
- le signataire de politiques de sécurité. Une base ne pouvant contenir qu'un seul signataire de politiques de sécurité, le signataire de la base source ne sera pas importé si la base à mettre à jour en contient déjà un.

5. La page suivante est la dernière page précédant l'opération de mise à jour. Vous êtes invité à relire les informations collectées.

Cliquez sur **Terminer** pour lancer la mise à jour.

Cette opération peut être longue, suivant le nombre d'utilisateurs à importer.

La dernière page de l'assistant affiche en temps réel les opérations en cours et effectuées.

Notez que si vous annulez le processus, toutes les opérations déjà effectuées sont annulées et la base revient à son état initial.

Un fichier de journalisation est généré en parallèle et fournit des informations plus détaillées.

Ce fichier de journalisation, de nom *BaseUpgrade.txt*, est créé dans le dossier des journaux (voir la section Journalisation). Il peut être ouvert directement depuis l'assistant grâce au bouton **Ouvrir le fichier de journalisation**.

> **NOTE**
> Un message de mise en garde est affiché dans l'arbre et dans le journal si l'importation des fichiers listes d'un utilisateur ou d'un modèle n'a pu être effectuée. Prenez garde à remédier à l'absence de ces fichiers dans l'arborescence de la base destination, car la diffusion des utilisateurs concernés, ou des utilisateurs dérivant des modèles concernés, échouera à cause de l'absence de ces fichiers.

5.7 Ouverture/Fermeture de session sur une base

Pour travailler sur une base de données, vous devez préalablement ouvrir une session sur cette base.

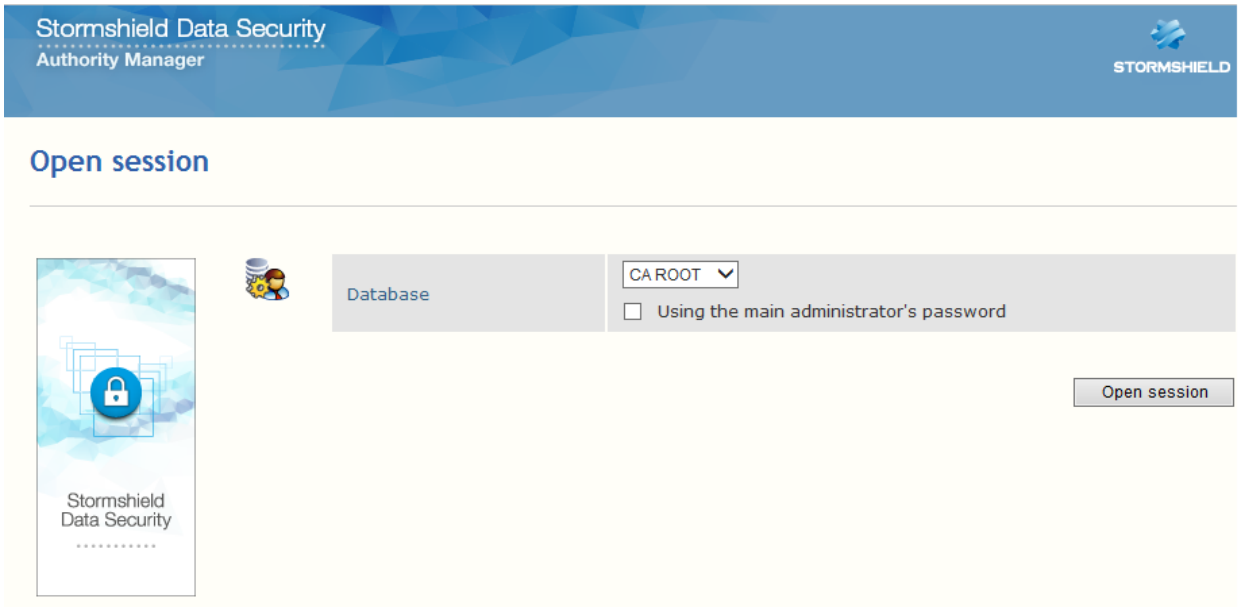
5.7.1 Ouverture de session sur une base

Pour ouvrir une session sur une base de données, saisissez l'URL `<manager_root_url>/OpenSession` où `<manager_root_url>` est l'URL racine définie à la section URL d'accès au serveur .

Elle propose la liste des bases démarrées (section Démarrage/Arrêt d'une base de données).

Lancez votre authentification pour la base sélectionnée en appuyant sur le bouton **Ouvrir**.

Si, pour la base sélectionnée, l'ouverture d'une session à l'aide du mot de passe de l'administrateur principal a été autorisée lors de sa création (voir la section Assistant de création), une case à cocher proposant ce mode d'authentification (voir la section Administrateur principal et autres administrateurs) apparaît.



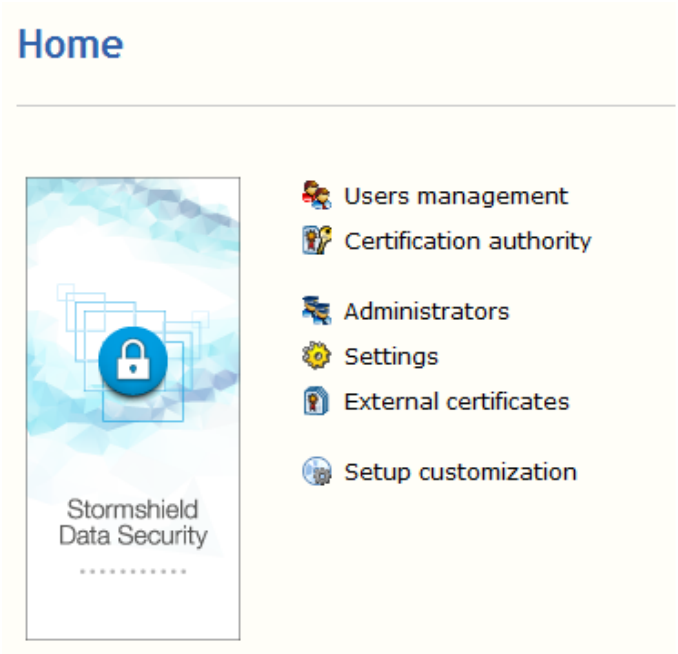
Cette session est automatiquement fermée par Stormshield Data Authority Manager au bout d'une durée d'inactivité de 15 minutes par défaut. Cette durée est modifiable dans le fichier *manager.ini* (voir la section Session).

5.7.2 Page d'accueil

La page d'accueil est la page centrale de Stormshield Data Authority Manager.

Elle propose :

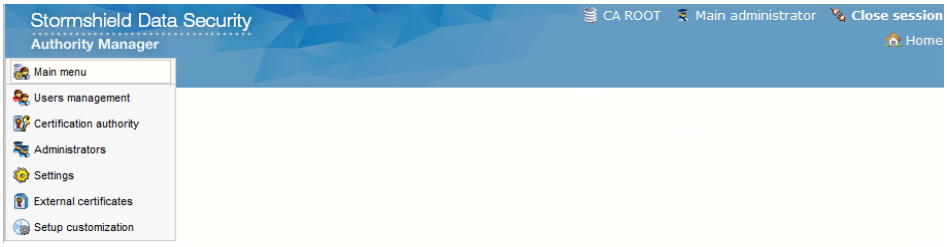
- un lien vers la gestion des utilisateurs (section Page Liste des utilisateurs) ;
- un lien vers l'autorité de certification (section Fonctionnement d'une autorité de certification) ;
- un lien vers la gestion des administrateurs de la base (section Page Liste des administrateurs) ;
- un lien vers les paramètres généraux de la base (section Page Paramètres) ;
- un lien vers la gestion des certificats externes à la base (section Autres certificats externes) ;
- création d'une procédure d'installation personnalisée (section Personnalisation de l'installation).



5.7.3 Fermeture de session sur la base

Le bandeau en haut de chaque page contient :

- le libellé de la base ;
- le libellé de l'administrateur authentifié ;
- un lien qui permet de fermer la session sur la base ;
- une liste de liens de navigation du type "Vous êtes ici" ;
- un menu déroulant qui reprend les liens de la page d'accueil.



En cliquant sur le lien **Fermer la session**, vous fermez votre session. La page de compte rendu qui s'affiche rappelle le libellé de la base, le nom de l'administrateur authentifié, et contient un lien vers la page d'ouverture d'une session.

Vous ne pouvez plus effectuer d'opération sur la base tant que vous ne vous êtes pas de nouveau authentifié.

5.8 Saisie des paramètres d'une base de données

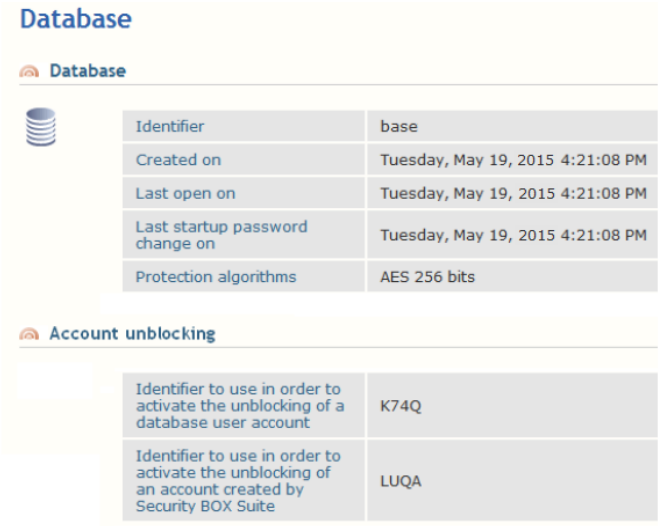
5.8.1 Page Paramètres

Pour consulter ou éditer les paramètres d'une base de données, ouvrez une session sur cette base et cliquez sur le lien **Paramètres** de la page **Accueil** (voir la section Page d'accueil) ou dans le menu déroulant. Elle affiche un menu d'opérations qui permet de :

- d'accéder à la page contenant les données propres à la base (voir les sections Page Base de données, Modification du mot de passe de démarrage et Modification du mot de passe de l'administrateur principal) ;
- consulter et modifier :
- les paramètres qui définissent les échanges entre Stormshield Data Authority Manager et un annuaire LDAP (section Configuration LDAP),
- les paramètres du serveur de courrier sortant pour les e-mails (voir la section Serveur de courrier sortant),
- et les paramètres des modèles de certificats (voir la section Modèles de certificats);
- consulter et modifier :
- les paramètres de gestion des utilisateurs (voir la section Gestion des utilisateurs),
- les paramètres de configuration des composants (voir la section Paramètres de la configuration des composants),
- et les autorités de certification externes (voir la section Autorités de certification externes) ;
- consulter et modifier les paramètres de l'autorité de certification (section Paramètres de gestion des certificats) et des modèles de certificats (section Modèles de certificats).

5.8.2 Page Base de données

Pour afficher les données spécifiques à la base, cliquer sur le lien **Base de données** dans la page **Paramètres** (voir la section Page Paramètres) ou dans le menu déroulant principal.



Les deux identifiants fournis dans cette page permettent d'activer les deux fonctionnalités de déblocage de compte « à distance » (voir la section Déblocage de compte à distance). L'identifiant doit être communiqué par l'utilisateur avant d'entreprendre l'opération de déblocage correspondante, afin de vérifier que le compte à débloquer est bien lié à la base sur laquelle la session est ouverte. Ils sont indiqués ici afin de vous aider à retrouver le lien entre les utilisateurs diffusés et la base de données.

Ce besoin est surtout présent pour les comptes créés par Stormshield Data Security à partir d'un master issu de la base de données (voir la section Diffusion d'un master), dans la mesure où vous utilisez plusieurs base de données.

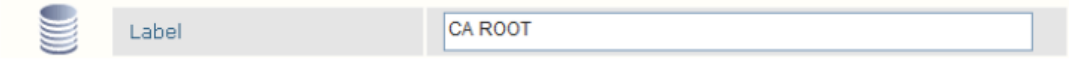
Dans le bandeau en haut de la page, un menu est proposé :

- dans l'onglet *Propriétés*, vous accédez aux propriétés de la base (voir la section Propriétés de la base de données) ;
- dans l'onglet *Opérations*, vous pouvez :
  - modifier le mot de passe de démarrage (voir la section Modification du mot de passe de démarrage) ;
  - modifier le mot de passe de l'administrateur principal (voir la section Modification du mot de passe de l'administrateur principal).

5.8.3 Propriétés de la base de données

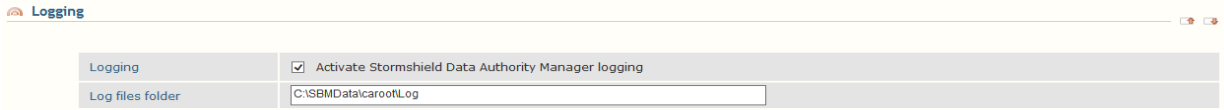
Cette page est accessible à partir du menu déroulant **Propriétés** de la page **Base de données** (voir la section Page Base de données) ou à partir du menu déroulant principal.

Libellé de la base



Le libellé de la base qui a été défini lors de sa création peut être modifié.

Journalisation



Une case à cocher permet d'activer ou non la journalisation des actions effectuées sur la base de données. Si vous l'activez, saisissez le chemin complet du dossier dans lequel sera créé le fichier de journalisation. Ce fichier a le même nom que la base de données avec l'extension .txt. Lors de chaque action, une ligne est ajoutée au fichier. Elle contient :

- la date et l'heure ;
- le nom de la machine ;
- le nom de l'utilisateur Windows ;
- le nom de la base ou le nom de l'utilisateur sur lequel s'applique l'action ;
- un descriptif de l'action effectuée.

Ce dossier peut également contenir le fichier de journalisation de mise à jour de base de données, il est nommé *BaseUpgrade.txt*.

NOTE
Stormshield Data Authority Manager ne se charge pas de vider le fichier de journalisation.

5.8.4 Modification du mot de passe de démarrage

Cette page vous permet de modifier le mot de passe de démarrage. Elle est accessible en cliquant sur le lien **Modifier le mot de passe de démarrage** du menu déroulant **Opérations** (voir la section Page Base de données).

Le mot de passe de démarrage est exigé lors du démarrage et de l'arrêt de la base (section Démarrage/Arrêt d'une base de données). Il est défini lors de son initialisation (Saisie du mot de passe de démarrage).

5.8.5 Modification du mot de passe de l'administrateur principal

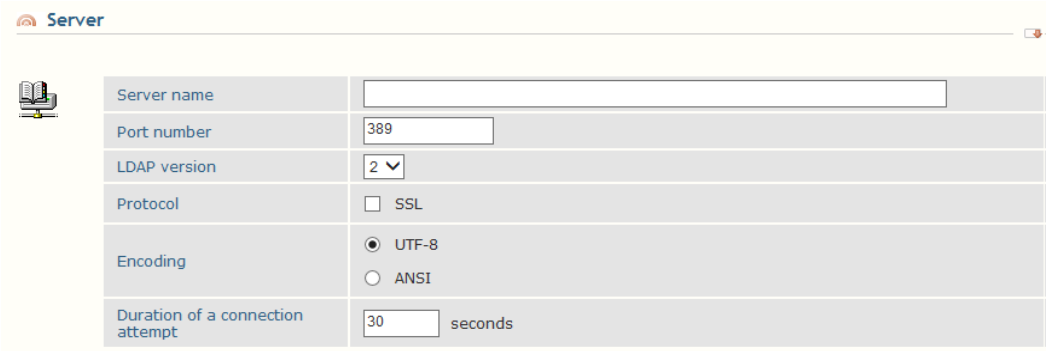
Cette page permet de modifier le mot de passe de l'administrateur principal. Elle est accessible en cliquant sur le lien **Mot de passe de l'administrateur principal** du menu déroulant **Opérations** (section Page Paramètres).

Le mot de passe de l'administrateur principal est exigé lors de l'ouverture d'une session sur la base "à l'aide du mot de passe" (section Ouverture de session sur une base et section Administrateur principal et autres administrateurs).

5.8.6 Configuration LDAP

La page des paramètres LDAP est accessible à partir de la page **Paramètres** (voir la section Page Paramètres) ou à partir du menu déroulant principal.

Serveur LDAP

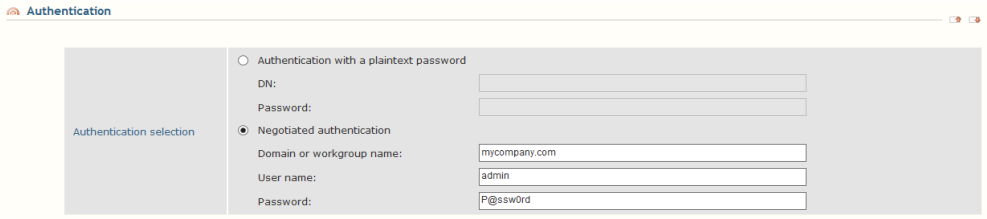


Ces paramètres définissent le serveur LDAP auquel doit se connecter Stormshield Data Authority Manager lors de chaque opération LDAP.

Vous pouvez choisir de mettre en œuvre le protocole SSL, et saisir une durée maximale d'attente lors d'une tentative de connexion. Pour plus d'informations sur ce sujet, référez-vous à l'*Annexe C. Configuration LDAPS* du *Guide d'administration* Stormshield Data Security.

Vous devez sélectionner l'encodage utilisé par le serveur LDAP : ANSI ou UTF-8. Stormshield Data Authority Manager utilisera cet encodage pour transmettre les requêtes au serveur, puis pour lire les données retournées par celui-ci.

Authentification

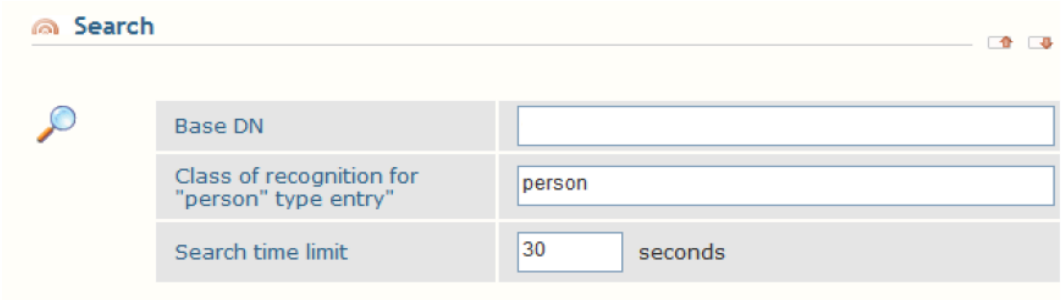


Vous pouvez vous connecter au serveur LDAP avec :

- Un login en saisissant un DN et un mot de passe. Si ces champs ne sont pas renseignés la connexion est anonyme.
- En effectuant une authentification négociée : l'authentification est effectuée avec la méthode la plus appropriée parmi celles disponibles sur le serveur. Vous devez saisir les identifiants à utiliser pour l'authentification : domaine ou workgroup (facultatif), nom d'utilisateur et mot de passe. L'authentification en mode NTLM est gérée.

NOTE
Si le nom ou le mot de passe est absent, l'authentification est effectuée avec les identifiants de « l'utilisateur réseau » sous lequel tourne le serveur Web.

Recherche

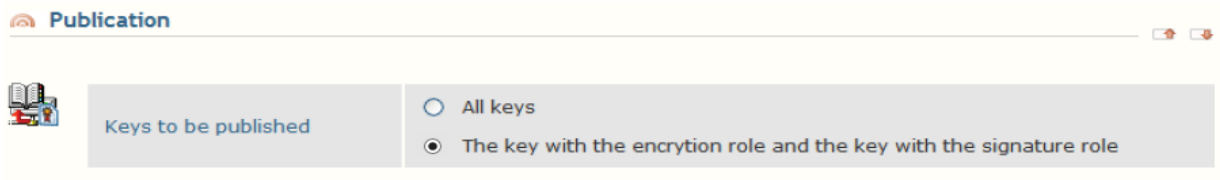


Vous saisissez ici des données qui seront proposées par défaut dans les critères de recherche des entrées dans l'annuaire LDAP (voir la section Association d'un utilisateur à une entrée LDAP) :

- le DN de base ;
- le nom de la classe qui sera utilisé pour constituer le filtre de recherche des entrées associées à des utilisateurs (classe standard de type "personne" (ayant pour valeur "person"), ou héritée).

Vous pouvez aussi fixer une durée maximale d'attente d'une requête de recherche soumise à l'annuaire.

Publication



Lors de l'opération de publication sur le serveur LDAP des certificats des utilisateurs, l'administrateur choisit, à l'aide de ce paramètre, l'une de ces deux options :

- publier le certificat courant de toutes les clés de l'utilisateur ;
- publier uniquement le certificat courant de la clé qui a le rôle de chiffrement et le certificat courant de la clé qui a le rôle de signature.

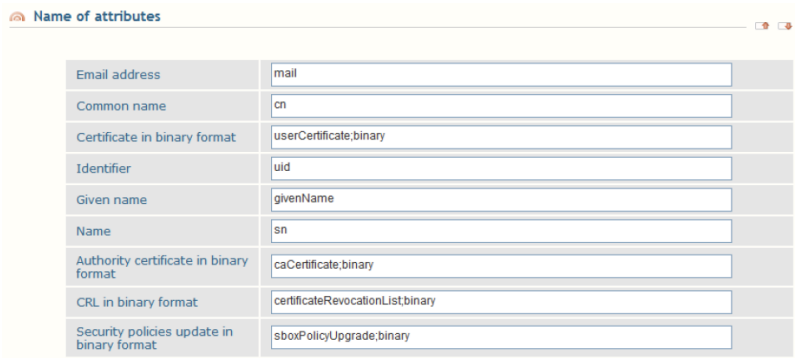
Publication des nouveaux certificats

Vous pouvez saisir le masque de résolution du DN LDAP des utilisateurs, qui sera proposé lors de la création d'un utilisateur, et qui sera utilisé lors de la publication de ses certificats.

Il doit être un DN LDAP dans lequel vous pouvez inclure les tags <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>, <SecurityBoxUserId>.

Lors de la résolution du masque, ces tags seront remplacés par les champs correspondants de l'identité de l'utilisateur.

Nom des attributs



Modifiez le nom de ces attributs LDAP s'ils sont différents des noms standards indiqués.

L'attribut de mise à jour des politiques de sécurité est propre aux produits Stormshield Data Security. L'annuaire LDAP doit être paramétré pour le supporter. Un exemple d'utilisation est décrit à la Section E.2, « Configuration annuaire LDAP ».

L'attribut CRL certificateRevocationList est standard : il est supporté par la classe cRLDistributionPoint (RFC 4523). L'entrée LDAP dans laquelle la CRL est publiée doit dériver de cette classe. Un exemple d'utilisation est décrit à la Section G.2, « Configuration annuaire LDAP ».

5.8.7 Serveur de courrier sortant

La page de paramétrage du serveur de courrier sortant (SMTP) est accessible à partir de la page **Paramètres** ou à partir du menu déroulant principal (voir la section Page Paramètres).

Il est nécessaire de paramétrer un serveur de courrier sortant pour avoir accès aux fonctionnalités de :

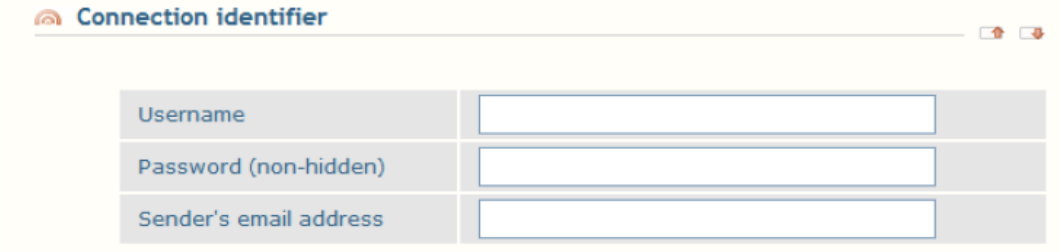
- diffusion de fichiers de mises à jour (*.usx*) ou de fichiers d'installation (*.usi*) par e-mail (voir la section Envoi par e-mail) ;
- notifications par e-mail (voir la section Notifications par e-mail).

Serveur SMTP

Spécifiez le nom et éventuellement le numéro de port du serveur SMTP qui acheminera les e-mails émis par Stormshield Data Authority Manager.

Le nom du serveur local est inscrit par le serveur distant dans l'entête RFC 822 du message (champ **Received: from <...>**) ; il ne doit évidemment contenir ni espaces, ni caractères spéciaux.

Identifiant de connexion et nom de l'expéditeur



Si le serveur SMTP ne requiert pas d'authentification, les champs **Nom d'utilisateur** et **Mot de passe** doivent rester vides. Ils doivent être renseignés si vous vous connectez à un serveur SMTP authentifié.

Stormshield Data Authority Manager supporte les mécanismes d'authentification LOGIN, PLAIN et CRAM-MD5.

L'adresse e-mail de l'expéditeur doit être obligatoirement remplie, quel que soit le serveur SMTP. Cette adresse peut respecter un des formats suivants :

- manager@company.com
- Stormshield Data Authority Manager<manager@company.com>

NOTE
Certains serveurs SMTP n'acceptent une connexion que si l'adresse e-mail de l'expéditeur fait partie d'une liste d'adresses e-mail autorisées.

5.8.8 Gestion des utilisateurs

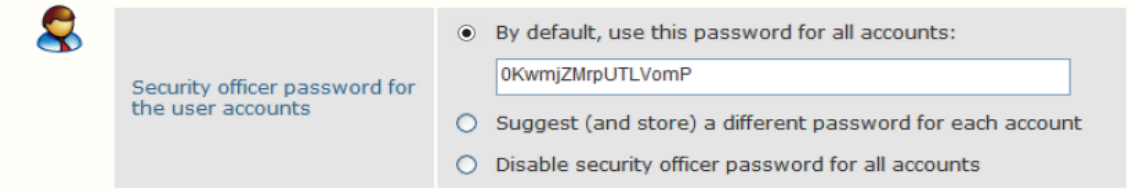
Cette page est accessible à partir du lien **Gestion des utilisateurs** sur la page **Paramètres** (voir la section Page Paramètres) ou à partir du menu déroulant principal.

A partir de ce menu, vous accédez aussi au déblocage de compte à distance (voir la section Déblocage de compte à distance).

Mot de passe de secours

Définissez une politique par défaut pour le mot de passe de secours qui sera mise en œuvre à chaque création avancée de compte (voir la section Création avancée) :

- en saisissant un mot de passe qui sera proposé à chaque création de compte ;
- en choisissant de proposer, lors de chaque création de compte, un mot de passe tiré aléatoirement ;
- en choisissant de condamner le mot de passe de secours.



NOTE
La fonctionnalité de déblocage de compte à distance (voir la section Déblocage de compte à distance) ne peut pas être mise en œuvre pour un compte diffusé avec un mot de passe de

secours de plus de 16 caractères. Cette limite est la longueur des mots de passe de secours aléatoires proposés par Stormshield Data Authority Manager.

Identité

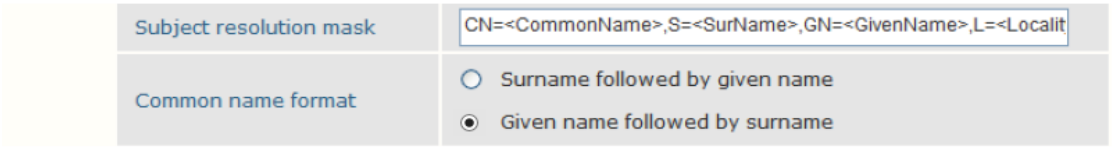
1. Définissez le masque de constitution du sujet utilisé lors de la génération et du renouvellement des certificats des utilisateurs.

Il doit être un DN (Distinguished Name) conforme à la norme RFC 2253, c'est à dire qu'il peut contenir les attributs suivants :

Masque de résolution de l'utilisateur	
Forme abrégée	Tag
CN	Common Name
S	Surname
GN	Given name
I	Initials
GQ	Generation
DNQ	DN Qualifier
C	Country
L	Locality
ST	State
O	Organization
OU	Org Unit
T	Title
E	P9 e-mail
N	Name
SN	Serial Number
STREET	Street Address
D	Description
BC	Business Category
POC	Postal Code
TN	Telephone Number
UID	X500 User id
MB	DPAT RFC822 Mailbox
DC	DPAT Domain Component
DNSA	DNS Record

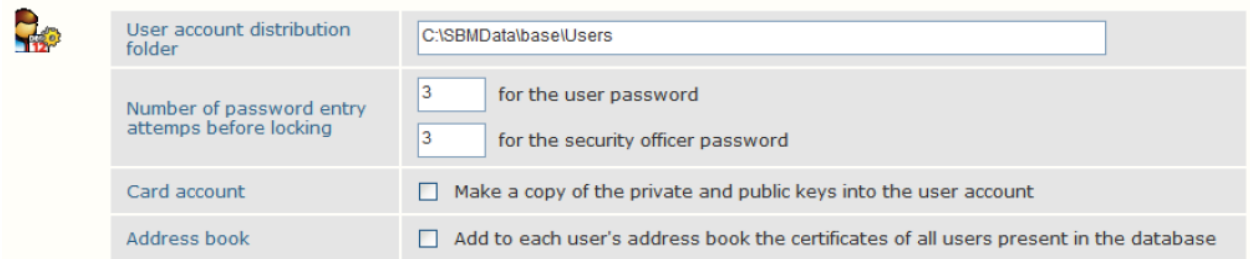
Stormshield Data Authority Manager permet de placer dans le masque les tags <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <e-mail>. Lors de la résolution du DN, ces tags sont remplacés par les champs correspondants de l'identité de l'utilisateur. Le résultat constitue le sujet présent dans le certificat.

2. Définissez la règle de construction du nom usuel d'un utilisateur.



Diffusion des comptes

1. Choisissez le dossier de génération des comptes utilisateur `<user_account_dir>`. Par défaut, il s'agit de `<sdam_data_install_dir>\SBMData\<base_id>\Users` dans lequel `<sdam_data_install_dir>` est le dossier de données et `<base_id>` est l'identifiant de la base.
2. Choisissez le nombre de tentatives de saisie du mot passe utilisateur et du mot de passe de secours avant blocage du compte.
3. Si, lors de la diffusion d'un compte carte, le fichier compte (fichier *.usr*) créé contient la clé publique et la clé privée.
4. Si l'annuaire généré lors de la diffusion contient uniquement le certificat de l'utilisateur et les certificats des autorités de la base, ou s'il contient en plus tous les certificats des utilisateurs de la base.

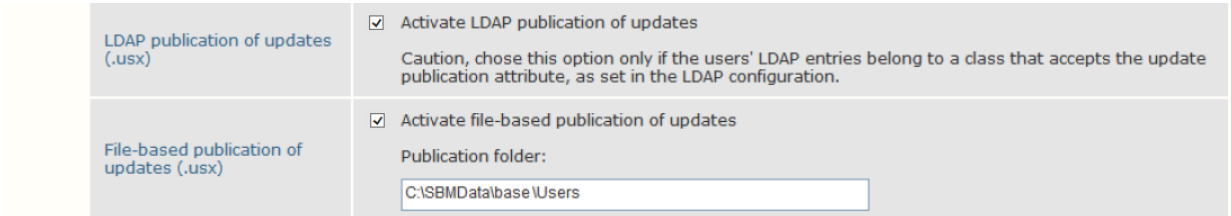


Publication des mises à jour de politiques de sécurité

Vous pouvez :

- activer la publication LDAP des mises à jour de politiques de sécurité (voir la section Diffusion des comptes utilisateurs).
- activer la publication par fichier des mises à jour de politiques de sécurité (voir la section Diffusion des comptes utilisateurs). Vous devez saisir le dossier dans lequel les fichiers d'installation seront copiés.

Pour plus d'informations à propos des fichiers de mise à jour de politiques de sécurité, reportez vous à la section Fichier de mise à jour de la politique de sécurité (.usx) .



Publication des fichiers d'installation

Vous pouvez activer la publication des fichiers d'installation (*.usi*). Lorsque cette option est activée, la publication est proposée dans la page de diffusion des comptes (voir la section Diffusion des comptes utilisateurs). Vous devez saisir le dossier dans lequel les fichiers d'installation seront copiés.

Pour plus d'informations à propos des fichiers d'installation, reportez vous à la section Fichier d'installation (.usi).

Importation, exportation et demande de certificats

Saisissez le dossier par défaut contenant les certificats à importer et les certificats exportés `<certs_dir>`. Par défaut, il s'agit de `<sdam_data_install_dir>\SBMData\<base_id>\Certs` dans lequel `<sdam_data_install_dir>` représente le répertoire de données et `<base_id>` est l'identifiant de la base.

Pour l'importation de certificats, vous pouvez autoriser l'importation de certificats dont les dates de début de validité sont antérieures à celles des certificats présents dans la base (voir la section Règles d'importation).

Pour l'exportation de certificats, positionnez les choix qui seront proposés par défaut :

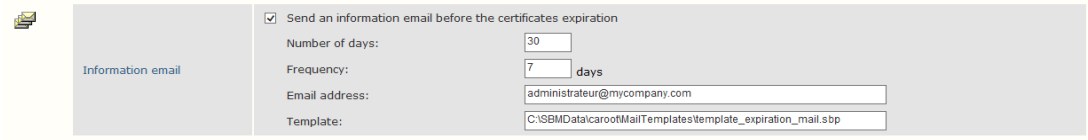
- ajouter ou non la parenté ;
- l'extension du fichier d'exportation de certificats multiples.

Saisissez le format qui sera :

- celui proposé par défaut pour l'exportation unitaire d'un certificat (voir la section Exportation de certificat) ;
- celui des exportations de certificat à partir de la page **Listes des utilisateurs** (voir la section Exportation de plusieurs certificats).

Notification par e-mail

Cette section vous permet d'activer et de paramétrer la notification d'expiration de certificat par e-mail (voir la section Notification d'expiration de certificat).



- la case à cocher sert à activer la fonctionnalité d'envoi ;
- le premier champ de saisie permet d'indiquer la période d'anticipation avant expiration d'un certificat : si la date du jour, augmentée de la durée indiquée dans le champ, est postérieure à la date d'expiration du certificat, ce dernier est alors signalé dans l'e-mail de notification ;

```
Si (date courante + Nombre jours) > (date expiration certificat) =>
Signaler certificat
```

- le second champ permet de définir la fréquence des recherches de certificats dans la base. Cette valeur devrait être inférieure à la période d'anticipation pour ne pas risquer d'omettre de certificats dont l'expiration est imminente. La recherche de certificats, si elle s'est révélée fructueuse, est suivie de l'envoi de l'e-mail ;
- le troisième champ permet de renseigner les coordonnées de la boite e-mail du destinataire du message de notification ;
- le dernier champ permet de spécifier l'emplacement du fichier utilisé comme modèle pour la génération de l'e-mail. Il comporte des informations de formatage pour le mode texte et pour le mode html.

5.8.9 Paramètres de la configuration des composants

La page de paramétrage de la configuration des composants est accessible à partir de la page **Paramètres** (voir la section Page Paramètres) ou à partir du menu déroulant principal en cliquant sur le lien **Configuration des composants**.

Les paramètres spécifiés dans cette page ne sont pas directement inclus dans les comptes utilisateurs diffusés, ils servent à faciliter le remplissage des pages de configuration des composants (section Accès aux configurations d'un utilisateur) des utilisateurs.

Stormshield Data Kernel : téléchargement des politiques de sécurité

Pour chaque masque de résolution de point de distribution spécifié, un bouton est ajouté à la page de configuration du téléchargement des politiques de sécurité des utilisateurs ou modèles. Ce bouton permet d'ajouter automatiquement le masque de point de distribution à la liste des points de distribution.

Le masque, une fois ajouté à la liste des points de distribution, est résolu lors de la diffusion de l'utilisateur.

Le masque de point de distribution LDAP doit être une URI LDAP valide, dans laquelle vous pouvez inclure les tags `<LdapHost>`, `<LdapPort>`, `<LdapDn>`, `<UserId>`. Lors de la résolution du masque, les tags sont remplacés par le paramètre LDAP correspondant (section Configuration LDAP) et par l'identifiant de l'utilisateur diffusé. Exemple :

```
ldap://<LdapHost>:<LdapPort>/<LdapDn>?SboxPolicyUpgrade;binary
```

Le masque de point de distribution HTTP doit être une URI valide, dans laquelle vous pouvez inclure le tag `<UserId>`. Lors de la résolution du masque, le tag est remplacé par l'identifiant de l'utilisateur diffusé. Exemple :

```
http://server/SecurityPolicies/<UserId>.usx
```

Pour plus d'information, voir la sectionConfiguration du composant Téléchargement des politiques de sécurité.

5.8.10 Paramètres de gestion des certificats

Cette page est accessible à partir de la page **Paramètres** (section Page Paramètres) ou à partir du menu déroulant principal.

Autorité de certification

Vous pouvez spécifier le masque de constitution du sujet de l'autorité de certification.

Ce masque sera utilisé lors du renouvellement du certificat de l'autorité si vous choisissez de renouveler le sujet (pour plus d'informations, voir la section Page Clé et certificat de l'autorité).

Il doit être un DN (Distinguished Name) conforme à la norme RFC 2253, c'est-à-dire qu'il peut contenir les attributs suivants :

Masque de l'autorité de certification	
Forme abrégée	Tag
CN	Common Name
S	Surname
GN	Given name
I	Initials
GQ	Generation
DNQ	DN Qualifier
C	Country
L	Locality
ST	State
O	Organization
OU	Org Unit
T	Title
E	P9 Email
N	Name
SN	Serial Number
STREET	Street Address
D	Description
BC	Business Category
POC	Postal Code

Masque de l'autorité de certification	
TN	Telephone Number
UID	X500 User id
MB	DPAT RFC822 Mailbox
DC	DPAT Domain Component
DNSA	DNS Record

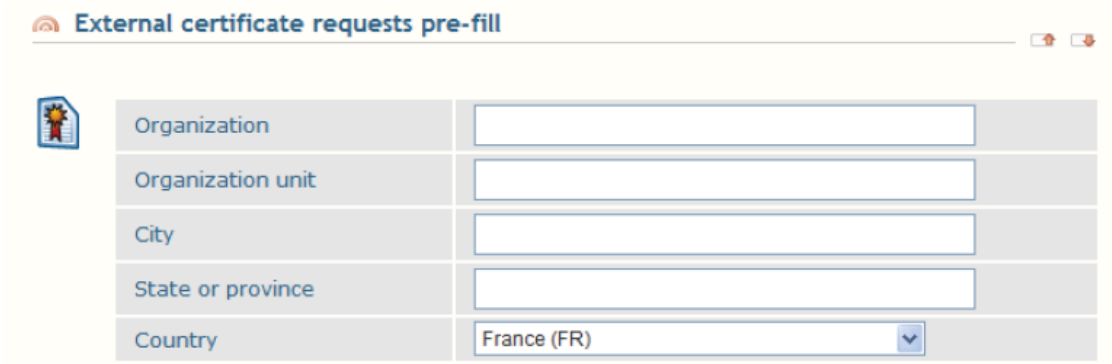
Stormshield Data Authority Manager permet de placer dans le masque les tags <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>.

Lors de la résolution du DN, ces tags seront remplacés par les champs correspondants de l'identité de l'autorité de certification. Le résultat constituera le sujet présent dans la demande de certificat.

Pré-remplissage des demandes de certificats externes

Pour simplifier le remplissage des demandes de certificats externes, vous pouvez spécifier des valeurs par défaut pour pré-remplir les champs **Organisation**, **Unité**, **Ville**, **Etat** et **Pays** de l'identité des demandes de certificats externes.

Ces valeurs seront utilisées dans les pages de demandes (voir les sections Remplir et soumettre une demande de certificat et Remplir et soumettre une demande de certificat avancé).



Certificats générés

1. Choisissez la durée par défaut d'un certificat.

Cette durée n'est utilisée que lorsque aucun modèle de certificat ne s'applique, c'est-à-dire lorsque l'utilisateur a demandé un certificat avancé et personnalisé.

2. Choisissez la taille de clé proposée par défaut aux CSP (Cryptographic Service Providers).

Lorsqu'un CSP ne propose pas la taille de clé choisie, la taille la plus proche supportée par le CSP sera sélectionnée.

Pour plus d'informations sur le mécanisme de génération de clé par les CSP, reportez-vous à la section Remplir et soumettre une demande de certificat.

3. Choisissez l'algorithme de signature de certificat.

Adoptez de préférence l'algorithme "SHA-512 et RSA". Si vous craignez de rencontrer des problèmes d'interopérabilité avec des solutions ne supportant pas le SHA-512, choisissez "SHA-256 et RSA".

4. Choisissez l'emplacement de l'adresse e-mail dans les certificats standards :

- laissez l'adresse e-mail dans l'identité uniquement ;
- copiez l'adresse e-mail de l'identité dans le champ **Subject Alternative Name** du certificat ;
- déplacez l'adresse e-mail de l'identité dans le champ **Subject Alternative Name** du certificat.

Si vous choisissez de déplacer l'adresse e-mail de l'identité dans le champ **Subject Alternative Name**, pour obtenir le fonctionnement souhaité, vous devez veiller à :

- pour la génération ou le renouvellement des certificats des utilisateurs, ne pas positionner l'adresse e-mail dans le masque de résolution du sujet défini dans la section Identité (`E=<Email>` présent par défaut) ;
- lors de la validation d'une demande de certificat (voir la section Demande de certificat), ne pas conserver la valeur binaire du sujet issue de la structure *PKCS#10*, si cette valeur contient l'e-mail. Vous devez utiliser alors le sujet proposé en remplacement

5. Choisissez le masque de constitution du DN LDAP des certificats externes.

Ce masque sera utilisé lors de la validation des demandes de certificats externes, si vous avez paramétré un serveur LDAP (section Configuration LDAP).

Il doit être un filtre de recherche LDAP valide, dans lequel vous pouvez inclure les tags <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>.

Lors de la résolution du DN, ces tags seront remplacés par les champs correspondants du sujet ou du champ **Subject Alternative Name** du certificat généré. Le résultat constituera le DN proposé pour publier le certificat.

Si vous souhaitez effectuer par défaut une recherche par critère pour trouver l'entrée LDAP de publication, vous pouvez laisser le masque de résolution de DN vide.

6. Choisissez le masque de constitution du filtre de recherche de l'entrée LDAP.

Ce masque sera utilisé lors de la validation des demandes de certificats externes, si vous avez paramétré un serveur LDAP (section Configuration LDAP).

Il doit être un filtre de recherche LDAP valide, dans lequel vous pouvez inclure les tags <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>.

Lors de la résolution du DN, ces tags seront remplacés par les champs correspondants du sujet ou du champ Subject Alternative Name du certificat généré. Le résultat constituera le filtre proposé pour rechercher l'entrée LDAP de publication.

7. Choisissez l'action par défaut sur les certificats déjà présents sur le serveur LDAP :

- les conserver ;
- les supprimer ;
- remplacer les certificats ayant les mêmes usages et le même émetteur.

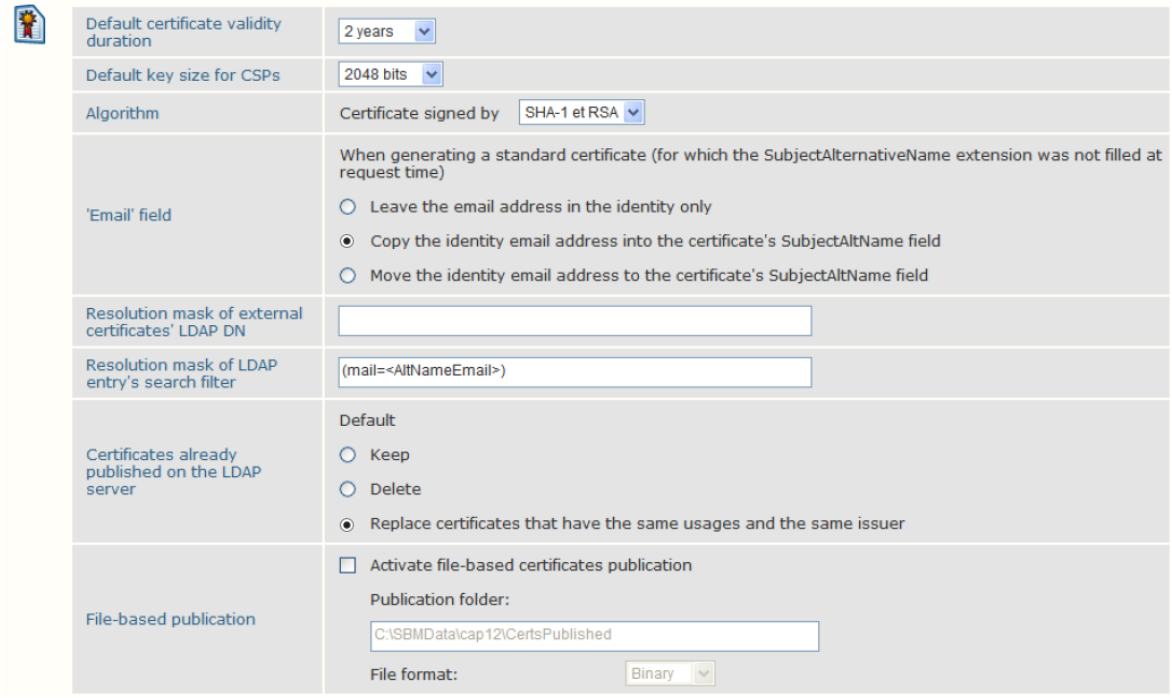
Pour plus d'informations, reportez-vous à la section Publication d'un certificat.

8. Choisissez l'activation et le paramétrage de la publication par fichier.

Activer la publication par fichier ajoute une option à toutes les publications de certificat.

Cette option consiste en l'écriture du certificat dans un fichier placé dans un dossier à spécifier. Le format du fichier à écrire (binaire ou "base 64") doit aussi être spécifié.

Le dossier de publication peut être destiné à être partagé, à être archivé ou encore être un dossier de documents d'un serveur web.



Listes de révocation (CRLs)

Pour plus d'informations sur la publication et le téléchargement des CRL, reportez-vous à l'annexe Publication et téléchargement des CRL.

1. Choisissez la durée de validité d'une CRL, en heures.

Elle sera utilisée pour calculer la date "Next Update" qui sera présente dans la CRL.

Si vous activez le service de génération automatique de CRLs, il est cohérent de choisir une durée de validité de CRL égale à la fréquence de génération.

2. Définissez le DN LDAP de publication des CRLs.

Le fait de remplir un DN active la publication automatique sur l'annuaire LDAP des CRLs générées ; à l'inverse, un DN vide désactive cette publication.

3. Définissez l'emplacement de génération de la CRL courante.

Saisissez ici le nom de fichier complet, incluant le dossier, du fichier dans lequel sera écrite la CRL courante.

A chaque génération de CRL, ce fichier sera remplacé par la nouvelle CRL courante.

4. Choisissez le dossier d'archivage des CRLs.

Ce dossier est facultatif. Si vous le remplissez, chaque nouvelle CRL générée sera copiée dans ce dossier. Elle n'écrasera pas d'anciennes CRLs, car le numéro de série de la CRL est utilisé dans le nom du fichier.

5. Définissez la génération de CRL par défaut à chaque révocation.

La génération de CRL est proposée à chaque révocation. Cette option permet de la sélectionner par défaut.

6. Définissez l'inclusion des certificats périmés dans la CRL.

D'après la norme RFC 3280 chapitre 5, une CRL liste les certificats non-périmés qui ont été révoqués. Donc, par défaut, un certificat révoqué ne sera pas inclus dans les CRLs postérieures à sa date de péremption. Cette option permet d'inclure également dans la CRL les certificats révoqués périmés.

7. Choisissez les points de distribution de CRLs

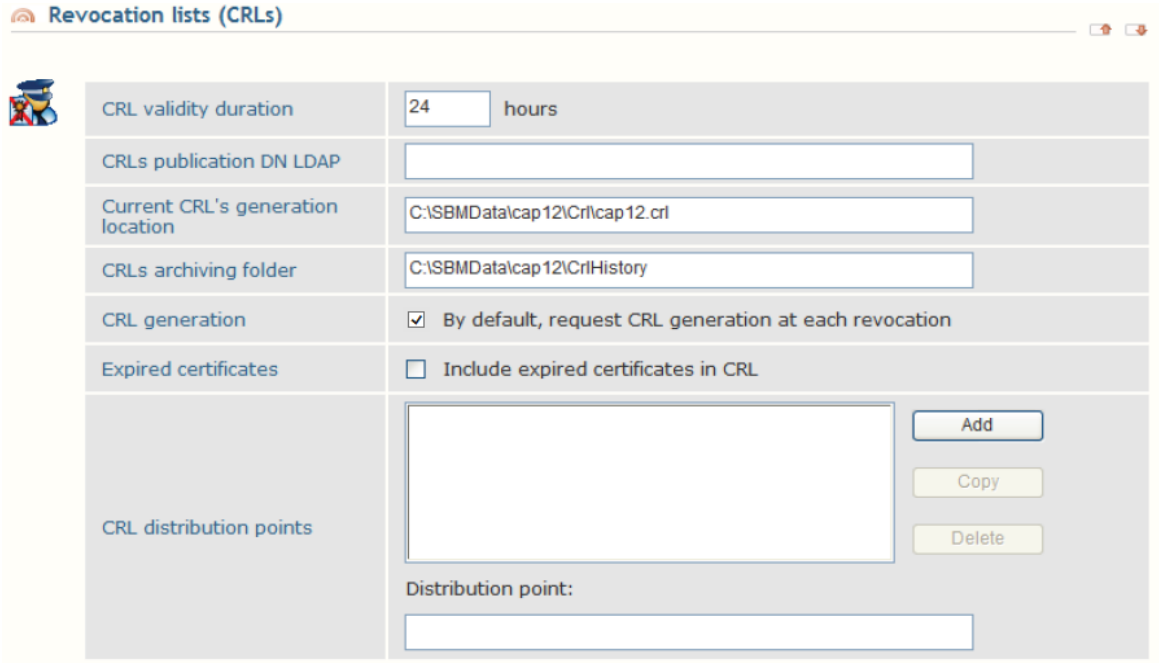
Les points de distribution de CRLs seront automatiquement inclus dans le champ CrlDistributionPoint de tous les certificats générés.

C'est à vous de les remplir en cohérence avec les paramètres de publication de CRLs et l'organisation de votre serveur.

Les protocoles supportés sont http, https, ldap, ldaps et file. Le contrôle syntaxique du point de distribution impose donc que celui-ci commence par http://, https://, ldap://, ldaps:// ou file://.

Exemple de points de distribution valides utilisant le protocole file :

- chemin local : **file:///c:/folder/file.crl**
- chemin réseau : **file://server/sharing/folder/file.crl**



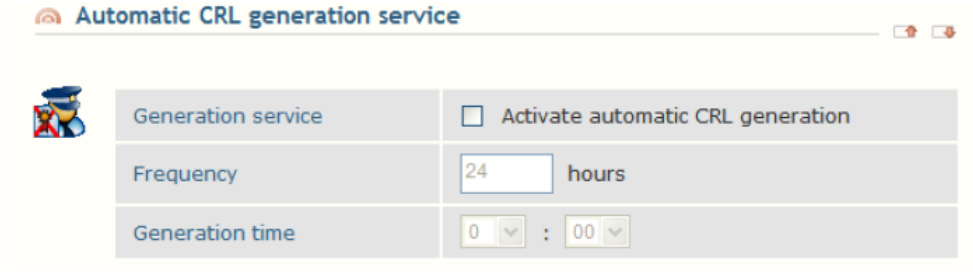
NOTE
L'adresse du répondeur OCSP utilisée dans la vérification est celle inscrite dans le certificat. Vous ne pouvez pas ajouter ou modifier cette adresse dans le contrôleur de révocation.

Service de génération automatique des CRLs

Si vous activez le service de génération automatique des CRLs, Stormshield Data Authority Manager génèrera automatiquement les listes de révocations à la fréquence et à l'heure que vous souhaitez.

La fréquence est à saisir en heures.

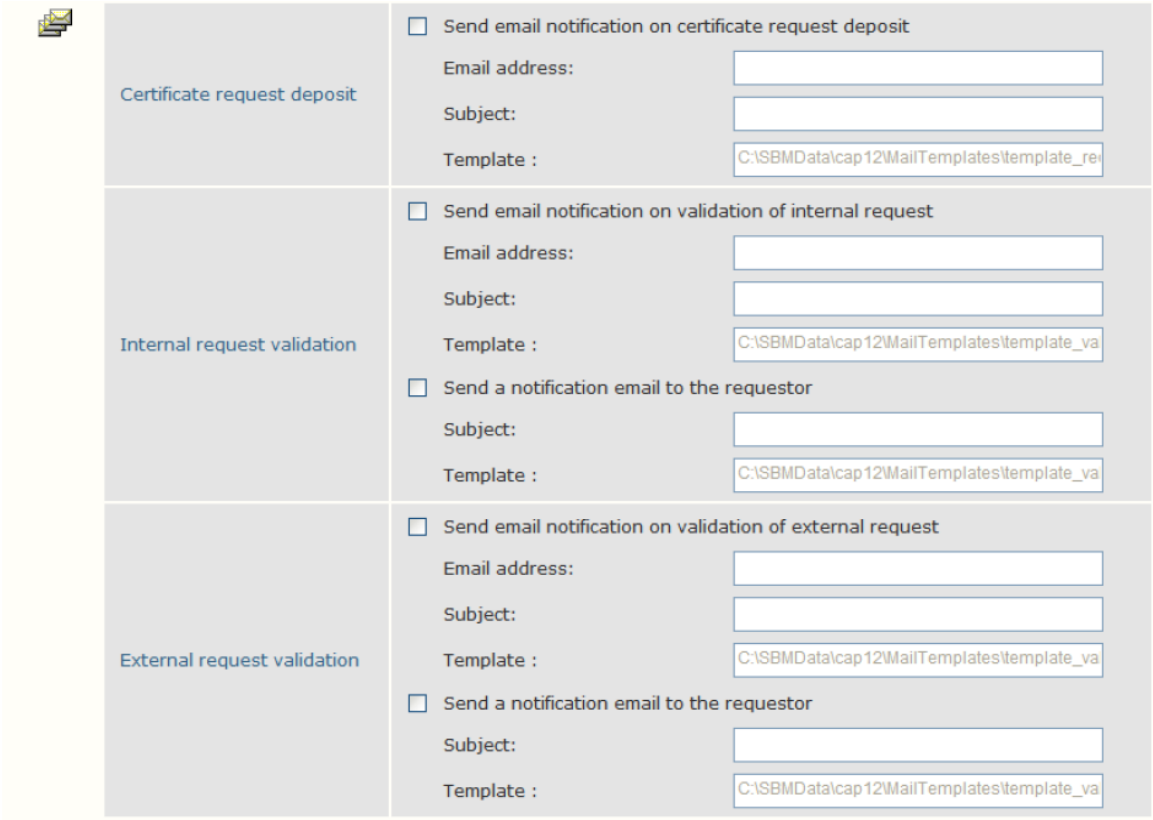
L'heure de génération est utilisée pour initialiser le service de génération, à chaque fois que vous démarrez la base ou que vous mettez à jour les paramètres de gestion des certificats. Ensuite, la fréquence est utilisée pour déterminer la prochaine date de génération.



Notifications par e-mail

Les notifications par e-mail offrent un moyen aux administrateurs de rester informés des opérations qui ont été effectuées, et aux utilisateurs de savoir que leurs demandes ont été traitées.

Dans Stormshield Data Authority Manager elles sont disponibles dès lors qu'un serveur de courrier sortant (SMTP) est paramétré (section Serveur de courrier sortant).



Pour chaque notification disponible, spécifiez :

- le sujet de l'e-mail ;
- le chemin complet d'un modèle d'e-mail (fichier *.sbp*).

Ce paramètre permet d'utiliser des modèles d'e-mail différents pour chaque base Stormshield Data Authority Manager. Vous pouvez en effet personnaliser les e-mails de notification en modifiant leur modèle. Si vous personnalisez un modèle, attention de conserver une structure MIME valide et d'utiliser exclusivement les tags disponibles dans le modèle original. Vous pouvez utiliser la balise
 pour effectuer des retours à la ligne ; elle doit être placée dans le texte saisi.

Pour les notifications destinées aux administrateurs, spécifiez également l'adresse e-mail de destination. Cette adresse peut respecter un des formats suivants :

- bob@company.com
- Alice <alice@company.com>

Un exemple d'utilisation est disponible dans l'annexe Renouvellement d'un certificat.

5.8.11 Modèles de certificats

Cette page est accessible à partir de la page **Paramètres** (section Page Paramètres) ou à partir du menu déroulant principal.

Les modèles de certificat permettent de générer facilement des certificats pour un usage donné.

Les modèles sont complètement paramétrables et leur nombre n'est pas limité. Par défaut, à l'installation de Stormshield Data Authority Manager, il en existe trois :

- certificat pour une clé de chiffrement (modèle standard) ;
- certificat pour une clé de signature (modèle standard) ;
- certificat d'autorité (modèle avancé).

Ces trois modèles par défaut peuvent être modifiés, mais ne peuvent pas être supprimés, car ils sont susceptibles d'être utilisés en interne par Stormshield Data Authority Manager.

Pour chaque modèle de certificat, choisissez :

1. Le nom du modèle.
2. La disponibilité du modèle dans une demande de certificat standard.

Les modèles disponibles dans une demande standard sont aussi appelés modèles standards. Ils seront également disponibles dans la création de comptes utilisateurs Stormshield Data Security (voir la section Opérations disponibles).

3. Les usages de la clé. Ils seront inscrits dans l'extension X.509 "Key Usage" du certificat.
4. Les usages étendus de la clé. Ils seront inscrits dans l'extension X.509 "Extended Key Usage" du certificat.
5. La durée de validité du certificat.
6. Le type de certificat (certificat d'autorité ou non).
7. La profondeur de transmission de la capacité de certification (autrement dit le nombre de sous-autorités autorisées), si le type de certificat est d'autorité.
8. L'inclusion de l'identifiant de la clé de l'autorité. Il sera inscrit dans l'extension X.509 "Authority Key Identifier" du certificat.

Il est conseillé d'inclure cet identifiant dans tous les certificats non-racines, car il permet d'établir de manière sûre la relation de parenté entre ce certificat et son autorité.

9. L'inclusion de l'identifiant de la clé du titulaire. Il sera inscrit dans l'extension X.509 "Subject Key Identifier" du certificat.

Il est conseillé d'inclure cet identifiant dans tous les certificats d'autorité, car il permettra d'établir de manière sûre la relation de parenté entre ce certificat et les certificats qu'il signera (si ces certificats ont un "Authority Key Identifier").

5.8.12 Autorités de certification externes

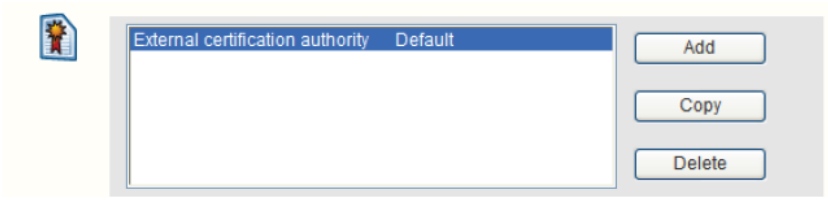
Pour la clé de l'autorité de certification et pour chaque clé de chaque utilisateur, même si certifiée par l'autorité de certification interne à la base, il est possible d'effectuer une demande de certificat à une autorité de certification externe (voir la section Demande de certificat).

La page de **gestion d'autorités de certification externes**, accessible à partir de la page **Paramètres** ou du menu déroulant principal, permet de définir une liste d'autorités de certification externes et de saisir pour chacune d'entre elles les paramètres d'accès associés.

A chaque clé est associée une autorité de certification externe. Vous pouvez modifier cette association dans la page **Propriétés** de la clé.

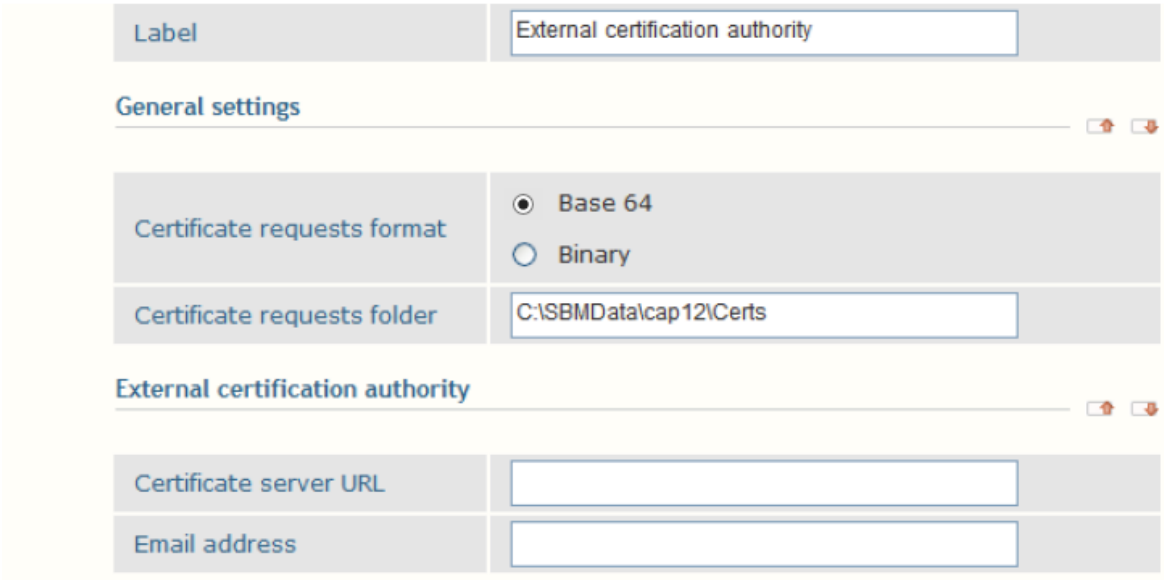
La page permettant d'effectuer la demande de certificat est pré-remplie à l'aide des données de l'autorité de certification externe associée à la clé (voir la section Création de demande). De même, ce sont ces données qui sont utilisées pour chaque clé lors de la création de plusieurs demandes en une seule opération (voir la section Création de plusieurs demandes).

Une autorité de certification externe par défaut est présente et ne peut être supprimée. Elle est associée à chaque clé certifiée par l'autorité de certification interne à la base. Ceci permet à l'administrateur d'effectuer une éventuelle demande de certificat à une autorité de certification externe si nécessaire.



Pour chaque autorité vous pouvez saisir :

- un libellé utilisé dans Stormshield Data Authority Manager pour identifier l'autorité ;
- le format de la demande de certificat (base 64 ou binaire) ;
- le dossier dans lequel sont créés les fichiers contenant les demandes de certificat, lorsque ce mode de diffusion est utilisé. Par défaut, il s'agit de `<sdam_data_install_dir>\SBMData\<base_id>\Certs` dans lequel `<sdam_data_install_dir>` représente le dossier de données et `<base_id>` est l'identifiant de la base ;
- une adresse e-mail et l'URL du serveur qui seront affichées comme valeurs par défaut lorsqu'une demande de certificat au format "base 64" est faite (voir la section Formats binaire et base 64) ;



- les paramètres d'un serveur Stormshield Data Authority Manager distant :

- l'URL racine `<manager_root_url>` du serveur Stormshield Data Authority Manager distant.
- l'identifiant de la base, présente sur ce serveur, qui contient l'autorité de certification à utiliser.
- le libellé du modèle de certificat, présent dans cette base, qui doit être utilisé pour générer le certificat.
- un "timeout" réseau en millisecondes.

Ces paramètres concernent les demandes qui sont soumises automatiquement au serveur de certification distant Stormshield Data Authority Manager (voir la section **Demande de certificat à un serveur Stormshield Data Authority Manager distant**).

6. Définition des administrateurs et de leurs rôles

Cette section décrit comment définir les administrateurs de bases de données et leurs rôles.

6.1 Introduction

Une base de données peut être gérée par plusieurs administrateurs physiques : chaque administrateur peut avoir des rôles différents, et doit disposer d'un compte Stormshield Data Security afin d'être authentifié de manière forte.

Un administrateur physique peut être un utilisateur dont le compte est géré dans la base de données : on parle alors d'administrateur "interne". Reportez-vous à la section **Ajout d'un administrateur interne à la base** pour définir un utilisateur comme administrateur interne.

Un administrateur physique peut également avoir un compte Stormshield Data Security non géré dans la base de données : on parle alors d'administrateur "externe", qui est défini et identifié à l'aide de son certificat, comme cela est expliqué à la section **Ajout d'un administrateur externe à la base**.

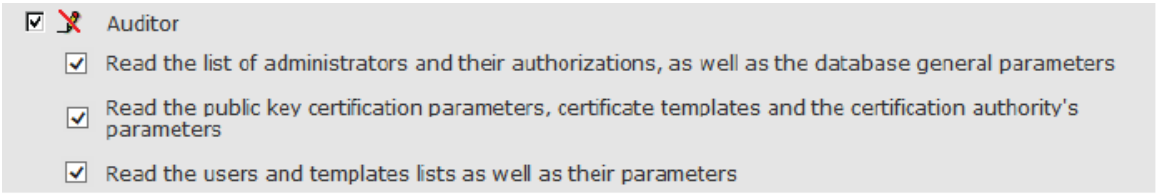
NOTE
Dans cette version du produit, la révocation d'un administrateur externe n'est pas contrôlée.

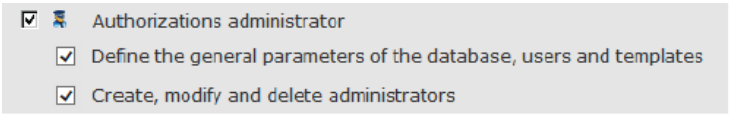
6.2 Autorisations

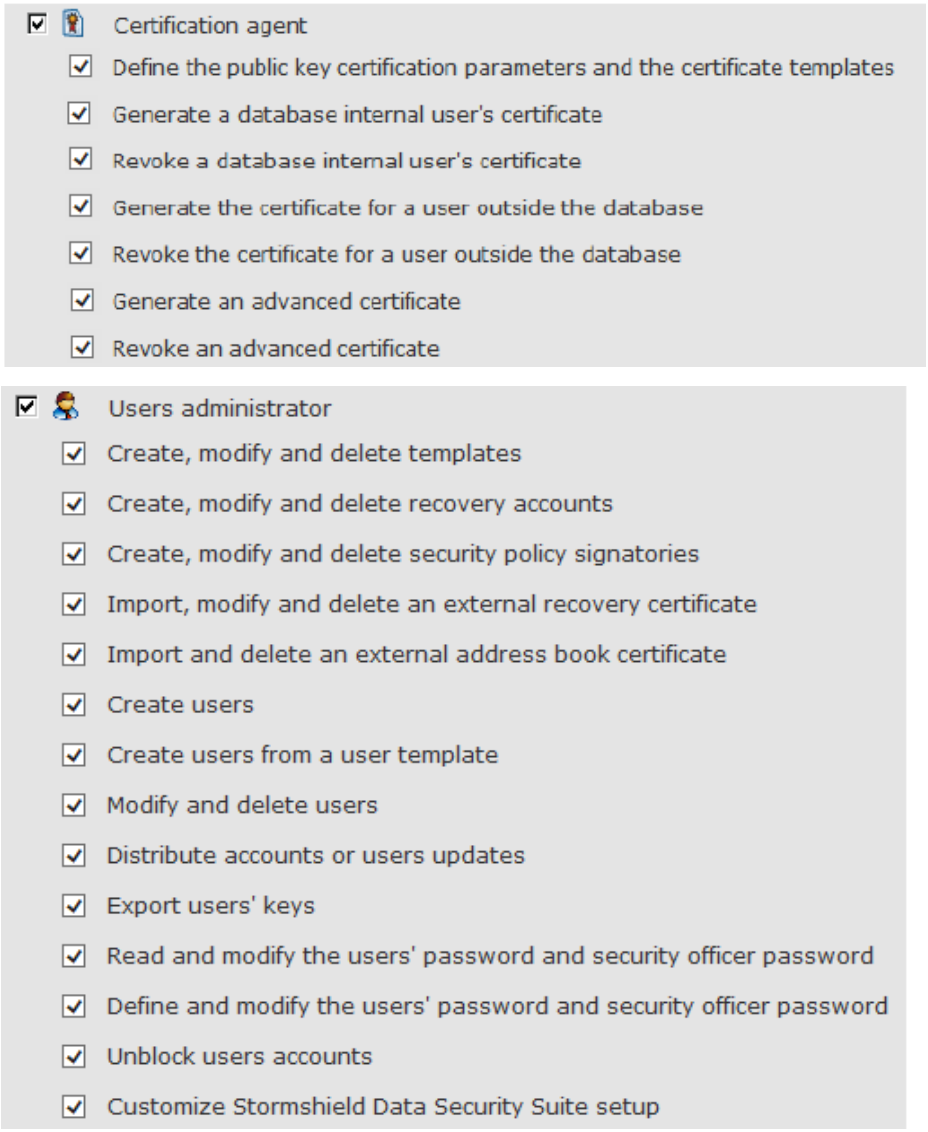
	Profil	L'administrateur peut principalement :
	Auditeur	• lire tous les paramètres • lire la liste des utilisateurs
	Administrateur des autorisations	• définir les administrateurs et leurs rôles
	Agent de certification	• générer / révoquer des certificats
	Administrateur des utilisateurs	• créer / modifier / diffuser des utilisateurs

Les autorisations de chaque profil sont détaillées dans les captures suivantes.

Les différentes options d'autorisation pour chaque profil sont décrites sur l'interface. Vous pouvez sélectionner une ou plusieurs autorisations par profil. Vous pouvez aussi sélectionner un ou plusieurs profils par administrateur.







6.3 Page Liste des administrateurs

Pour afficher la liste des administrateurs, dans la page d'accueil (voir la section Page d'accueil), cliquez sur le lien **Administrateurs**.

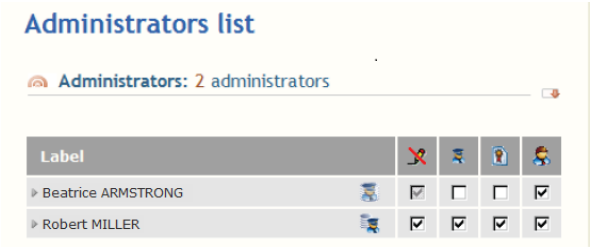
A partir du menu déroulant **Opérations** vous pouvez ajouter un administrateur externe (section Ajout d'un administrateur externe à la base).

La page affiche ensuite la liste des administrateurs. Pour chaque administrateur :

- la première colonne contient le libellé de l'administrateur (s'il est tronqué à l'affichage, il est visible en entier dans une bulle), ainsi qu'une icône indiquant le type d'administrateur :
- administrateur externe,
- administrateur interne ;
- les quatre colonnes suivantes résument les autorisations de l'administrateur. Pour chacun des quatre profils d'autorisations (section Autorisations), une case à cocher indique que l'administrateur a :

- tous les droits correspondant au profil ;
- certains droits correspondant au profil ;
- aucun droit correspondant au profil.

En cliquant sur le libellé de l'administrateur vous accédez à la page **Administrateur** qui affiche toutes les propriétés de l'administrateur.



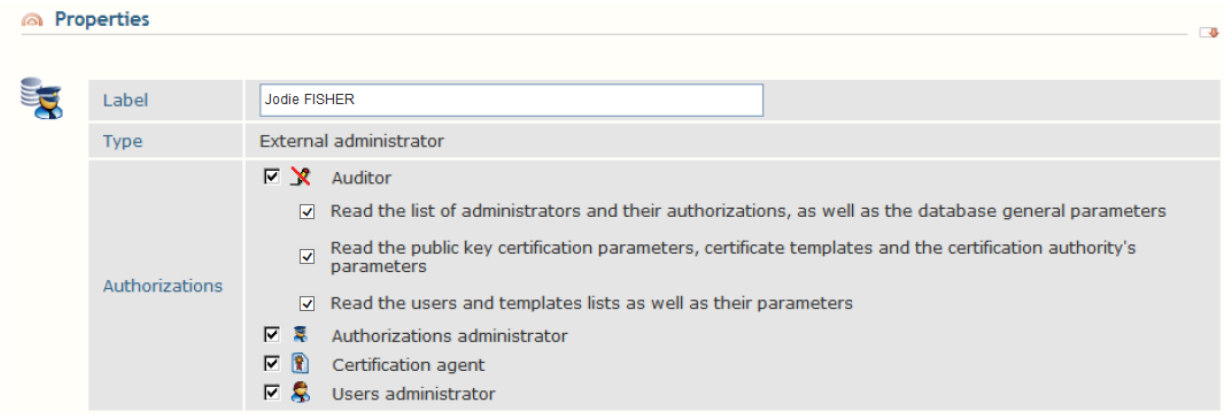
6.4 Page Administrateur

Cette page est accessible à partir de la page **Liste des administrateurs** (section Page Liste des administrateurs) en cliquant sur le libellé de l'administrateur.

Elle affiche les propriétés de l'administrateur :

- le libellé que vous pouvez modifier
- le type d'administrateur (externe ou interne)
- toutes les autorisations, divisées en quatre sections correspondant aux quatre profils d'autorisations. Chaque section peut être affichée ou masquée en cliquant sur le libellé du profil :
- cochez ou décochez chaque autorisation à l'aide des cases à cocher qui sont en face des autorisations
- cochez ou décochez toutes les autorisations correspondant à un profil à l'aide des cases à cocher qui sont en face des profils d'autorisations.

Pour prendre en compte vos modifications, cliquez sur le bouton **Appliquer les modifications**.



Le menu déroulant **Gestion de l'administrateur** propose l'opération de suppression de l'administrateur.

Si l'administrateur est externe, le menu déroulant **Certificat** propose de :

- afficher le contenu du certificat de clé de signature de l'administrateur ;
- importer un nouveau certificat de clé de signature pour cet administrateur (voir la section Importation d'un certificat de clé de signature).

6.5 Ajout d'un administrateur

6.5.1 Ajout d'un administrateur externe à la base

Ajout de l'administrateur

1. Pour ajouter un administrateur externe, dans la page **Liste des administrateurs** (section Page Liste des administrateurs), cliquez sur le lien **Ajouter un administrateur externe**.
2. Dans la page des propriétés de l'administrateur (section Page Administrateur) :

a. Saisissez son libellé.

b. Définissez ses autorisations.

c. Validez l'ajout de l'administrateur en cliquant sur le bouton **Créer l'administrateur**.

3. Importer ensuite le certificat de sa clé de signature (voir la section Importation d'un certificat de clé de signature).

Importation d'un certificat de clé de signature

La première page permet d'importer le certificat soit en collant sa valeur (format "base 64"), soit en sélectionnant un fichier.

Le certificat doit comporter un usage X.509 parmi "signature numérique" ou "non répudiation".

La page suivante affiche le contenu du certificat. Dans cette page, validez l'importation du certificat en cliquant sur le bouton **Importer le certificat**.

6.5.2 Ajout d'un administrateur interne à la base

Un utilisateur de la base peut être défini comme administrateur de la base à partir de sa page **Utilisateur** (section Page Utilisateur), dans l'onglet *Propriétés* en cliquant sur le lien **Administrer la base**.

Dans la page des propriétés de l'administrateur (section Page Administrateur) :

1. Saisissez son libellé en tant qu'administrateur de la base.
2. Définissez ses autorisations.
3. Validez l'ajout de l'administrateur en cliquant sur le bouton **Créer l'administrateur**.

7. Fonctionnement d'une autorité de certification

Cette section explique comment gérer les clés des autorités de certification (CA) et les demandes de certificats.

La gestion des certificats comprend les fonctions habituelles d'infrastructure à clés publiques (PKI) en accès public et en accès authentifié.

7.1 Introduction

7.1.1 Services offerts

Stormshield Data Authority Manager offre les services de gestion de certificats suivants :

- le dépôt d'une demande de certificat ;
- la validation ou le rejet d'une demande ;
- la publication sur un serveur LDAP des certificats délivrés ;
- la révocation et la publication de CRL ;
- la consultation des certificats émis et révoqués ;
- l'envoi d'un e-mail de notification :
- à un administrateur quand un utilisateur dépose une demande de certificat,
- à l'utilisateur demandeur quand une demande est validée ou rejetée.

7.1.2 Accès public et accès authentifié

Les services destinés aux utilisateurs finaux sont offerts via un accès "public" (c'est-à-dire qui ne nécessite pas une authentification). Ces services sont :

- le dépôt d'une demande de certificat ;
- la consultation du statut d'une demande ;
- la consultation des certificats émis et révoqués.

Les services destinés à l'agent de certification nécessitent quant à eux l'authentification de cet agent (on parlera d'accès "authentifié"). Ces services sont :

- la validation / le rejet d'une demande de certificat ;
- la publication sur un serveur LDAP des certificats délivrés ;
- la révocation et la publication de CRL.

Toutes les pages en accès public, à la différence des pages en accès authentifié, sont compatibles avec les navigateurs de la famille Mozilla Firefox et Internet Explorer. Toutes les pages en accès authentifié sont compatibles uniquement avec Internet Explorer.

7.2 Page d'accueil

7.2.1 Page d'accès public

La page d'accueil public de l'autorité de certification est accessible directement, sans authentification.

Son URL d'accès direct est de la forme :

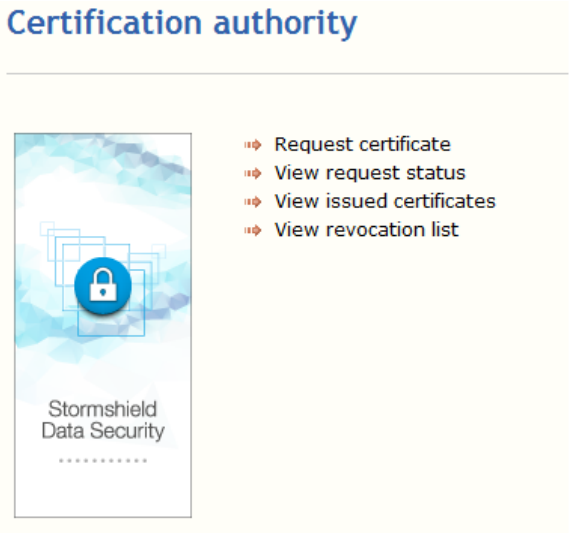
```
<manager_root_url>/PkiIndex?baseid=<base_id>
```

où `<manager_root_url>` est l'URL racine définie à la section URL d'accès au serveur , et `<base_id>` est l'identifiant de la base qui a été choisi lors de sa création.

Il est recommandé de communiquer cette URL aux utilisateurs finaux par l'intermédiaire d'un lien sur un site Intranet, ou par e-mail.

Cette page propose un menu d'opérations, permettant de :

- demander un certificat (section Dépôt d'une demande de certificat) ;
- afficher le statut d'une demande de certificat ;
- consulter les certificats émis (section Recherche de certificat) ;
- consulter la liste de révocation (section Consultation de la liste de révocation), dès lors qu'une liste de révocation a été générée.



7.2.2 Accès authentifié

La page d'accueil de l'autorité de certification en accès authentifié est accessible à partir du lien **Autorité de certification** de la page d'accueil de Stormshield Data Authority Manager (section Page d'accueil).

Elle propose un menu d'opérations, permettant de :

- afficher les demandes de certificat en attente (section Liste des demandes en attente) ;
- consulter les certificats émis (section Recherche de certificat) ;
- consulter la liste de révocation (section Consultation de la liste de révocation), dès lors qu'une liste de révocation a été générée ;
- générer et diffuser une nouvelle liste de révocation (section Génération d'une liste de révocation) ;
- accéder à la page de gestion de la clé et du certificat de l'autorité de certification (section Page Clé et certificat de l'autorité).

Si l'autorité de certification n'a pas encore de certificat, seule la page de gestion de la clé et du certificat (section Page Clé et certificat de l'autorité) est disponible.

7.3 Gestion de la clé de l'autorité de certification

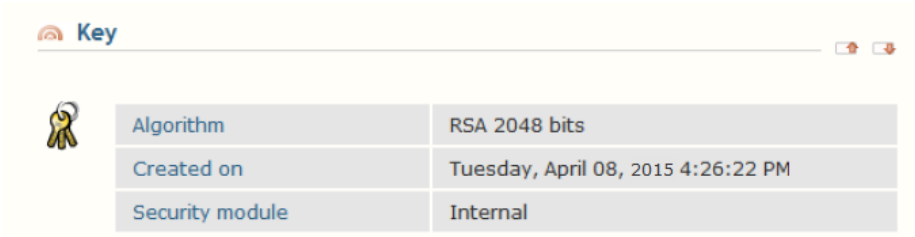
7.3.1 Page Clé et certificat de l'autorité

La page **Clé et certificat de l'autorité** est accessible à partir de la page d'accueil de l'autorité de certification (section Accès authentifié), en accès authentifié uniquement.

L'Annexe H, Autorité de certification racine contient un complément d'information sur la gestion particulière d'une autorité de certification racine.

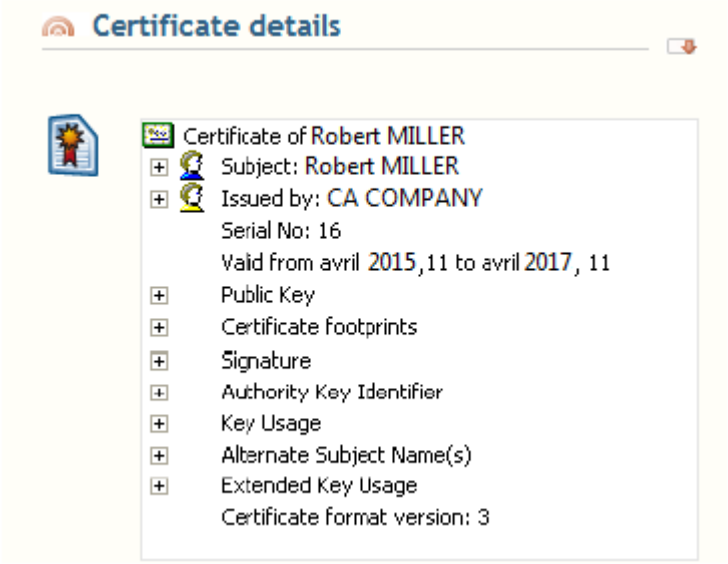
Elle présente tout d'abord son nom usuel et des informations concernant la clé de l'autorité de certification :

- l'**algorithme** de chiffrement avec sa force ;
- la **date de création** de la clé ;
- le **module de sécurité** dans lequel est stockée cette clé.



Lorsque la clé de l'autorité est certifiée, la page présente ensuite le contenu complet de son certificat sous la forme d'un arbre.

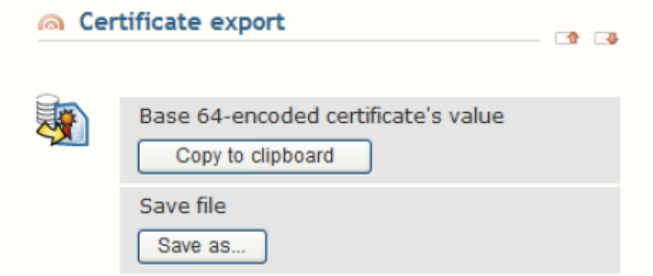
Lorsque la clé n'est pas certifiée, la page présente l'identité complète de l'autorité.



Dans la section suivante, on affiche les informations concernant une éventuelle demande de certificat :

- date de l'éventuelle demande de certificat en cours pour cette clé ;
- date de l'éventuelle dernière importation de certificat pour cette clé ;
- le nom de l'autorité de certification externe associée à la clé (voir la section Autorités de certification externes).

Lorsque la clé de l'autorité est certifiée, le certificat peut être exporté, par copier-coller de sa valeur "base 64" ou par enregistrement dans un fichier. Pour plus d'informations, consulter la section Exportation de certificat).



Dans le bandeau en haut de la page, un menu d'opérations permet :

- d'accéder aux propriétés de la clé dans l'onglet *Propriétés*. Dans cette page, vous pouvez modifier l'autorité de certification externe associée à la clé.
- lorsque la clé de l'autorité est certifiée :
- d'exporter la clé dans l'onglet *Gestion de la clé* (voir la section Exportation de la clé),
- dans l'onglet *Gestion du certificat* :

- de faire une demande de certificat (section Demande de certificat),
- de faire une demande de certificat avec renouvellement du sujet (section Demande de certificat).

Dans ce cas le sujet de la demande *PKCS#10* est recréé à partir de l'identité de l'autorité.

NOTE
Ceci n'est pas conseillé si vous n'avez pas positionné systématiquement un AuthorityKeyIdentifier dans tous les certificats générés, ou si le certificat de l'autorité ne possède pas de SubjectKeyIdentifier. En effet, dans ce cas, la relation de parenté entre les certificats émis et l'autorité est obtenue par comparaison du sujet de l'émetteur des certificats avec le sujet de l'autorité. Cette relation sera cassée si le sujet de l'autorité est renouvelé.

- d'importer un nouveau certificat (section Importation d'un nouveau certificat).
- lorsque la clé de l'autorité n'est pas encore certifiée, dans l'onglet *Gestion du certificat* :
- de faire une demande de certificat (section Demande de certificat),
- d'importer un nouveau certificat (section Importation d'un nouveau certificat).

7.3.2 Demande de certificat

La page de **Demande de certificat** pour une autorité de certification est accessible à partir de la page **Clé et certificat de l'autorité** (section Page Clé et certificat de l'autorité)

Il est possible de faire une demande en conservant le sujet de l'ancien certificat ou de faire une demande avec renouvellement du sujet, selon le lien utilisé pour accéder à la page. Pour plus d'informations, consultez le paragraphe section Page Clé et certificat de l'autorité .

Cette page est identique à la page de demande de certificat pour un utilisateur Stormshield Data Security (voir la section Création de demande).

7.3.3 Importation d'un nouveau certificat

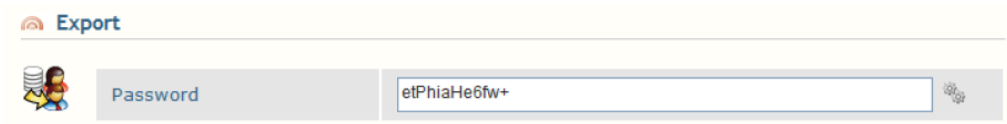
La page **Importation d'un certificat** est accessible à partir de la page **Clé et certificat de l'autorité** (section Page Clé et certificat de l'autorité).

Elle est identique à la page d'importation d'un certificat pour un utilisateur Stormshield Data Security (voir la section Importation de certificat).

Les règles d'importation d'un certificat pour l'autorité sont décrites dans la section Importation de certificat.

7.3.4 Exportation de la clé

La page **Exportation de la clé** est accessible à partir de la page **Clé et certificat de l'autorité** (section Page Clé et certificat de l'autorité).



Vous devez saisir le mot de passe de protection du fichier, puis cliquer sur **Exporter la clé**. Une page de compte rendu est ensuite affichée. Elle propose de sauvegarder le fichier *PKCS#12* créé, et dans lequel la clé et le certificat associé ont été copiés.

Afin de garantir la confidentialité des données, il est conseillé de saisir un mot de passe non trivial. Pour aider à la saisie du mot de passe, un tirage aléatoire est proposé en appuyant sur l'icône .

7.4 Dépôt d'une demande de certificat

Une demande de certificat ne peut être déposée qu'en accès public.

La page **Demande de certificat**, accessible à partir de la page d'accueil de l'autorité de certification (voir la section Page d'accueil), permet de choisir quel type de demande de certificat vous souhaitez déposer.

Une demande de certificat "standard" est adaptée aux cas les plus courants : certificat de chiffrement, de signature ou d'authentification pour un utilisateur (section Dépôt d'une demande de certificat standard).

Une demande de certificat avancée permet de demander un certificat pour un usage plus spécifique, par exemple pour un serveur SSL/HTTPS ou une sous-autorité (section Dépôt d'une demande de certificat avancé).

7.4.1 Dépôt d'une demande de certificat standard

Une demande de certificat standard est une demande simplifiée pour les usages les plus courants (certificat de signature, de chiffrement).

Une demande standard comprend les informations concernant le demandeur et sa clé, et indique le modèle de certificat demandé.

Remplir et soumettre une demande de certificat

Dans la page **Demande de certificat** (section Dépôt d'une demande de certificat), cliquez sur le lien **Remplir et soumettre une demande de certificat**.

La page affichée permet de générer une demande de certificat pour une clé fournie par un module cryptographique présent dans votre navigateur (CSP pour Cryptographic Service Provider sous Internet Explorer).

- La plupart des modules cryptographiques procèdent au tirage d'une paire clé privée/clé publique, stockent la clé privée en interne et fournissent la clé publique dans la demande.

Si CSP de Microsoft stocke la clé privée dans le magasin d'Internet Explorer, les CSP de fournisseurs de cartes à puce ou tokens stockent la clé privée dans la carte ou le token.

- Le CSP Stormshield Data Security récupère une des clés présentes dans le compte de l'utilisateur connecté à la suite Stormshield Data Security et génère une demande pour la clé publique.

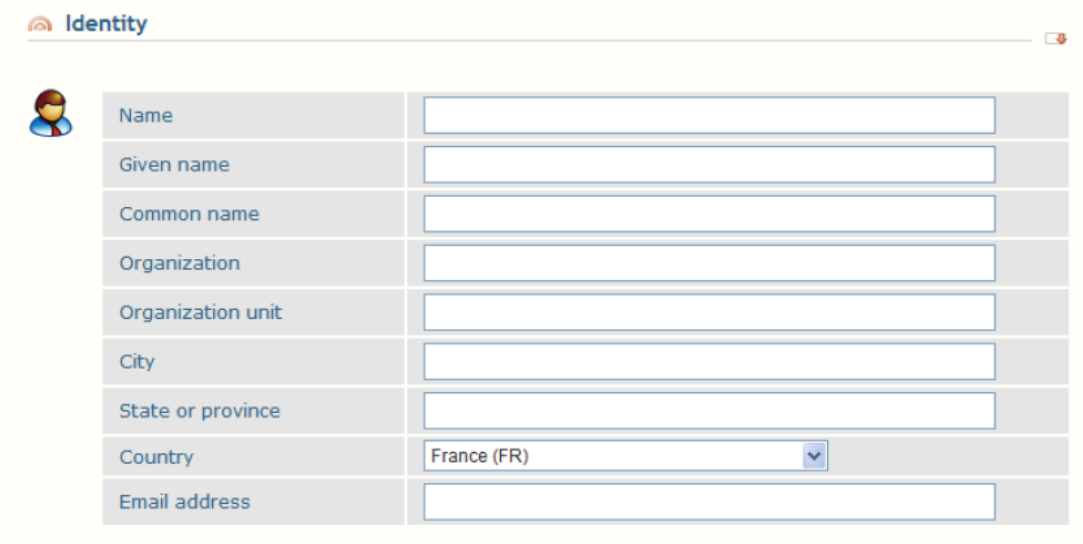
Dans tous les cas, la clé privée n'est jamais fournie à Stormshield Data Authority Manager. Seule la demande de certificat, ne contenant que l'identité du demandeur et la clé publique, lui est envoyée.

NOTE
En fonction de la zone de sécurité de l'explorateur dans laquelle s'exécute le serveur Stormshield Data Authority Manager, une autorisation d'exécution du module cryptographique peut être demandée à l'utilisateur. Vous pouvez éviter cette demande en définissant le serveur Stormshield Data Authority Manager dans les sites de confiance de l'explorateur.

La première partie de la page permet de saisir l'identité de l'utilisateur. Elle sera inscrite dans la demande de certificat. Ensuite, lors de la validation de la demande par un agent de certification, elle pourra être modifiée, avant d'être inscrite dans le sujet du certificat généré.

L'adresse e-mail sera automatiquement copiée ou déplacée dans le champ **Subject Alternative Name** du certificat selon les paramètres généraux de gestion des certificats (voir la section Certificats générés).

Afin de simplifier la procédure et d'éviter les erreurs, il est possible de paramétrer Stormshield Data Authority Manager pour que les champs **Organisation**, **Unité**, **Ville**, **Etat** et **Pays** soient pré-remplis avec des valeurs par défaut. Les valeurs par défaut sont spécifiées dans les paramètres généraux de gestion des certificats (voir la sectionPré-remplissage des demandes de certificats externes).

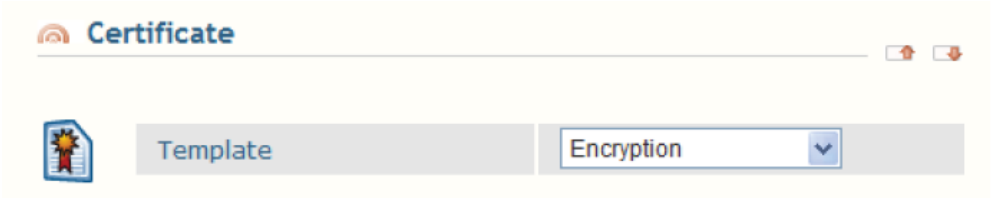


La deuxième partie de la page concerne la génération des clés par le CSP ou le module de sécurité. Le bi-clé est généré par un fournisseur de services cryptographiques. Vous pouvez choisir :

- le fournisseur de services cryptographiques, ou Cryptographic Service Provider (CSP) qui génère le bi-clé et la demande ;
- l'utilisation de la clé (Toute utilisation, Exchange ou Signature). Ce paramètre est utilisé par le CSP pour générer la clé, il est indépendant du modèle de certificat Stormshield Data Authority Manager à spécifier par la suite ;
- la taille de la clé RSA. Les valeurs possibles dépendent du CSP et de l'utilisation choisie pour la clé ;
- de marquer les clés comme exportables, si vous souhaitez à l'avenir pouvoir exporter les clés sous forme de fichiers *PKCS#12* ;
- d'activer la protection renforcée de la clé privée.

Dans le cas du CSP Stormshield Data Security, étant donné que la clé n'est pas générée mais récupérée, ces options ne sont pas prises en compte.

La troisième section permet de sélectionner un modèle de certificat, parmi tous les modèles de certificats standards (section Modèles de certificats). Ce modèle de certificat définit les propriétés du certificat demandé (dates de validité, usages…). Si vous souhaitez générer un certificat particulier, utilisez la page de **Demande de certificat avancé** (voir la section Remplir et soumettre une demande de certificat avancé).



La dernière section permet de spécifier les informations qui permettront à l'administrateur qui validera la demande de rentrer en contact avec le demandeur. Ces informations sont facultatives.

Pour valider votre demande, cliquez sur **Envoyer la demande**.

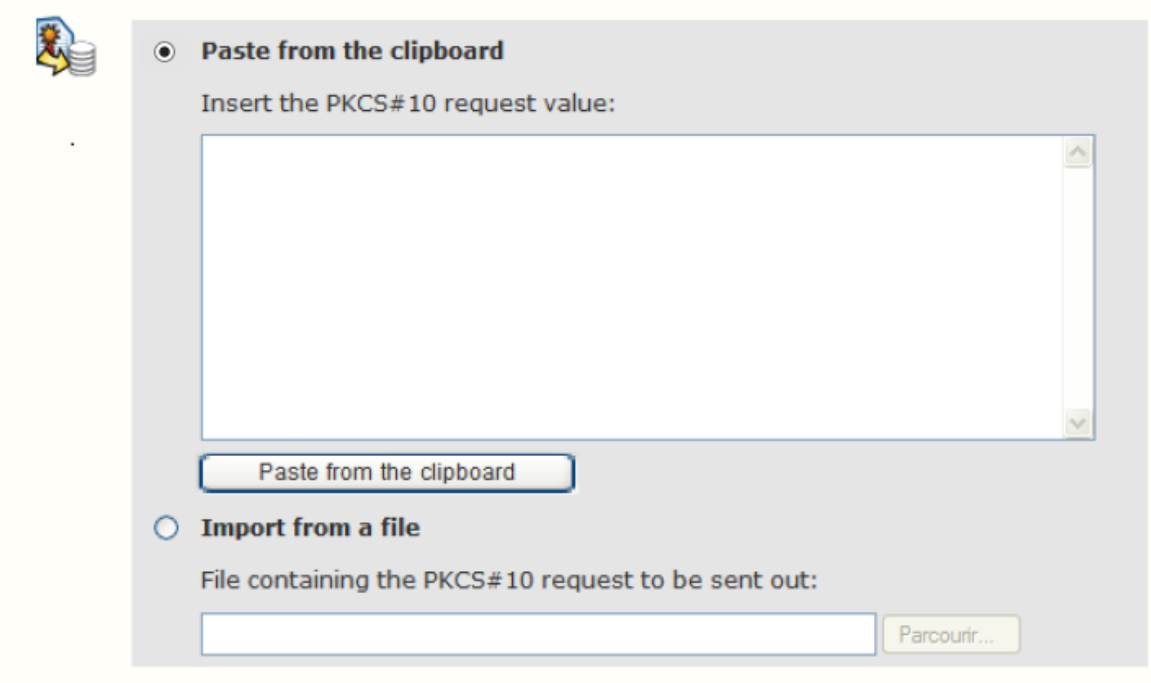
Dans le compte rendu qui s'affiche, notez bien l'identifiant de la demande : il vous permet de consulter à tout moment le statut de votre demande.

Soumettre une demande de certificat à partir d'une structure *PKCS#10*

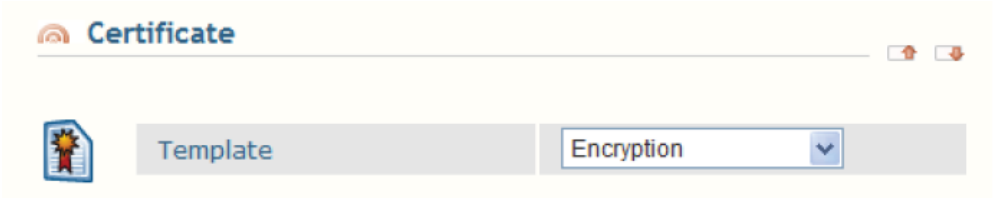
Dans la page **Demande de certificat** (section Dépôt d'une demande de certificat), cliquez sur le lien **Soumettre une demande de certificat à partir d'une structure *PKCS#10***.

La page affichée permet de soumettre une demande de certificat pour une clé déjà existante, à partir d'une structure *PKCS#10* provenant d'un produit quelconque.

Vous pouvez coller la valeur de la structure *PKCS#10* encodée au format "base 64" ou sélectionner un fichier.



La deuxième section permet de sélectionner un modèle de certificat, parmi tous les modèles de certificats standards (section Modèles de certificats). Ce modèle de certificat définit les propriétés du certificat demandé (dates de validité, usages…). Si vous souhaitez générer un certificat particulier, utilisez la page de **Demande de certificat avancé** (voir la section Remplir et soumettre une demande de certificat avancé).



La dernière section permet de spécifier les informations qui permettront à l'administrateur qui validera la demande de rentrer en contact avec le demandeur. Ces informations sont facultatives.

Pour valider votre demande, cliquez sur **Envoyer la demande**.

Dans le compte rendu qui s'affiche, notez bien l'identifiant de la demande : il permet de consulter à tout moment le statut de votre demande.

7.4.2 Dépôt d'une demande de certificat avancé

Une demande de certificat "avancé" permet de demander un certificat plus spécifique, comme par exemple un certificat SSL ou un certificat de sous-autorité.

Une demande avancée comprend :

- les informations concernant le demandeur et sa clé ;
- éventuellement, des informations qui seront stockées dans le champ **Subject Alternative Name** du certificat généré ;
- le modèle de certificat demandé, ou un contenu personnalisé.

Remplir et soumettre une demande de certificat avancé

Dans la page **Demande de certificat** (section Dépôt d'une demande de certificat) cliquez sur le lien **Certificat avancé**, puis sur le lien **Remplir et soumettre une demande de certificat avancé**.

La page affichée est similaire à la page de **Demande de certificat standard** (voir la section Remplir et soumettre une demande de certificat). Elle comporte en plus les éléments suivants.

Il est maintenant possible de renseigner des informations qui seront stockées dans le champ **Subject Alternative Name** du certificat :

- une adresse e-mail ;
- un nom de domaine ;
- une adresse IP ;
- un nom principal (UPN, Universal Principal Name, OID 1.3.6.1.4.1.311.20.2.3). Sa valeur est encodée en UTF-8.

Notez que l'adresse e-mail de l'identité ne sera pas copiée ou déplacée dans le **Subject Alternative Name**, contrairement à une demande de certificat standard. C'est au demandeur de spécifier explicitement quelles informations formeront le sujet du certificat généré et quelles informations formeront le **Subject Alternative Name**.

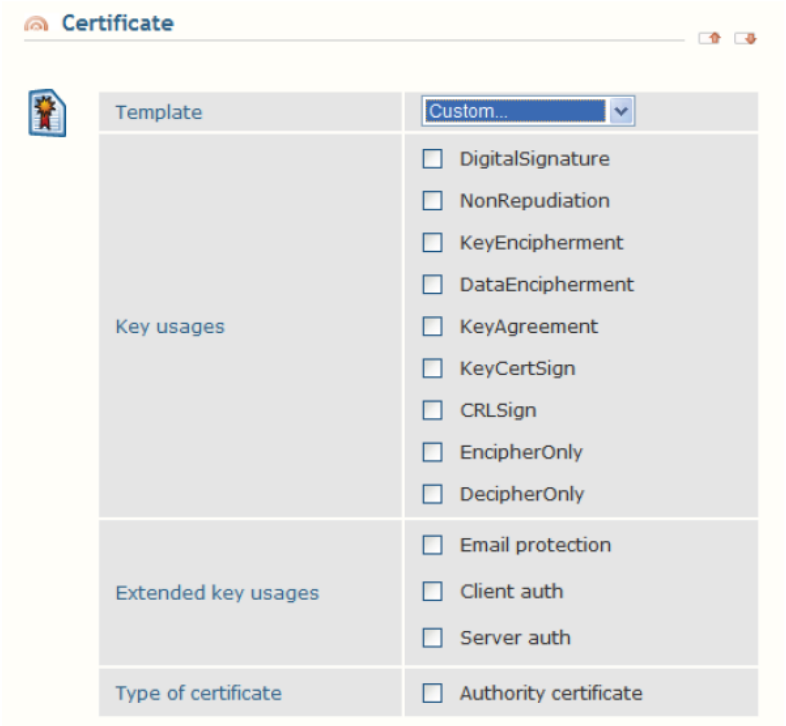
Le nom de domaine et l'adresse IP sont utiles si vous souhaitez générer un certificat serveur SSL.

Dans la section **Certificat**, il est maintenant possible de sélectionner un modèle de certificat parmi tous les modèles de certificats paramétrés dans la page **Modèles de certificats** (section Modèles de certificats). Ainsi, le modèle de certificat d'autorité est disponible, de même que les modèles spécifiques que vous aurez éventuellement ajoutés.

Le choix **Personnalisé** est également ajouté à la liste des modèles de certificats. Ce choix laisse apparaître des options supplémentaires permettant de demander un certificat pour lequel aucun modèle n'est adapté.

Les options supplémentaires sont :

- usages de la clé ;
- usages étendus de la clé ;
- type de certificat : certificat d'autorité ou non.



Pour valider votre demande, cliquez sur **Envoyer la demande**.

Dans le compte rendu qui s'affiche, notez bien l'identifiant de la demande : il vous permet de consulter à tout moment le statut de votre demande.

Soumettre une demande de certificat avancé à partir d'une structure *PKCS#10*

Dans la page **Demande de certificat** (section Dépôt d'une demande de certificat), cliquez sur le lien **Certificat avancé**, puis sur le lien **Soumettre une demande de certificat avancé à partir d'une structure *PKCS#10***.

La page affichée est similaire à la page de **Demande de certificat standard à partir d'une structure *PKCS#10*** (voir la section Soumettre une demande de certificat à partir d'une structure *PKCS#10*).

En plus, il est maintenant possible de renseigner des informations qui seront stockées dans le champ **Subject Alternative Name** du certificat :

- une adresse e-mail ;
- un nom de domaine ;
- une adresse IP ;
- un nom principal (UPN, Universal Principal Name, OID 1.3.6.1.4.1.311.20.2.3). Sa valeur est encodée en UTF-8.

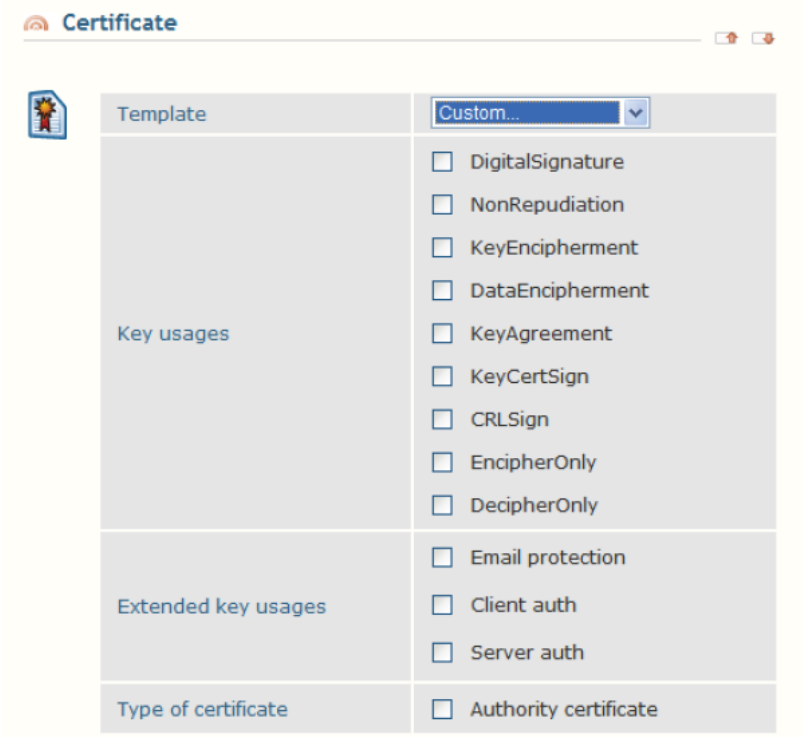
Notez que l'adresse e-mail de l'identité ne sera pas copiée ou déplacée dans le **Subject Alternative Name**, contrairement à une demande de certificat standard. C'est au demandeur de spécifier explicitement quelles informations formeront le sujet du certificat généré et quelles informations formeront le **Subject Alternative Name**.

Le nom de domaine et l'adresse IP seront utiles si vous souhaitez générer un certificat serveur SSL.

Dans la section **Certificat**, il est maintenant possible de sélectionner un modèle de certificat parmi tous les modèles de certificats paramétrés dans la page **Modèles de certificats** (section Modèles de certificats .) Ainsi, le modèle de certificat d'autorité est disponible, de même que les modèles spécifiques que vous aurez éventuellement ajoutés.

Le choix **Personnalisé** est également ajouté à la liste des modèles de certificats. Ce choix laisse apparaître des options supplémentaires permettant de demander un certificat pour lequel aucun modèle n'est adapté. Les options supplémentaires sont :

- usages de la clé ;
- usages étendus de la clé ;
- type de certificat : certificat d'autorité ou non.



Pour valider votre demande, cliquez sur **Envoyer la demande**.

Dans le compte rendu qui s'affiche, notez bien l'identifiant de la demande : il permet de consulter à tout moment le statut de votre demande.

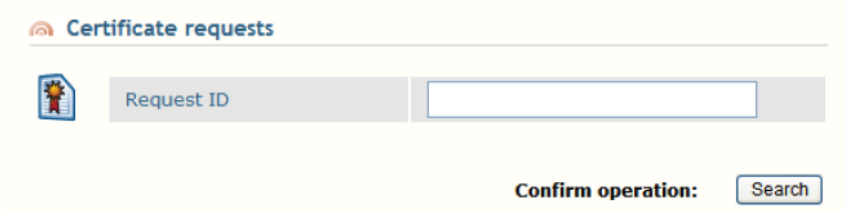
7.4.3 Consultation du statut d'une demande de certificat

La page **Statut d'une demande de certificat** est accessible à partir de la page d'accueil de l'autorité de certification (voir la section Page d'accès public), en accès public uniquement.

Elle propose de saisir l'identifiant d'une demande de certificat.

En cliquant sur **Rechercher**, vous affichez :

- un message indiquant que la demande est en attente si c'est le cas ;
- la date et la raison du rejet si la demande a été rejetée ;
- le certificat généré si la demande a été validée (section Affichage de certificat).



7.5 Affichage et traitement des demandes de certificat

7.5.1 Liste des demandes en attente

La page **Liste des demandes en attente** est accessible à partir de la page d'accueil de l'autorité de certification (section Liste des certificats émis), en accès authentifié uniquement.

Elle affiche toutes les demandes de certificat non traitées, c'est-à-dire non validées et non rejetées.

Les demandes sont affichées par page de 10 demandes. Si plus de 10 demandes sont en attente de traitement, vous pouvez utiliser les icônes présents en dessous de la liste pour naviguer entre les différentes pages.

Dans la liste, pour chaque demande de certificat :

- la première colonne contient l'identifiant de la demande ;
- la deuxième colonne contient :
- le nom usuel de la demande,
- le sujet complet de la demande,
- la date de la demande,
- le modèle de certificat demandé,
- la troisième colonne indique le type de la demande :
- demande de certificat standard ;
- demande de certificat avancée.

En cliquant sur l'identifiant d'une demande ou sur le nom usuel du demandeur, vous affichez la page de traitement de la demande (section Demande de certificat).

7.5.2 Demande de certificat

La page **Validation d'une demande de certificat** est accessible à partir de la page **Liste des demandes en attente** (section Liste des demandes en attente), en accès authentifié uniquement.

Elle permet, au choix :

- de modifier éventuellement la demande, puis de la valider, c'est-à-dire de générer un certificat pour la clé publique, signé par l'autorité de certification ;
- de rejeter la demande. Si vous souhaitez rejeter la demande, il est inutile de remplir toutes les options concernant le certificat à générer, vous pouvez simplement remplir le commentaire de rejet et choisir le bouton **Rejeter la demande**, en bas de la page.

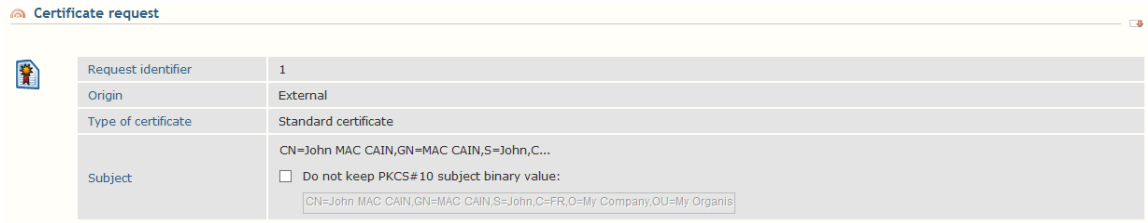
La première section de la page donne quelques informations générales sur la demande à traiter :

- l'identifiant de la demande ;
- son origine, qui peut être :
- externe, si la demande provient d'une page de demande de certificat en accès public ou d'une demande de certificat à distance envoyée par un autre serveur Stormshield Data Authority Manager,
- un compte Stormshield Data Security géré dans la base de données. Ce cas se produit uniquement si un administrateur n'ayant pas les droits de certification crée un utilisateur. Dans ce cas une demande est automatiquement générée et déposée à l'autorité de certification.

- le type de certificat demandé, qui peut être :
- avancé, si la demande provient d'une page de demande de certificat avancé en accès public,
- standard, dans tous les autres cas,
- le sujet du certificat demandé. Il peut être modifié.

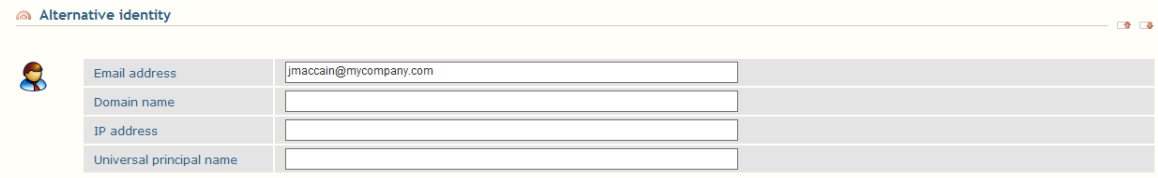
NOTE
Dans le cas du renouvellement du certificat d'une autorité de certification, il est conseillé de ne pas modifier le sujet mais de conserver la valeur binaire de l'ancien sujet, pour ne pas risquer de casser la relation de parenté entre cette autorité et les certificats qu'elle a générés.

Si vous choisissez de déplacer l'adresse e-mail de l'identité dans le champ **Subject Alternative Name** (paramètre champ **Email**, voir la section Certificats générés), pour obtenir le fonctionnement souhaité, vous devez veiller à ne pas conserver la valeur binaire du sujet issue de la structure *PKCS#10*, si cette valeur contient l'e-mail. Vous devez utiliser alors le sujet proposé en remplacement.



La deuxième section présente, et permet de modifier, les informations qui seront stockées dans le champ **Subject Alternative Name** du certificat :

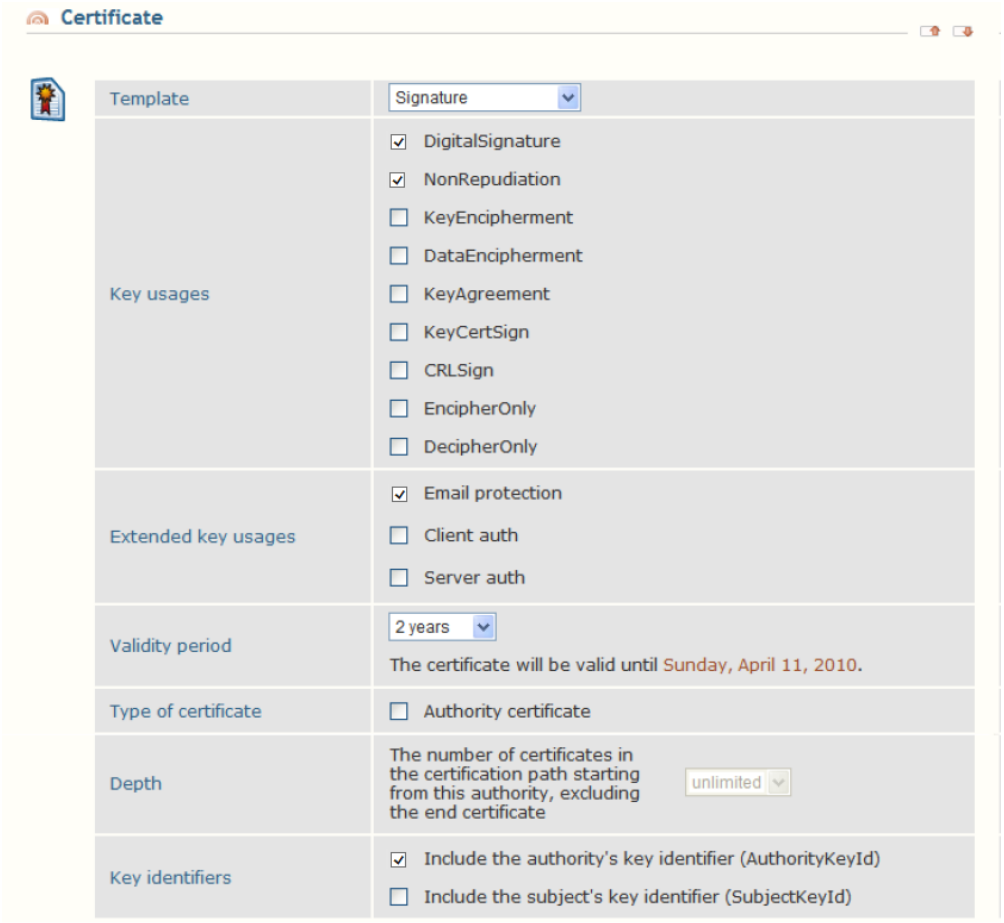
- une adresse e-mail ;
- un nom de domaine ;
- une adresse IP ;
- un nom principal (UPN, Universal Principal Name, OID 1.3.6.1.4.1.311.20.2.3). Sa valeur est encodée en UTF-8.



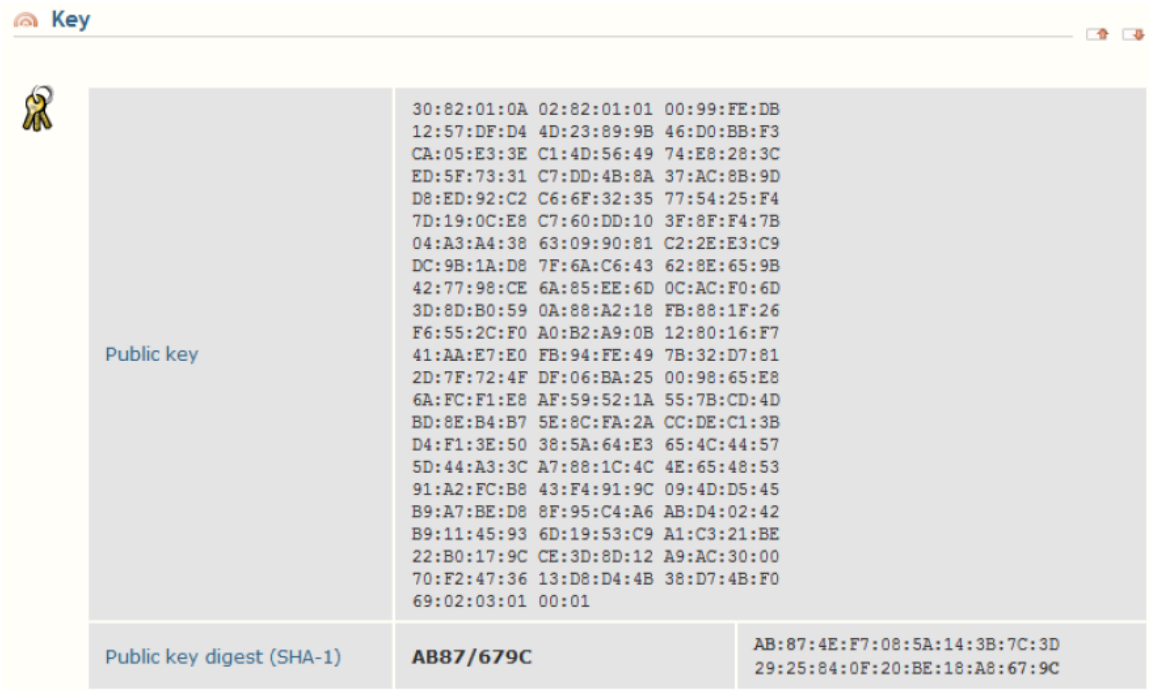
La troisième section présente, et permet de modifier, le modèle de certificat choisi lors de la demande.

Si aucun modèle n'est adapté au certificat que vous souhaitez générer, vous pouvez modifier chaque option manuellement. Cela peut servir par exemple à générer un certificat ayant une durée de validité plus courte pour un utilisateur particulier. Pour plus d'information sur les options disponibles, voir la section Modèles de certificats. Si vous modifiez une option manuellement, le modèle de certificat deviendra personnalisé.

Toutefois, il est conseillé d'utiliser des modèles de certificat le plus souvent possible, et au besoin de créer des nouveaux modèles (section Modèles de certificats).

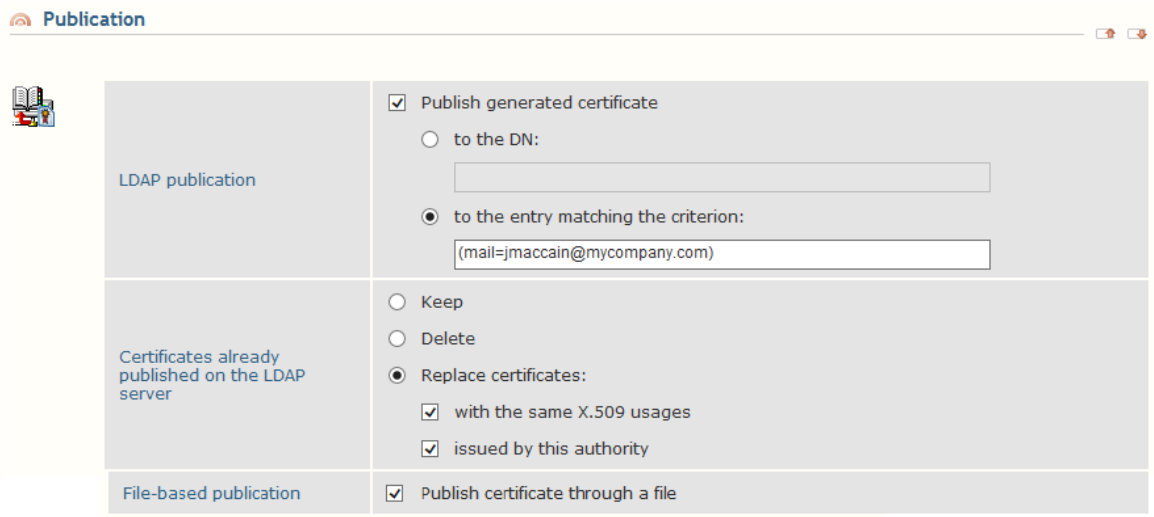


La quatrième section présente la valeur complète de la clé publique qui va être certifiée, et son empreinte SHA-1.

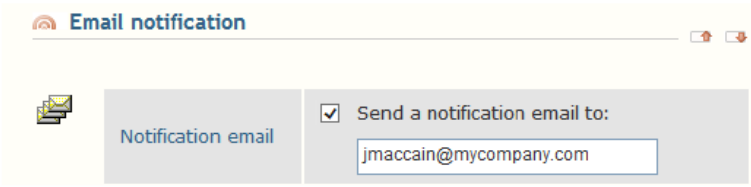


Selon vos paramètres généraux, une cinquième section propose éventuellement la publication du certificat généré. Si un serveur LDAP est paramétré (voir la section Configuration LDAP), les

options de publication LDAP sont disponibles. Si la publication par fichier est paramétrée (voir la section Publication d'un certificat).

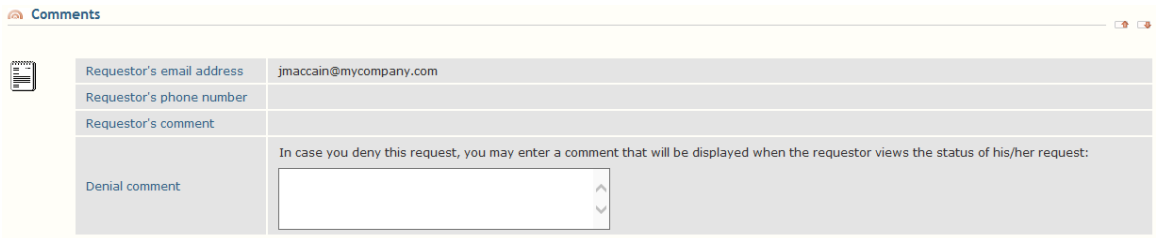


Si un serveur de courrier sortant (SMTP) est paramétré (voir la section Dépôt d'une demande de certificat).

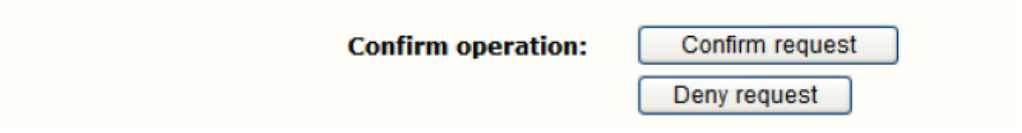


Enfin, la dernière section présente les informations concernant le demandeur du certificat, qui peuvent servir à rentrer en contact avec celui-ci avant de générer son certificat.

La dernière section permet également, au cas où vous ayez choisi de rejeter la demande, de remplir un commentaire pour expliquer la raison du refus au demandeur du certificat.



Choisissez enfin entre **Valider la demande** ou **Rejeter la demande** :



Dans ces deux cas, un e-mail est envoyé au demandeur. Cet e-mail contient un lien qui pointe sur :

- le détail du certificat généré, si la demande a été validée ;
- la raison du rejet, si la demande a été rejetée.

Le type du certificat généré peut différer du type initialement demandé.

- Une demande standard dans laquelle seule la période de validité a été modifiée donnera un certificat standard.
- Une demande standard dans laquelle le modèle de certificat a été changé pour un modèle avancé, ou a été remplacé par un paramétrage personnalisé, donnera un certificat avancé.
- Toute demande avancée donnera un certificat avancé, même si elle réfère à un modèle de certificat standard et qu'elle ne contient pas de **Subject Alternative Name**.

7.6 Affichage et traitement des certificats émis

7.6.1 Recherche de certificat

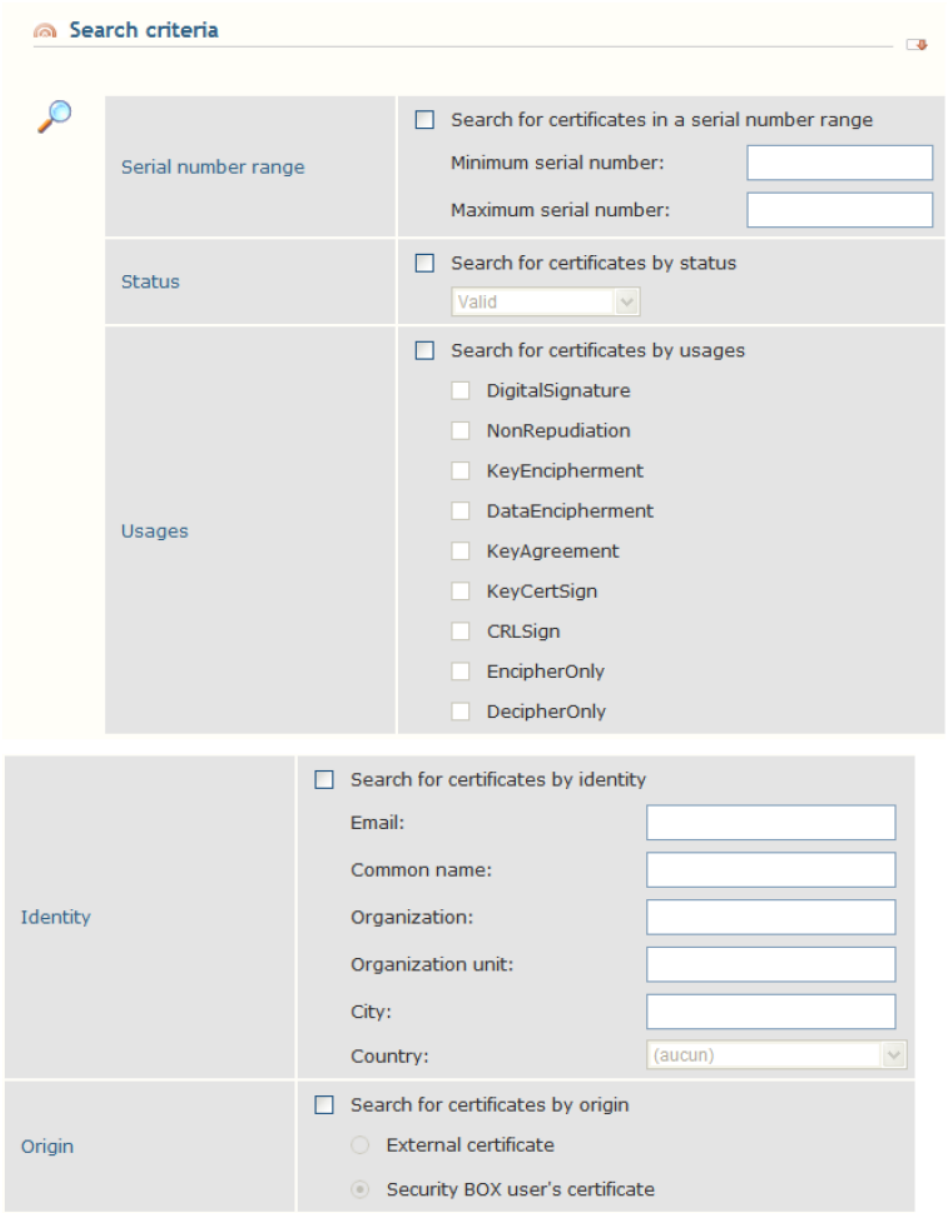
La page **Recherche de certificats émis** est accessible à partir de la page d'accueil de l'autorité de certification (section Accès authentifié), à la fois en accès public et en accès authentifié.

Elle propose différents critères permettant de rechercher efficacement un ou plusieurs certificats parmi tous les certificats émis par l'autorité de certification.

Si vous ne sélectionnez aucun critère de recherche, tous les certificats émis seront renvoyés. Si vous sélectionnez un ou plusieurs critères, la liste sera restreinte aux certificats vérifiant ces critères.

Les critères de recherche proposés sont :

- plage de numéros de série. Les numéros de série minimum et maximum sont à saisir au format hexadécimal (exemple : de 0a à ff) ;
- statut (valides, périmés, révoqués, révoqués ou périmés) ;
- usages ;
- identité ;
- origine.



7.6.2 Liste des certificats émis

La liste des certificats émis n'est accessible que par une recherche de certificats émis (section Recherche de certificat), en accès public ou authentifié. Si vous souhaitez afficher la liste totale de tous les certificats générés, vous pouvez lancer une recherche en ne spécifiant aucun critère.

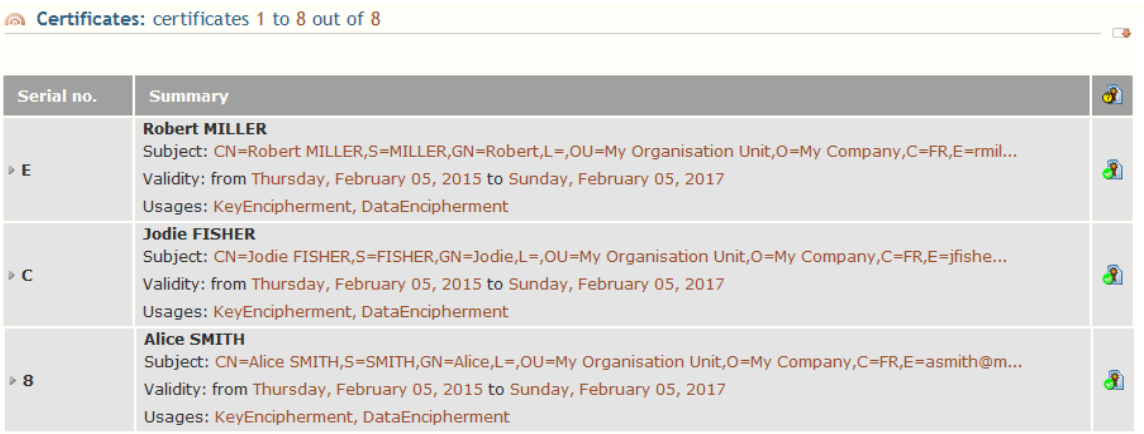
Les certificats sont affichés par page de 10 certificats. Si la recherche renvoie plus de 10 certificats, vous pouvez utiliser les icônes présents en dessous de la liste pour naviguer entre les différentes pages.

Dans la liste, pour chaque certificat :

- la première colonne contient le numéro de série du certificat ;
- la deuxième colonne contient :

- le nom usuel du certificat,
- le sujet complet du certificat,
- les dates de validité du certificat,
- les usages du certificat,
- la troisième colonne indique le statut du certificat :
- certificat valide,
- certificat révoqué ou périmé.

En cliquant sur le numéro de série d'un certificat ou sur le nom usuel de son titulaire, vous accédez à la page d'affichage du certificat (voir la section Affichage de certificat).



7.6.3 Affichage de certificat

La page **Détails d'un certificat** est disponible en accès public et en accès authentifié.

En accès authentifié, elle est disponible à partir de la liste des certificats émis (section Accès authentifié).

En accès public, elle est disponible à partir de la liste des certificats émis (section Accès authentifié), à partir de la demande de statut d'une demande lorsque cette demande a été validée, et il est également possible d'accéder directement à cette page par son URL :

```
<manager_root_url>/PkiCert?baseid=<base_id>&pkiSerialNumber=<serial_
number>
```

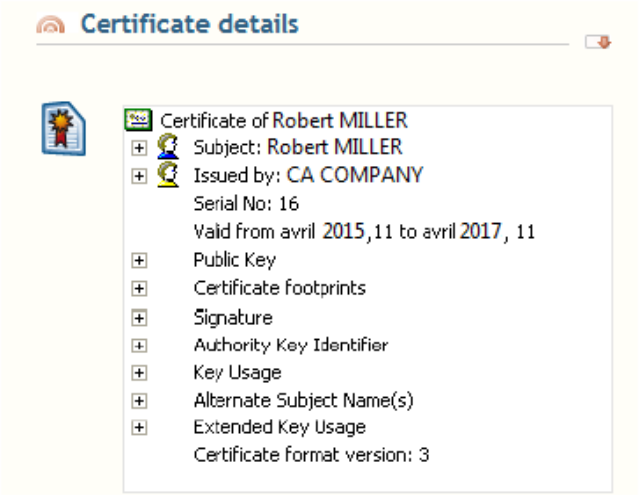
où `<manager_root_url>` est l'URL racine définie à la section URL d'accès au serveur , `<base_id>` est l'identifiant de la base qui a été choisi à sa création, et `<serial_number>` est le numéro de série du certificat en décimal.

La première section présente le contenu complet du certificat :

- dans un tableau en accès public ;
- sous la forme d'un arbre en accès authentifié.

Si le certificat est révoqué ou périmé, un avertissement apparaît en couleur rouge au-dessus des détails du certificat.

Le contenu d'un certificat complet est détaillé en ASN.1 dans l'annexe Contenu d'un certificat émis par la PKI.

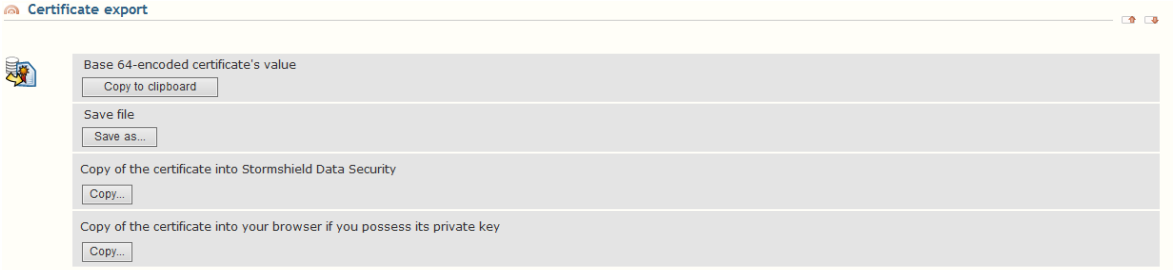


Le certificat peut être exporté, par copier-coller de sa valeur "base 64" ou par enregistrement dans un fichier (voir la section Exportation de certificat). En outre, il peut être :

- copié dans Stormshield Data Security. Cette opération lance l'assistant d'importation de certificat de Stormshield Data Security. Elle n'est pas disponible avec d'autres navigateurs qu'Internet Explorer.

NOTE
Pour que la page propose cette fonctionnalité à l'utilisateur, un ActiveX doit être installé et exécuté sur le poste client lors du chargement de la page. Pour ce faire, il faut que le serveur Stormshield Data Authority Manager soit présent dans les sites de confiances de l'explorateur (Internet Explorer ou Firefox) sur le poste client, et que l'exécution des ActiveX non marqués comme sécurisés soit autorisée (voir la section Configuration du poste administrateur).

- copié dans votre navigateur. Cette opération envoie le certificat à votre navigateur qui va l'associer à la clé correspondante dans son magasin de certificats. L'opération échouera si le magasin de certificats du navigateur ne contient pas de clé correspondante. Elle doit donc être effectuée depuis le navigateur ayant servi à générer la clé et à déposer la demande (voir la section Remplir et soumettre une demande de certificat).



En accès authentifié, la page permet également de procéder à différentes opérations sur le certificat affiché :

- publier le certificat (voir la section Publication d'un certificat) ;
- révoquer le certificat (voir la section Révocation de certificat).

7.6.4 Publication d'un certificat

Vous pouvez publier un certificat dès sa génération (section Demande de certificat), ou plus tard à partir de sa page (voir la section Affichage de certificat) en accès authentifié. Selon les

paramètres généraux, une section en bas de la page propose la publication du certificat.

Si un serveur LDAP est paramétré dans vos paramètres généraux (section Configuration LDAP), les options suivantes sont disponibles :

- Publier le certificat généré vers un DN donné.

Le DN proposé est résolu à partir du masque de DN spécifié dans les paramètres généraux et du sujet du certificat à publier.

- Publier le certificat généré vers l'entrée satisfaisant un critère donné.

Une recherche dans l'annuaire LDAP sera effectuée selon ce critère et, si elle retourne un unique résultat, le certificat sera publié vers l'entrée trouvée.

Le critère de recherche est résolu à partir du masque de critère de recherche spécifié dans les paramètres généraux et du sujet du certificat à publier.

Si vous souhaitez que cette option soit sélectionnée par défaut, il suffit de ne pas spécifier de masque de DN de publication dans les paramètres généraux.

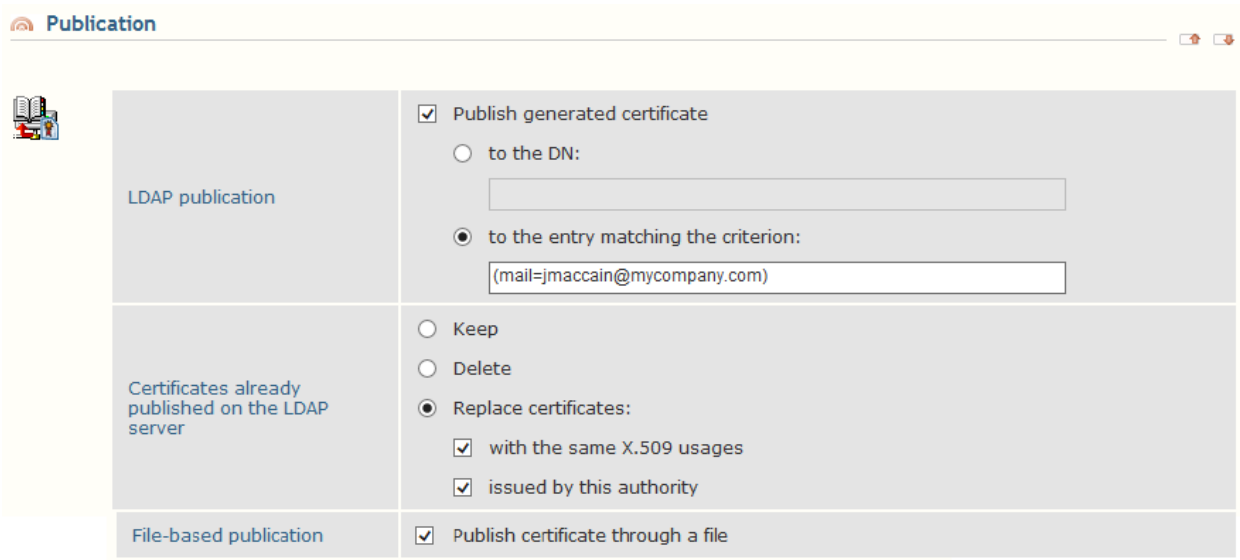
- Pour les certificats déjà publiés sur le serveur LDAP :

Il est proposé ici de paramétrer l'opération à effectuer sur les éventuels certificats déjà présents sur le serveur LDAP à l'entrée désignée par le DN ou trouvée par la recherche par critère :

- les conserver ;
- les supprimer ;
- remplacer les certificats ayant les mêmes usages X.509 ;
- remplacer les certificats émis par cette autorité.

Si cette option est choisie, les certificats seront conservés sauf ceux vérifiant tous les critères sélectionnés, qui seront remplacés par le certificat à publier.

Si la publication par fichier est activée dans vos paramètres généraux (voir la section Certificats générés), une option Publier le certificat par fichier est proposée.



7.6.5 Révocation de certificat

Pour révoquer un certificat, accédez à la page d'affichage du certificat (section Affichage de certificat) en accès authentifié. Si le certificat n'est pas déjà révoqué, une section en bas de la

page propose la révocation du certificat.

Plusieurs options de révocation sont disponibles :

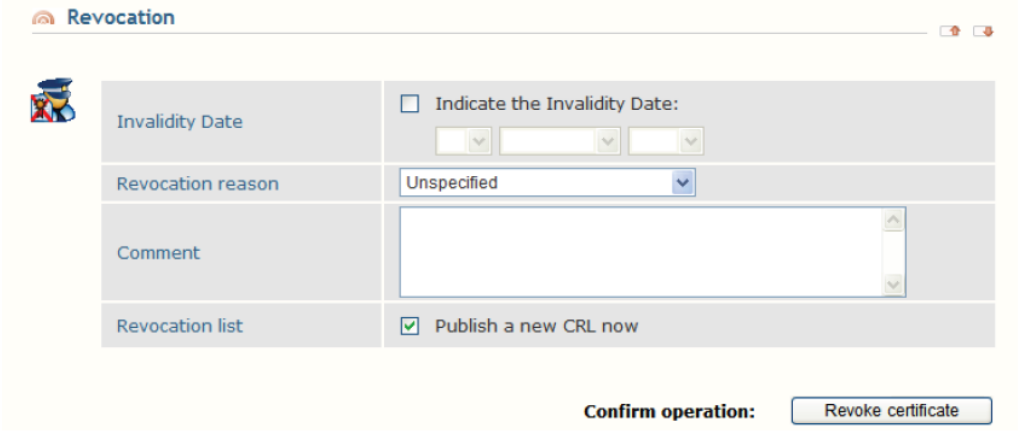
- la date d'invalidité ;

> **NOTE**
> A la différence de la date de révocation, qui sera systématiquement incluse et qui sera la date courante, la date d'invalidité est facultative. C'est la date à partir de laquelle le certificat sera invalide ou la date à laquelle la clé a été compromise. Elle sera incluse dans le champ **InvalidityDate** de l'entrée dans la CRL. Il est inutile de la spécifier si elle est identique à la date de révocation.

- la raison de la révocation ;
- le commentaire de révocation. Ce commentaire n'apparaîtra pas dans la CRL, il est interne à Stormshield Data Authority Manager. Il apparaîtra par contre dans la page d'affichage du certificat (section Affichage de certificat) ;
- la publication d'une nouvelle liste de révocation ;

Il est recommandé de publier une nouvelle liste de révocation immédiatement, afin que l'état de révocation du certificat soit pris en compte au plus tôt.

La CRL est générée et publiée conformément aux options spécifiées dans les "Paramètres généraux de gestion des certificats" (voir la section Listes de révocation (CRLs)).



Il est également possible de révoquer plusieurs certificats à la fois. Pour plus d'informations, reportez-vous à la section Révocation d'utilisateurs.

7.7 Gestion des listes de révocations (CRL)

Stormshield Data Authority Manager permet de révoquer des certificats (voir la section Révocation de certificat) et de générer des listes de révocation (voir la section Génération d'une liste de révocation et la section Génération automatique des listes de révocation).

Une liste de révocation (CRL) contient la liste de tous les certificats révoqués à une date donnée, signée par l'autorité de certification.

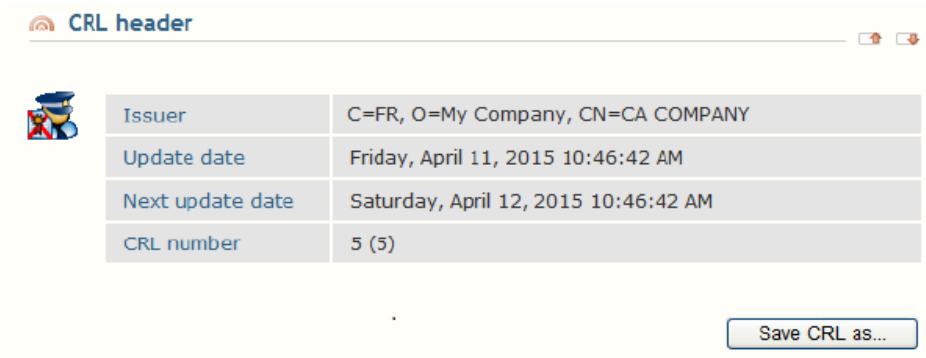
7.7.1 Consultation de la liste de révocation

La page **Liste de révocation** est accessible à partir de la page d'accueil de l'autorité de certification (voir la section Accès authentifié) en cliquant sur le lien **Consulter la liste de révocation**.

Elle est disponible à la fois en accès public et en accès authentifié.

La première section donne des informations concernant la CRL courante :

- émetteur de la CRL (ce sera le sujet de l'autorité de certification de la base) ;
- date de la mise à jour (champ **ThisUpdate** de la CRL) ;
- date de la prochaine mise à jour (champ **NextUpdate** de la CRL). Cette date dépend de la durée de validité des CRLs personnalisable dans les paramètres généraux de gestion des certificats (voir la section Listes de révocation (CRLs)) ;
- numéro de la CRL (champ **CrlNumber** de la CRL). ;



La section suivante présente la liste des certificats révoqués dans la CRL courante. Pour chaque certificat :

- la première colonne contient le numéro de série du certificat ;
- la deuxième colonne contient la date à laquelle le certificat a été révoqué ;
- la troisième colonne contient la raison de la révocation du certificat, renseignée par l'administrateur ayant procédé à la révocation.

En cliquant sur le numéro de série d'un certificat, vous affichez la page de détail de ce certificat (voir la section Affichage de certificat).

Serial no.	Revocation date	Reason
11	Friday, April 11, 2015 10:48:37 AM	Cessation of operation
14	Friday, April 11, 2015 10:48:03 AM	Key compromise
13	Friday, April 11, 2015 10:46:38 AM	Unspecified
15	Friday, April 11, 2015 10:46:31 AM	Unspecified
16	Friday, April 11, 2015 10:46:18 AM	Unspecified

7.7.2 Génération d'une liste de révocation

L'opération de génération d'une liste de révocation est disponible dans la **Page d'accueil de l'autorité de certification** en accès authentifié (voir la section Accès authentifié).

Cette opération ne propose pas de page de sélection d'options, mais génère et publie immédiatement la nouvelle CRL conformément aux options spécifiées dans les paramètres généraux de gestion des certificats (voir la section Listes de révocation (CRLs)).

Lorsque l'opération est terminée, le compte rendu de l'opération est affiché, suivi de la nouvelle CRL. Pour plus d'information sur l'affichage de la nouvelle CRL, référez-vous à la section Consultation de la liste de révocation .

7.7.3 Génération automatique des listes de révocation

Stormshield Data Authority Manager peut générer automatiquement les listes de révocation à la fréquence et à l'heure souhaitée.

Pour que cette opération soit active, la base doit être démarrée.

La fréquence de génération se définit dans la page **Paramètres généraux de gestion des certificats** (voir la section Service de génération automatique des CRLs).

8. Gestion des utilisateurs

Cette section présente les différents types d'utilisateurs et décrit comment définir, créer et diffuser les comptes utilisateurs.

8.1 Types d'utilisateurs

Les utilisateurs sont associés à un compte de sécurité qui contient leurs clés et les paramètres de fonctionnement de la suite Stormshield Data Security. Tous les utilisateurs dont la clé publique est certifiée par la même autorité de certification sont regroupés dans la même base de données. La segmentation et la répartition des utilisateurs dépendent de considérations organisationnelles et de choix d'entreprise.

Les différents types d'utilisateurs gérés sont :

- le modèle d'utilisateur (voir la section Modèle) ;
- le compte de recouvrement (voir la section Compte de recouvrement) ;
- le signataire de politiques de sécurité (voir la section Signataire de politiques de sécurité) ;
- l'utilisateur "standard", qui peut éventuellement dériver d'un modèle (voir la section Utilisateur standard).

8.1.1 Modèle

Un modèle d'utilisateur n'est pas un utilisateur comme les autres : il possède ni clés, ni certificats. Par contre, il possède les informations nécessaires pour créer les clés et les certificats des utilisateurs qui vont dériver de lui. Il possède aussi les configurations des composants de la suite Stormshield Data Security. Elles peuvent être diffusées dans un master.

Un modèle permet :

- de créer des utilisateurs plus rapidement en réutilisant les paramètres du modèle (voir la section Création à partir d'un modèle et la section Création à partir d'un annuaire LDAP) ;
- de centraliser la gestion du mot de passe de secours (voir la section Modifications des mots de passe)
- de centraliser la définition des configurations des composants Stormshield Data Security (voir la section Présentation) :
  - Stormshield Data Virtual Disk ;
  - Stormshield Data File ;
  - Stormshield Data Kernel ;
  - Stormshield Data Mail ;
  - Stormshield Data Shredder ;
  - Stormshield Data Sign ;
  - Stormshield Data Team.

8.1.2 Compte de recouvrement

IMPORTANT
La création d'un compte de recouvrement nécessite de prendre certaines précautions sur le stockage de ce compte : il est critique pour la sécurité des données chiffrées avec les comptes

utilisateurs utilisant ce recouvrement. Il doit être muni d'un mot de passe suffisamment robuste et être conservé en lieu sûr ou mieux, être équipé d'une carte à puce.

La création de comptes de recouvrement dans la base des utilisateurs est liée à un choix d'organisation pour le fonctionnement de la politique de confidentialité en entreprise.

Un compte de recouvrement est un compte utilisateur normal pour l'utilisation des composants de Stormshield Data Security. Vous pouvez, avec un tel compte, déchiffrer tout ce qui a été automatiquement chiffré avec son certificat.

Le certificat de la clé de recouvrement d'un compte de recouvrement créé dans la base est intégré automatiquement à tous les comptes utilisateurs créés dans cette base. Ainsi, tout ce que les utilisateurs chiffreront sera chiffré avec le certificat de recouvrement.

Après la création d'un compte de recouvrement le certificat de celui-ci est automatiquement rajouté aux comptes des utilisateurs lors d'une mise à jour de politique de sécurité (*.usx*).

La suppression des comptes de recouvrement n'est pas gérée par cette fonctionnalité, c'est-à-dire que leurs certificats ne sont pas supprimés des comptes des utilisateurs.

Lors d'un renouvellement de certificat d'un compte de recouvrement, cette fonctionnalité ajoute le nouveau certificat sans mettre à jour l'ancien certificat dans les comptes des utilisateurs.

Si vous souhaitez mettre en place une politique de cloisonnement (c'est-à-dire des comptes Stormshield Data Security avec des clés de recouvrement différentes), utilisez plusieurs bases d'utilisateurs.

8.1.3 Signataire de politiques de sécurité

IMPORTANT
La création d'un signataire de politiques de sécurité nécessite de prendre certaines précautions sur le stockage de ce compte : il est critique pour la définition de votre politique de sécurité.

Un signataire de politiques de sécurité est utilisé lors de la diffusion d'une mise à jour de compte utilisateur. C'est le certificat de ce compte qui authentifie Stormshield Data Authority Manager. Il permet de garantir l'authenticité et la validité des fichiers de mise à jour des politiques de sécurité.

On ne peut créer qu'un seul signataire de politiques de sécurité par base de données.

Lors de la diffusion d'un compte utilisateur, les règles de diffusion du certificat du signataire de politiques de sécurité sont les suivantes :

- lors d'une diffusion complète, si un signataire existe, son certificat est ajouté au compte de l'utilisateur ;
- lors de la diffusion d'une mise à jour, la présence d'un signataire étant obligatoire, son certificat est ajouté au fichier de mise à jour.

Ainsi, lorsque l'utilisateur utilise le fichier de mise à jour :

- si le certificat du signataire est identique dans le fichier de mise à jour et dans son compte Stormshield Data Security, alors les configurations des composants sont mises à jour. L'authentification effectuée garantit que les mises à jour des configurations ont bien été générées par Stormshield Data Authority Manager ;
- dans le cas contraire, l'utilisateur doit accorder sa confiance au certificat provenant de son fichier de mise à jour pour valider l'opération. Le certificat du signataire est alors importé dans le compte utilisateur.

Il est donc préférable de créer un signataire de politiques de sécurité avant de faire une diffusion complète.

Le certificat du signataire de politiques de sécurité est visible dans le panneau de configuration de Stormshield Data Security, dans le porte-clés de l'utilisateur, dans l'onglet Stormshield Data Authority Manager.

Vous pouvez créer un signataire de politique de sécurité à partir d'un fichier *PKCS#12* (voir la section Création à partir d'un fichier PKCS#12).

8.1.4 Utilisateur standard

Un utilisateur standard n'a aucune des propriétés particulières d'une autorité de certification, d'un modèle, d'un compte de recouvrement ou d'un signataire de politiques de sécurité.

L'utilisateur peut posséder plus de deux clés.

Mais une seule clé peut avoir le rôle de chiffrement .

Et une seule clé peut avoir le rôle de signature .

Les autres clés sont, soit des clés qui ont simplement l'usage de signature , soit des clés de déchiffrement .

L'usage de la clé (chiffrement et / ou signature) dépend des usages X.509 du certificat associé à la clé.

Le rôle de la clé (clé de chiffrement / clé de déchiffrement, clé de signature / clé avec l'usage de signature) est modifiable dans la page des **Propriétés** de la clé (voir la section Page Propriétés de la clé).

8.2 Page Gestion des utilisateurs

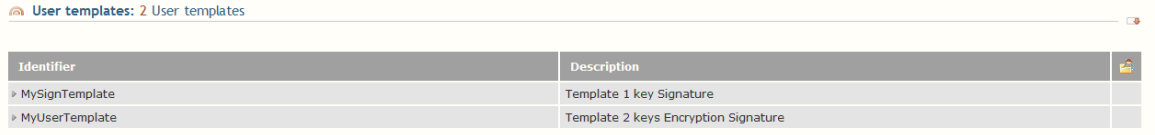
La page **Gestion des utilisateurs** est une page de menu centrale qui conduit à :

- la gestion des modèles d'utilisateur (voir la section Page Liste des modèles) ;
- la liste des utilisateurs (voir la section Page Liste des utilisateurs) ;
- la gestion des certificats externes de recouvrement (voir la section Certificats externes de recouvrement).

Cette page est accessible à partir de la page d'accueil ou à partir du menu déroulant principal.

8.3 Page Liste des modèles

La page **Liste des modèles** est la page centrale de gestion des modèles dans Stormshield Data Authority Manager. Elle est accessible à partir de la page **Gestion des utilisateurs** ou du menu déroulant principal.



Elle affiche la liste des modèles présents dans la base, en indiquant pour chacun :

- l'identifiant du modèle. S'il est tronqué à l'affichage, il est visible en entier dans une bulle ;
- la description saisie lors de la création du modèle. S'il est tronqué à l'affichage, il est visible en entier dans une bulle ;
- un indicateur de diffusion d'un master à partir de ce modèle.

A partir du menu déroulant **Opérations**, vous pouvez créer un modèle (voir la section Création d'un modèle d'utilisateur).

En cliquant sur l'identifiant du modèle, vous accédez à sa page (voir la section Page Modèle).

8.3.1 Création d'un modèle d'utilisateur

Vous accédez à la page de création d'un modèle d'utilisateur à partir du menu déroulant **Opérations** de la page **Liste des modèles**.

Les données d'un modèle sont de deux natures :

- celles qui concernent uniquement le modèle ;
- celles qui sont utilisées lors de la création d'un utilisateur à partir de ce modèle.

Les données du modèle sont :

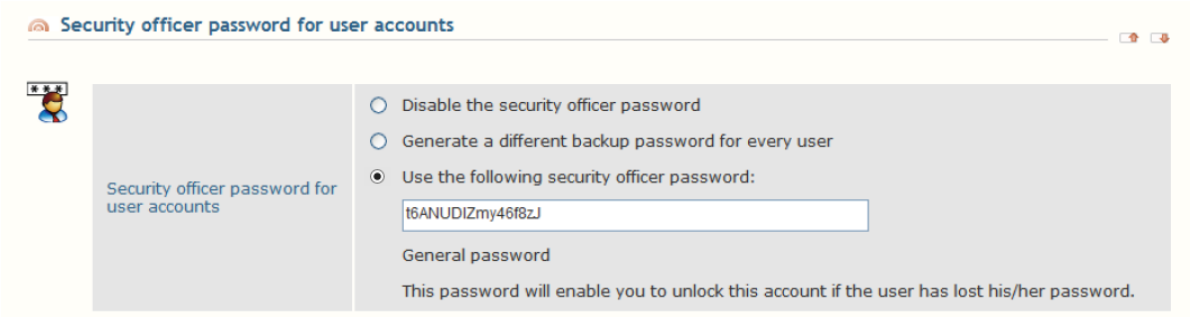
- l'identifiant utilisé par Stormshield Data Authority Manager pour référencer le modèle. Cet identifiant est utilisé comme nom pour le master, et il ne doit pas contenir les caractères \ / : * ? <> |
- une description optionnelle ;
- un mot de passe de protection d'un éventuel master diffusé à partir de ce modèle (un tirage aléatoire de 16 caractères est proposé par défaut).
- Le DN de l'entrée LDAP utilisée lors de la publication dans l'annuaire LDAP du fichier de mise à jour.

Les données utilisées pendant la création

Les données destinées à la création d'un utilisateur à partir de ce modèle sont :

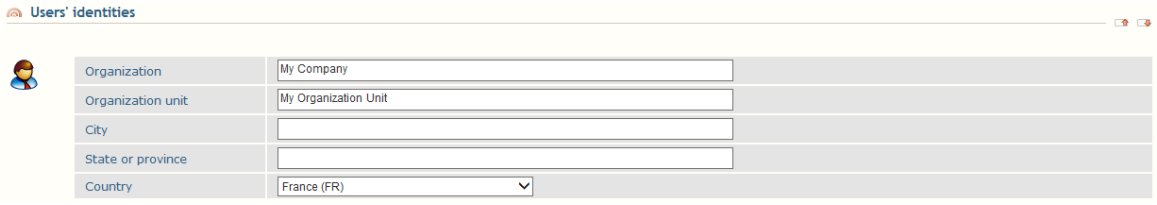
- un algorithme de chiffrement (par défaut AES 256 bits) ;
- un algorithme d'empreinte (par défaut SHA-512) ;

- le mot de passe de secours. Cette section est initialisée selon la configuration définie dans les paramètres généraux (voir la section Mot de passe de secours). Vous pouvez en plus choisir d'imposer la génération d'un mot de passe de secours aléatoire pour chaque utilisateur créé à partir du modèle.

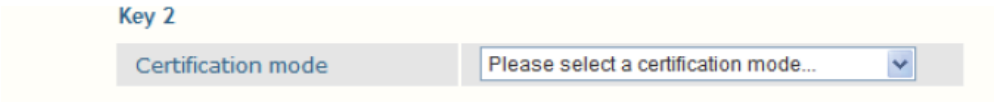


NOTE
La fonctionnalité de déblocage de compte à distance (voir la section Déblocage de compte à distance) ne peut pas être mise en œuvre pour un compte diffusé avec un mot de passe de secours de plus de 16 caractères. Cette limite est la longueur des mots de passe de secours aléatoires proposés par Stormshield Data Authority Manager.

- l'identité de l'utilisateur. Elle sera inscrite dans son certificat.



- les données pour créer et certifier les clés. Vous pouvez indiquer la création d'une seule clé en ne sélectionnant aucun mode de certification pour une des deux clés.



Pour chaque clé, les données sont :

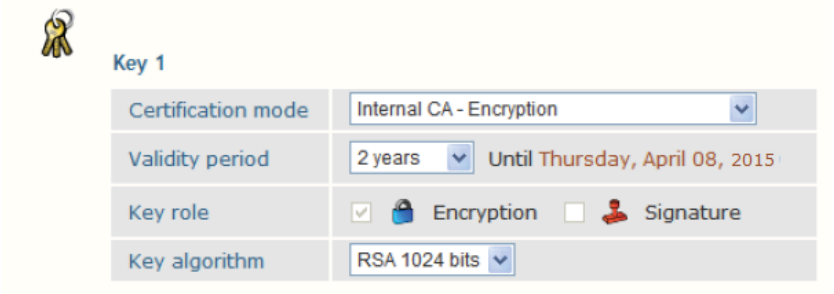
- l'algorithme de chiffrement avec sa force ;
- le mode de certification : en plus de la ligne indiquant que vous devez sélectionner un mode de certification, et qui permet de ne pas créer de clé, le menu déroulant contient la liste des modèles de certificat et la liste des autorités de certification externes.

Si vous sélectionnez un modèle de certificat :

- si la base possède une autorité de certification interne certifiée, la clé sera certifiée par cette autorité de certification,
- sinon, la clé sera auto-certifiée. Cette information est alors précisée.

Dans les deux cas, les données du modèle de certificat seront utilisées.

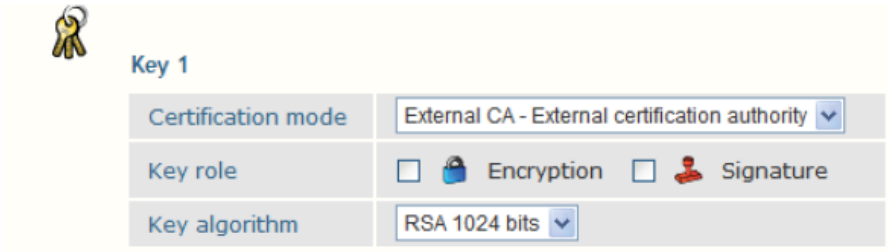
- La durée de validité, pré-remplie à l'aide de celle du modèle de certificat, est modifiable.
- La ligne **Rôle de la clé** indique quels seront le ou les rôles de la future clé. Ils sont déterminés à partir des usages X.509 du modèle de certificat. Ils ne sont donc pas modifiables.



Si vous sélectionnez une autorité de certification externe, lors de la création de l'utilisateur, la clé sera tirée mais pas certifiée. Vous devrez effectuer une demande de certificat pour cette clé et ensuite importer le certificat fourni.

L'autorité de certification externe sélectionnée est associée à la clé et ses données seront utilisées lors de la demande de certificat.

Afin de faciliter par la suite la gestion des clés de l'utilisateur, vous pouvez indiquez sur la ligne **Rôle de la clé**, à l'aide des cases à cocher, le rôle souhaité pour cette clé. Sachant que, à terme, ce seront les usages X.509 du futur certificat qui feront foi, et fixeront le ou les rôles de la clé.



8.3.2 Page Modèle

La page **Modèle** est accessible à partir de la page **Liste des modèles** en cliquant sur l'**identifiant** du modèle.

Elle affiche :

- les données propres au modèle : identifiant, description, DN de l'entrée LDAP, date de création, date de dernière modification et éventuellement date de diffusion d'un master ;
- les données destinées à la création d'un utilisateur à partir de ce modèle : identité, liste des clés, algorithmes de protection du compte.

La liste des clés indique : le mode de certification choisie, la durée de validité du futur certificat dans le cas du choix d'un modèle de certificat, le rôle de la clé et l'algorithme de chiffrement avec sa force.

Dans le bandeau en haut de la page, un menu contient les options suivantes :

- dans l'onglet *Propriétés*, vous accédez à la page des propriétés du modèle (voir la section Modifications des mots de passe)
- dans l'onglet *Gestion du modèle*, vous pouvez :
- diffuser un master (voir la section Diffusion d'un master) :
- avec la configuration de connexion mode mot de passe ou avec la configuration de connexion mode carte dans le but de l'utiliser avec Stormshield Data Security (fichier *.usr*),
- avec toutes les configurations dans le but d'exporter un modèle vers une autre base (fichier *.msr*),
- diffuser un fichier de mise à jour de la politique de sécurité (*.usx*) soit avec la configuration "mot de passe" soit avec la configuration "carte" (voir la section Diffusion d'un fichier de mise à jour de la politique de sécurité (.usx)) ;
- dupliquer un modèle (voir la section Création de modèle par duplication d'un modèle existant) ;
- supprimer le modèle. Cette opération est possible seulement si le modèle n'est pas référencé par un utilisateur ou la personnalisation de l'installation ;
- dans l'onglet *Composants*, vous pouvez :
- configurer les composants suivants :
- Stormshield Data Virtual Disk ;
- Stormshield Data File ;
- Stormshield Data Kernel ;
- Stormshield Data Mail ;
- Stormshield Data Shredder ;
- Stormshield Data Sign ;
- Stormshield Data Team ;
- importer les configurations des composants à partir d'un master (fichier *.msr*) ;
- dans l'onglet *Opérations*, ouvrir la page de création d'un utilisateur à partir d'un modèle (voir la section Création à partir d'un modèle).

8.3.3 Page Propriétés du modèle

La page **Propriétés du modèle** est accessible à partir de la page **Modèle** (voir la section Page Modèle), dans l'onglet *Propriétés*.

Elle est identique à la page de création (voir la section Création d'un modèle d'utilisateur). Dans cette page, vous pouvez modifier tout à l'exception de l'identifiant du modèle. Si le modèle a deux clés, vous pouvez supprimer une clé en ne sélectionnant aucun mode de certification pour une des deux clés.

La section traitant du mot de passe de secours est composée de deux parties :

- Une partie **Mot de passe de secours des comptes utilisateurs** qui permet de condamner, générer un mot de passe de secours différent pour chaque utilisateur ou utiliser un mot de passe défini.

> **NOTE**
> La fonctionnalité de déblocage de compte à distance (voir la section Déblocage de compte à distance) ne peut pas être mise en œuvre pour un compte diffusé avec un mot de passe de

secours de plus de 16 caractères. Cette limite est la longueur des mots de passe de secours aléatoires proposés par Stormshield Data Authority Manager.

- Une partie **Historique des mots de passe de secours** qui contient la liste des mots de passe de secours déjà définis pour le modèle. Cette liste présente les événements du plus récent au plus ancien.

L'administrateur doit ensuite cliquer sur **Appliquer les modifications** si un nouveau mot de passe de secours a été saisi ou s'il est condamné.

Le dernier mot de passe de secours saisi s'affiche automatiquement à chaque affichage de la page **Propriétés du modèle** dans la boîte **Utiliser le mot de passe de secours suivant**.

8.3.4 Diffusion d'un master

Cette opération est disponible à partir de l'onglet *Gestion du modèle*, du menu de la page **Modèle**.

Cette opération crée un master dans le dossier `<user_account_dir>/<template_id>` où `<user_account_dir>` est le dossier de diffusion défini dans les paramètres généraux, et `<template_id>` est l'identifiant du modèle.

Si des fichiers listes sont associés aux configurations des composants Stormshield Data File et Stormshield Data Shredder, ils sont aussi copiés dans le dossier `<user_account_dir>/<template_id>`.

Dans le cas de la diffusion avec une configuration de connexion mode mot de passe ou avec une configuration de connexion mode carte (voir la section Configurations du composant Stormshield Data Kernel), le master est un fichier *.usr*.

Lors de la création de ce fichier master, si les tags `<LdapDn>` ou `<UserId>` sont utilisés dans les points de distribution présents dans la configuration du composant **Téléchargement des politiques de sécurité**, ils sont remplacés par les données du modèle (voir la section Configuration du composant Téléchargement des politiques de sécurité).

Dans le cas de la diffusion avec toutes les configurations, le master est un fichier *.msr*. Cette fonctionnalité, associée à la fonction **importation des configurations des composants à partir d'un master (fichier *.msr*)**, permet d'échanger des modèles entre plusieurs bases.

8.3.5 Importation de configuration des composants à partir d'un master (fichier *.msr*)

Cette opération est disponible à partir de l'onglet *Composants*, du menu de la page **Modèle**.

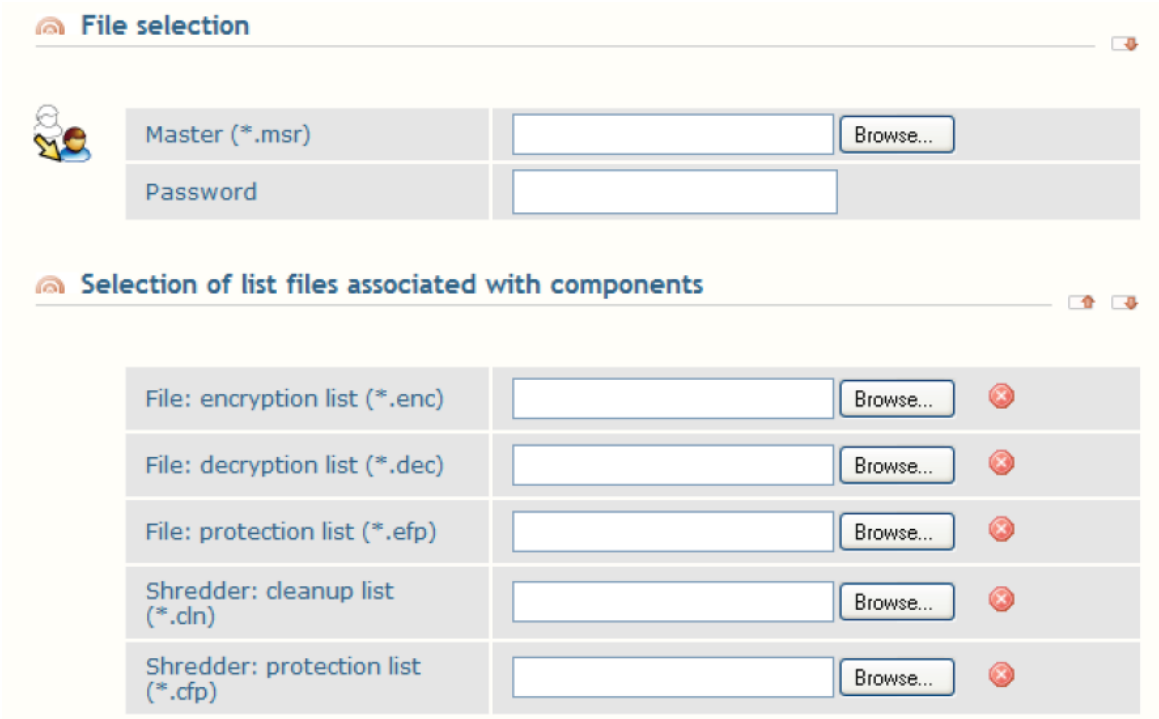
Elle permet d'importer les configurations des composants à partir d'un master (fichier *.msr*), ainsi que les éventuels fichiers listes associés aux configurations des composants Stormshield Data File et Stormshield Data Shredder.

Un master (fichier *.msr*) est obtenu en exportant un modèle (voir la section Diffusion d'un master). Vous pouvez utiliser cette fonctionnalité pour échanger des modèles entre plusieurs bases.

IMPORTANT
Lors de cette opération, les configurations des composants sont remplacées par celles provenant du fichier, et sont donc définitivement perdues.

Pour importer les configurations:

1. Sélectionnez un master (fichier *.msr*).
2. Saisissez son mot de passe.
3. Sélectionnez les éventuels fichiers listes associés aux composants.
4. Cliquer sur **Importer**.



8.3.6 Diffusion d'un fichier de mise à jour de la politique de sécurité (*.usx*)

Diffusion

Cette opération est disponible à partir de l'onglet *Gestion du modèle*, du menu de la page **Modèle**.

Cette opération crée un fichier de mise à jour de la politique de sécurité dans le dossier `<user_account_dir>/<template_id>` où `<user_account_dir>` est le dossier de diffusion défini dans les paramètres généraux, et `<template_id>` est l'identifiant du modèle.

Pour diffuser des fichiers de mise à jour, il faut au préalable créer un compte signataire de politique de sécurité (section Création d'un signataire de politiques de sécurité).

Utilisation

Cette mise à jour, générée à partir d'un modèle, peut s'appliquer à tous les utilisateurs. Elle contient soit la configuration « mot de passe » soit la configuration « carte » (voir la section Configurations du composant Stormshield Data Kernel).

Lors de la création de ce fichier de mise à jour "générique", si les tags `<LdapDn>` ou `<UserId>` sont utilisés dans les points de distribution présents dans la configuration du composant **Téléchargement des politiques de sécurité**, ils sont remplacés par les données du modèle (voir la section Configuration du composant Téléchargement des politiques de sécurité).

Publication

Afin que les mises à jour soient disponibles par téléchargement automatique, Stormshield Data Authority Manager permet de les publier :

- dans l'annuaire LDAP (voir la section Création d'un modèle d'utilisateur), dans l'attribut `sboxPolicyUpgrade;binary` défini dans les paramètres LDAP (voir la section Nom des attributs).

> **NOTE**
> Vérifiez que les entrées LDAP des utilisateurs appartiennent à une classe acceptant cet attribut. Si nécessaire, vous pouvez créer une nouvelle classe `sboxPerson` acceptant cet attribut, et faire dériver les entrées de vos utilisateurs de cette classe.

- par fichier. Le fichier de mise à jour est copié dans le dossier paramétré (voir la section Publication des mises à jour de politiques de sécurité).

8.3.7 Création de modèle par duplication d'un modèle existant

Cette opération est disponible à partir de l'onglet *Gestion du modèle*, du menu de la page **Modèle**.

Vous pouvez créer un modèle à partir d'un modèle existant. Cette fonctionnalité permet, par exemple, de créer rapidement des modèles similaires à l'intérieur de la même base.

Vous avez seulement à saisir :

- l'identifiant utilisé par Stormshield Data Authority Manager pour référencer le modèle. Cet identifiant est utilisé comme nom du master et ne doit pas contenir les caractères \ / : * ? < > |
- une description optionnelle ;
- un mot de passe de protection d'un éventuel master diffusé à partir de ce modèle (un tirage aléatoire de 16 caractères est proposé par défaut).

Après validation, le modèle est créé et vous accédez à une page de compte rendu qui comporte un lien d'accès au modèle créé, et qui permet de recommencer l'opération de duplication.

8.4 Page Liste des utilisateurs

La page **Liste des utilisateurs** est la page centrale de la gestion des utilisateurs dans Stormshield Data Authority Manager.

8.4.1 Opérations disponibles

Le bandeau en haut de la page propose un menu d'opérations.

Création d'utilisateurs spéciaux

Les sections suivantes décrivent la création des différents utilisateurs spéciaux :

- comptes de recouvrement (section Création d'un compte de recouvrement) ;
- signataires de politiques de sécurité (section Création d'un signataire de politiques de sécurité).

Création d'utilisateurs standards

Les sections suivantes décrivent la création des différents utilisateurs standards :

- création avancée (voir la section Création avancée) ;
- création à partir d'un modèle (voir la section Création à partir d'un modèle) ;
- création à partir d'une liste contenue dans un fichier (voir la section Création d'un grand nombre d'utilisateurs à partir d'un fichier) ;
- création à partir d'une carte à puce (voir la section Création à partir d'un support cryptographique physique) ;
- création à partir d'un fichier *PKCS#12* (voir la section Création à partir d'un fichier PKCS#12) ;
- création à partir d'un fichier utilisateur (voir la section Création à partir d'un fichier utilisateur).

Gestion des utilisateurs

Actions à effectuer pour les utilisateurs sélectionnés parmi les utilisateurs des deux listes de la page :

- renouvellement de clé (voir la section Renouveler plusieurs clés).
- certification (voir la section Renouvellement de plusieurs certificats) ;
- diffusion (voir la section Diffusion de plusieurs comptes) ;
- suppression (voir la section Suppression de plusieurs utilisateurs) ;
- révocation des utilisateurs (voir la section Révocation d'utilisateurs).

A partir de ce menu vous accédez aussi au déblocage de compte à distance (voir la section Déblocage de compte à distance).

Gestion des certificats

Actions à effectuer pour les utilisateurs sélectionnés parmi les utilisateurs des deux listes de la page :

- création des demandes de certificats (voir la section Création de demande) ;
- annulation des demandes de certificats (voir la section Annulation de demande) ;
- importation de certificats (voir la section Importation de plusieurs certificats) ;
- exportation de certificats (voir la section Exportation de plusieurs certificats).

Gestion du LDAP

- opérations de synchronisation avec un serveur LDAP (voir la section Synchronisation avec un annuaire LDAP) ;

8.4.2 Recherche d'utilisateurs

La liste d'utilisateurs contient le résultat de la recherche effectuée dans la base de données.

Une recherche peut être rapidement effectuée en cliquant sur une des lettres du bandeau : tous les utilisateurs dont le nom usuel commence par cette lettre sont alors affichés.

Il est possible d'afficher tous les utilisateurs en cliquant sur l'icône .

Les critères de recherche sont affichés ou masqués en cliquant sur le lien **Critères de recherche**.

L'icône permet de réinitialiser tous les critères de recherche.

Les critères de recherche sont organisés en cinq thèmes :

1. Le filtre de présélection d'identifiants à partir d'un fichier *.csv* : sélectionnez un fichier *.csv* au format ANSI, contenant les identifiants des utilisateurs en première colonne. Le séparateur utilisé dans le fichier *.csv* peut être une virgule, un point-virgule, un espace, une barre verticale.
   Si vous quittez la page de recherche, le nom du fichier *.csv* n'est pas conservé. Il faut donc le sélectionner de nouveau.
2. L'identité de l'utilisateur : nom usuel, adresse e-mail, identifiant, description, organisation, unité, ville, état et pays. Pour chaque élément, à l'exception du pays, vous pouvez saisir une chaîne pouvant contenir le méta caractère * en début et/ou en fin de mot pour remplacer plusieurs caractères.
3. L'une des propriétés suivantes du compte :

- « Nécessitant une diffusion » : le compte est considéré par Stormshield Data Authority Manager comme étant à diffuser, quand :
  - il n'a pas encore été diffusé ;
  - le mot de passe usuel ou le mot de passe de secours de l'utilisateur a été modifié ;
  - un nouveau certificat a été importé pour l'utilisateur ;
  - la configuration d'un composant a été modifiée pour cet utilisateur ou ce modèle ;
  - un compte de recouvrement a été créé ou supprimé ;
  - un nouveau certificat a été importé pour un compte de recouvrement ;
  - les propriétés d'un compte de recouvrement ont été modifiées ;
  - un certificat externe a été ajouté ou supprimé.
- « Ayant pour modèle » : la configuration des composants du compte dérive de celle du modèle sélectionné. Il est possible aussi de sélectionner les utilisateurs ne dérivant d'aucun modèle.
- « Associé à une carte » : le compte a été créé à partir d'une carte, ou bien a été créé puis associé à une carte.
- « Possédant une clé non certifiée » : au moins une des clés de l'utilisateur n'est pas certifiée.

4. Une propriété du certificat courant d'au moins une de ses clés :

- Délais d'expiration ;
- Demande de certificat en cours ou non ;
- Auto-certifié.

5. Le type d'utilisateur : standard ou spécial (recouvrement, signataire de politiques de sécurité).

Ces critères de recherche s'ajoutent.

La recherche est effectuée en cliquant sur le bouton **Lancer la recherche**. La page est alors rechargée, et la liste d'utilisateurs est mise à jour.

L'affichage du résultat est effectué par lots, c'est-à-dire qu'un nombre limité d'utilisateurs trouvés est affiché dans la page. Ce nombre d'utilisateurs est défini dans la section **Affichage** des critères de recherche. Des boutons de navigation permettent de se déplacer d'une page de résultat à l'autre.

Les utilisateurs sont affichés dans l'ordre alphabétique. Dans la liste, pour chaque utilisateur, les informations sont structurées de la façon suivante :

1. La première colonne contient le nom usuel de l'utilisateur. S'il est tronqué à l'affichage, il est visible en entier dans la bulle. Si l'utilisateur est un utilisateur spécial une icône est affichée dans cette colonne :

- compte de recouvrement ;
- signataire de politique de sécurité.

2. La deuxième colonne contient l'e-mail de l'utilisateur. S'il est tronqué à l'affichage, il est visible en entier dans la bulle.
3. La case à cocher de la troisième colonne permet de sélectionner l'utilisateur afin que lui soit appliquée une action.

Le nombre total d'utilisateurs présents dans la base est affiché dans le titre de la section.

Le nombre d'utilisateurs satisfaisants les critères de recherche est affiché dans le titre de la première colonne. Elle contient aussi le lot d'utilisateurs affichés dans la page.

Le nombre d'utilisateurs sélectionnés à l'aide de la case à cocher de la troisième colonne est affiché dans le titre de la deuxième colonne. Vous pouvez sélectionner tous les utilisateurs retournés par la recherche en cliquant sur l'icône , et tous les désélectionner en cliquant sur l'icône .

La dernière icône indique si tous les utilisateurs de la page sont sélectionnés (icône), si certains utilisateurs sont sélectionnés (icône), ou si aucun utilisateur n'est sélectionné (icône). Cliquer sur ces icônes permet de sélectionner ou de désélectionner tous les utilisateurs de la base.

8.5 Création d'utilisateurs

Les opérations de création décrites dans cette section sont accessibles à partir de la page principale **Liste des utilisateurs** (section Page Liste des utilisateurs).

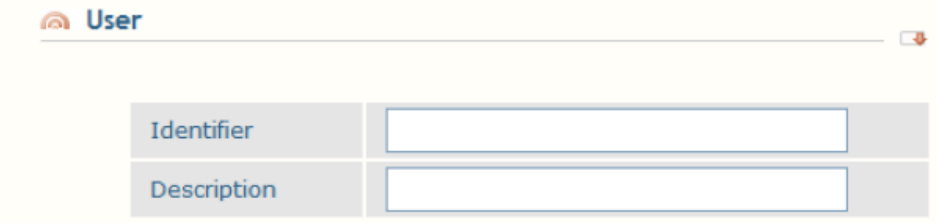
8.5.1 Création avancée

L'opération de **Création avancée** est disponible à partir de l'onglet *Créations d'utilisateurs*, du menu de la page **Liste des utilisateurs**.

1. Dans la section **Utilisateur** de la page de création, saisissez :

a. l'identifiant du compte utilisateur. Cet identifiant est utilisé comme nom du fichier compte et du fichier annuaire, il ne doit donc pas contenir les caractères \ / : * ? " < > | . Il est limité à 32 caractères.

b. une description.

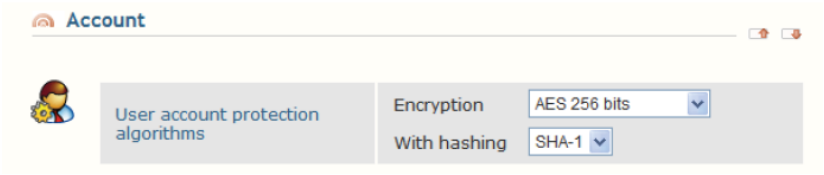


2. Dans la section **Compte** saisissez :

a. un algorithme de chiffrement (par défaut AES 256 bits) ;

b. ainsi qu'un algorithme d'empreinte (par défaut SHA-512).

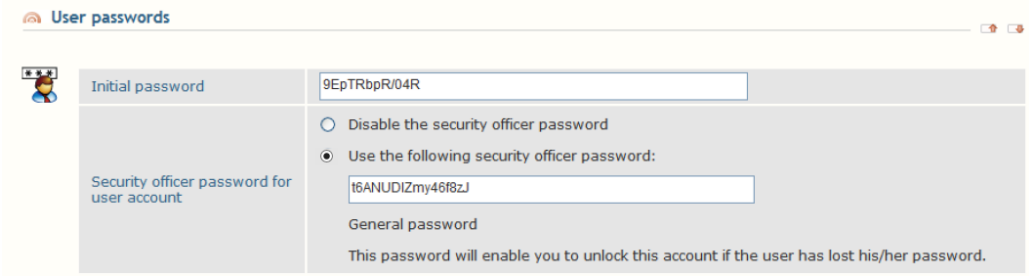
Ils servent à protéger le compte.



3. Dans la section des **mots de passe** saisissez :

a. le mot de passe du compte (un tirage aléatoire de 16 caractères est proposé par défaut) ;

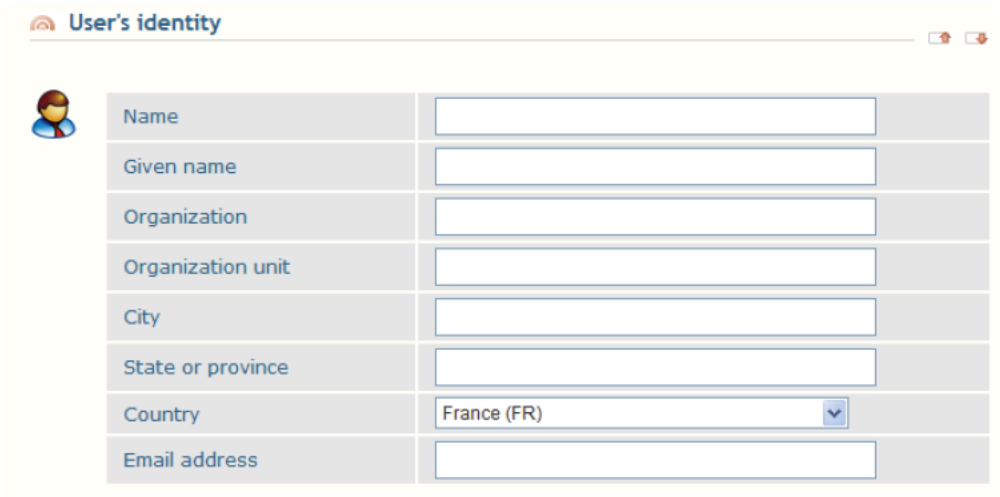
b. le mot de passe de secours. Cette section est initialisée selon la configuration définie dans les paramètres généraux (voir la section Mot de passe de secours).



NOTE

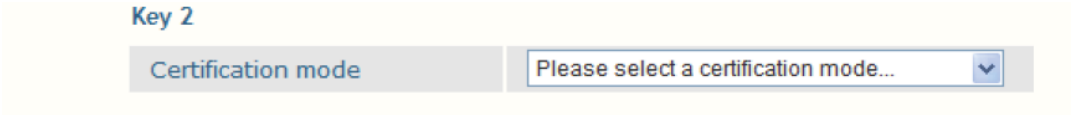
La fonctionnalité de déblocage de compte à distance (voir la section Déblocage de compte à distance) ne peut pas être mise en œuvre pour un compte diffusé avec un mot de passe de secours de plus de 16 caractères. Cette limite est la longueur des mots de passe de secours aléatoires proposés par Stormshield Data Authority Manager.

4. Saisissez ensuite l'identité de l'utilisateur. Elle sera inscrite dans son certificat.



5. La section suivante permet de définir le nombre et le rôle des clés de l'utilisateur, ainsi que les données nécessaires à leur certification :

Vous pouvez indiquer la création d'une seule clé en ne sélectionnant aucun mode de certification pour une des deux clés.



Pour chaque clé les données sont :

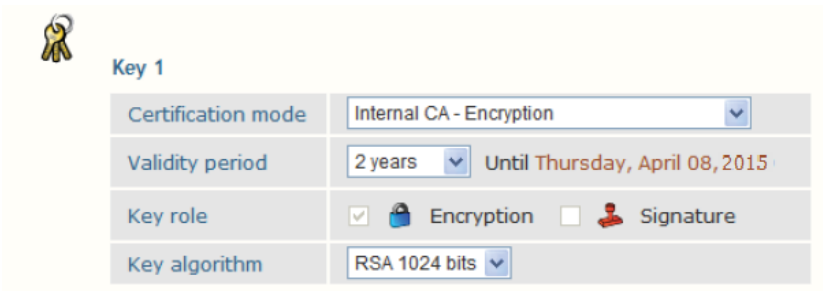
- l'algorithme de chiffrement avec sa force ;
- le mode de certification : en plus de la ligne indiquant que vous devez sélectionner un mode de certification, et qui permet de ne pas créer de clé, le menu déroulant contient la liste des modèles de certificat et la liste des autorités de certification externes.

Si vous sélectionnez un modèle de certificat :

- si la base possède une autorité de certification interne certifiée, la clé est certifiée par cette autorité de certification ;
- sinon, la clé est auto-certifiée. Cette information est alors précisée.

Dans les deux cas, les données du modèle de certificat sont utilisées.

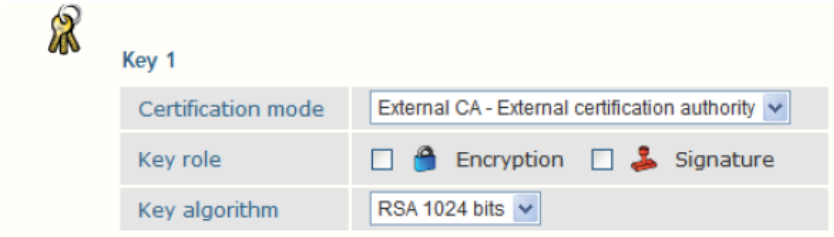
- La durée de validité, pré-remplie à l'aide de celle du modèle de certificat, est modifiable.
- La ligne **Rôle de la clé** indique quels seront le ou les rôles de la future clé. Ils sont déterminés à partir des usages X.509 du modèle de certificat. Ils ne sont donc pas modifiables.



Si vous sélectionnez une autorité de certification externe, la clé est tirée mais pas certifiée. Vous devez effectuer une demande de certificat pour cette clé et ensuite importer le certificat fourni.

L'autorité de certification externe sélectionnée est associée à la clé et ses données seront utilisées lors de la demande de certificat.

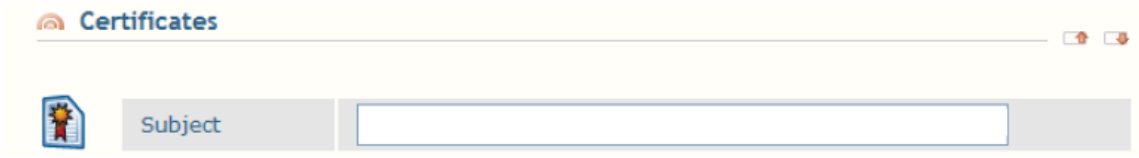
Afin de faciliter par la suite la gestion des clés, vous pouvez indiquez sur la ligne **Rôle de la clé**, à l'aide des cases à cocher, le rôle souhaité pour cette clé. Sachant que, à terme, ce seront les usages X.509 du futur certificat qui feront foi, et fixeront le ou les rôles de la clé.



6. Vérifiez le sujet qui est inclus dans le certificat. Ce sujet est obtenu automatiquement par résolution du masque spécifié dans les paramètres généraux (voir la section Identité) en utilisant l'identité de l'utilisateur. Vous pouvez le modifier manuellement, mais il doit rester conforme à la norme RFC 2253.

Lorsque le compte possède deux clés, le sujet est identique dans les deux certificats, il n'est donc à spécifier qu'une seule fois.

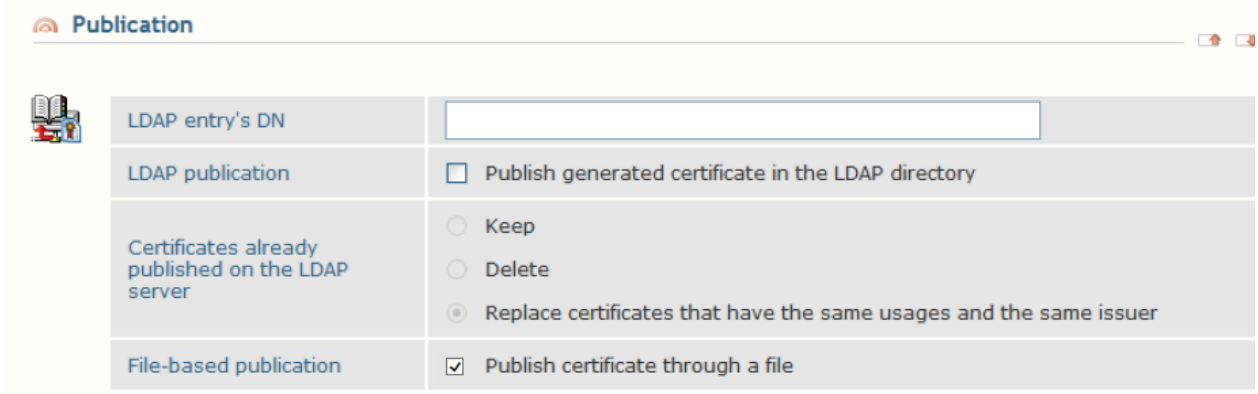
Les clés sont générées automatiquement par le module cryptographique logiciel Stormshield Data Crypto.



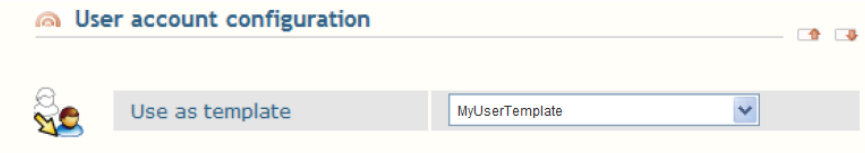
7. Dans la section **Publication** :

a. Saisissez le masque de résolution du DN LDAP en incluant les tags <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>,<State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>, <SecurityBoxUserId>. Lors de la résolution du DN, ces tags sont remplacés par les champs correspondants de l'identité de l'utilisateur.

b. Choisissez le mode de publication des certificats (section Publication d'un certificat).



Vous pouvez choisir d'avoir un utilisateur standard qui hérite de la politique de sécurité d'un modèle (voir la section Modèle). Ce choix peut être modifié après la création du compte (voir la section Choix du modèle). La liste contient les modèles présents dans la base.



8.5.2 Création à partir d'un modèle

Cette opération est disponible à partir de l'onglet *Créations d'utilisateurs*, du menu de la page **Liste des utilisateurs**, en cliquant sur le lien **A partir d'un modèle** (section Opérations disponibles).

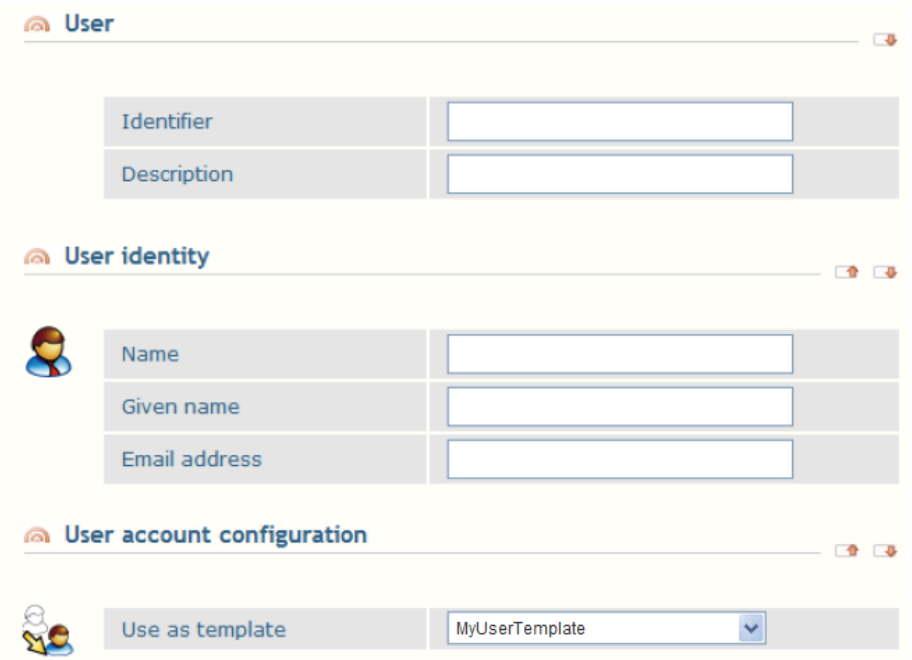
1. Saisissez l'identifiant, la description, le nom, le prénom et l'adresse e-mail.
2. Choisissez le mode de publication du ou des certificats (section Publication d'un certificat).
3. Sélectionnez un modèle parmi les modèles présents dans la base.

Le mot de passe du compte est composé de 16 caractères tirés aléatoirement. Vous pourrez consulter et modifier ce mot de passe une fois l'utilisateur créé.

Les autres informations sont extraites automatiquement du modèle :

- l'algorithme de chiffrement du compte ;
- l'algorithme d'empreinte ;
- les autres informations générales constituant l'identité de l'utilisateur ;
- le nombre de clés, leurs tailles et le mode de certification.

L'utilisateur hérite aussi du mot de passe de secours (voir la section section Page Utilisateur et Choix du modèle).



8.5.3 Création d'un grand nombre d'utilisateurs à partir d'un fichier

Cette opération est disponible à partir de l'onglet *Créations d'utilisateurs*, du menu de la page **Liste des utilisateurs**, en cliquant sur le lien **A partir d'un fichier** (section Opérations disponibles).

Elle permet de créer à partir d'un fichier, et de manière automatique, un grand nombre d'utilisateurs.

Pour que cette opération soit disponible, la base de données doit posséder au moins un modèle.

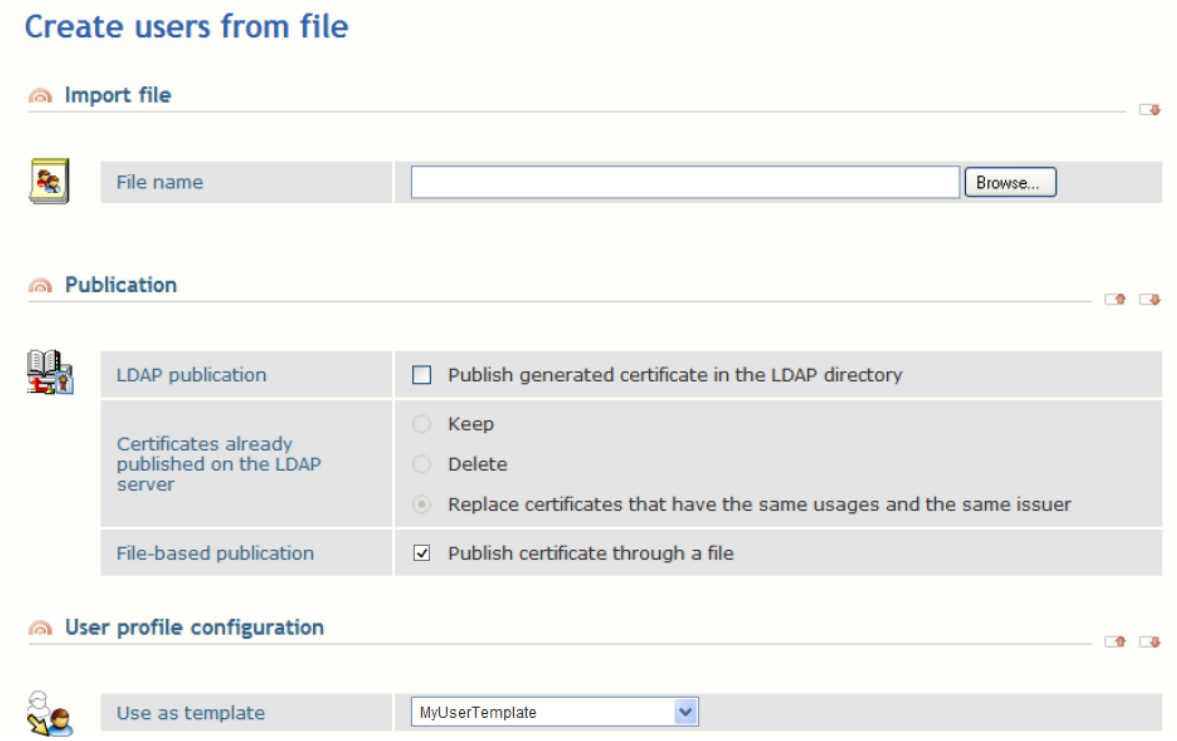
Le fichier est un fichier texte au format CSV (extension *.csv*). Chaque ligne du fichier correspond à un utilisateur à créer. Elle est composée de 6 champs (le nom, le prénom, l'identifiant, l'adresse e-mail, le mot de passe et la description) séparés par des ";". Les 3 derniers champs sont optionnels.

```
Nom1;Prénom1;Nom1_Prénom1;Prenom1.Nom1@arkoon.fr;code_secret_
1;description1
Nom2;Prénom2;Nom2_Prénom2;Prenom2.Nom2@arkoon.fr;code_secret_2
Nom3;Prénom3;Nom3_Prénom3;Prenom3.Nom3@arkoon.fr;;description3
Nom4;Prénom4;Nom4_Prénom4;;;description4
Nom5;Prénom5;Nom5_Prénom5;;code_secret_5
Nom6;Prénom6;Nom6_Prénom6;Prenom6.Nom6@arkoon.fr
Nom7;Prénom7;Nom7_Prénom7
```

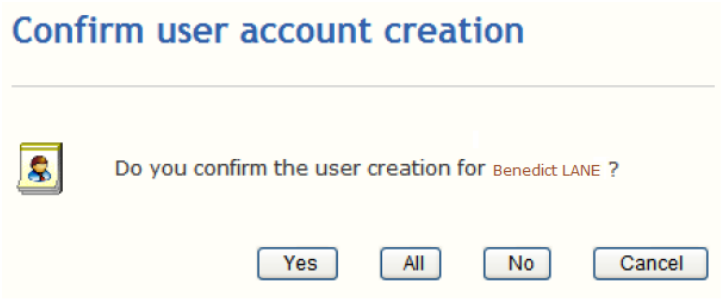
Si le mot de passe n'est pas renseigné ou vide alors un mot de passe aléatoire de 16 caractères est généré.

La mécanique de création de l'utilisateur est la même que pour la création à partir d'un modèle (voir la section Création à partir d'un modèle).

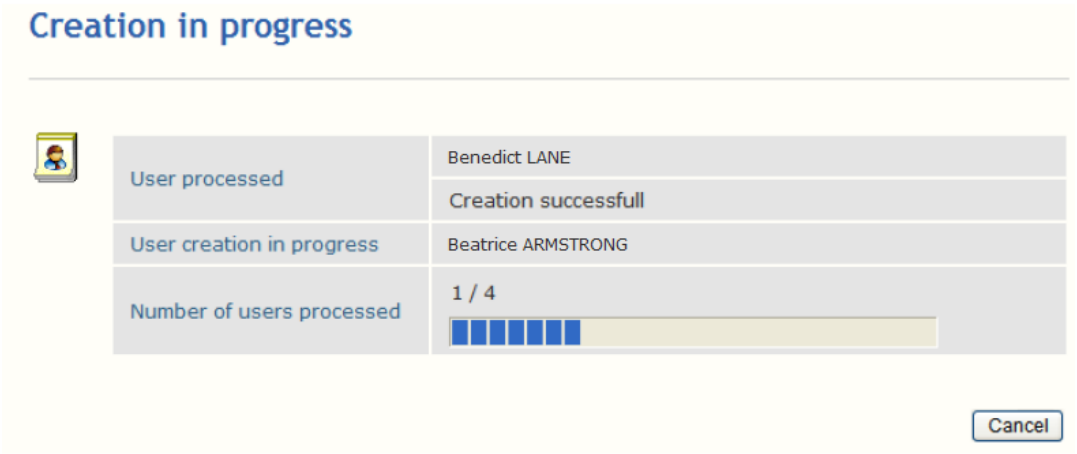
1. Sélectionnez le fichier *.csv* à traiter.
2. Sélectionnez un modèle parmi les modèles présents dans la base.



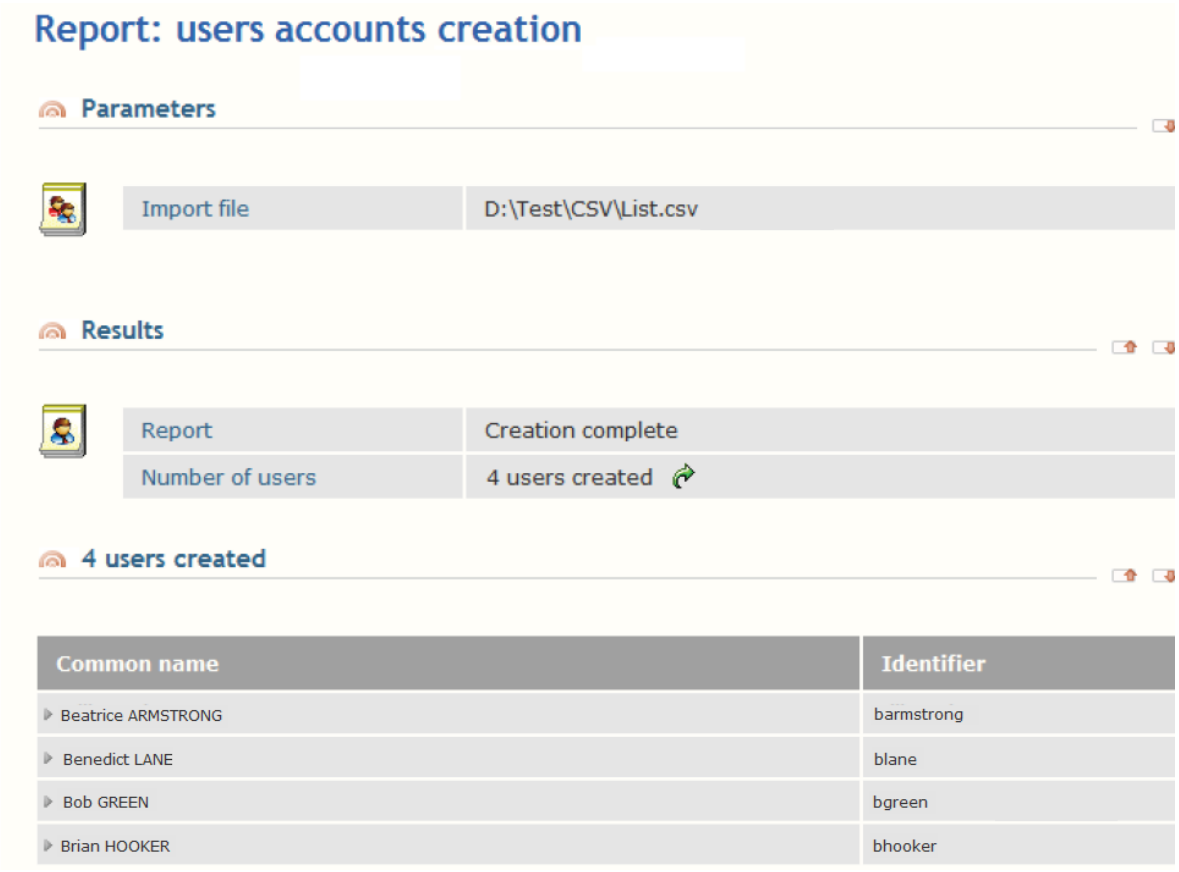
Après chaque création, Stormshield Data Authority Manager fournit un compte rendu et demande une confirmation pour la création suivante :



Évitez ces demandes de confirmation en activant la création automatique par appui sur le bouton Tous :



Lorsque toutes les lignes du fichier *.csv* ont été traitées, Stormshield Data Authority Manager affiche une page de compte rendu :



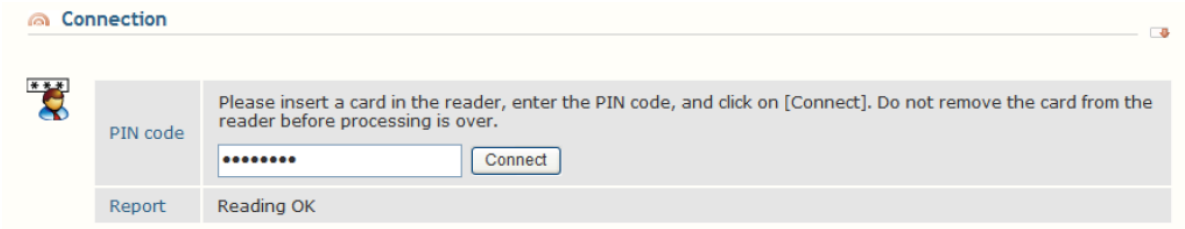
Cette page affiche la liste des utilisateurs qui ont été créés, et éventuellement la liste des utilisateurs pour lesquels la création a échoué. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 utilisateurs. Les listes complètes sont téléchargeables en cliquant sur l'icône .

8.5.4 Création à partir d'un support cryptographique physique

Cette opération est disponible à partir de l'onglet *Créations d'utilisateurs*, du menu de la page **Liste des utilisateurs**, en cliquant sur le lien **A partir d'une carte à puce** (section Opérations disponibles). Elle permet de créer un utilisateur à partir d'une carte à puce physique ou d'un token contenant déjà des clés et des certificats.

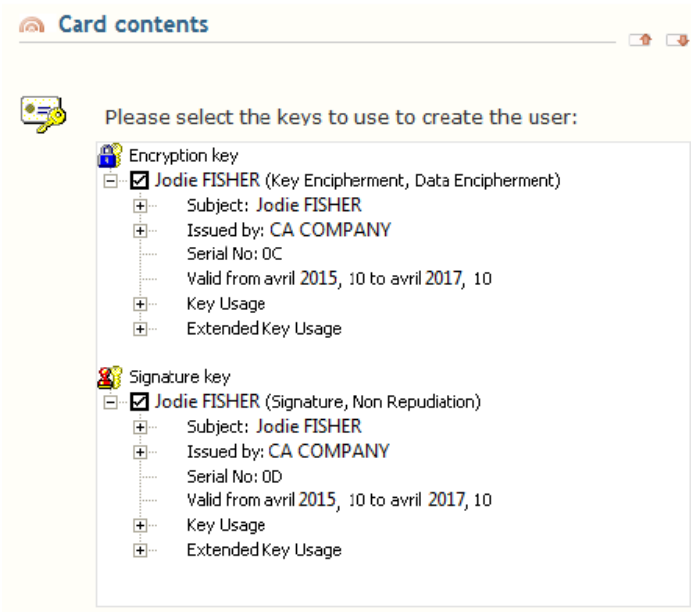
Pour que cette opération soit disponible, la base de données doit posséder au moins un modèle.

1. Connectez-vous à la carte pour que Stormshield Data Authority Manager en lise le contenu et affiche toutes les clés trouvées dans la carte.

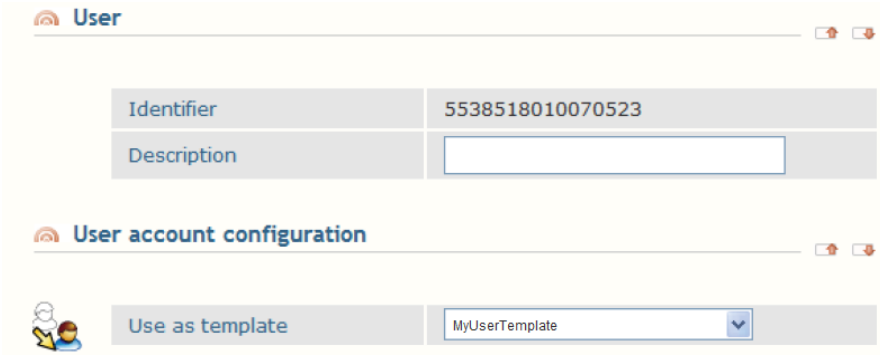


Les clés sont triées par rôle : chiffrement, signature et personnelle pour celles qui ont les deux rôles à la fois. Le rôle de la clé est déterminé à partir des usages X.509 du certificat associé.

2. Sélectionnez les clés à utiliser pour créer le compte.



3. L'identifiant du compte utilisateur est le numéro de la carte. Saisissez la description du compte et sélectionnez un modèle parmi les modèles présents dans la base.



Pour cette création, les informations extraites du modèle sont :

- l'algorithme de chiffrement du compte ;
- l'algorithme d'empreinte.

L'utilisateur hérite aussi de la configuration des composants du modèle (voir les sections Page Utilisateur et Choix du modèle).

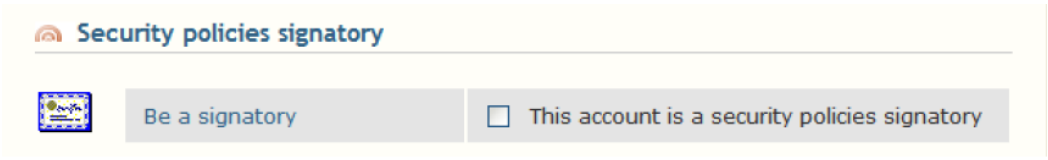
Stormshield Data Authority Manager extrait l'identité de l'utilisateur et les clés publiques à partir des certificats présents dans la carte. Il recopie les certificats dans la base, mais pas les clés privées.

8.5.5 Création à partir d'un fichier PKCS#12

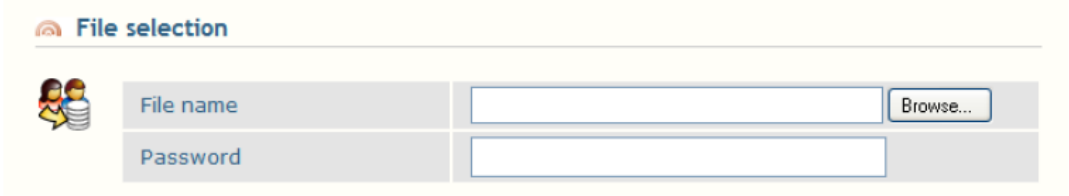
Cette opération est disponible à partir de l'onglet *Créations d'utilisateurs*, du menu de la page **Liste des utilisateurs**, en cliquant sur le lien **A partir d'un fichier PKCS#12** (section Opérations disponibles). Elle permet de créer un utilisateur à partir d'un fichier d'échange de clés (format *PKCS#12*). La ou les clés présentes dans le fichier, ainsi que les certificats associés, sont attribués à l'utilisateur créé.

Pour que cette opération soit disponible, la base de données doit posséder au moins un modèle.

Si la base de données ne contient pas un compte signataire de politiques de sécurité, la page de création d'un utilisateur à partir d'un fichier *PKCS#12* affiche une case à cocher permettant d'indiquer la création d'un compte signataire de politiques de sécurité.

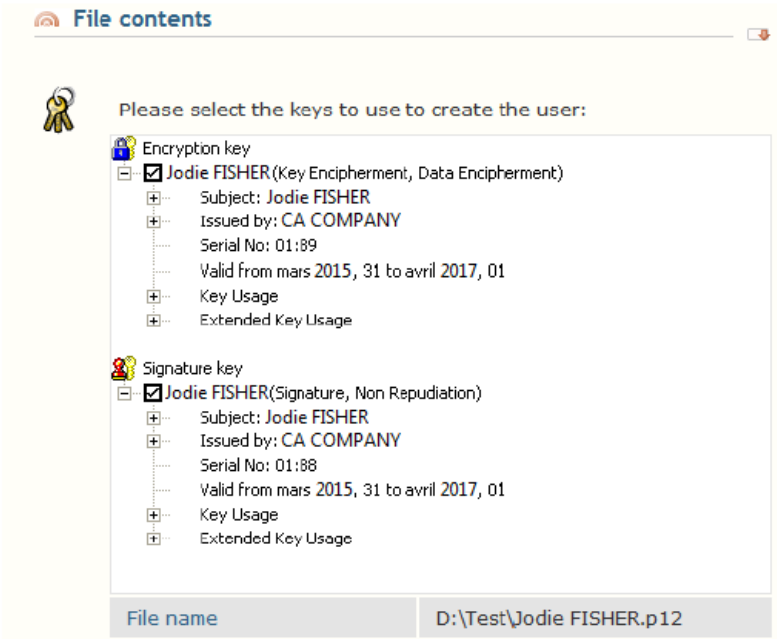


Saisissez le mot de passe du fichier PKCS#12 pour accéder à son contenu.

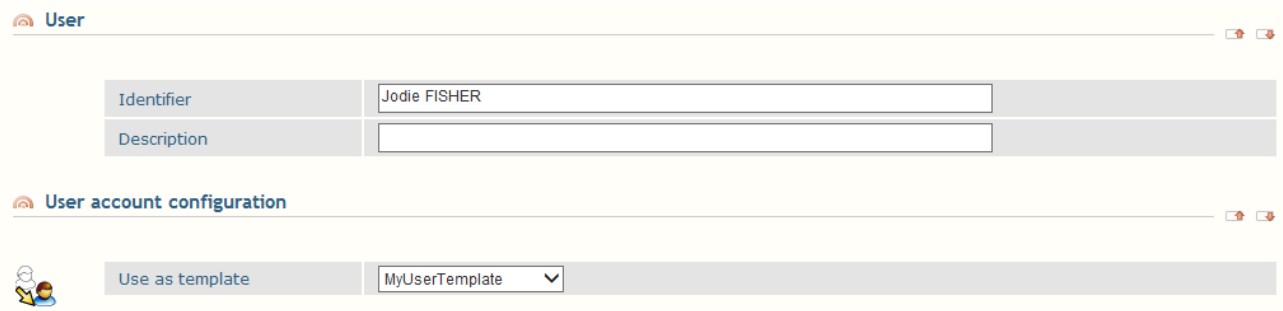


Après vérification du mot de passe, le contenu du fichier est affiché :

- La liste des clés. Les clés sont triées par rôle : chiffrement, signature et personnelle pour celles qui ont les deux rôles à la fois. Le rôle de la clé est déterminé à partir des usages X.509 du certificat associé.



- L'identité de l'utilisateur.



Pour créer l'utilisateur :

1. Sélectionnez les clés à utiliser pour créer le compte.
2. Saisissez un identifiant et une description.
3. Sélectionnez un modèle parmi les modèles présents dans la base.

Pour cette création, les informations extraites du modèle sont :

- l'algorithme de chiffrement du compte ;
- l'algorithme d'empreinte ;

L'utilisateur hérite aussi du mot de passe de secours (voir la section section Page Utilisateur et Choix du modèle).

Le mot de passe du compte est composé de 16 caractères tirés aléatoirement. Vous pourrez consulter et modifier ce mot de passe une fois l'utilisateur créé.

L'identité de l'utilisateur est obtenue à partir du sujet présent dans un des certificats. Si l'e-mail n'est pas renseigné dans le sujet, il est recherché dans le **Subject Alternative Name**.

Dans la page **Liste des utilisateurs**, le lien d'accès à un utilisateur est son nom usuel. Si aucun nom usuel n'est présent dans le sujet du certificat, on le crée en concaténant le prénom et le nom, s'ils existent. Ainsi, si le certificat ne contient ni nom usuel, ni nom, ni prénom, l'utilisateur créé sans nom usuel ne pourra pas être manipulé faute de lien. Il pourra toutefois être supprimé.

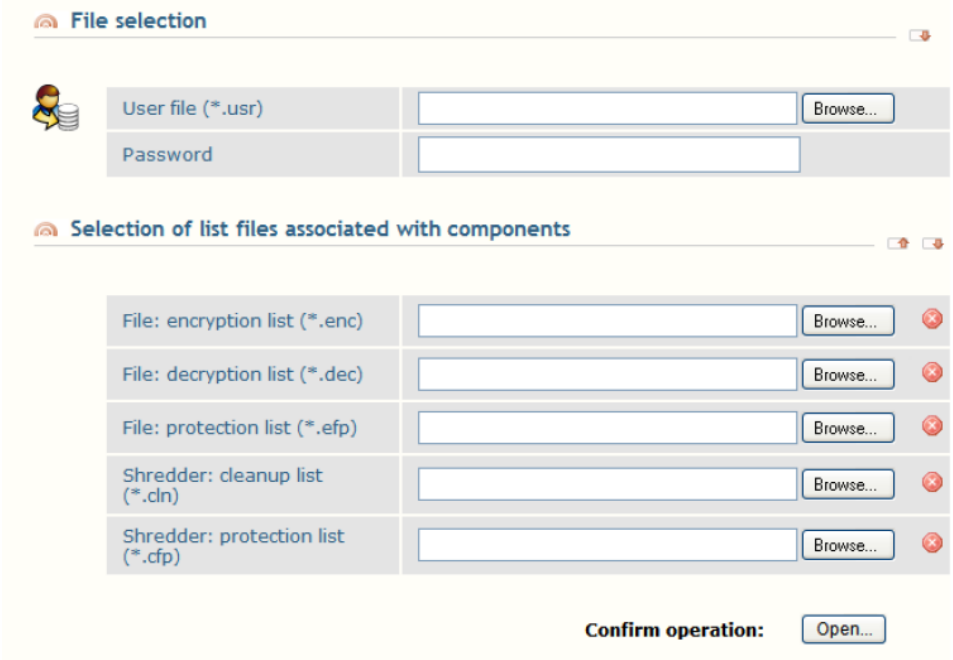
8.5.6 Création à partir d'un fichier utilisateur

Cette opération est disponible à partir de l'onglet *Créations d'utilisateurs*, du menu de la page **Liste des utilisateurs** en cliquant sur le lien **A partir d'un fichier utilisateur** (section Opérations disponibles). Elle crée un utilisateur à partir d'un fichier utilisateur *.usr* en conservant :

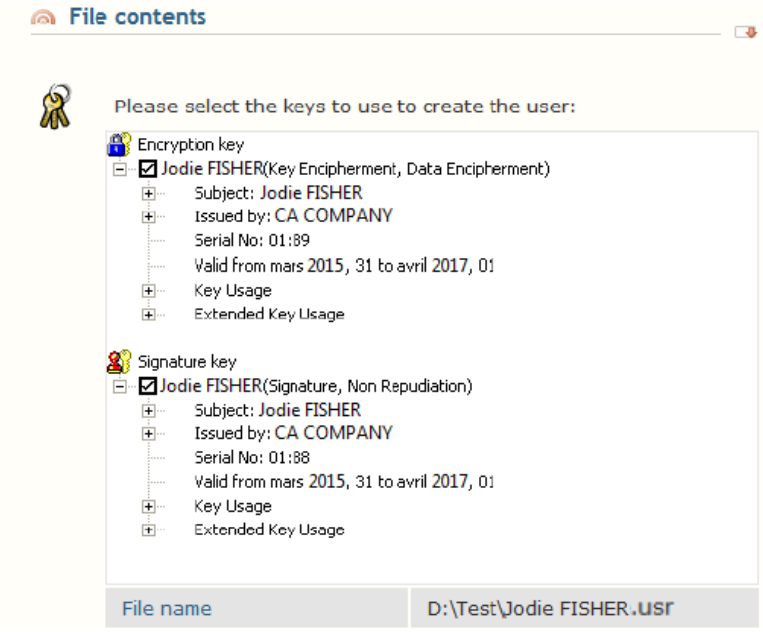
- les clés ;
- les certificats associés (courants et anciens) ;
- les configurations des composants.
- un fichier utilisateur associé à une carte à puce n'est pas accepté
- pour les composants Stormshield Data Sign, Contrôleur de révocation et Téléchargement automatique, seules les configurations effectuées à l'aide de Stormshield Data Authority Manager sont conservées.
- le fichier ne doit pas être en cours d'utilisation (l'utilisateur ne doit pas être connecté).

Pour afficher le contenu du fichier :

1. Sélectionnez un fichier utilisateur.
2. Saisissez son mot de passe.
3. Sélectionnez les éventuels fichiers liste associés aux composants.



Après vérification du mot de passe, une page affiche la liste des clés. Les clés sont triées par rôle : chiffrement, signature et personnelle pour celles qui ont les deux rôles à la fois. Le rôle de la clé est déterminé à partir des usages X.509 du certificat associé. Elles sont affichées pour information. Elles ne sont pas sélectionnables.



Pour créer l'utilisateur :

1. Saisissez un identifiant et une description.
2. Choisissez le mot de passe de secours.

NOTE
La fonctionnalité de déblocage de compte à distance (voir la section Déblocage de compte à distance) ne peut pas être mise en œuvre pour un compte diffusé avec un mot de passe de secours de plus de 16 caractères. Cette limite est la longueur des mots de passe de secours aléatoires proposés par Stormshield Data Authority Manager.

8.5.7 Création à partir d'un annuaire LDAP

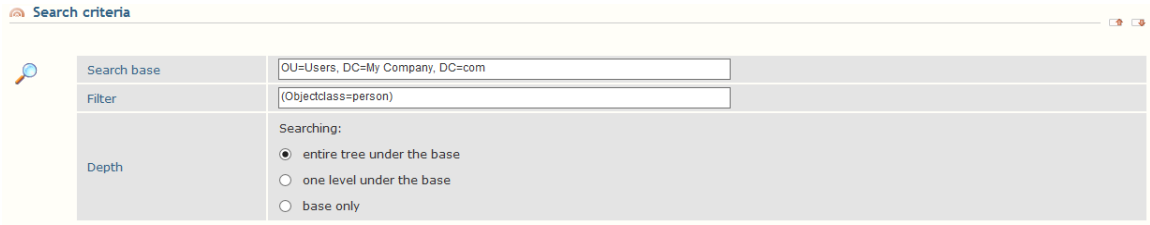
Cette opération est accessible à partir de la page principale de la synchronisation avec un annuaire LDAP (section Synchronisation avec un annuaire LDAP).

Pour que cette opération soit disponible, la base de données doit posséder au moins un modèle.

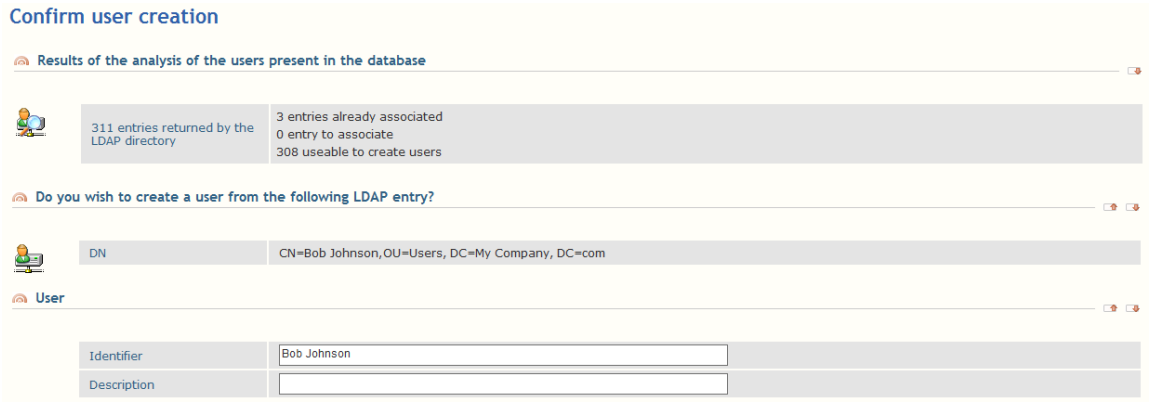
1. Lancez l'opération en recherchant les entrées LDAP "A associer ou à utiliser pour créer des utilisateurs".

Stormshield Data Authority Manager parcourt les entrées de l'annuaire LDAP (voir la sélection de l'annuaire section Configuration LDAP) selon les critères de recherche saisis.

NOTE
Si le résultat de la recherche indique qu'aucune entrée n'a été trouvée, peut-être est-ce dû à un échec de l'authentification. Veuillez vérifier les données d'authentification saisies dans les paramètres de la configuration LDAP.

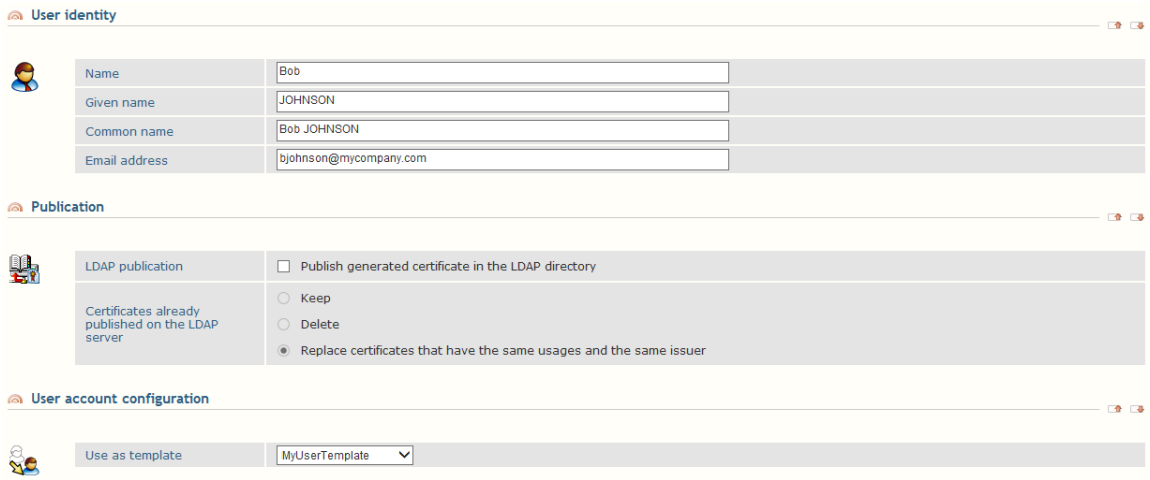


2. Stormshield Data Authority Manager propose de créer un utilisateur à partir de chaque entrée qui ne peut pas être associée à un utilisateur de la base (section Association d'un utilisateur à une entrée LDAP).



3. Pour créer l'utilisateur :

Les champs sont pré-remplis par Stormshield Data Authority Manager en fonction des attributs trouvés dans l'annuaire LDAP, conformément aux noms des attributs saisis dans les paramètres LDAP (section Configuration LDAP). Si besoin, vous pouvez modifier l'identifiant, la description, le nom, le prénom, le nom usuel et l'adresse e-mail.



4. Choisissez le mode de publication des certificats (section Publication d'un certificat).
5. Sélectionnez un modèle parmi les modèles présents dans la base.

Les règles de création de l'utilisateur sont les mêmes que pour la création à partir d'un modèle (voir la section Création à partir d'un modèle).

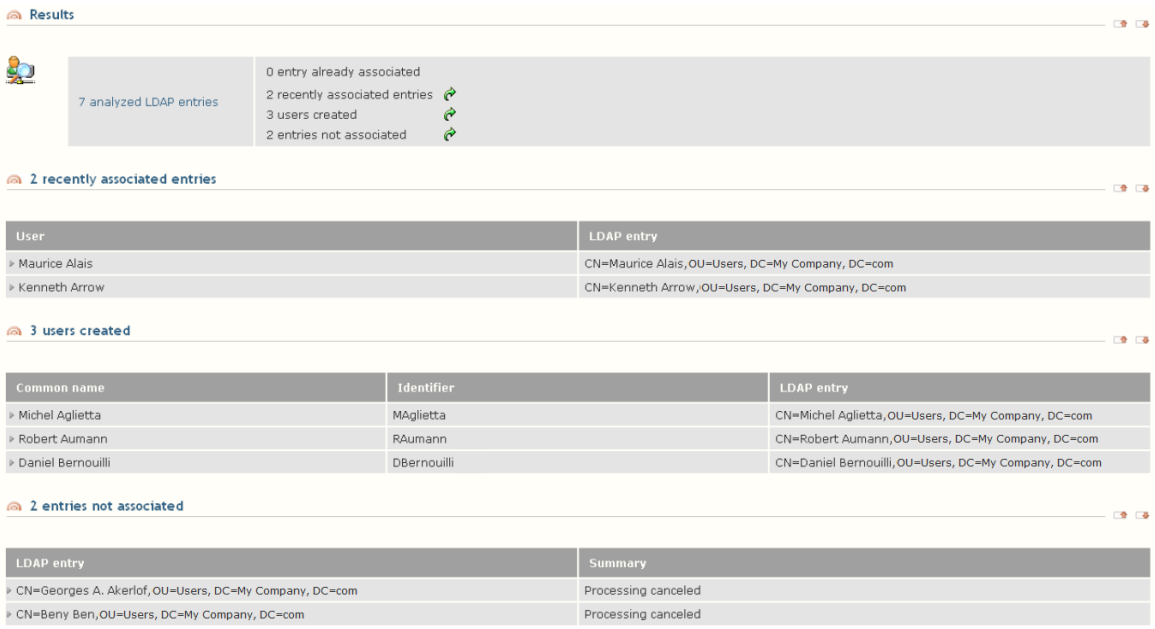
Chaque utilisateur créé est automatiquement associé à l'entrée LDAP traitée.

Après le traitement, Stormshield Data Authority Manager affiche un compte rendu et demande une confirmation pour l'action suivante (association ou création).

Évitez ces demandes de confirmation en activant le traitement automatique des entrées (association ou création) par appui sur le bouton **Tous**. Lors du traitement automatique,

Stormshield Data Authority Manager essaye dans un premier temps d'associer l'entrée à un utilisateur de la base, puis, si ce n'est pas possible, crée un utilisateur à partir de cette entrée. Cette création échoue si l'identifiant ou le nom sont absents.

Lorsque toutes les entrées ont été traitées, une page de compte rendu est affichée :



Cette page affiche la liste des entrées associées, la liste des utilisateurs créés, et la liste des entrées pour lesquelles ni l'association ni la création n'a été possible. Afin de limiter le temps d'affichage de la page, ces listes sont limitées à 100 lignes. Les listes complètes sont téléchargeables en cliquant sur l'icône .

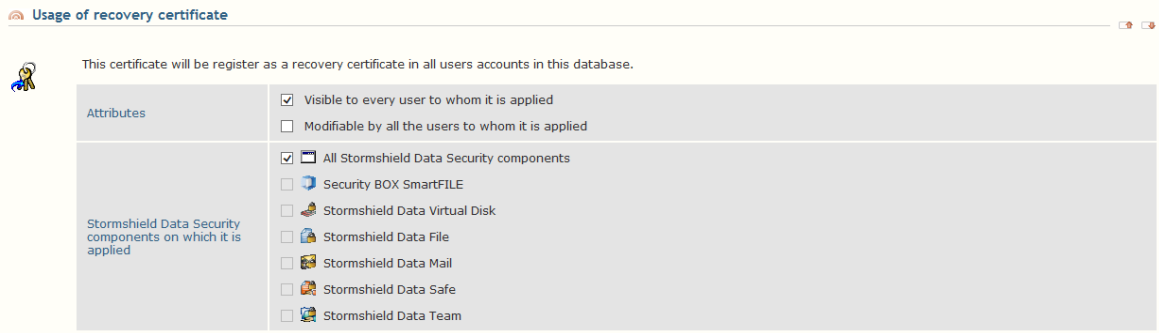
8.6 Création d'un compte de recouvrement

Cette opération est disponible à partir de l'onglet *Utilisateurs spéciaux*, du menu de la page **Liste des utilisateurs**, en cliquant sur le lien **Compte de recouvrement** (section Opérations disponibles).

Un compte de recouvrement ne possède qu'une seule clé dont le certificat doit posséder les usages X.509 de chiffrement.

Les premières sections de la page de création sont décrites dans la section Création avancée.

Configurez les paramètres de recouvrement :



Vous pouvez modifier ces choix après la création du compte (section Modification des propriétés d'un compte de recouvrement).

IMPORTANT
La création d'un (ou plusieurs) compte de recouvrement nécessite de prendre certaines précautions sur le stockage de ce compte. En effet, il est critique pour la sécurité des données chiffrées avec les comptes utilisateurs contenant ce certificat de recouvrement. Il doit donc être muni d'un mot de passe suffisamment robuste et être conservé en lieu sûr s'il est diffusé.

8.7 Création d'un signataire de politiques de sécurité

Cette opération est disponible à partir de l'onglet *Utilisateurs spéciaux*, du menu de la page **Liste des utilisateurs**, en cliquant sur le lien **Signataire de politiques** (voir la section Opérations disponibles).

Un signataire ne possède qu'une seule clé avec l'usage de clé de signature.

Il est également possible de créer le signataire de politiques à partir d'un fichier *PKCS#12* (voir la section Création à partir d'un fichier PKCS#12).

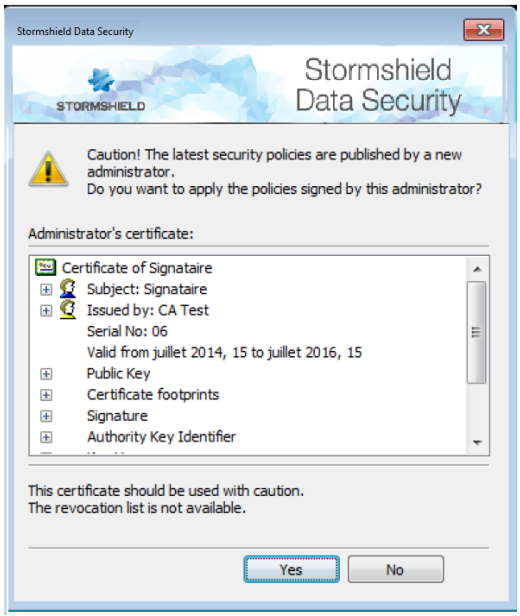
IMPORTANT
La création d'un signataire de politiques de sécurité nécessite de prendre certaines précautions sur le stockage de ce compte. En effet, il est critique pour la définition de votre politique de sécurité. Il doit être muni d'un mot de passe suffisamment robuste.

8.7.1 Renouvellement d'un signataire de politiques de sécurité

Pour renouveler le signataire de politiques de sécurité, il faut d'abord renouveler sa clé de signature.

Pour cela, sur la page de l'utilisateur signataire, cliquez sur le numéro de série du certificat de signature, puis cliquez sur le lien **Renouveler le certificat** du menu **Gestion du certificat**.

Une fois le signataire de politiques renouvelé, vous devez rediffuser les fichiers de mise à jour des utilisateurs concernés. À leur prochaine connexion, ils devront accorder leur confiance au certificat provenant du fichier de mise à jour, en cliquant sur **Oui** dans la boîte de dialogue suivante :



Si l'utilisateur clique sur **Non**, la mise à jour ne sera pas appliquée et sera reproposée à la prochaine connexion.

8.7.2 Recréation d'un signataire de politiques de sécurité

Plutôt que de renouveler le signataire de politiques de sécurité, il est également possible de le créer à nouveau. Pour cela, sur la page de l'utilisateur signataire, cliquez sur le lien **Supprimer** du menu **Gestion de l'utilisateur** afin de supprimer le compte.

Pour recréer le compte de signataire, reportez-vous à la section Création d'un signataire de politiques de sécurité.

Une fois le signataire créé, de la même manière que pour le renouvellement, il est nécessaire de rediffuser les fichiers de mise à jour des utilisateurs concernés (voir la section précédente).

8.8 Page Utilisateur

Cette page est accessible à partir de la page **Liste des utilisateurs** (section Page d'accueil) en cliquant sur le nom usuel d'un utilisateur.

Elle affiche, tout d'abord les informations liées à l'identité de l'utilisateur :

La ligne **Propriétés de l'utilisateur** indique, à l'aide d'une icône, la nature des utilisateurs spéciaux :

compte de recouvrement ;

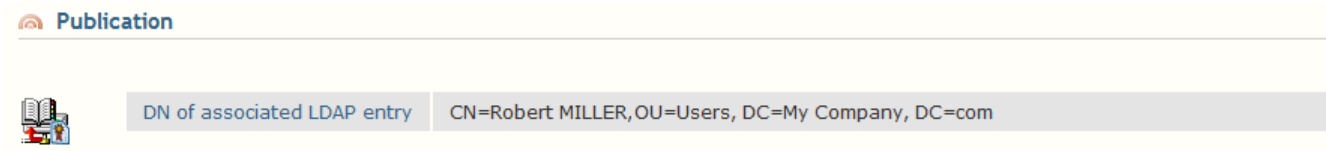
signataire de politiques de sécurité.

La ligne **Modèle** s'affiche si l'utilisateur dérive d'un modèle. Elle contient l'identifiant du modèle sous la forme d'un lien permettant d'accéder à sa page (voir la section Page Modèle).

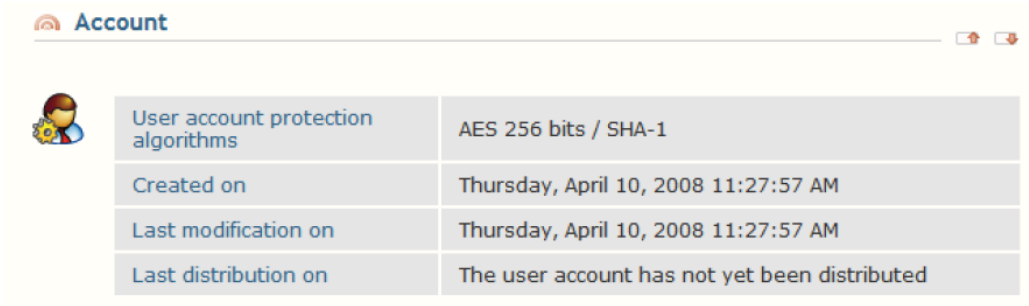
Ensuite, la page affiche la liste des clés de l'utilisateur :

- le rôle de la clé (voir la section Utilisateur standard) ;
- le numéro de série du certificat associé à la clé. En cliquant sur ce lien vous accédez aux propriétés de la clé ;
- la période de validité du certificat.

Puis la page affiche, s'il existe, le DN LDAP de l'utilisateur :



Elle affiche ensuite les informations liées au compte de l'utilisateur :



Dans le bandeau en haut de la page, un menu est proposé. Le contenu du menu varie en fonction du type d'utilisateur (compte carte, modèle, compte de recouvrement).

Dans l'onglet *Propriétés*, vous pouvez :

- modifier le mot de passe et le mot de passe de secours de l'utilisateur (voir la section Modifications des mots de passe) ;
- modifier l'identité de l'utilisateur (voir la section Modification de l'identité) ;
- choisir ou modifier le modèle (voir la section Choix du modèle) ;
- modifier les propriétés d'un compte de recouvrement (voir la section Modification des propriétés d'un compte de recouvrement) ;
- supprimer l'association de l'utilisateur avec une entrée LDAP (voir la section Suppression de l'association de l'utilisateur avec une entrée LDAP) ;

Dans l'onglet *Gestion de l'utilisateur*, vous pouvez :

- diffuser le compte de l'utilisateur (voir la section Diffusion des comptes utilisateurs) ;
- débloquer le compte de l'utilisateur (voir la section Déblocage de compte à distance ;
- associer le compte à une carte à puce (voir la section Association d'un support cryptographique physique) ;
- définir l'utilisateur comme administrateur de la base ;
- supprimer l'utilisateur (voir la section Suppression d'utilisateurs).

Dans l'onglet *Clés et certificats*, vous pouvez :

- exporter les clés de l'utilisateur dans un fichier PKCS#12 (voir la section Exportation des clés dans un fichier PKCS#12) ;
- renouveler une clé.

L'onglet *Composants* apparaît si l'utilisateur ne dérive pas d'un modèle. Vous pouvez :

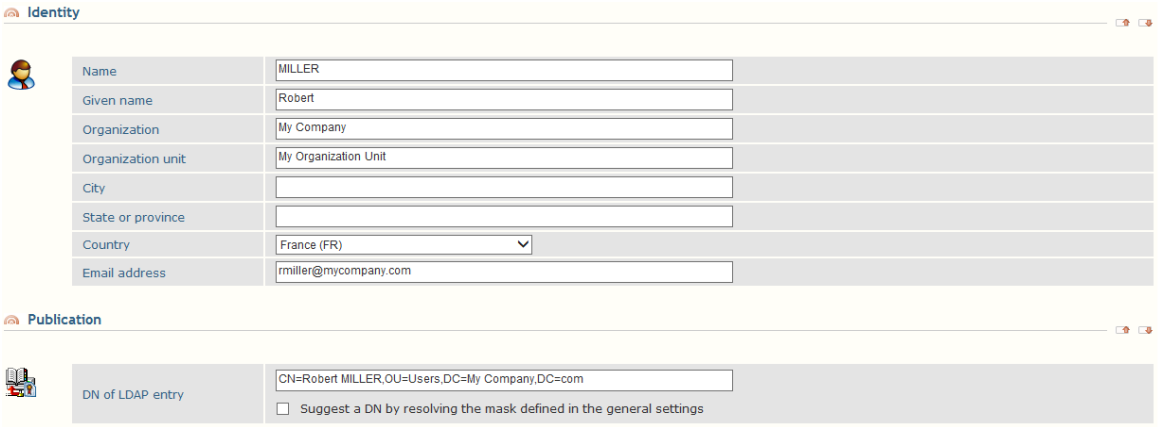
- configurer les composants (voir la section Configuration des composants).

8.8.1 Modification de l'identité

Cette page permet de modifier l'identité de l'utilisateur. Elle est accessible à partir de la page **Utilisateur** (section Page Utilisateur) à partir de l'onglet *Propriétés* en cliquant sur le lien **Identité**.

Tous les champs composant l'identité de l'utilisateur, ainsi que sa description et le DN de l'entrée LDAP qui lui est associée, peuvent être modifiés.

Le DN de l'entrée LDAP peut-être directement saisi, ou proposé par le composant par résolution du masque défini dans les paramètres LDAP (voir la section Publication des nouveaux certificats).



8.8.2 Modifications des mots de passe

Cette page permet de modifier le mot de passe de l'utilisateur et son mot de passe de secours. Elle est accessible à partir de la page Utilisateurs (section Page Utilisateur) à partir de l'onglet *Propriétés* en cliquant sur le lien **Mots de passe**.

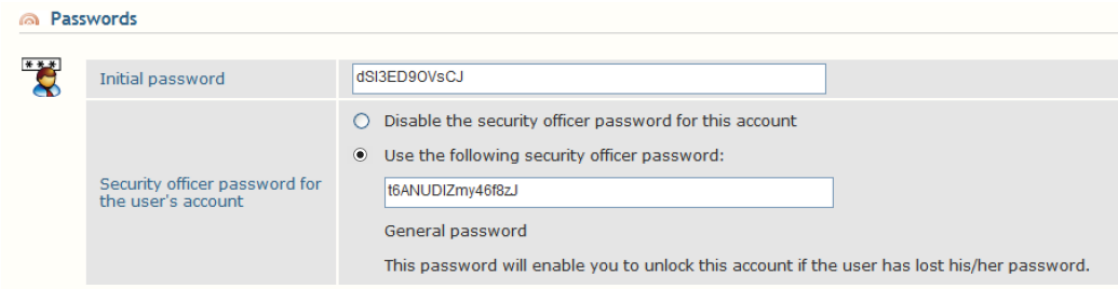
Gestion du mot de passe de secours

- Si l'utilisateur ne dérive pas d'un modèle :

La gestion du mot de passe de secours s'effectue au niveau de l'utilisateur.

Si vous choisissez d'utiliser un mot de passe de secours alors qu'il était condamné, le fonctionnement de Stormshield Data Authority Manager dépend de la configuration des paramètres généraux (voir la section Mot de passe de secours) :

- Si l'option **Par défaut, utiliser le mot de passe suivant pour tous les comptes** est sélectionnée, le mot de passe de secours général est proposé.
- Si une des deux autres options est sélectionnée Stormshield Data Authority Manager propose un mot de passe spécifique tiré aléatoirement.



- Si le compte de l'utilisateur dérive d'un modèle :

La gestion du mot de passe de secours s'effectue au niveau du modèle :

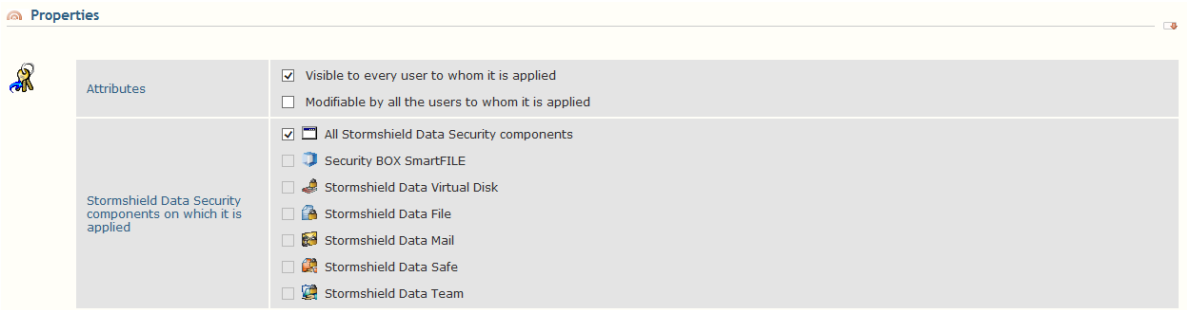
- soit il est condamné au niveau du modèle ;
- soit une valeur est imposée au niveau du modèle ;
- soit l'existence d'un mot de passe de secours est imposée au niveau du modèle, mais sa valeur est modifiable dans cette page.

Dans tous les cas, la section **Historique des mots de passe de secours** affiche la liste des mots de passe de secours diffusés, avec leur date de diffusion. Ils sont présentés du plus récent au plus ancien.

> **NOTE**
> La fonctionnalité de déblocage de compte à distance (voir la section Déblocage de compte à distance) ne peut pas être mise en œuvre pour un compte diffusé avec un mot de passe de secours de plus de 16 caractères. Cette limite est la longueur des mots de passe de secours aléatoires proposés par Stormshield Data Authority Manager.

8.8.3 Modification des propriétés d'un compte de recouvrement

Cette page permet de modifier les propriétés d'un compte de recouvrement après sa création. Elle est accessible à partir de la page **Utilisateur** (section Page Utilisateur) à partir de l'onglet *Propriétés* en cliquant sur le lien **Recouvrement**.



8.8.4 Suppression de l'association de l'utilisateur avec une entrée LDAP

Cette opération permet de supprimer l'association entre l'utilisateur et l'entrée LDAP (section Association d'un utilisateur à une entrée LDAP). Elle est accessible à partir de la page **Utilisateurs** (section Page Utilisateur) à partir de l'onglet *Propriétés* en cliquant sur le lien **Supprimer l'association LDAP**.

La date de dernière publication des certificats de l'utilisateur sur l'annuaire LDAP est aussi supprimée.

8.8.5 Choix du modèle

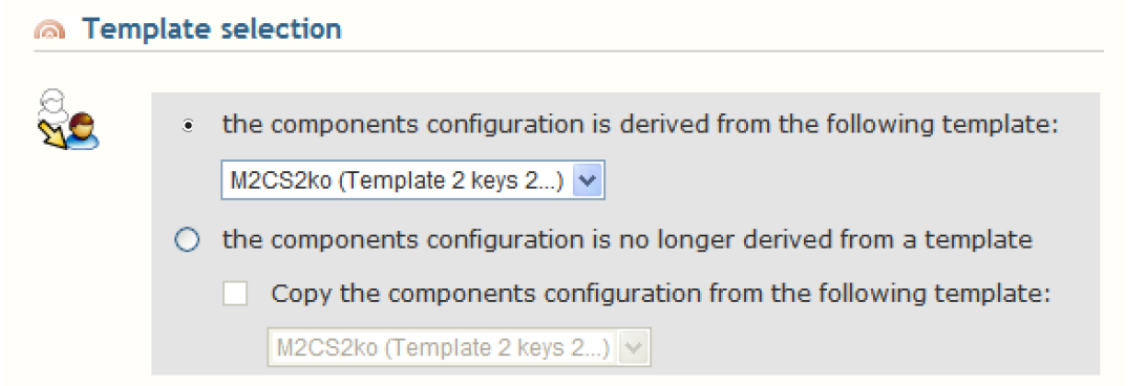
Cette page est accessible à partir de la page **Utilisateurs** (section Page Utilisateur) à partir de l'onglet *Propriétés*.

Les choix proposés dans la page dépendent de l'utilisateur.

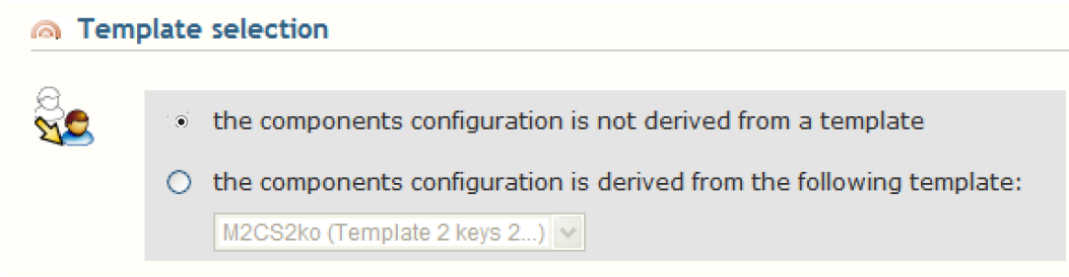
Si l'utilisateur dérive d'un modèle, en cliquant sur le lien **Changer de modèle**, vous pouvez le faire dériver d'un autre modèle.

Si l'utilisateur ne dérive pas d'un modèle, mais :

- sa configuration des composants hérite d'un modèle, en cliquant sur le lien **Changer de modèle**, vous pouvez faire l'une des deux opérations suivantes :
- la faire hériter d'un autre modèle parmi ceux présents dans la base ;
- ne plus la faire hériter d'un modèle. Vous pouvez alors choisir d'affecter à l'utilisateur les configurations d'un modèle que vous sélectionnez parmi ceux présents dans la base ; sinon l'utilisateur aura les configurations par défaut de Stormshield Data Security.



- sa configuration des composants n'hérite pas d'un modèle, en cliquant sur le lien **Choisir un modèle**, vous pouvez choisir de la faire hériter d'un modèle présent dans la base.



Pour plus d'information sur la configuration des composants, reportez-vous à la section Configuration des composants.

8.8.6 Association d'un support cryptographique physique

L'association d'un utilisateur de la base à une carte à puce physique ou à un token est accessible à partir de la page **Utilisateurs** (section Page Utilisateur), à partir de l'onglet *Gestion de l'utilisateur* en cliquant sur le lien **Associer une carte à puce**.

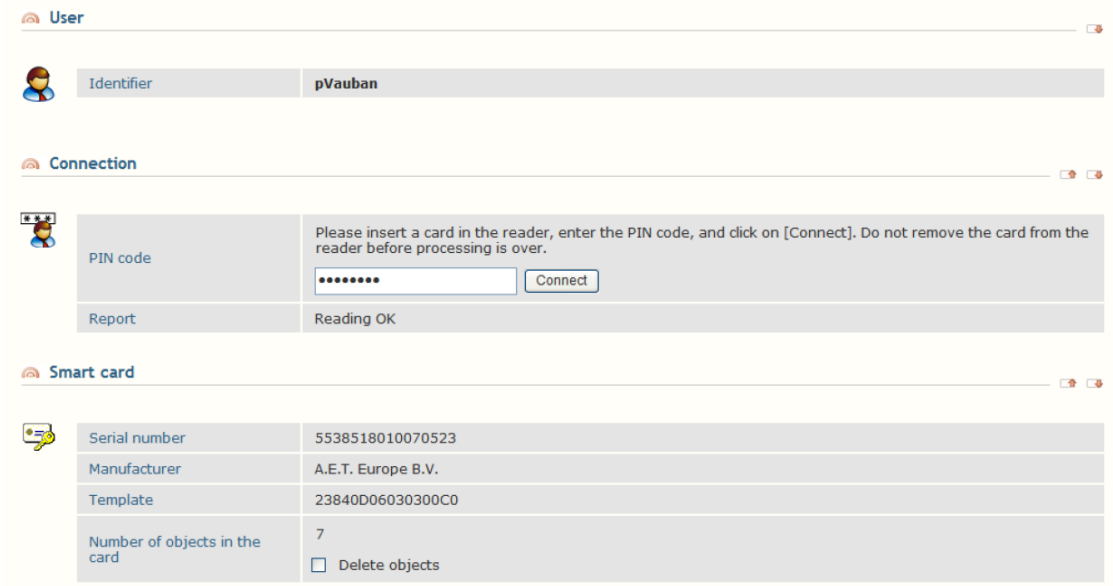
Toutes ses clés doivent être certifiées.

Connectez-vous à la carte pour que Stormshield Data Authority Manager en lise le contenu. Si la connexion réussit, Stormshield Data Authority Manager affiche des informations générales concernant la carte et propose de valider l'association.

Lors de l'association, Stormshield Data Authority Manager écrit dans la carte les clés privées, les certificats, et les clés publiques de l'utilisateur. L'échec de l'écriture des clés publiques n'entraîne pas l'échec de l'association ; un message spécifique est affiché dans la page de compte rendu.

Par défaut, les objets déjà présents dans la carte sont conservés. Pour les supprimer, cochez la case **Supprimer les objets**.

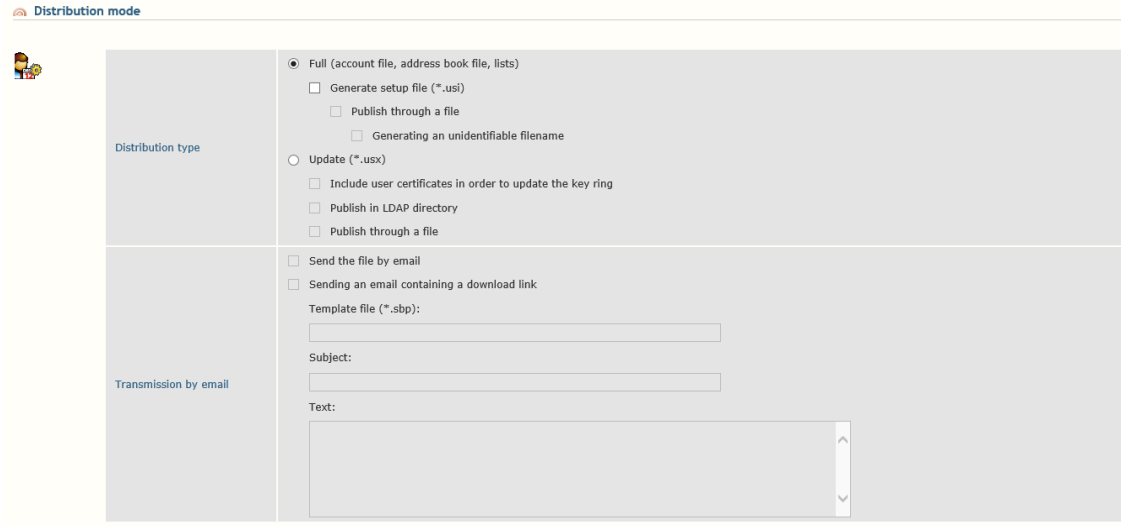
Lors de l'association, le numéro de la carte devient le nouvel identifiant du compte utilisateur, et le code confidentiel de la carte devient le code confidentiel du compte.



8.9 Diffusion des comptes utilisateurs

Les comptes utilisateurs et fichiers de mise à jour sont diffusés dans le répertoire `<user_account_dir>/<user_id>`, dans lequel `<user_account_dir>` est le répertoire de diffusion défini dans les paramètres généraux, et `<user_id>` est l'identifiant de l'utilisateur.

Les fichiers de mise à jour peuvent en plus être publiés dans l'annuaire LDAP ou par fichier, si ces fonctionnalités ont été paramétrées (voir la section Diffusion des comptes).



Les différents modes de diffusion sont :

- la diffusion complète qui crée le fichier compte (*.usr*), le fichier annuaire (*.usd*), et déplace dans le dossier de l'utilisateur les éventuels fichiers listes définis dans la configuration des composants Stormshield Data File et Stormshield Data Shredder (section Présentation).

Les fichiers issus de la diffusion complète peuvent être encapsulés dans un fichier d'installation (*.usi*, section Fichier d'installation (.usi)). Si la publication du fichier a été activée dans les paramètres généraux, une case à cocher proposant l'opération est affichée ;

- la génération d'un fichier de mise à jour (*.usx*, section Fichier de mise à jour de la politique de sécurité (.usx)). Si la publication dans un annuaire LDAP a été activée dans les paramètres généraux, une case à cocher proposant l'opération est affichée. De même pour la publication par fichier.

Stormshield Data Authority Manager permet d'envoyer automatiquement par e-mail :

- le fichier de mise à jour ou le fichier d'installation ;
- un lien de téléchargement du fichier de mise à jour ou du fichier d'installation publié.

8.9.1 Fichier d'installation (*.usi*)

Définition

Un fichier d'installation *.usi* est un script qui installe un compte utilisateur. L'utilisateur n'a donc pas besoin de copier manuellement les fichiers de son compte.

Après l'installation de Stormshield Data Security sur son poste, l'utilisateur peut double-cliquer sur le fichier *.usi*. La procédure d'installation copie alors tous les fichiers du compte utilisateur qui devient ainsi opérationnel.

Publication

Afin que les fichiers d'installation soient disponibles par téléchargement, Stormshield Data Authority Manager permet de les publier dans un dossier. Ce dossier est défini dans les paramètres généraux (voir la section Publication des fichiers d'installation). Il peut être un dossier de votre serveur Web, ainsi le fichier sera accessible par téléchargement HTTP.

Il est possible de publier le fichier avec un nom non identifiable. Ce nom généré aléatoirement n'est pas sauvegardé. En conséquence, cette option s'utilise avec l'envoi par mail d'un lien de téléchargement du fichier publié (voir la section Envoi par e-mail). Cette fonctionnalité permet de diffuser auprès des utilisateurs leur fichier d'installation, à l'aide d'un lien de téléchargement, sans qu'un utilisateur malveillant puisse s'inspirer de son lien pour télécharger les fichiers d'installation d'autres utilisateurs nommément identifiés.

8.9.2 Fichier de mise à jour de la politique de sécurité (*.usx*)

Définition

Un fichier de mise à jour permet de modifier les politiques de sécurité Stormshield Data Security dans le compte de l'utilisateur (ajout ou suppression de restrictions par exemple), tout en conservant la configuration personnalisée par l'utilisateur.

Lorsqu'un fichier *.usx* est pris en compte, une fusion est réalisée entre la configuration actuelle de l'utilisateur et les nouvelles règles de configuration contenues dans le fichier.

Pour que la modification d'un paramètre soit prise en compte lors de la fusion, ce qui signifie la perte de l'éventuelle personnalisation effectuée par l'utilisateur sur ce paramètre, il faut que, dans la configuration, la modification par l'utilisateur du dit paramètre soit interdite. Sinon la configuration de l'utilisateur est conservée.

Le fichier de mise à jour permet aussi :

- d'importer automatiquement dans l'annuaire de l'utilisateur les certificats externes (voir la section Certificats externes) présents dans Stormshield Data Authority Manager.
- d'importer dans le porte-clés de l'utilisateur le certificat courant de chacune de ses clés. Cette fonctionnalité doit être sélectionnée dans la page de diffusion.

NOTE
Cette opération ne permet pas de mettre à jour les fichiers listes associés aux composants. Donc les éventuelles modifications des listes de chiffrement, déchiffrement et protection de Stormshield Data File, ainsi que des listes de nettoyage et protection de Stormshield Data Shredder, ne seront pas prises en compte. Elle ne permet pas non plus de modifier un fichier [*.ini*] de configuration, de supprimer des certificats ni de mettre à jour les identifiants et les mots de passe d'un compte.

Utilisation

Deux techniques permettent de prendre en compte un fichier de mise à jour :

- La première est interactive : l'utilisateur doit double-cliquer sur le fichier *.usx* qu'on lui a fourni ;
- La seconde est automatique : le fichier de mise à jour est téléchargé à la connexion de l'utilisateur (à partir de Stormshield Data Security) (voir la section Publication des fichiers d'installation).

Un compteur interne au fichier permet à Stormshield Data Security de reconnaître et d'appliquer uniquement les politiques les plus récentes.

Ce compteur n'est pas pris en compte si l'utilisateur double-clique sur le fichier [*.usx*] pour l'installer manuellement.

Pour diffuser des fichiers de mise à jour, il faut au préalable créer un compte signataire de politique de sécurité (voir la section Création d'un signataire de politiques de sécurité).

La mise à jour des politiques de sécurité s'utilise après une première configuration, une diffusion complète du compte et une installation de cette configuration sur le poste utilisateur.

Publication

Afin que les mises à jour soient disponibles par téléchargement automatique, Stormshield Data Authority Manager permet de les publier :

- dans l'annuaire LDAP (voir Annexe E, Publication et téléchargement des mises à jour de sécurité à l'aide d'un annuaire LDAP). Le fichier de mise à jour est publié vers le DN de l'utilisateur, dans l'attribut `sboxPolicyUpgrade;binary` défini dans les paramètres LDAP (voir la section Nom des attributs).

NOTE
Vérifiez que les entrées LDAP des utilisateurs appartiennent à une classe acceptant cet attribut. Si nécessaire, vous pouvez créer une nouvelle classe `sboxPerson` acceptant cet attribut, et faire dériver les entrées de vos utilisateurs de cette classe.

- par fichier. Le fichier de mise à jour est copié dans le dossier paramétré (voir la section Publication des mises à jour de politiques de sécurité).

8.9.3 Configurations du composant Stormshield Data Kernel

Configuration Téléchargement des politiques de sécurité

Lors de la diffusion d'un compte utilisateur ou d'un fichier de mise à jour, que les configurations des composants dérivent d'un modèle ou non, si les tags `<LdapDn>` ou `<UserId>` sont utilisés dans les points de distribution présents dans la configuration du composant **Téléchargement des politiques de sécurité**, ils sont remplacés par les données de l'utilisateur diffusé (voir la section Configuration du composant Téléchargement des politiques de sécurité).

Configuration Code secret et connexion

Le composant Stormshield Data Kernel dispose de deux configurations "Code secret et connexion" (voir la section Configuration du compte utilisateur) : une pour un compte "mot de passe", une pour un compte "carte".

Ces deux configurations existent en deux versions selon la version de Stormshield Data Security installée sur le poste de l'utilisateur : versions antérieures ou postérieures à la version 5.

Lors de la diffusion d'un compte utilisateur, Stormshield Data Authority Manager écrit uniquement dans le fichier compte les deux versions de la configuration du mode concerné : "mot de passe" ou "carte".

Configuration Porte-clés

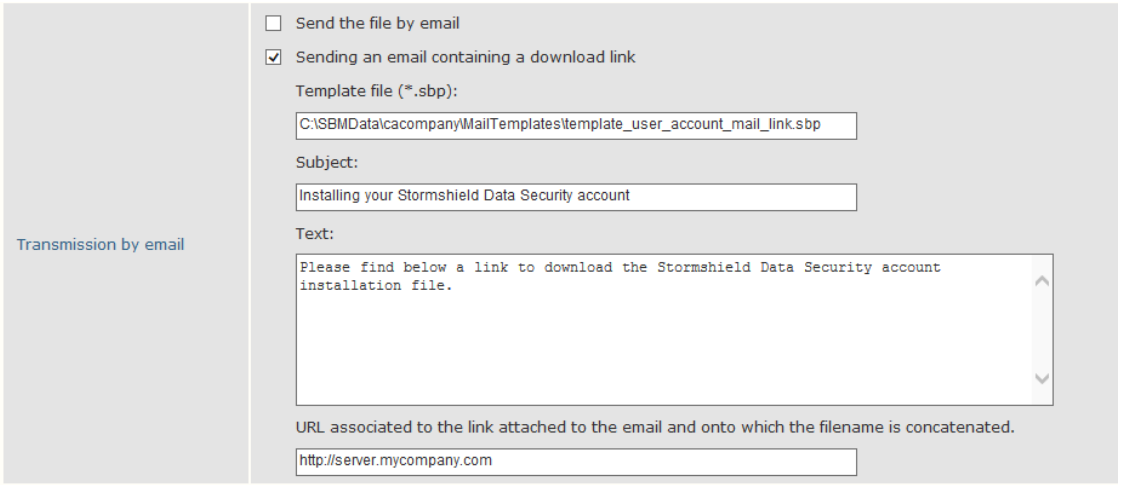
L'application Stormshield Data Kernel a deux configurations "Porte-clés" : une pour un "simple bi-clé" et une pour un "double bi-clé" (voir la section Configuration du compte utilisateur). Lors de la diffusion d'un compte utilisateur, Stormshield Data Authority Manager écrit toujours dans le fichier compte la configuration correspondant au nombre de clés de l'utilisateur.

8.9.4 Envoi par e-mail

Si un serveur de courrier sortant (SMTP) est paramétré (section Serveur de courrier sortant), il est possible de diffuser par e-mail :

- un fichier d'installation *.usi* qui installe le compte utilisateur ;
- un fichier de mise à jour *.usx* qui configure les composants Stormshield Data Security sur le poste utilisateur ;
- un lien de téléchargement du fichier d'installation *.usi* publié ;
- un lien de téléchargement du fichier de mise à jour *.usx* publié.

L'e-mail est envoyé à l'adresse électronique de l'utilisateur en cours de diffusion. Le fichier modèle *.sbp*, l'objet et le contenu de l'e-mail sont paramétrables :



Les modifications apportées à ces données sont conservées afin d'être proposées lors de l'envoi par mail suivant. Un message apparaît dans le compte rendu de la diffusion si l'e-mail n'a pas pu être envoyé (adresse incorrecte par exemple).

Pour un e-mail contenant un lien de téléchargement, il est nécessaire de saisir une URL à laquelle Stormshield Data Authority Manager concaténera automatiquement le nom du fichier publié.

8.9.5 Diffusion d'un compte

Cette diffusion s'exécute à partir de la page **Utilisateurs** (section Page Utilisateur) à partir de l'onglet *Gestion de l'utilisateur* en cliquant sur le lien **Diffuser le compte**.

Elle s'applique uniquement à l'utilisateur courant.

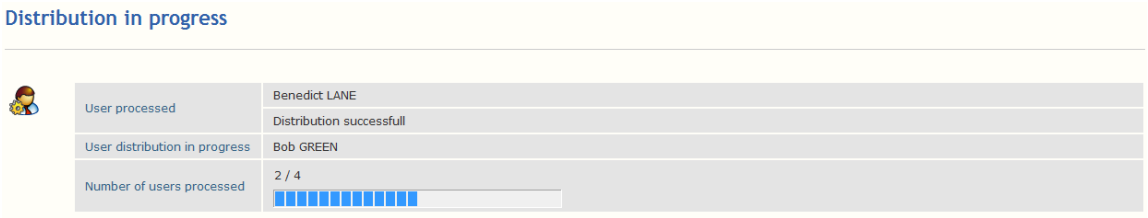
8.9.6 Diffusion de plusieurs comptes

Cette diffusion de plusieurs utilisateurs en une seule opération s'exécute à partir de la page principale **Liste des utilisateurs** (section Page d'accueil) à partir de l'onglet *Gestion des utilisateurs*.

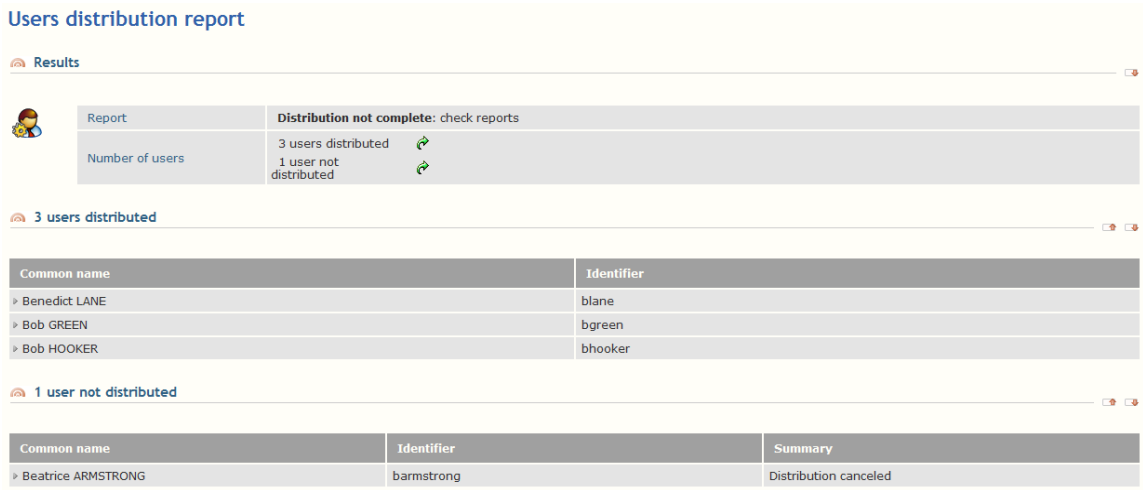
1. Sélectionnez les utilisateurs dont vous souhaitez diffuser les comptes. Cette sélection s'effectue en cochant la case à cocher présente sur la ligne de chaque utilisateur. Vous lancez ensuite la diffusion par appui sur le lien **Diffuser les utilisateurs**.

Après chaque diffusion, Stormshield Data Authority Manager fournit un compte rendu et demande une confirmation pour la diffusion suivante :

2. Vous pouvez évitez ces demandes de confirmation en activant la diffusion automatique par appui sur le bouton **Tous** :



3. Lorsque tous les utilisateurs ont été traités, Stormshield Data Authority Manager affiche une page de compte rendu :



Cette page affiche la liste des utilisateurs qui ont été diffusés, et éventuellement la liste des utilisateurs pour lesquels la diffusion a échoué. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 utilisateurs. Les listes complètes sont téléchargeables en cliquant sur l'icône .

8.10 Déblocage de compte à distance

Cette fonctionnalité permet de débloquer un compte utilisateur à distance sans que le mode opératoire de déblocage puisse être reproduit par une autre personne. Pour être débloqué, le compte doit avoir été généré par Stormshield Data Authority Manager ou créé à partir d'un modèle lui-même créé par Stormshield Data Authority Manager.

L'accès aux fonctions de déblocage de compte à distance nécessite la permission **Débloquer les comptes des utilisateurs** du rôle **Administrateur des utilisateurs**. Reportez-vous à la section Autorisations.

> **NOTE**
> Cette fonctionnalité est disponible uniquement si la longueur du mot de passe de secours n'excède pas 16 caractères.

Dans cette partie du produit, afin de réduire les erreurs de saisie, toutes les données à renseigner sont encodées en Base32. C'est-à-dire que vous pouvez rencontrer uniquement les caractères suivants : ABCDEFGHIJKLMNOPQRSTUVWXYZ234567.

8.10.1 Gestion des mots de passe de secours

L'historique des mots de passe de secours d'un modèle ou d'un utilisateur doit être conservé pour éviter une désynchronisation entre le mot de passe de secours du keystore bloqué et le

dernier mot de passe de secours saisi par l'administrateur si celui-ci n'a pas diffusé le keystore.

Chaque mot de passe de secours est identifié par une référence. Elle est transmise par l'utilisateur lors de sa demande de déblocage de compte.

Pour chaque modèle, vous pouvez choisir entre affecter le même mot de passe de secours à tous les utilisateurs dérivant du modèle ou définir un mot de passe de secours différent pour chaque utilisateur dérivant du modèle.

8.10.2 Diffusion d'un compte

Lors de la diffusion d'un compte :

Si l'utilisateur ne dérive pas d'un modèle et s'il ne condamne pas son mot de passe de secours, ou bien s'il dérive d'un modèle pour lequel l'option **Générer un mot de passe de secours différent pour chaque utilisateur** est sélectionnée, si un nouveau mot de passe de secours a été défini, celui-ci est alors placé dans l'historique des mots de passe de l'utilisateur.

Si l'utilisateur dérive d'un modèle imposant le mot de passe de secours, le mot de passe de secours est placé dans l'historique des mots de passe de l'utilisateur.

Si l'utilisateur dérive d'un modèle condamnant le mot de passe ou si l'utilisateur ne dérive pas d'un modèle et condamne son mot de passe de secours, la diffusion avec mot de passe de secours condamné est placée dans l'historique des mots de passe de l'utilisateur.

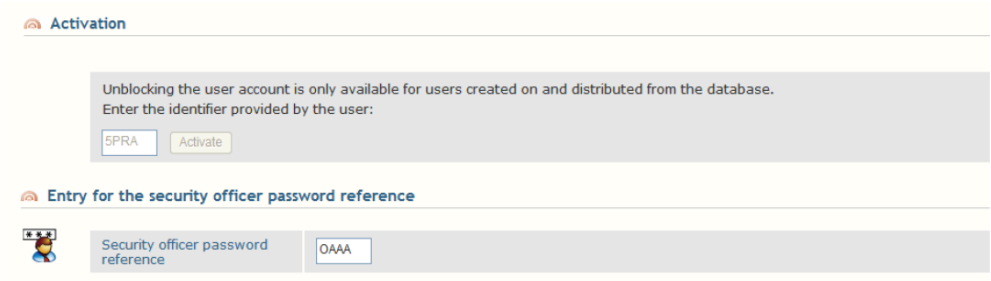
8.10.3 Déblocage d'un compte généré par Stormshield Data Authority Manager

La fonction **Débloquer un compte** est accessible depuis

- la page **Liste des utilisateurs** dans le menu **Gestion des utilisateurs, Débloquer**, en cliquant sur **Le compte d'un utilisateur de la base** (voir la section Page Liste des utilisateurs).
- la page **Utilisateurs** dans le menu **Gestion de l'utilisateur**, en cliquant sur **Débloquer le compte** (voir la section Page Utilisateur).

Si la fonction a été appelée depuis la page Liste des utilisateurs :

1. Saisissez l'identifiant communiqué par l'utilisateur puis cliquez sur **Activer** pour vérifier l'identifiant et rendre accessible la zone de saisie de la référence du mot de passe de secours (voir la section Page Base de données).
2. Saisissez la référence du mot de passe de secours communiqué par l'utilisateur.

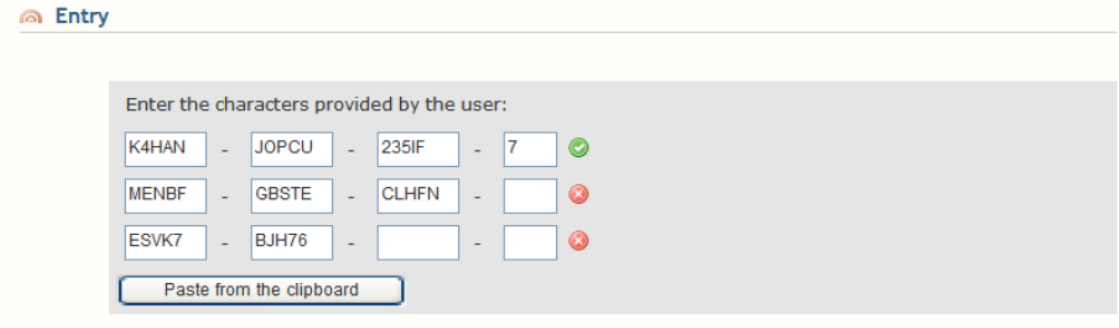


3. Cliquez sur **Rechercher les utilisateurs**.

Stormshield Data Authority Manager recherche le mot de passe de secours identifié par la référence fournie, puis affiche la liste des utilisateurs diffusés avec ce mot de passe.

L'affichage de cette liste est limité à 100 utilisateurs. La liste complète peut être téléchargée en cliquant sur .

4. Saisissez les caractères communiqués par l'utilisateur :



Lorsque tous les caractères d'une ligne sont renseignés, le contrôle de saisie est effectué et l'icône en indique le résultat.

5. Cliquez sur **Chiffrer le mot de passe de secours**.

Stormshield Data Authority Manager affiche une nouvelle page contenant les données à communiquer à l'utilisateur pour débloquer son compte.

Si la fonction a été appelée depuis la page Utilisateur :

1. Saisissez l'identifiant communiqué par l'utilisateur puis cliquez sur **Activer** pour vérifier l'identifiant et rendre accessible la zone de saisie de la référence du mot de passe de secours (voir la section Page Base de données).
2. Saisissez la référence du mot de passe de secours communiqué par l'utilisateur.
3. Cliquez sur **Vérifier**.

Stormshield Data Authority Manager vérifie que l'utilisateur a bien été diffusé avec ce mot de passe de secours, puis affiche une nouvelle page de saisie.

4. Saisissez les caractères communiqués par l'utilisateur.

Lorsque tous les caractères d'une ligne sont renseignés, le contrôle de saisie est effectué et l'icône indique le résultat.

5. Cliquez sur **Chiffrer le mot de passe de secours**.

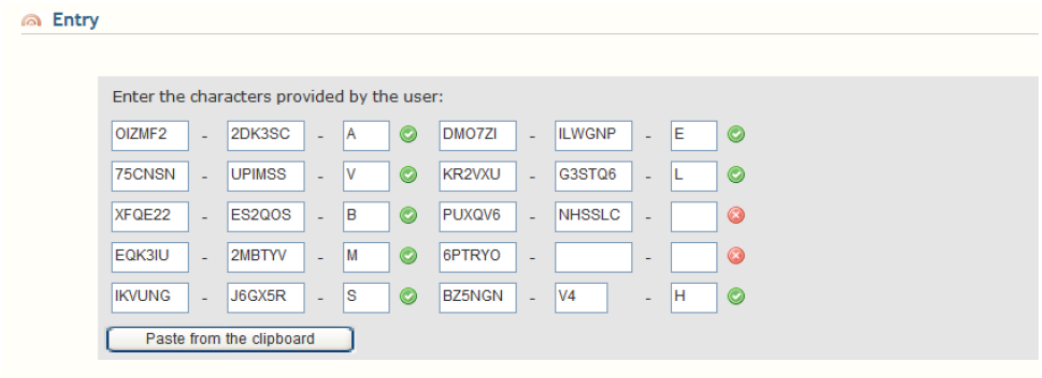
Stormshield Data Authority Manager affiche une nouvelle page contenant les données à communiquer à l'utilisateur pour débloquer son compte.

8.10.4 Déblocage d'un compte généré par Stormshield Data Security

La fonction de déblocage est accessible depuis la page **Liste des utilisateurs** dans le menu **Gestion des utilisateurs, Débloquer**, en cliquant sur **Un compte créé par Stormshield Data Security** (voir la section Page Liste des utilisateurs).

Vous devez :

1. saisir un identifiant communiqué par l'utilisateur puis cliquer sur **Activer** pour vérifier l'identifiant et rendre accessible la zone de saisie de la référence du mot de passe de secours (voir la section Page Base de données).
2. saisir les caractères communiqués par l'utilisateur.



Lorsque tous les caractères d'une ligne sont renseignés, le contrôle de saisie est effectué et l'icône indique le résultat :

3. cliquer sur **Retrouver le mot de passe de secours**.

Stormshield Data Authority Manager affiche une nouvelle page contenant les données à communiquer à l'utilisateur pour débloquer son compte.

8.11 Suppression d'utilisateurs

Un utilisateur peut être supprimé de la base de données.

> **NOTE**
> Cette opération ne supprime ni les fichiers qui sont générés lors de la diffusion du compte, ni les certificats éventuellement publiés.

8.11.1 Suppression d'un utilisateur

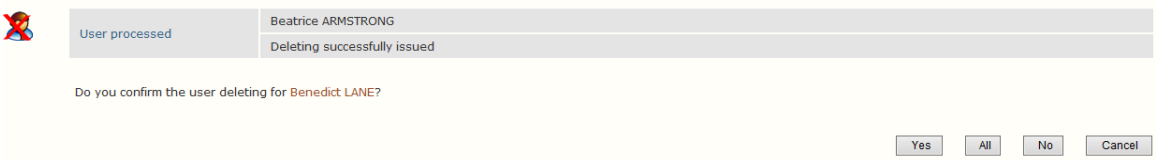
Cette suppression s'exécute à partir de la page **Utilisateur** (section Page Utilisateur) à partir de l'onglet *Gestion de l'utilisateur* en cliquant sur le lien **Supprimer**.

Elle s'applique uniquement à l'utilisateur courant.

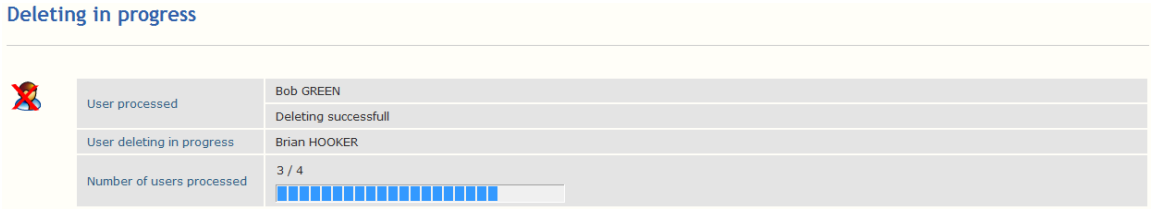
8.11.2 Suppression de plusieurs utilisateurs

Cette suppression de plusieurs utilisateurs en une seule opération s'exécute à partir de la page principale **Liste des utilisateurs** (section Page d'accueil) à partir de l'onglet *Gestion des utilisateurs*.

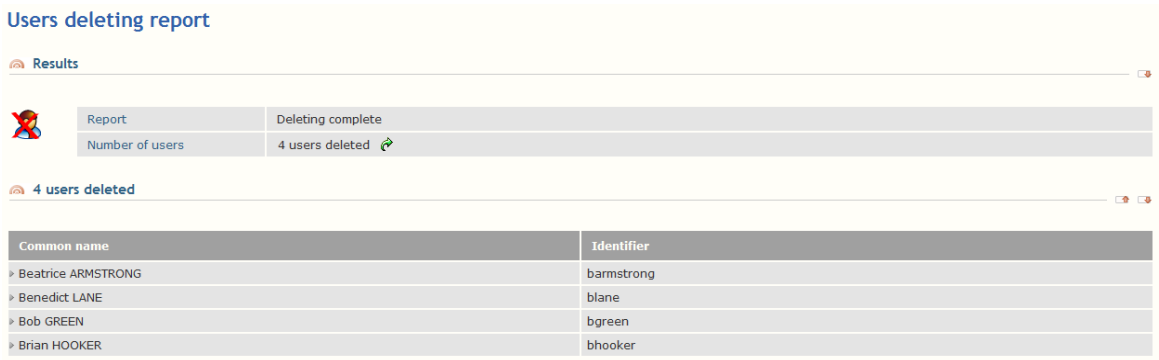
1. Vous sélectionnez les utilisateurs que vous souhaitez supprimer. Cette sélection s'effectue en cochant la case à cocher présente sur la ligne de chaque utilisateur.
2. Vous lancez ensuite la suppression par appui sur le lien **Supprimer les utilisateurs**.
3. Après chaque suppression, Stormshield Data Authority Manager fournit un compte rendu et demande une confirmation pour la suppression suivante :



4. Vous pouvez éviter ces demandes de confirmation en activant la suppression automatique par appui sur le bouton **Tous** :



5. Lorsque tous les utilisateurs ont été traités, Stormshield Data Authority Manager affiche une page de compte rendu :



Cette page affiche la liste des utilisateurs qui ont été supprimés, et éventuellement la liste des utilisateurs pour lesquels la suppression a échoué. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 utilisateurs. Les listes complètes sont téléchargeables en cliquant sur l'icône .

8.12 Révocation d'utilisateurs

Les certificats des utilisateurs peuvent être révoqués.

Vous avez la possibilité de révoquer un seul certificat ou plusieurs certificats à la fois.

Il est recommandé de publier une nouvelle liste de révocation dès qu'un certificat est révoqué, afin que l'état de révocation du certificat soit pris en compte au plus tôt.

La CRL est générée et publiée conformément aux options spécifiées dans les "Paramètres généraux de gestion des certificats" (voir la section Listes de révocation (CRLs)).

8.12.1 Révocation d'un utilisateur

Un utilisateur peut être révoqué depuis la page d'affichage de son certificat ou depuis la page principale **Liste des utilisateurs**.

Pour révoquer un utilisateur depuis la page d'affichage de son certificat, reportez-vous à la section Révocation de certificat.

Pour révoquer un utilisateur depuis la page principale **Liste des utilisateurs** (section Page d'accueil) :

1. Cochez l'utilisateur que vous souhaitez révoquer.
2. Ouvrez le menu **Gestion des utilisateurs** et cliquez sur **Révoquer les utilisateurs**. Plusieurs options de révocation sont disponibles :
   - la date d'invalidité ;

     > **NOTE**
     > A la différence de la date de révocation, qui sera systématiquement incluse et qui sera la date courante, la date d'invalidité est facultative. C'est la date à partir de laquelle le certificat sera invalide ou la date à laquelle la clé a été compromise. Elle sera incluse dans le champ **InvalidityDate** de l'entrée dans la CRL. Il est inutile de la spécifier si elle est identique à la date de révocation.

   - le commentaire de révocation. Ce commentaire n'apparaîtra pas dans la CRL, il est interne à Stormshield Data Authority Manager. Il apparaîtra par contre dans la page d'affichage du certificat (section Affichage de certificat) ;
   - la publication d'une nouvelle liste de révocation.
3. Cliquez sur **Révoquer les utilisateurs**. Une page de compte-rendu s'affiche.

8.12.2 Révocation de plusieurs utilisateurs

Pour révoquer plusieurs utilisateurs à la fois depuis la page principale **Liste des utilisateurs** (section Page d'accueil) :

1. Sélectionnez les utilisateurs que vous souhaitez révoquer.
2. Ouvrez le menu **Gestion des utilisateurs** et cliquez sur **Révoquer les utilisateurs**. Plusieurs options de révocation sont disponibles :
   - la date d'invalidité ;

     > **NOTE**
     > A la différence de la date de révocation, qui sera systématiquement incluse et qui sera la date courante, la date d'invalidité est facultative. C'est la date à partir de laquelle le certificat sera invalide ou la date à laquelle la clé a été compromise. Elle sera incluse dans le champ **InvalidityDate** de l'entrée dans la CRL. Il est inutile de la spécifier si elle est identique à la date de révocation.

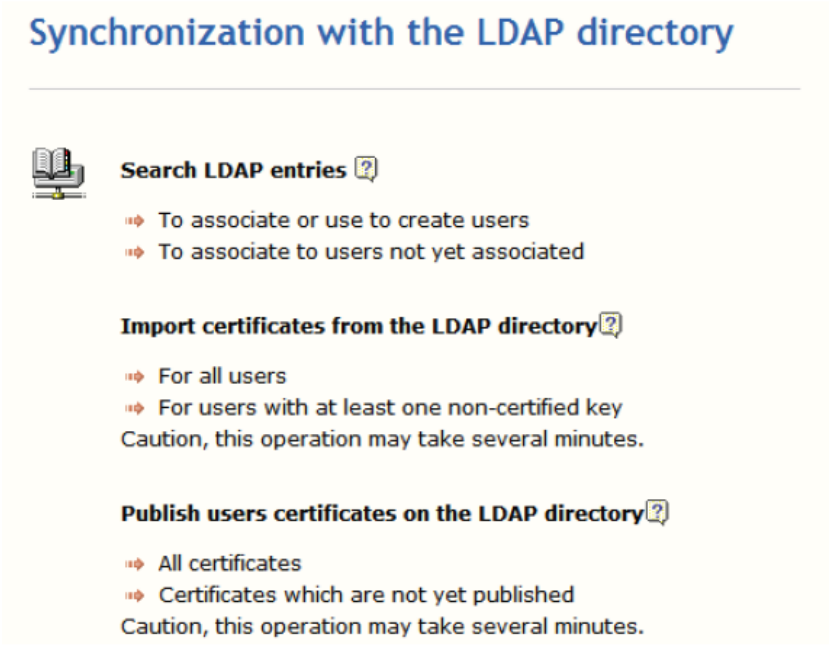
   - le commentaire de révocation. Ce commentaire n'apparaîtra pas dans la CRL, il est interne à Stormshield Data Authority Manager. Il apparaîtra par contre dans la page d'affichage du certificat (section Affichage de certificat) ;
   - la publication d'une nouvelle liste de révocation.
3. Cliquez sur **Révoquer les utilisateurs**.
4. Après chaque révocation, Stormshield Data Authority Manager fournit un compte rendu et demande une confirmation pour la révocation suivante.
5. Lorsque tous les utilisateurs ont été traités, Stormshield Data Authority Manager affiche une page de compte rendu.

8.13 Synchronisation avec un annuaire LDAP

La page principale de la synchronisation avec un annuaire LDAP est accessible à partir de l'onglet *Autres* de la page **Liste des utilisateurs** à partir du lien **Synchronisation LDAP** (voir la

section Opérations disponibles).

Le serveur LDAP auquel Stormshield Data Authority Manager se connecte, est défini dans les paramètres généraux (voir la section Serveur LDAP).



Cette page propose un menu d'opérations qui permet :

- d'associer des entrées LDAP à des utilisateurs de la base (section Association d'un utilisateur à une entrée LDAP) ;
- de créer des utilisateurs à partir d'entrées LDAP (voir la section Création à partir d'un annuaire LDAP) ;
- d'importer, à partir de l'annuaire, des certificats pour les utilisateurs associés à des entrées LDAP (voir la section Importation de certificats à partir d'un annuaire LDAP) ;
- de publier dans l'annuaire les certificats des utilisateurs associés à des entrées LDAP (section Publication de certificat sur un annuaire LDAP).

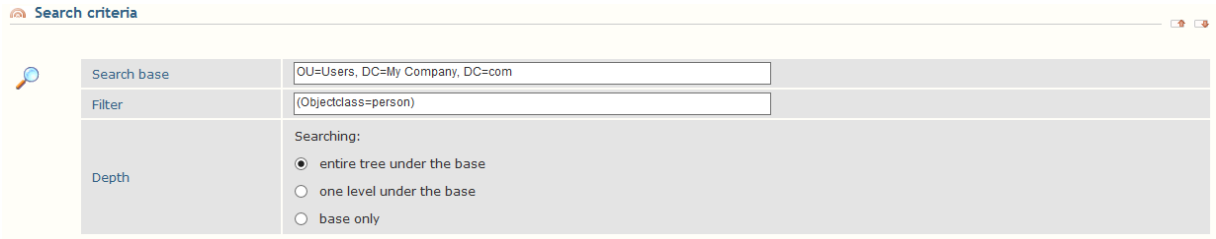
8.14 Association d'un utilisateur à une entrée LDAP

Stormshield Data Authority Manager propose d'associer une entrée LDAP à un utilisateur de la base lorsqu'ils ont la même adresse e-mail, et / ou le même nom usuel, et / ou le même identifiant, et / ou les mêmes nom et prénom. L'adresse e-mail et le nom usuel sont obligatoires.

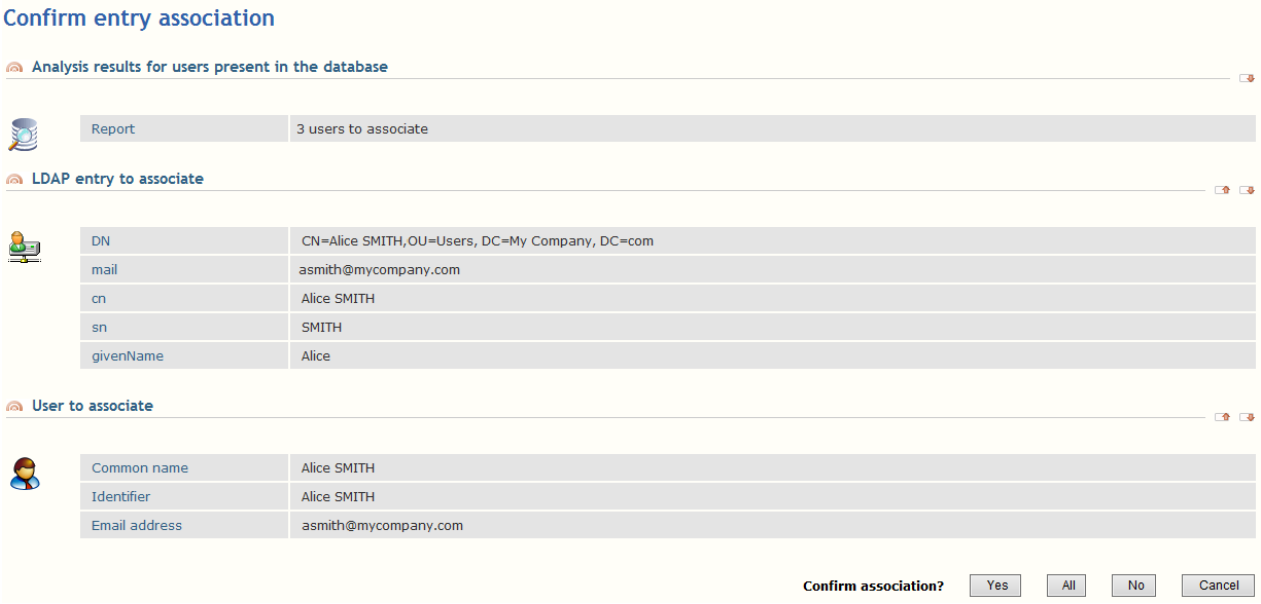
La recherche dans l'annuaire des entrées à associer aux utilisateurs de la base peut être lancée de deux manières :

- soit en cliquant sur le lien **A associer ou à utiliser pour créer des utilisateurs**. Stormshield Data Authority Manager recherche alors, pour chaque entrée lue dans l'annuaire, un utilisateur présent dans la base qui peut lui être associé. En cas d'échec, elle propose alors de créer un utilisateur à partir de cette entrée (voir la section Création à partir d'un annuaire LDAP) ;
- soit en cliquant sur le lien **A associer aux utilisateurs non déjà associés**. Stormshield Data Authority Manager recherche alors, pour chaque utilisateur de la base non encore associé, une entrée présente dans l'annuaire qui peut lui être associée.

Dans les deux cas, Stormshield Data Authority Manager parcourt les entrées de l'annuaire LDAP (voir la sélection de l'annuaire section Configuration LDAP) selon les critères de recherche saisis :

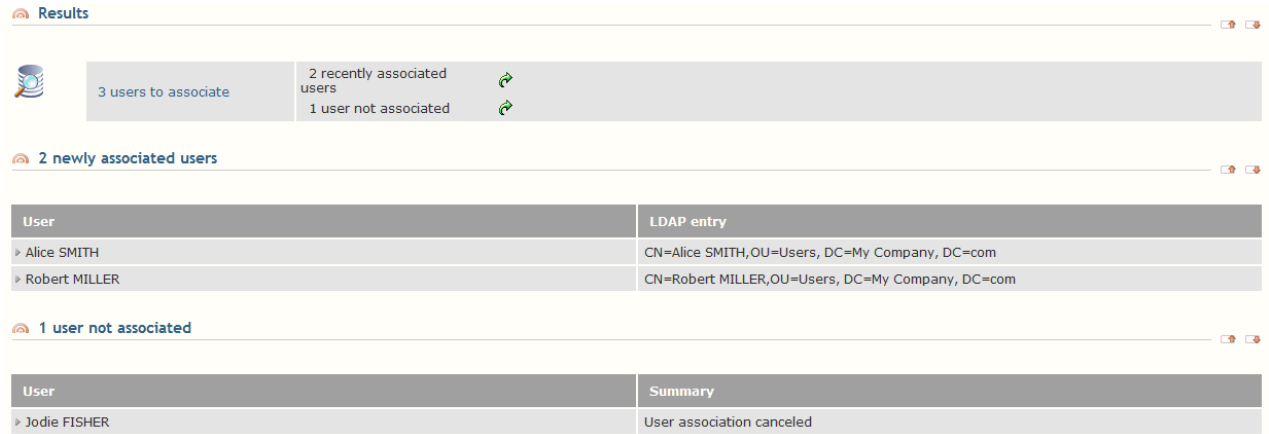


Pour chaque association possible, Stormshield Data Authority Manager affiche une page de confirmation :



Vous pouvez évitez ces demandes de confirmation en activant l'association automatique des entrées par appui sur le bouton **Tous**.

Lorsque toutes les associations possibles ont été proposées, une page de compte rendu est affichée :



Cette page affiche la liste des utilisateurs associés, et éventuellement la liste des utilisateurs pour lesquels l'association a échoué. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 utilisateurs. Les listes complètes sont téléchargeables en cliquant sur l'icône .

9. Gestion des clés des utilisateurs

Cette section décrit comment gérer les clés des utilisateurs.

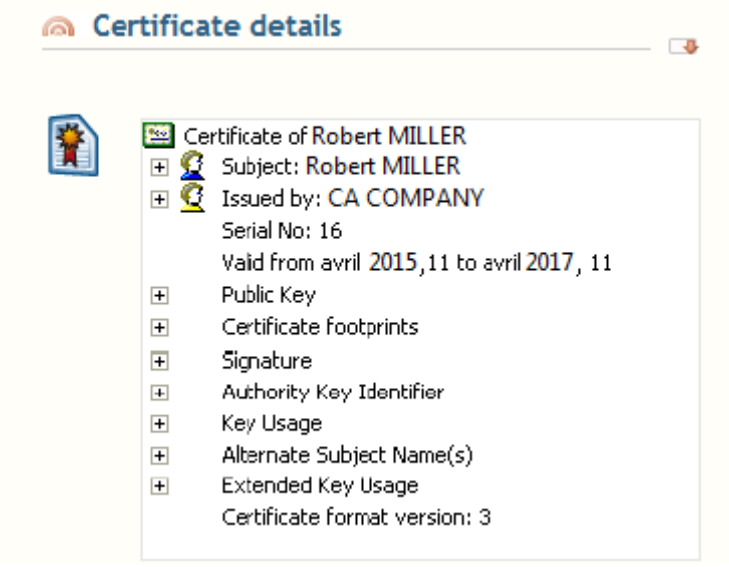
9.1 Page Clé et certificat

Cette page est accessible à partir de la page **Utilisateurs** (sectionPage Utilisateur) en cliquant sur le numéro de série du certificat de la clé.

La première section indique :

- l'algorithme de chiffrement avec sa force.
- le rôle de la clé (voir la section Utilisateur standard).

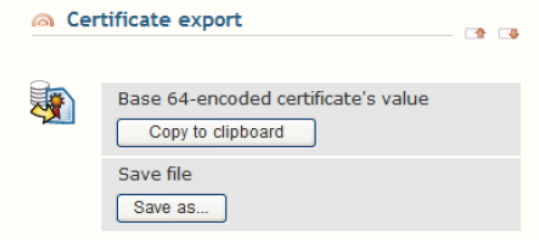
La deuxième section affiche le contenu complet du certificat sous la forme d'un arbre.



Dans la section suivante, on affiche les informations concernant une éventuelle demande de certificat :

- la date d'une éventuelle demande de certificat en cours pour cette clé ;
- le nom de l'autorité de certification externe associée à la clé (voir la section Autorités de certification externes).

Dans la dernière section, vous pouvez exporter le certificat par copier-coller de sa valeur "base 64" ou par enregistrement dans un fichier (voir la section Exportation de certificat).



Dans le bandeau en haut de la page, un menu est proposé.

- dans l'onglet *Propriétés*, vous accédez aux propriétés de la clé ;
- dans l'onglet *Gestion de la clé*, vous pouvez supprimer la clé ;

IMPORTANT
Si vous supprimez une clé de chiffrement, vous ne pourrez plus déchiffrer les données chiffrées à l'aide de cette clé. Cette opération n'est pas proposée si l'utilisateur est associé à une carte.

- dans l'onglet Gestion du certificat, vous pouvez :
- renouveler le certificat pour la clé (voir la section Renouvellement de certificat),
- effectuer une demande de certificat pour la clé (voir la section Création de demande),
- importer un certificat pour la clé (voir la section Importation de certificat interne),
- si la clé a été certifiée par l'autorité de certification interne à la base, accéder à la page du **Certificat** dans la partie autorité de certification, où vous pourrez révoquer le certificat.

9.2 Page Propriétés de la clé

La page des propriétés de la clé est accessible à partir de la page **Clé et certificat** dans l'onglet *Propriétés*.

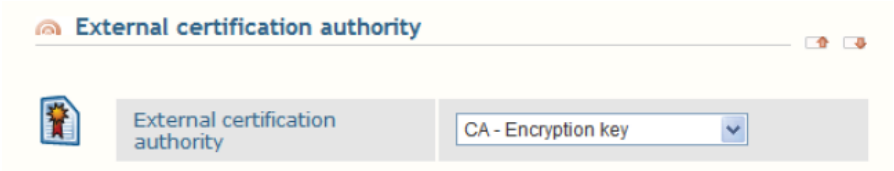
Vous pouvez paramétrer :

- Le rôle de la clé : parmi l'ensemble des clés de l'utilisateur, au même instant, une seule clé peut posséder le rôle de chiffrement, et une seule clé peut posséder le rôle de signature, sachant qu'une même clé peut posséder les deux.

Pour une clé de chiffrement : rôle de chiffrement ou de déchiffrement. Lorsque vous attribuez le rôle de chiffrement à une clé, si une autre clé possède déjà ce rôle, elle le perd automatiquement pour devenir une clé de déchiffrement.

Pour une clé de signature : rôle de signature, sinon elle est simplement une clé qui possède l'usage de signature. Lorsque vous attribuez le rôle de signature à une clé, si une autre clé possède déjà ce rôle, celle-ci le perd automatiquement.

- Le nom de l'autorité de certification externe associée à la clé (voir la section Autorités de certification externes).



9.3 Renouveler les clés

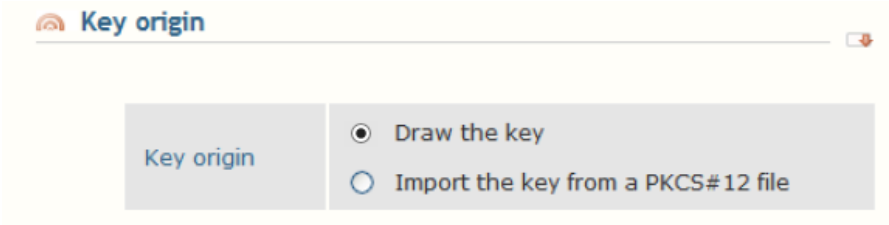
9.3.1 Renouveler une clé

Vous pouvez renouveler une clé à partir de la page **Utilisateurs** (voir la section Page Utilisateur) à partir de l'onglet *Clés et certificats* en cliquant sur le lien **Renouveler une clé**.

Cette opération consiste en fait à ajouter une clé à l'utilisateur. Cette clé obtient automatiquement le ou les rôles que son certificat lui octroie, rôles déterminés à partir des usages X.509 du certificat. Les clés qui possédaient ces rôles auparavant, deviennent mécaniquement des clés de déchiffrement ou simplement des clés qui possèdent l'usage de signature.

Dans la première partie de la page vous sélectionnez l'origine de la clé à ajouter de l'une des deux manières suivantes :

- tirer la clé (voir la section Tirer la clé) ;
- ou bien importer la clé à partir d'un fichier *PKSC#12* (voir la section Importation de clé à partir d'un fichier PKCS#12).



Tirer la clé

Dans le cas où la clé doit être tirée, procédez de la manière suivante :

1. Sélectionnez l'algorithme de chiffrement avec sa force.
2. Sélectionnez le mode de certification : en plus de la ligne indiquant que vous devez sélectionner un mode de certification, le menu déroulant contient la liste des modèles de certificat et la liste des autorités de certification externes.

- Si vous sélectionnez un modèle de certificat :
- si la base possède une autorité de certification interne certifiée, la clé est certifiée par cette autorité de certification ;
- sinon, la clé est auto-certifiée. Cette information est alors précisée.

Dans les deux cas, les données du modèle de certificat sont utilisées.

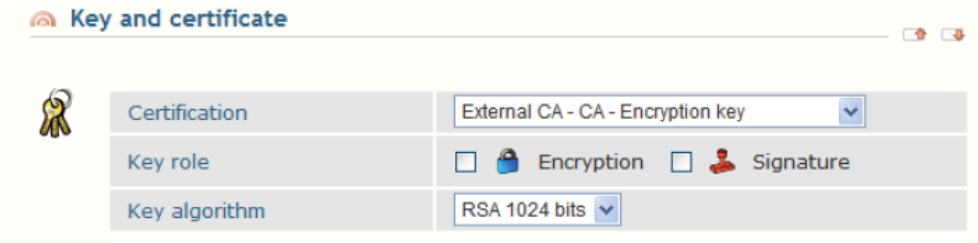
La durée de validité, pré-remplie à l'aide de celle du modèle de certificat, est modifiable.

La ligne **Rôle de la clé** indique quels seront le ou les rôles de la future clé. Ils sont déterminés à partir des usages X.509 du modèle de certificat. Ils ne sont donc pas modifiables.

- Si vous sélectionnez une autorité de certification externe, la clé est tirée mais pas certifiée. Vous devez effectuer une demande de certificat pour cette clé et ensuite importer le certificat fourni.

L'autorité de certification externe sélectionnée est associée à la clé et ses données seront utilisées lors de la demande de certificat.

Afin de faciliter par la suite la gestion des clés, vous pouvez indiquez sur la ligne **Rôle de la clé**, à l'aide des cases à cocher, le rôle souhaité pour cette clé. Sachant que, à terme, ce seront les usages X.509 du futur certificat qui feront foi, et fixeront le ou les rôles de la clé.

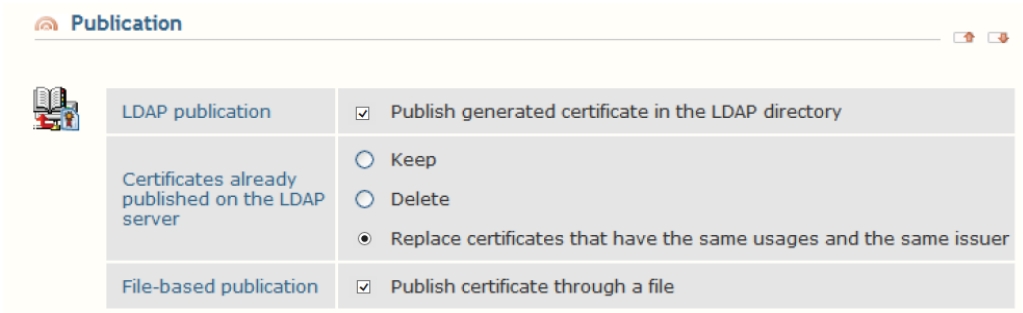


3. Selon vos paramètres généraux, une section propose éventuellement la publication du ou des certificats générés.

Si un serveur LDAP est paramétré (voir la section Configuration LDAP), vous pouvez choisir de publier le certificat dans l'annuaire LDAP. Paramétrez l'opération à effectuer sur les éventuels certificats déjà présents sur le serveur LDAP à l'entrée désignée par le DN :

- les conserver ;
- les supprimer ;
- remplacer les certificats ayant les mêmes usages X.509 et émis par cette autorité.

4. Si la publication par fichier est paramétrée (voir la section Publication d'un certificat).



Importation de clé à partir d'un fichier *PKCS#12*

1. Dans le cas où la clé est importée à partir d'un fichier *PKCS#12* , vous devez sélectionner le fichier *PKCS#12*.
2. Saisissez son mot de passe.

Après la vérification du mot de passe, la liste des clés contenues dans le fichier est affichée.

Les clés sont triées par rôle : chiffrement, signature et personnelle pour celles qui ont les deux rôles à la fois. Le rôle de la clé est déterminé à partir des usages X.509 du certificat associé.

3. Sélectionnez la clé que vous voulez ajouter puis validez. Une seule clé doit être sélectionnée.

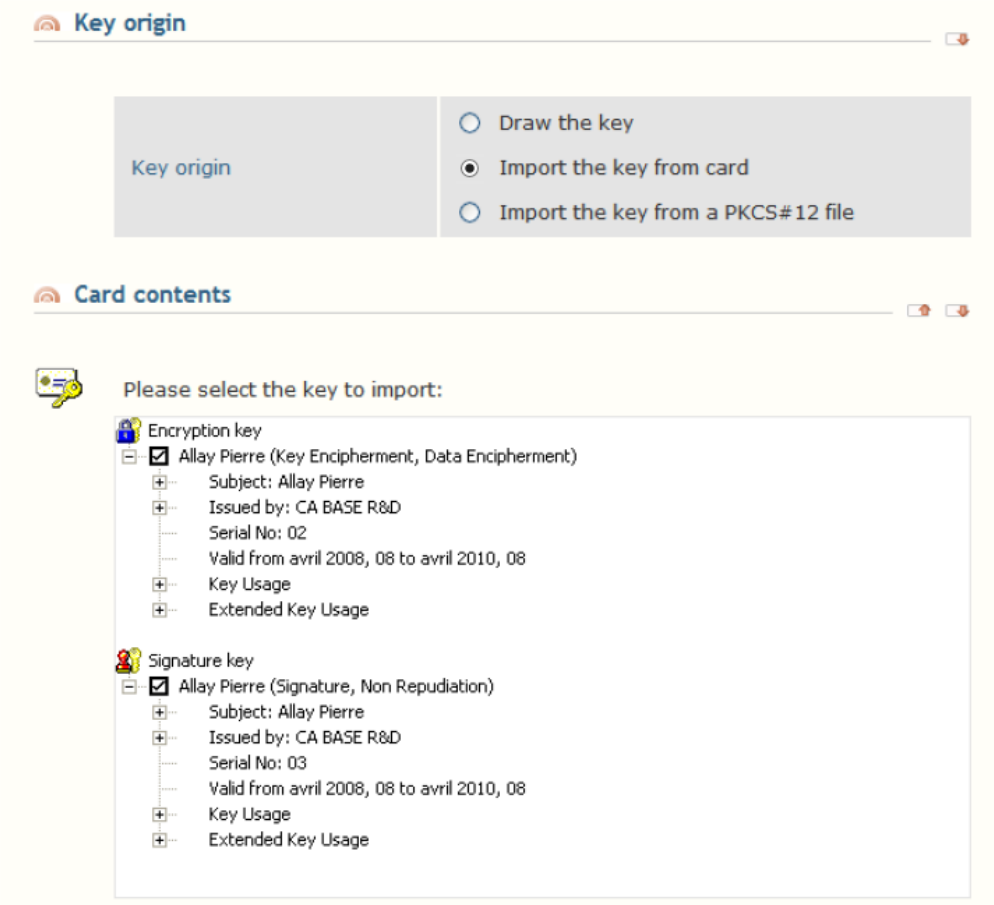
Utilisateur associé à une carte

Dans le cas particulier d'un utilisateur associé à une carte à puce, les deux opérations décrites précédemment se poursuivent par l'écriture dans la carte de la clé tirée ou importée à partir du fichier PKCS#12. Vous devez vous reconnecter à la carte et confirmer l'écriture.

Vous avez en plus la possibilité d'importer la clé à partir de la carte.

1. Pour ce faire, vous devez tout d'abord vous connecter à la carte.
2. Lorsque vous sélectionnez l'importation à partir de la carte, la liste des clés est affichée.

Les clés sont triées par rôle : chiffrement, signature et personnelle pour celles qui ont les deux rôles à la fois. Le rôle de la clé est déterminé à partir des usages X.509 du certificat associé.



3. Sélectionnez la clé que vous voulez ajouter puis validez. Une seule clé doit être sélectionnée.

9.3.2 Renouveler plusieurs clés

Le renouvellement de plusieurs clés en une seule opération est exécuté à partir de la page principale **Liste des utilisateurs** (section Page Liste des utilisateurs).

NOTE
Pour le renouvellement de plusieurs clés en une seule opération, il est uniquement possible de tirer les clés.

Pour renouveler une clé pour chaque utilisateur :

1. Sélectionnez les utilisateurs pour lesquels vous souhaitez renouveler une clé. Cette sélection s'effectue en cochant la case à cocher présente sur la ligne de chaque utilisateur concerné par l'opération.
2. Lancez ensuite le renouvellement en cliquant sur le lien **Renouveler une clé** dans le menu **Gestion des utilisateurs**.
3. Dans la page suivante, sélectionnez le mode de certification : en plus de la ligne indiquant que vous devez sélectionner un mode de certification, le menu déroulant contient la liste des modèles de certificat et la liste des autorités de certification externes.

- Si vous sélectionnez un modèle de certificat :
- si la base possède une autorité de certification interne certifiée, la clé est certifiée par cette autorité de certification ;
- sinon, la clé est auto-certifiée. Cette information est alors précisée.

Dans les deux cas, les données du modèle de certificat sont utilisées.

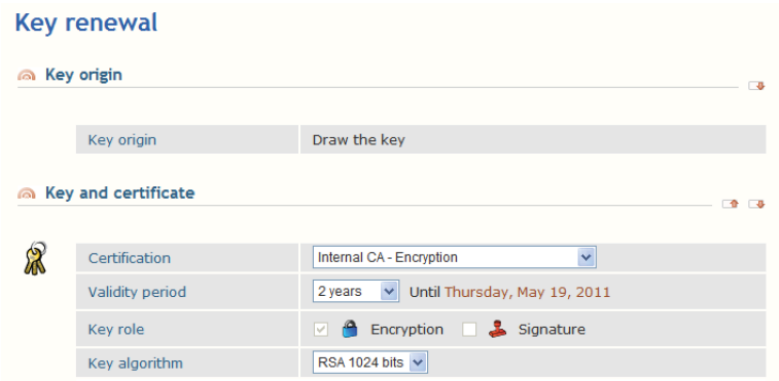
La durée de validité, pré-remplie à l'aide de celle du modèle de certificat, est modifiable.

La ligne **Rôle de la clé** indique quels seront le ou les rôles de la future clé. Ils sont déterminés à partir des usages X.509 du modèle de certificat. Ils ne sont donc pas modifiables.

- Si vous sélectionnez une autorité de certification externe, la clé est tirée mais pas certifiée. Vous devez effectuer une demande de certificat pour cette clé et ensuite importer le certificat fourni.

L'autorité de certification externe sélectionnée est associée à la clé et ses données seront utilisées lors de la demande de certificat.

Afin de faciliter par la suite la gestion des clés, vous pouvez indiquez sur la ligne **Rôle de la clé**, à l'aide des cases à cocher, le rôle souhaité pour cette clé. Sachant que, à terme, ce seront les usages X.509 du futur certificat qui feront foi, et fixeront le ou les rôles de la clé.

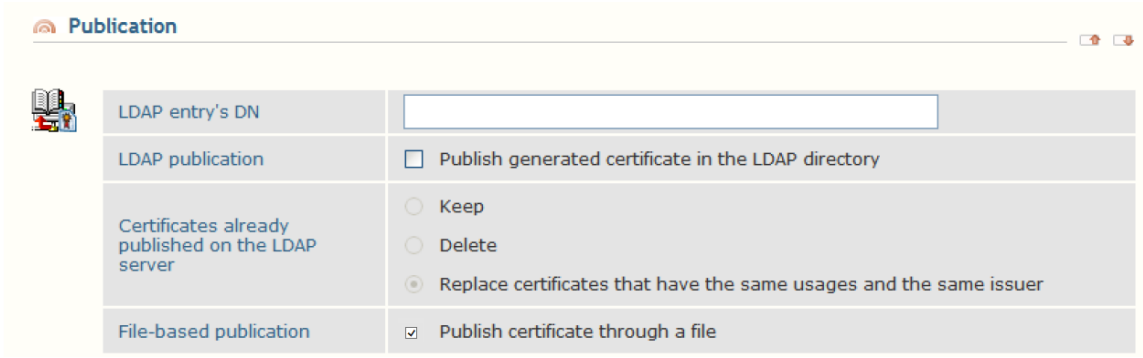


4. Selon vos paramètres généraux, une section propose éventuellement la publication du ou des certificats générés.

Si un serveur LDAP est paramétré (section Configuration LDAP), vous pouvez choisir de publier le certificat dans l'annuaire LDAP. La publication aura toujours lieu vers le DN de l'utilisateur dont on renouvelle le ou les certificats. Paramétrez l'opération à effectuer sur les éventuels certificats déjà présents sur le serveur LDAP à l'entrée désignée par le DN :

- les conserver ;
- les supprimer ;
- remplacer les certificats ayant les mêmes usages X.509 et émis par cette autorité.

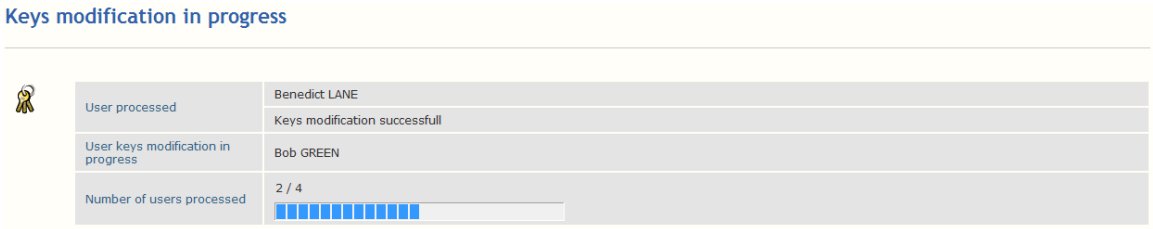
Si la publication par fichier est paramétrée (voir la section Publication d'un certificat).



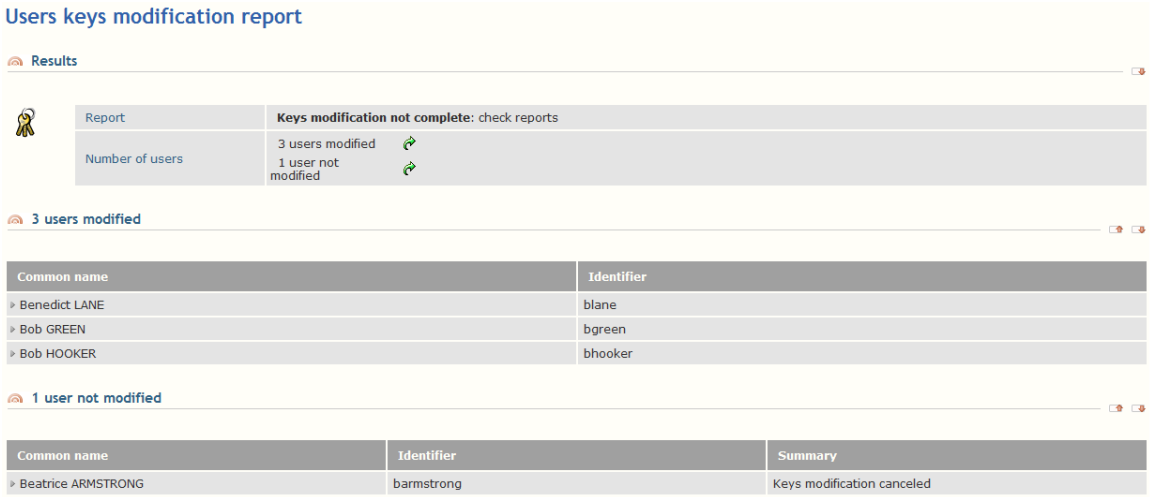
5. Lancez l'opération en cliquant sur le bouton **Renouveler**.

Après chaque renouvellement, Stormshield Data Authority Manager affiche un compte rendu et demande une confirmation pour le renouvellement suivant :

Evitez ces demandes de confirmation en activant le renouvellement automatique par appui sur le bouton **Tous** :



Lorsque toutes les clés ont été renouvelées, Stormshield Data Authority Manager affiche une page de compte rendu :



Cette page affiche la liste des utilisateurs pour lesquels une clé a été renouvelée, et éventuellement la liste des utilisateurs pour lesquels le renouvellement a échoué. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 utilisateurs. Les listes complètes sont téléchargeables en cliquant sur l'icône .

9.4 Exportation des clés dans un fichier PKCS#12

Cette opération s'exécute à partir de la page **Utilisateurs** (section Page Utilisateur) à partir de l'onglet *Clés et certificats* en cliquant sur le lien **Exporter les clés**.

1. La liste des clés de l'utilisateur est affichée. Vous sélectionnez les clés à exporter à l'aide de la case à cocher présente sur chaque ligne. L'icône indique si toutes les clés sont sélectionnées certaines clés sont sélectionnées ou aucune clé n'est sélectionnée Cliquer sur ces icônes sélectionne ou désélectionne toutes les clés.
2. Saisissez le mot de passe.

Afin de garantir la confidentialité des données, il est conseillé de saisir un mot de passe non trivial. Pour aider à la saisie du mot de passe, un tirage aléatoire est proposé en appuyant sur l'icône .

3. Cliquez sur **Exporter la clé**.
4. Une page de compte rendu s'affiche. Elle propose de sauvegarder le fichier *PKCS#12* créé, et dans lequel les clés et certificats associés ont été copiés.

10. Gestion des certificats

Cette section décrit les différents types de certificats internes et externes, et explique comment les importer et les exporter.

10.1 Certificats externes

Stormshield Data Authority Manager permet de gérer des certificats non générés par Stormshield Data Authority Manager : les certificats externes.

Il existe deux types de certificats externes :

- les certificats externes de recouvrement (section Certificats externes de recouvrement), qui sont intégrés aux comptes utilisateurs en tant que recouvrement ;
- les autres certificats externes (section Autres certificats externes), qui peuvent être des certificats d'autorités de certification, sont :
- ajoutés aux annuaires des utilisateurs (*.usd*) et aux fichiers de mise à jour des utilisateurs (*.usx*),
- utilisés pour constituer la parenté des certificats générés par l'autorité de certification interne.

10.1.1 Certificats externes de recouvrement

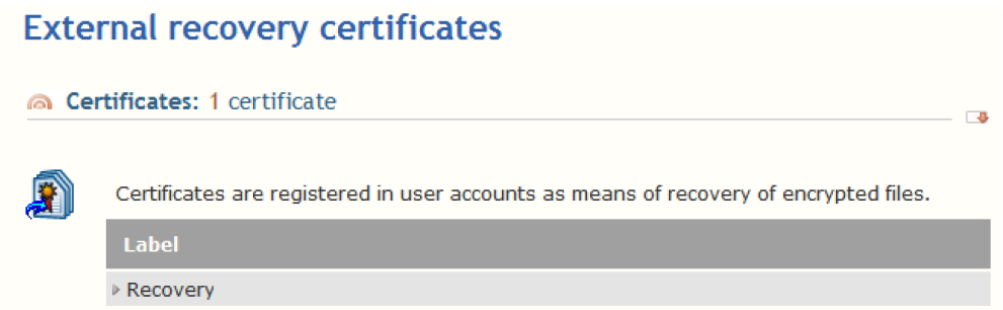
Pour gérer des certificats externes de recouvrement, aller à la page **Gestion des utilisateurs** (section Page Liste des utilisateurs) et aussi à la page **Liste des utilisateurs** (voir la section Page Liste des utilisateurs).

Lors de la diffusion, ces certificats sont inscrits dans le compte utilisateur comme recouvrement des données chiffrées.

Après l'importation d'un certificat externe de recouvrement, celui-ci est automatiquement rajouté aux comptes des utilisateurs lors d'une mise à jour de politique de sécurité (*.usx*).

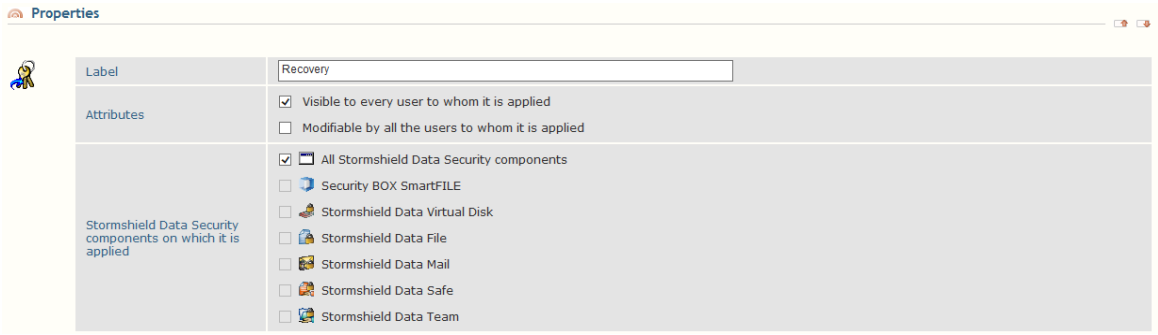
NOTE
La suppression des certificats externes de recouvrement n'est pas gérée par cette fonctionnalité, c'est-à-dire que les certificats ne sont pas supprimés des comptes des utilisateurs.

La page des certificats externes de recouvrement présente la liste des certificats de recouvrement déjà importés dans la base. Vous pouvez importer un nouveau certificat à partir du menu déroulant **Opérations** (section Importation de certificats externes).



Les certificats sont identifiés par un libellé. En cliquant sur ce libellé vous affichez la page des propriétés du certificat. Dans cette page vous pouvez :

- voir le contenu détaillé du certificat ;
- modifier le libellé du certificat ainsi que ses propriétés de recouvrement ;
- supprimer le certificat.



10.1.2 Autres certificats externes

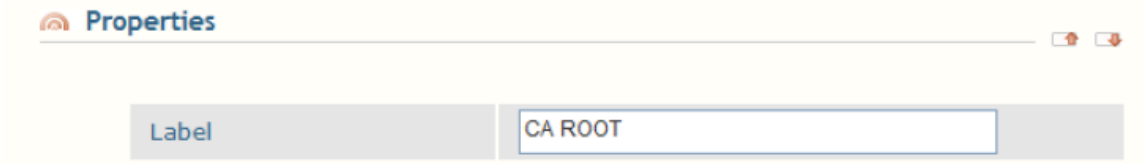
La gestion des certificats externes à ajouter aux annuaires, aux fichiers de mise à jour (*.usx*), et constituant la chaîne de parenté est accessible dans la page d'accueil (section Page d'accueil).

Ces certificats sont ajoutés aux annuaires de tous les utilisateurs lors de leur diffusion. Les certificats d'autorités sont présents dans l'onglet *Autorités* de l'annuaire, les autres certificats sont présents dans l'onglet *Certificats*.

Ils sont copiés dans le fichier de mise à jour (*.usx*) de l'utilisateur afin d'être importés dans son annuaire.

Ces certificats servent également à constituer la chaîne de parenté des certificats générés par l'autorité de certification interne. Lors de l'exportation d'un certificat généré par l'autorité de certification interne (section Exportation de certificat interne), Stormshield Data Authority Manager lit le certificat de l'autorité et parcourt ces certificats externes pour constituer la chaîne de parenté la plus complète possible. Ainsi, si vous souhaitez exporter des certificats avec leur parenté (*.p7b*, *.p7c*), importez dans les certificats externes tous les certificats de la chaîne de parenté.

La page des certificats externes présente la liste des certificats déjà importés dans la base, et un lien permettant d'importer un nouveau certificat (section Importation de certificats externes).



Les certificats sont identifiés par un libellé. En cliquant sur ce libellé vous affichez la page des propriétés du certificat. Dans cette page vous pouvez :

- voir le contenu détaillé du certificat,
- modifier le libellé du certificat,
- supprimer le certificat.

10.2 Notification d'expiration de certificat

Vous pouvez être notifié par e-mail lorsque des certificats d'utilisateurs sont sur le point d'expirer.

L'e-mail vous fournit des informations relatives aux utilisateurs concernés, telles que leur identifiant, leur nom et prénom ainsi que leur adresse e-mail. Il fournit également des informations propres aux certificats telles que leur numéro de série, leur date d'expiration et leur usage cryptographique (ex : signature ou chiffrement). Pour activer et paramétrer cette fonctionnalité, voir la section Notification par e-mail.

- Pour bénéficier de cette fonctionnalité, vous devez paramétrer au préalable les informations de connexion au serveur SMTP (voir la section Serveur SMTP) ;
- Seuls les certificats courants des utilisateurs sont listés dans l'e-mail de notification. Les anciens certificats ainsi que les certificats révoqués ne sont pas signalés ;
- Les e-mails de notification sont émis, à la fréquence qui a été paramétrée dans le champ approprié, même lorsque les certificats ont dépassé leur date d'expiration ;
- La liste peut contenir des certificats correspondants à des clés renouvelées ;
- Stormshield Data Authority Manager n'envoie aucun e-mail lorsqu'aucun certificat n'est sur le point d'expirer.

10.3 Création de demandes de certificats *PKCS#10*

Stormshield Data Authority Manager permet de générer des demandes de certificats au format *PKCS#10* pour les clés des utilisateurs.

La date de création de la demande de certificat en cours apparaît dans la page **Clé et certificat**.

10.3.1 Formats binaire et base 64

Le choix du format s'effectue dans les paramètres de l'autorité de certification externe associée à la clé (voir la section Autorités de certification externes).

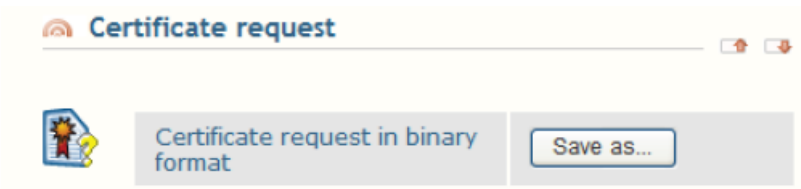
La demande de certificat au format "base 64" est éditable. Elle peut être copiée-collée, envoyée par e-mail, ou saisie dans un formulaire HTML.

10.3.2 Création de demande

Cette opération crée une demande de certificat pour la clé d'un utilisateur. Elle s'effectue à partir de la page **Clé et certificat** dans l'onglet *Gestion du certificat* en cliquant sur le lien **Faire une demande de certificat**.

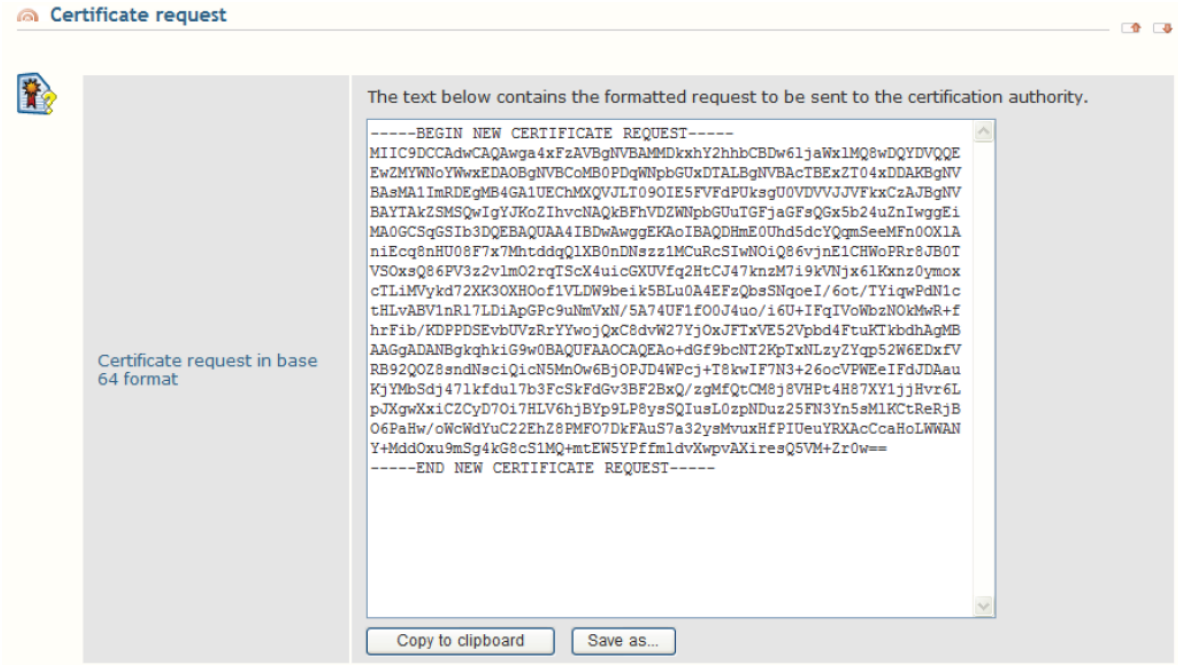
Lorsque la page s'affiche, la demande a été générée. Vous choisissez le mode de distribution de cette demande.

Si la demande de certificat est au format "binaire", seul l'enregistrement de la demande dans un fichier *PKCS#10* est possible.

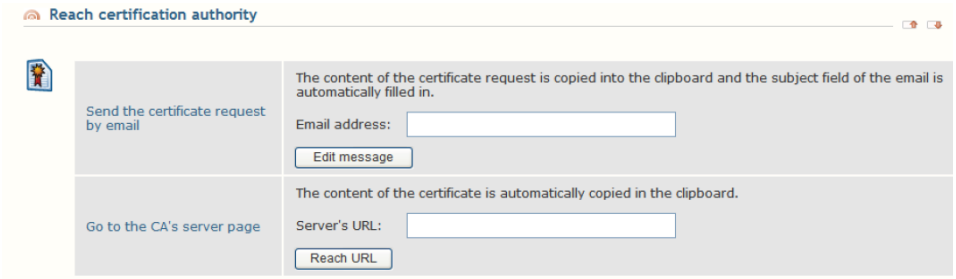


Si la demande de certificat est au format "base 64", vous pouvez :

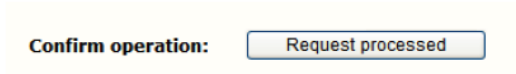
- copier la demande dans le presse-papier ;
- enregistrer la demande dans un fichier *PKCS#10* ;



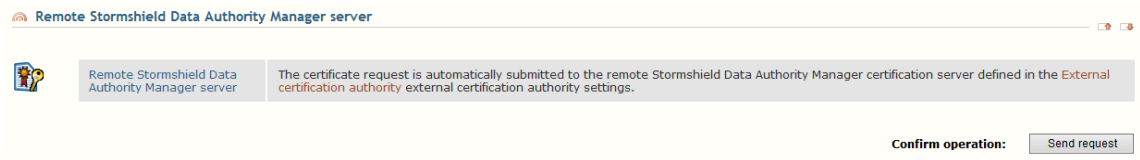
- envoyer la demande par e-mail. L'adresse e-mail est remplie par défaut à l'aide de l'adresse saisie dans les paramètres de l'autorité de certification externe associée à la clé (voir la section Autorités de certification externes). L'objet de l'e-mail est rempli automatiquement en incluant l'usage de la clé et le nom de l'utilisateur. Vous devez coller dans le corps du message, la demande de certificat qui a été automatiquement placée dans le presse-papier ;
- atteindre un serveur de certification. L'URL est remplie par défaut à l'aide de l'URL saisie dans les paramètres de l'autorité de certification externe associée à la clé. La demande de certificat est automatiquement placée dans le presse-papier.



Vous devez valider l'opération pour que Stormshield Data Authority Manager mémorise qu'une demande de certificat a été effectuée et sauvegarde la date.



Vous pouvez également choisir de soumettre la demande à un serveur Stormshield Data Authority Manager (voir la section Demande de certificat à un serveur Stormshield Data Authority Manager distant). Aucun paramétrage n'est demandé dans la page : la demande est envoyée au serveur de certification Stormshield Data Authority Manager distant défini dans les paramètres de l'autorité de certification externe associée à la clé. La date est automatiquement sauvegardée.



La page de compte rendu affiche l'identifiant de la demande de certificat retourné par le serveur de certification distant.

10.3.3 Création de plusieurs demandes

La création de plusieurs demandes de certificat en une seule opération est exécutée à partir de la page principale **Liste des utilisateurs** (voir la section Opérations disponibles) dans l'onglet *Gestion des certificats*.

Cette création multiple permet :

- de créer des demandes *PKCS#10* enregistrées dans des fichiers *PKCS#10*. Chaque requête est créée dans un fichier *PKCS#10* spécifique. Le format des requêtes ("binaire" ou "base 64") et le répertoire de destination sont ceux définis dans les paramètres de l'autorité de certification externe associée à la clé (voir la section Autorités de certification externes).

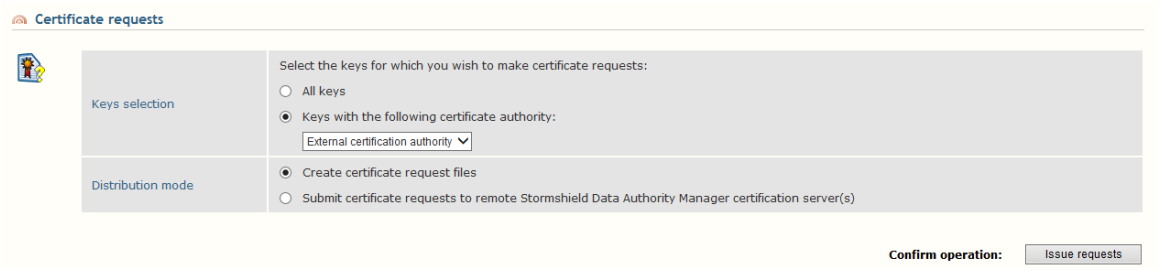
Le nom du fichier est l'identifiant de l'utilisateur, concaténé avec le rôle de la clé ([Chiffrement], [Signature] ou [Chiffrement, Signature]), suivi d'un compteur pour garantir l'unicité du fichier.

- de créer des demandes *PKCS#10* et de les soumettre à un serveur Stormshield Data Authority Manager distant. La demande est envoyée au serveur de certification Stormshield Data Authority Manager distant défini dans les paramètres de l'autorité de certification externe associée à la clé.

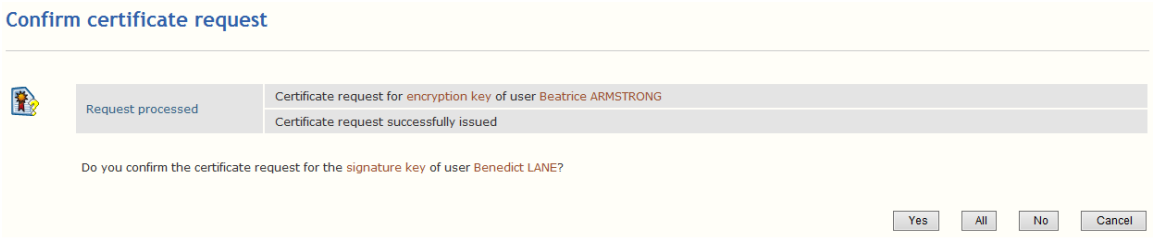
Pour chaque utilisateur sélectionné, l'opération est appliquée uniquement à la clé qui a le rôle de chiffrement, et/ou la clé qui a le rôle de signature.

Pour créer les demandes :

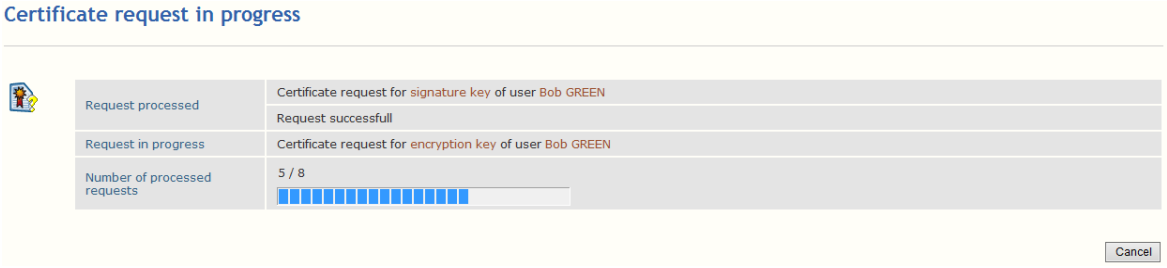
1. Sélectionnez les utilisateurs pour lesquels vous souhaitez créer une demande de certificat. Cette sélection s'effectue en cochant la case à cocher présente sur la ligne de chaque utilisateur.
2. Lancez la création en cliquant sur le lien **Créer les demandes**.
3. Dans la page suivante, sélectionnez les clés pour lesquelles vous souhaitez créer des demandes de certificat . La sélection s'effectue à l'aide de l'autorité de certification externe.
4. Spécifiez si les demandes doivent être soumises à un serveur Stormshield Data Authority Manager distant (voir la section Demande de certificat à un serveur Stormshield Data Authority Manager distant) au lieu d'être enregistrées dans des fichiers.



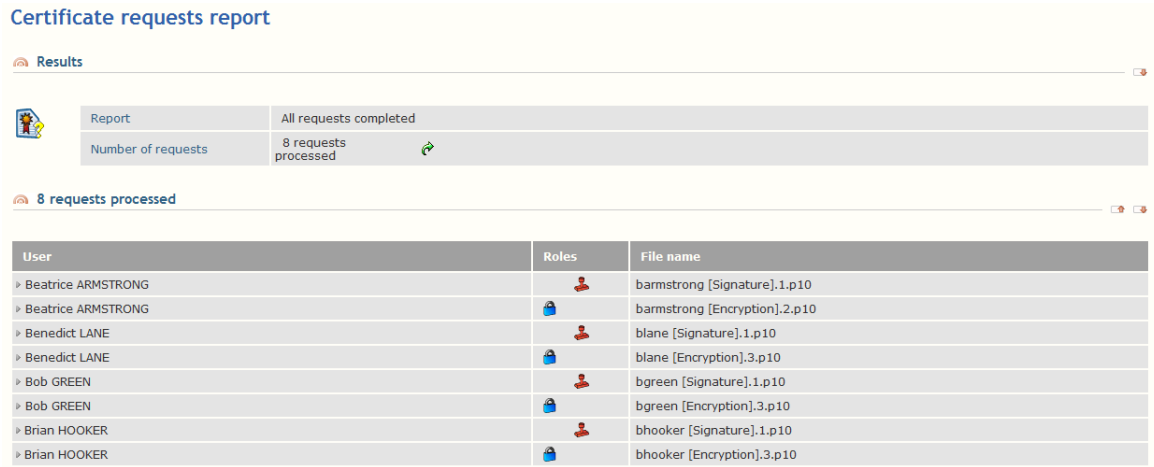
Après chaque création, Stormshield Data Authority Manager fournit un compte rendu et demande une confirmation pour la création suivante :



Évitez ces demandes de confirmation en activant la création automatique des demandes par appui sur le bouton **Tous** :



Lorsque toutes les demandes ont été traitées, Stormshield Data Authority Manager affiche une page de compte rendu :



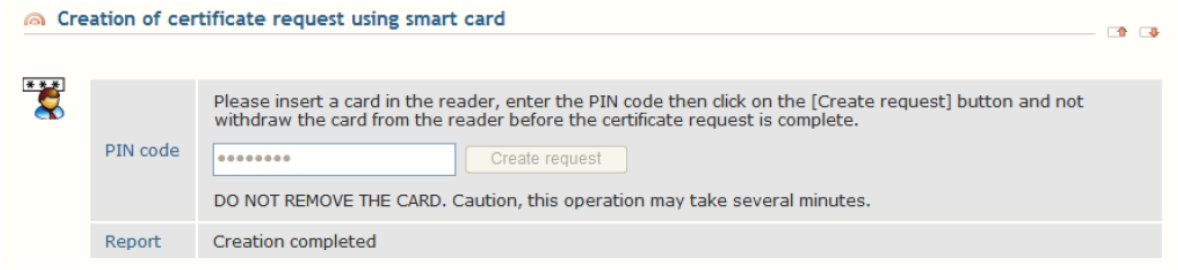
Cette page affiche la liste des clés pour lesquelles une demande a été effectuée, et éventuellement la liste des clés pour lesquelles la demande a échoué. Pour chacune les informations suivantes sont affichées : le nom usuel de l'utilisateur propriétaire de la clé, le rôle de celle-ci, et le nom du fichier créé ou l'identifiant de la demande. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 clés. Les listes complètes sont téléchargeables en cliquant sur l'icône .

10.3.4 Signature d'une demande par un support cryptographique physique

Une demande de certificat est signée par la clé privée. Pour un utilisateur créé à partir d'une carte à puce physique, la clé privée est seulement présente dans la carte. La demande doit donc être signée par la carte.

Cette opération est uniquement effectuée à partir de la page **Clé et certificat** dans l'onglet *Gestion du certificat*, en cliquant sur le lien **Faire une demande de certificat**.

Stormshield Data Authority Manager demande l'insertion de la carte pour créer la demande de certificat : insérez la carte à puce (ou le token), saisissez le mot de passe et lancez la création de la demande.



Ensuite, Stormshield Data Authority Manager propose différents modes de distribution de la demande en fonction de son format. Ils sont décrits dans la section Création de demande.

10.3.5 Demande de certificat à un serveur Stormshield Data Authority Manager distant

Une demande de certificat peut être automatiquement soumise à un serveur Stormshield Data Authority Manager distant. Cette opération peut être effectuée à partir d'une création de demande unitaire (voir la section Création de demande) ou multiple (voir la section Création de plusieurs demandes).

La demande est envoyée au serveur de certification Stormshield Data Authority Manager distant défini dans les paramètres de l'autorité de certification externe associée à la clé : URL du serveur distant, identifiant de la base, libellé du modèle de certificat.

Cette opération :

- envoie la demande au serveur distant, par une requête HTTP ou HTTPS,
- ajoute la demande à la liste des demandes en attente de l'autorité de certification de la base spécifiée du serveur distant,
- affiche dans la page de compte rendu l'identifiant de demande retourné par le serveur distant. Cet identifiant permet de consulter le statut de la demande sur la page publique de consultation du statut d'une demande du serveur distant et de récupérer le certificat généré lorsque la demande est validée.

Notez que le paramétrage d'un proxy HTTP (section Accès à internet) est éventuellement nécessaire pour que la communication soit possible.

10.3.6 Annulation de demande

Une demande de certificat peut être annulée. Cette opération est interne à Stormshield Data Authority Manager. C'est-à-dire que cette annulation permet de modifier dans la base de données l'état de la demande :

- la clé n'a plus de demande de certificat en cours ;
- suppression de la date de la demande.

L'annulation d'une demande de certificat est uniquement accessible à partir de la page principale **Liste des utilisateurs** dans l'onglet *Gestion des certificats* en cliquant sur le lien **Annuler des demandes**.

La procédure est semblable à celle de demandes multiples décrite à la section Création de plusieurs demandes .

10.4 Renouvellement de certificat

Un exemple d'utilisation est disponible dans l'Annexe D, Renouvellement d'un certificat.

10.4.1 Renouvellement de certificat

La page de renouvellement du certificat d'un utilisateur est accessible à partir de la page **Clé et certificat** en cliquant sur le lien **Renouveler le certificat pour la clé**.

1. La première section propose de paramétrer le certificat à générer :

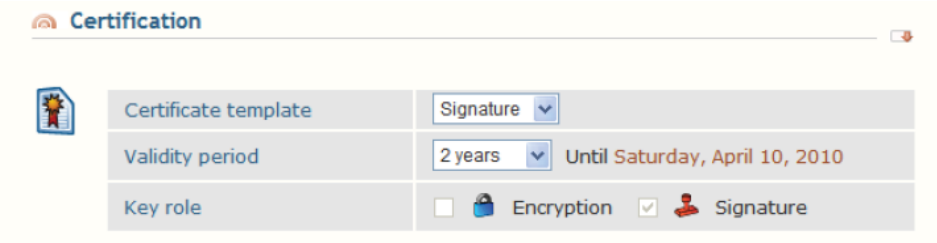
a. Choisissez parmi tous les modèles de certificats standards (section Modèles de certificats) le modèle de certificat à utiliser.

- si la base possède une autorité de certification interne certifiée, la clé est certifiée par cette autorité de certification ;
- sinon, la clé est auto-certifiée. Cette information est alors précisée.

Dans les deux cas, les données du modèle de certificat sont utilisées.

b. La ligne **Rôle de la clé** indique quels seront le ou les rôles de la future clé. Ils sont déterminés à partir des usages X.509 du modèle de certificat. Ils ne sont donc pas modifiables.

c. Choisissez la durée de validité du certificat généré. La durée proposée par défaut est celle du modèle de certificat sélectionné.



2. Si vous souhaitez générer un certificat personnalisé, pour lequel aucun modèle de certificat ne convient, vous devez :

a. Créer une demande (voir la section Création de demande).

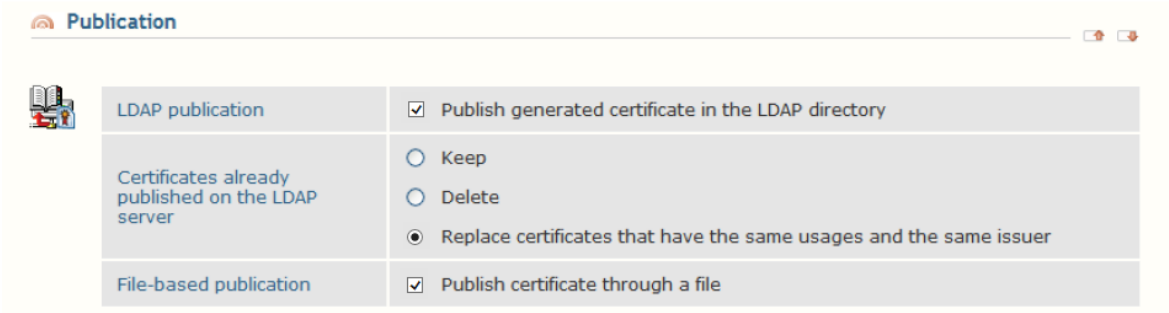
b. Vous connecter à l'accès public de l'autorité de certification (voir la section Page d'accès public).

c. Déposer la demande (voir la section Dépôt d'une demande de certificat).

d. La faire valider par un administrateur (voir la section Demande de certificat). Une personnalisation plus fine du certificat est en effet disponible à la validation.

3. Selon vos paramètres généraux, une deuxième section propose éventuellement la publication du certificat généré.

- Si un serveur LDAP est paramétré (section Configuration LDAP), vous pouvez choisir de publier le certificat dans l'annuaire LDAP. La publication aura toujours lieu vers le DN de l'utilisateur dont on renouvelle le certificat. Paramétrez l'opération à effectuer sur les éventuels certificats déjà présents sur le serveur LDAP à l'entrée désignée par le DN :
- les conserver,
- les supprimer,
- remplacer les certificats ayant les mêmes usages X.509 et émis par cette autorité.
- Si la publication par fichier est paramétrée (voir la section Publication d'un certificat).



4. Une fois les différentes options paramétrées, renouvelez le certificat en appuyant sur le bouton **Certifier la clé**.

10.4.2 Renouvellement de plusieurs certificats

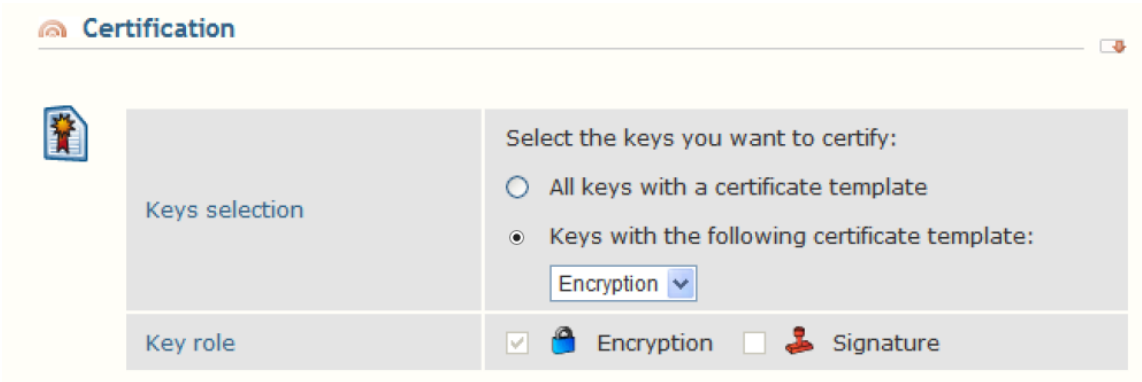
Le renouvellement de plusieurs certificats en une seule opération est exécuté à partir de la page principale **Liste des utilisateurs** (section Page Liste des utilisateurs).

1. Sélectionnez les utilisateurs pour lesquels vous souhaitez certifier ou recertifier l'une ou les deux clés. Cette sélection s'effectue en cochant la case à cocher présente sur la ligne de chaque utilisateur concerné par l'opération.
2. Lancez ensuite le renouvellement en cliquant sur le lien **Certifier les utilisateurs**.

Pour chaque utilisateur sélectionné, l'opération s'applique uniquement à la clé qui a le rôle de chiffrement et / ou à la clé qui a le rôle de signature.

3. Sélectionnez ensuite les clés à certifier.

La sélection s'effectue à l'aide du modèle de certificat associé à la clé. En conséquence, et contrairement au renouvellement de certificat « unitaire » décrit à la section précédente, vous ne pouvez pas certifier à l'aide de cette opération des clés qui ont été créées avec comme mode de certification une autorité de certification externe.



Si la base possède une autorité de certification interne certifiée, la clé est certifiée par cette autorité de certification. Sinon, la clé est auto-certifiée. Cette information est alors précisée.

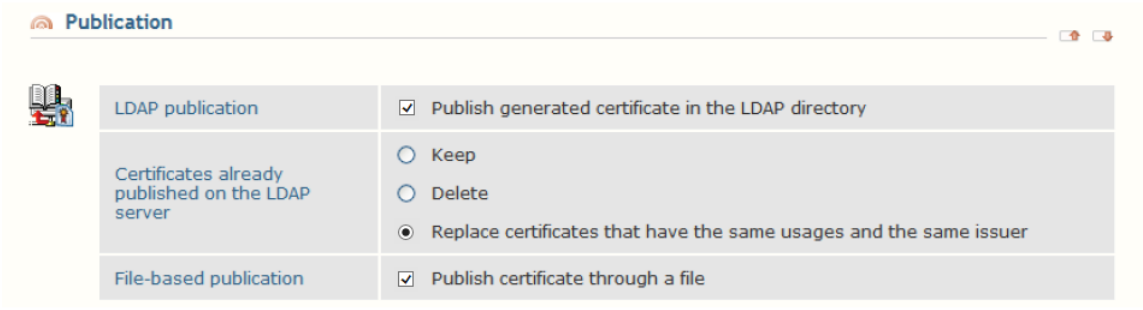
4. Selon vos paramètres généraux, une section propose éventuellement la publication du ou des certificats générés.

Si un serveur LDAP est paramétré (section Configuration LDAP), vous pouvez choisir de publier le certificat dans l'annuaire LDAP. La publication aura toujours lieu vers le DN de l'utilisateur dont on renouvelle le ou les certificats. Paramétrez l'opération à effectuer sur les éventuels certificats déjà présents sur le serveur LDAP à l'entrée désignée par le DN :

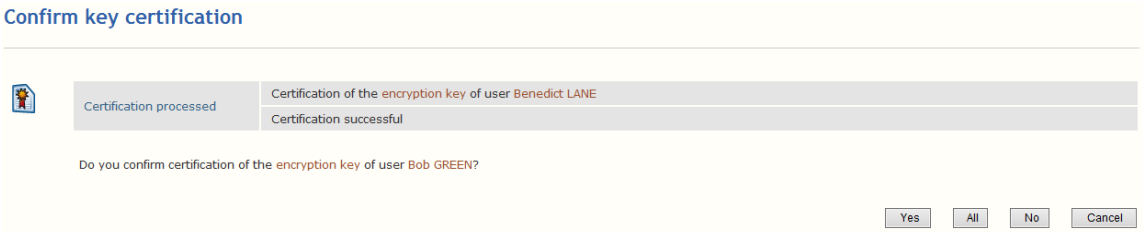
- les conserver ;
- les supprimer ;

- remplacer les certificats ayant les mêmes usages X.509 et émis par cette autorité.

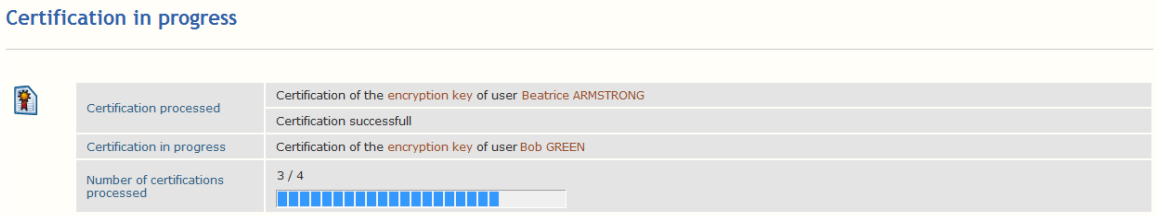
Si la publication par fichier est paramétrée (voir la section Publication d'un certificat).



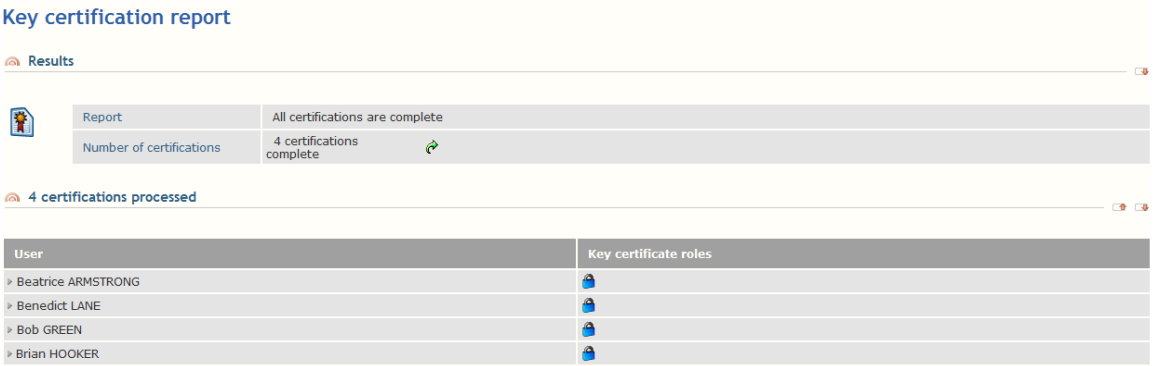
5. Stormshield Data Authority Manager propose alors la certification de chaque clé. Après chaque certification, un compte rendu est affiché et il est demandé de confirmer la certification suivante :



Evitez ces demandes de confirmation en activant la certification automatique par appui sur le bouton Tous :



6. Lorsque toutes les clés ont été certifiées, Stormshield Data Authority Manager affiche une page de compte rendu :



Cette page affiche la liste des clés certifiées, et éventuellement la liste des clés pour lesquelles la certification a échoué. Pour chacune on indique le nom usuel de l'utilisateur propriétaire de la clé, et le rôle de celle-ci. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 clés. Les listes complètes sont téléchargeables en cliquant sur l'icône .

10.5 Importation de certificat

10.5.1 Importation de certificats internes

Si la clé d'un utilisateur a été certifiée par une autorité de certification externe, par exemple pour renouveler son certificat, le nouveau certificat doit être importé.

Stormshield Data Authority Manager gère un historique des anciens certificats. Lors de la diffusion du compte, les anciens certificats de l'utilisateur sont insérés, permettant ainsi le déchiffrement d'anciennes données sans erreur.

Pour le nouveau certificat à importer, soit vous disposez de sa valeur au format "base 64", soit vous disposez d'un fichier (extension *.cer* ou *.crt* pour un certificat seul ; extension *.p7b* ou *.p7c* pour un certificat avec sa parenté).

Attribution des rôles de la clé

Lors de cette opération la clé conserve le ou les rôles qu'elle possède, dans la mesure où son nouveau certificat n'a pas perdu les usages X509 correspondants.

Les règles d'importation (voir la section Règles d'importation) autorisent l'importation d'un certificat possédant plus d'usages X509 que le certificat précédent. Dans ce cas, la clé n'obtient pas le ou les rôles supplémentaires auxquels lui donnent droit les nouveaux usages X509 de son nouveau certificat.

Les rôles de la clé sont modifiables dans la page de ses propriétés (voir la section Page Propriétés de la clé).

Règles d'importation

Lorsque vous importez un certificat, des contrôles de cohérence sont effectués.

Pour qu'un certificat soit considéré comme valide, il doit contenir au minimum :

- un sujet ;
- un émetteur ;
- un numéro de série ;
- les dates de validité ;
- les usages X509 ;
- les mécanismes de signature et de hash.

Quel que soit l'usage du certificat, l'importation est refusée dans les cas suivants :

- la clé publique ne correspond pas à celle de l'utilisateur en cours ;
- le certificat est périmé, c'est-à-dire que la date de fin de validité du certificat est dépassée ;
- le certificat est plus ancien, c'est-à-dire que la date de début de validité du certificat est antérieure à celle du certificat présent dans la base. Vous pouvez supprimer cette règle dans les paramètres généraux (voir la section Importation, exportation et demande de certificats) ;
- le certificat est identique à celui présent dans la base de données ;
- le format de certificat est incorrect ;
- le certificat n'a pas au moins un usage commun avec l'ancien certificat :
- il manque un attribut X509 de chiffrement (KeyEncipherment et / ou DataEncipherment) pour le certificat associé à la clé de chiffrement (ou personnelle si le compte a une seule clé),

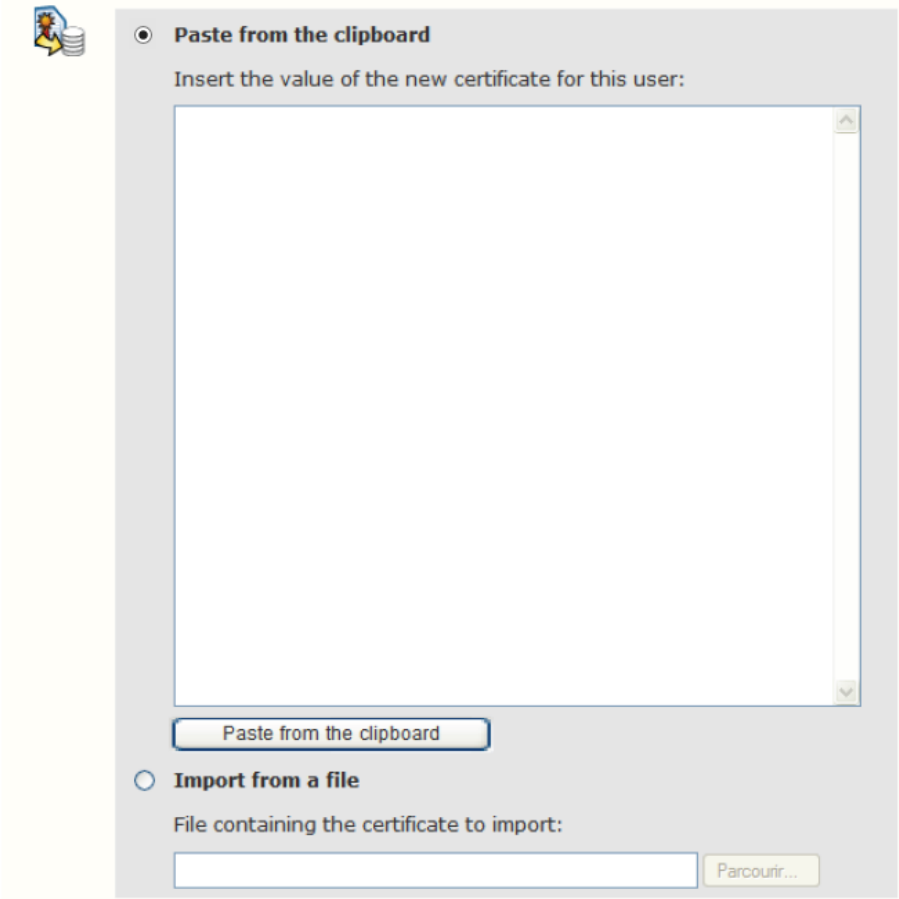
- il manque un attribut X509 de signature (DigitalSignature et / ou NonRepudiation) pour le certificat associé à la clé de signature (ou personnelle si le compte a une seule clé).

Dans le cas de l'importation d'un certificat pour le compte signataire de politiques de sécurité, le certificat doit avoir au moins l'usage X509 NonRepudiation ou l'usage X509 DigitalSignature.

Dans le cas de l'importation du certificat de l'autorité, l'importation est refusée si le certificat n'a pas l'attribut X.509 KeyCertSign. L'importation d'un certificat qui ne possède pas de BasicConstraints est possible s'il a l'attribut X.509 KeyCertSign.

Importation de certificat

A partir de la page **Clé et certificat**, vous pouvez importer un nouveau certificat pour la clé en cliquant sur le lien **Importer un nouveau certificat** dans l'onglet *Gestion du certificat*.



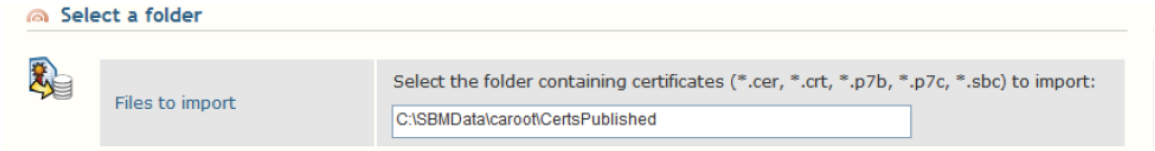
Vous pouvez coller la valeur du certificat (format "base 64"), ou sélectionner un fichier.

Si le nouveau certificat vérifie les règles de cohérence (voir la section Règles d'importation), son contenu est affiché et une dernière validation permet de l'importer dans la base de données.

Importation de plusieurs certificats

L'importation multiple permet de traiter tous les utilisateurs de la base de données en une opération.

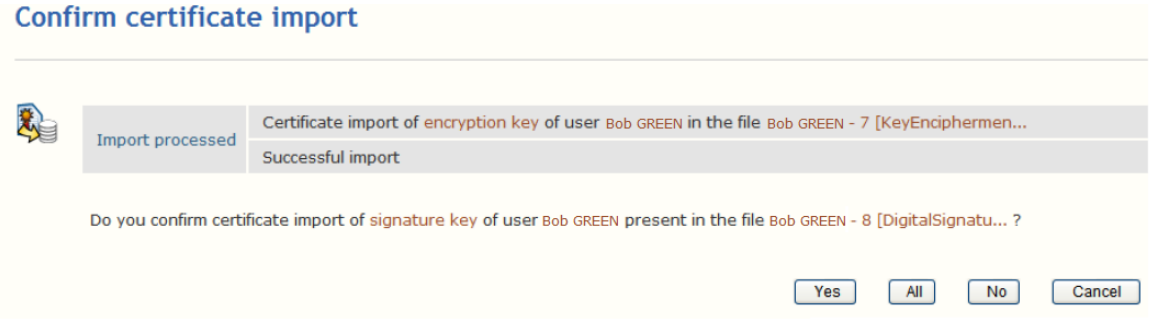
Vous sélectionnez un dossier. Stormshield Data Authority Manager propose par défaut le dossier <certs_dir> défini dans les paramètres généraux (voir la section Importation, exportation et demande de certificats). Tous les fichiers de ce dossier susceptibles de contenir des certificats (extensions *.cer*, *.crt*, *.p7b* et *.p7c*) sont analysés.



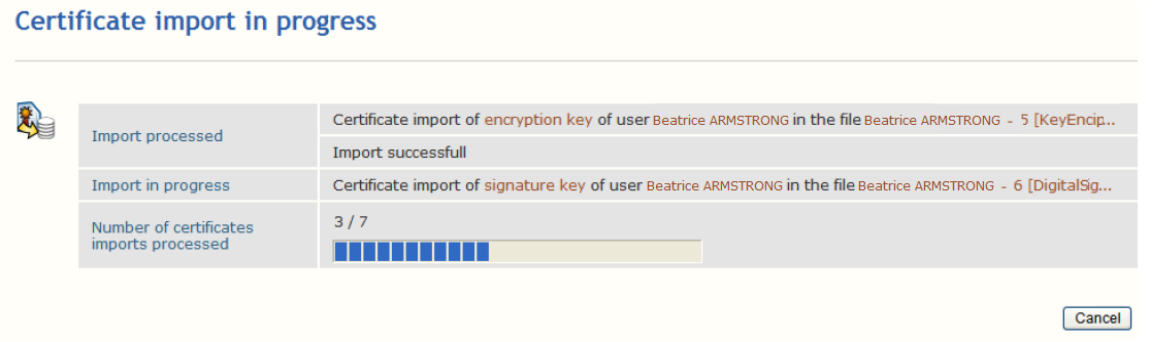
Pour chaque certificat, il y a un test d'association avec un utilisateur de la base de données.

Le certificat doit vérifier les règles de cohérence (voir la section Règles d'importation) et la règle suivante : s'il existe plusieurs certificats valides pour un même utilisateur, le certificat le plus récent est choisi. Un certificat est dit plus récent qu'un autre si sa date de début de validité est antérieure. La date peut aussi être antérieure à la date de début de validité du certificat de la base de données si l'importation d'anciens certificats est autorisée (voir la section Importation, exportation et demande de certificats).

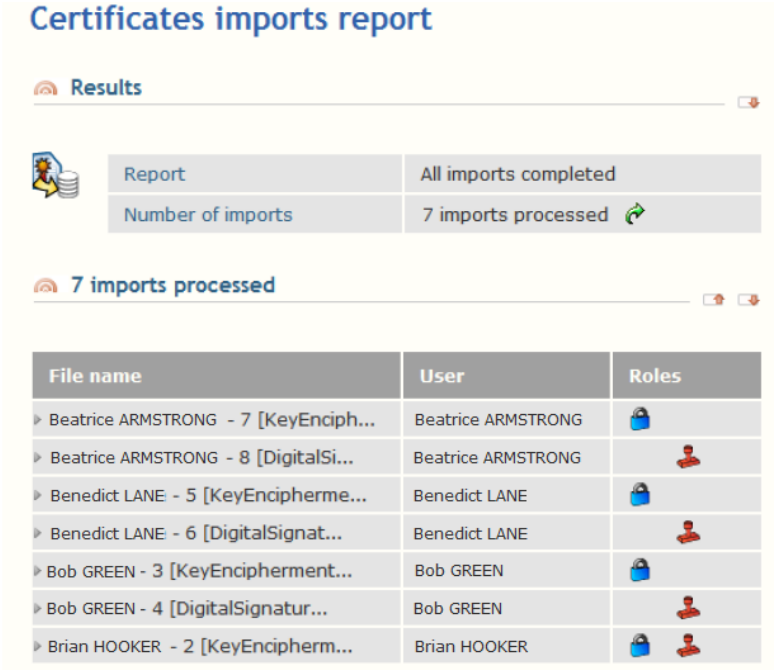
Stormshield Data Authority Manager propose l'importation de chaque certificat respectant ces règles. A chaque importation, il affiche une page de compte rendu et demande confirmation pour l'importation du certificat suivant :



Évitez ces demandes de confirmation en activant l'importation automatique par appui sur le bouton **Tous** :



Lorsque tous les fichiers ont été traités, Stormshield Data Authority Manager affiche une page de compte rendu :



Cette page affiche la liste des clés pour lesquelles un certificat a été importé, et éventuellement la liste des clés pour lesquelles l'importation a échoué. Pour chacune on indique le nom du fichier contenant le certificat importé, le nom usuel de l'utilisateur propriétaire de la clé et le rôle de celle-ci. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 clés. Les listes complètes sont téléchargeables en cliquant sur l'icône .

Importation de certificats à partir d'un annuaire LDAP

Pour un utilisateur associé à une entrée LDAP (section Association d'un utilisateur à une entrée LDAP), il est possible d'importer un certificat à partir de l'annuaire LDAP.

> **NOTE**
> Le certificat doit être au format binaire.

Définissez dans les paramètres LDAP (voir la section Publication des nouveaux certificats3) le nom de l'attribut à lire.

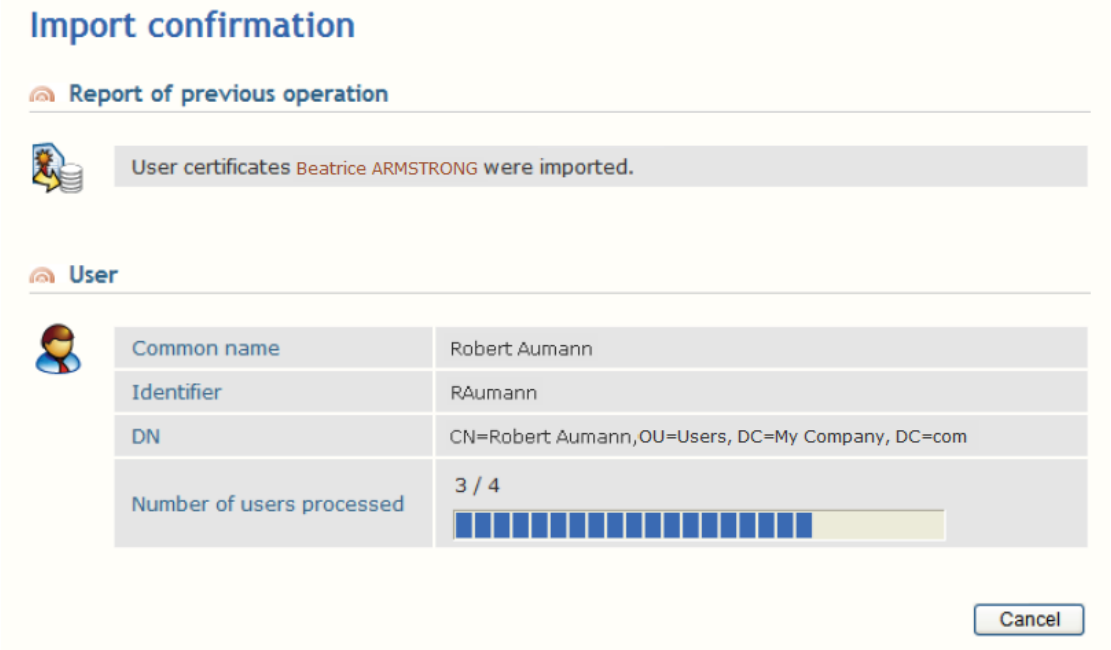
Lancez cette importation à partir de la page principale de la synchronisation avec un annuaire LDAP (section Synchronisation avec un annuaire LDAP) :

- Soit en cliquant sur le lien **Pour tous les utilisateurs** : pour chaque utilisateur associé à une entrée LDAP, Stormshield Data Authority Manager recherche l'attribut correspondant au certificat (voir la section Nom des attributs). Si elle le trouve, elle lit la valeur du certificat puis met en œuvre la mécanique d'importation décrite dans la section Règles d'importation. Si l'utilisateur possède plusieurs clés, Stormshield Data Authority Manager essaie d'importer le certificat pour chacune des clés.
- Soit en cliquant sur le lien **Pour les utilisateurs auto-certifiés** : pour chaque utilisateur associé à une entrée dont au moins un des certificats n'est pas émis par une autorité de certification, Stormshield Data Authority Manager recherche l'attribut correspondant au certificat (voir la section Nom des attributs. Si elle le trouve, elle lit la valeur du certificat puis met en œuvre la mécanique d'importation décrite dans la section Règles d'importation .

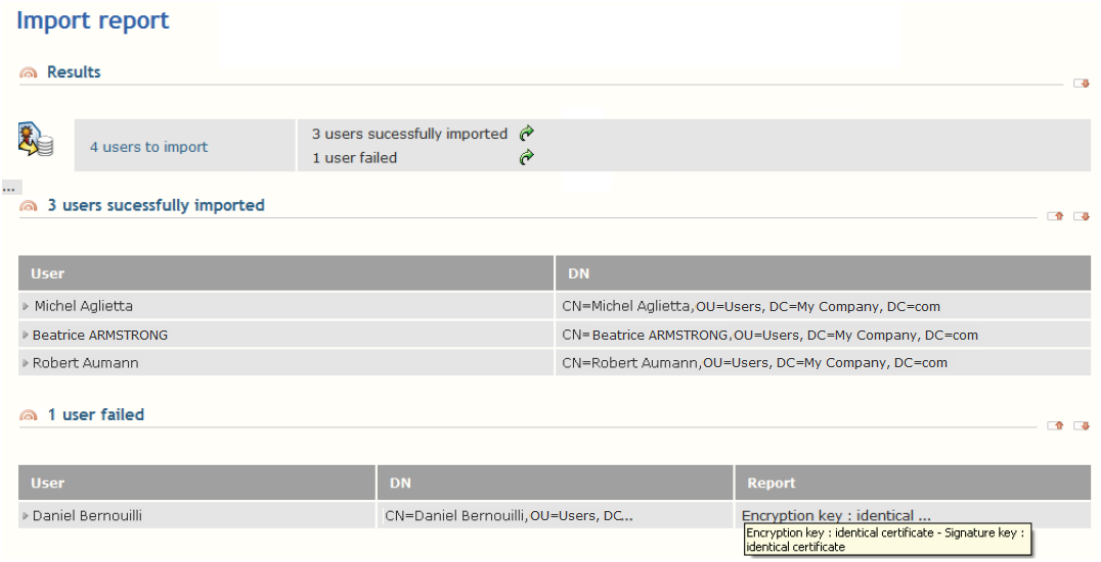
Dans les deux cas, la présentation et l'enchaînement des pages sont identiques.

Après chaque importation, Stormshield Data Authority Manager affiche un compte rendu et demande une confirmation pour l'importation suivante.

Évitez ces demandes de confirmation en activant l'importation automatique par appui sur le bouton **Tous** :



Lorsque tous les utilisateurs ont été traités, Stormshield Data Authority Manager affiche une page de compte rendu :



Cette page affiche la liste des utilisateurs pour lesquels au moins un certificat a été importé, et éventuellement la liste des utilisateurs pour lesquels l'importation a échoué. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 utilisateurs. Les listes complètes sont téléchargeables en cliquant sur l'icône .

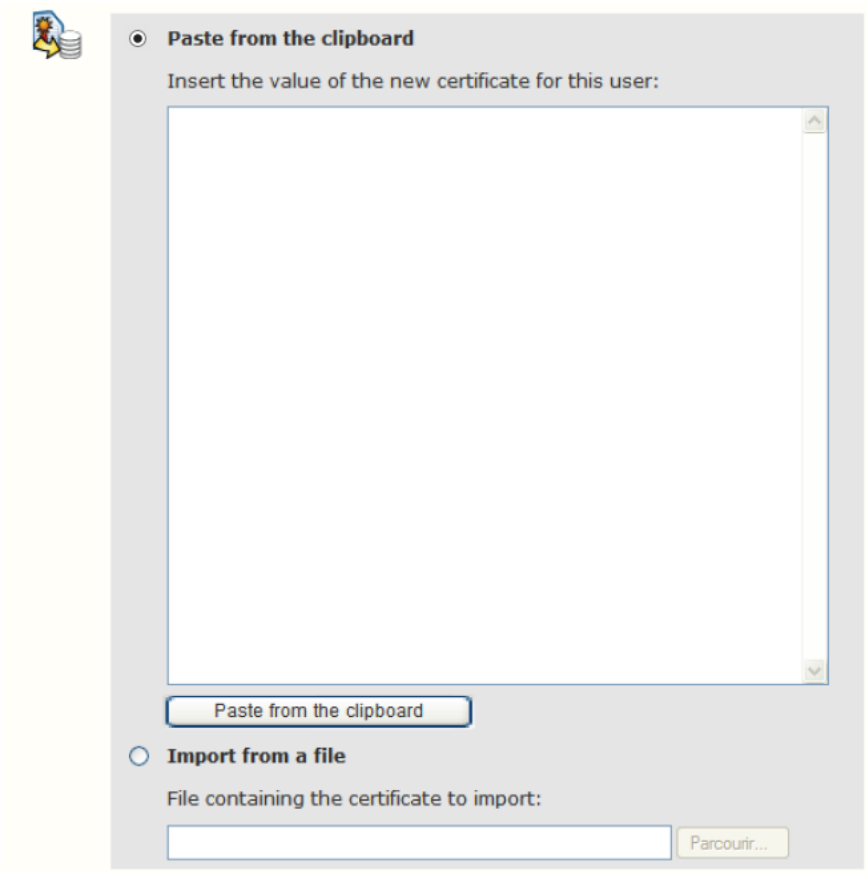
10.5.2 Importation de certificats externes

Un lien **Importer un nouveau certificat** est présent dans les pages des certificats externes (section Certificats externes de recouvrement et section Autres certificats externes). En cliquant sur ce lien vous affichez une page qui permet d'importer dans la base un nouveau certificat :

- soit par copier-coller de sa valeur codée en base 64 ;
- soit par sélection d'un fichier contenant un seul certificat (fichiers *.cer* ou *.crt*).

La validation de l'importation affiche une page qui détaille le contenu du certificat et permet de saisir les propriétés à associer au certificat lors de son importation dans la base :

- un libellé permettant d'identifier le certificat ;
- les paramètres de recouvrement dans le cas d'un certificat de recouvrement.



10.6 Exportation de certificat

10.6.1 Exportation de certificats internes

Stormshield Data Authority Manager permet d'exporter le certificat de la clé de l'autorité de certification (section Page Liste des utilisateurs).

Extensions des fichiers d'exportation :

- *.cer* : un seul certificat au format binaire ;
- *.crt* : un seul certificat au format base 64 ;
- *.p7b* ou *.p7c* (Stormshield Data Security Certificates) : plusieurs certificats au format binaire.

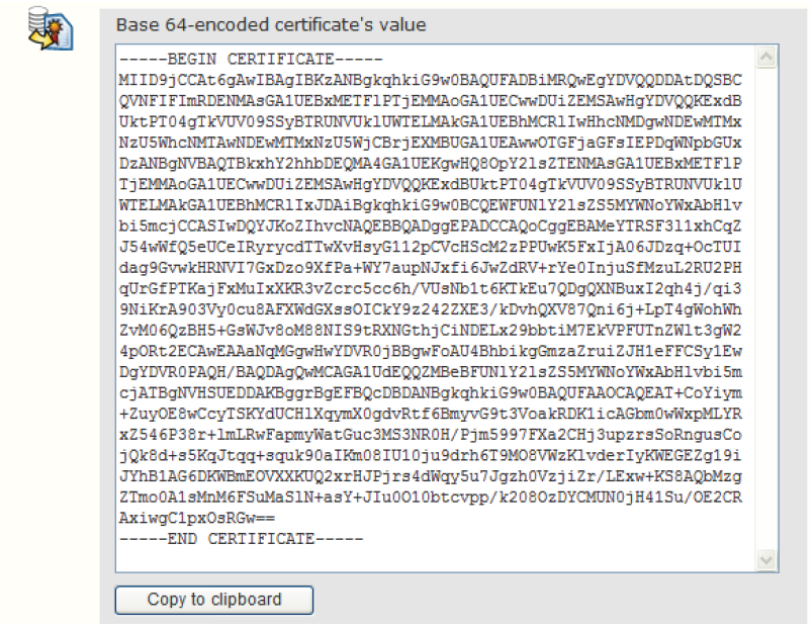
Exportation de certificat

L'exportation unitaire s'effectue dans la section **Exportation du certificat** des pages :

- **Clé et certificat** de l'autorité (section Page Clé et certificat de l'autorité) pour le certificat de la clé de l'autorité de certification
- **Clé et certificat** pour le certificat de la clé d'un utilisateur.

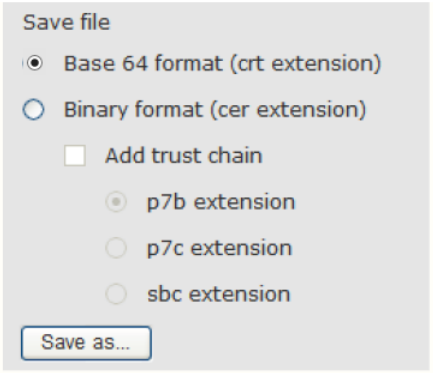
Affichez ou masquez la contenu des sections en cliquant sur les liens **Valeur du certificat en base 64** ou **Enregistrement dans un fichier**.

Le lien **Valeur du certificat en base 64** permet de visualiser et de copier la valeur "base 64" du certificat.



Le lien **Enregistrement dans un fichier** permet de sauvegarder la valeur du certificat dans un fichier. Précisez le format, l'ajout de la parenté et l'extension. La configuration définie dans les paramètres généraux (section Paramètres de gestion des certificats) est utilisée par défaut.

La case à cocher **Ajouter la parenté** est désactivée si aucune parenté n'est trouvée dans la base de données pour la clé.



Le nom du fichier est l'identifiant de l'utilisateur concaténé avec le rôle de la clé ([Chiffrement], [Signature] ou [Chiffrement, Signature]).

Exportation de plusieurs certificats

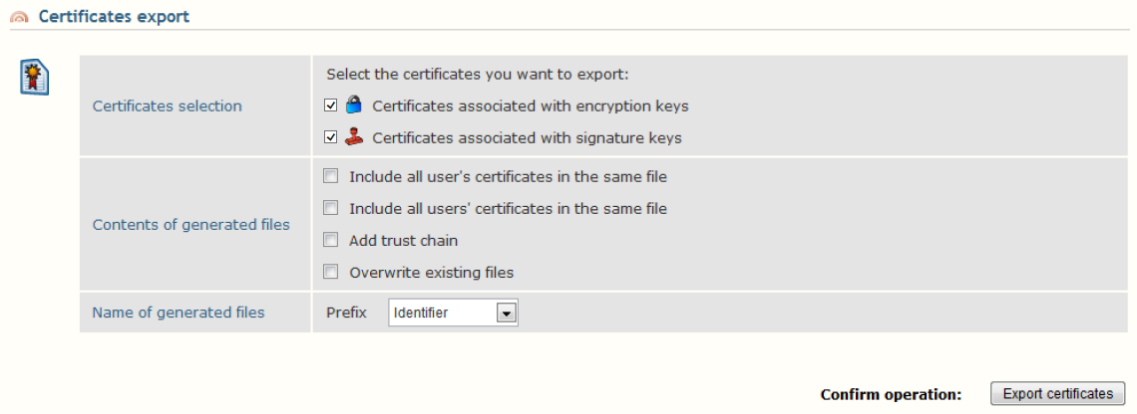
L'exportation de plusieurs certificats en une seule opération s'exécute à partir de la page **Liste des utilisateurs** (voir la section Opérations disponibles) :

1. Sélectionnez les utilisateurs dont vous voulez exporter les certificats. Cette sélection s'effectue en cochant la case à cocher présente sur la ligne de chaque utilisateur.
2. Lancez l'exportation des certificats en cliquant sur le lien **Exporter les certificats** dans l'onglet *Gestion des certificats*.
3. Dans la page suivante, sélectionnez les clés dont vous souhaitez exporter le certificat.
4. Définissez le contenu des fichiers à générer. Plusieurs combinaisons sont possibles :

- un fichier pour chaque certificat, avec ou sans sa parenté ;
- un fichier pour chaque utilisateur, avec ou sans la parenté des certificats ;

- un fichier contenant tous les certificats de tous les utilisateurs avec ou sans la parenté des certificats.

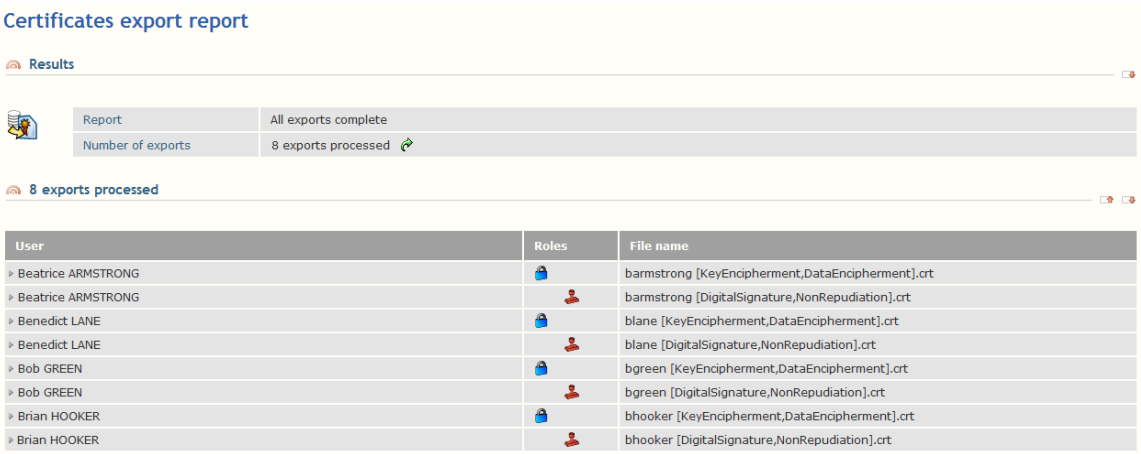
5. Sélectionnez l'écrasement ou non des fichiers existants.
6. Définissez le préfixe des fichiers générés : identifiant, nom usuel ou adresse e-mail de l'utilisateur. Le préfixe est utilisé uniquement dans le cas où un fichier est créé pour chaque certificat avec ou sans sa parenté, et si les usages des clés correspondent exactement aux usages [KeyEncipherment,DataEncipherment], [DigitalSignature,NonRepudiation] ou [DigitalSignature].



Afin de garantir l'unicité du fichier :

- Dans le cas où un fichier est créé pour chaque certificat (premier cas de figure de l'étape 4 ci-dessus), le nom du fichier généré est le préfixe sélectionné concaténé avec les usages de la clé définis à l'étape 6 ci-dessus ou concaténé avec le rôle de la clé ([Chiffrement], [Signature] ou [Chiffrement, Signature]) si les usages sont différents.
- Dans l'un des deux autres cas de l'étape 4, le nom du fichier généré est l'identifiant de l'utilisateur concaténé avec le rôle de la clé et le numéro de série du certificat.

Lorsque tous les fichiers sont générés, Stormshield Data Authority Manager affiche une page de compte rendu.



Cette page affiche la liste des clés pour lesquelles un certificat a été importé, et éventuellement la liste des clés pour lesquelles l'importation a échoué. Pour chacune on indique le nom usuel de l'utilisateur propriétaire de la clé, et le rôle de celle-ci, et le nom du fichier créé. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 clés. Les listes complètes sont téléchargeables en cliquant sur l'icône .

10.7 Publication de certificat sur un annuaire LDAP

Pour un utilisateur associé à une entrée LDAP (section Association d'un utilisateur à une entrée LDAP), il est possible de publier ses certificats sur l'annuaire.

1. Définissez dans les paramètres LDAP (section Configuration LDAP) le nom de l'attribut à écrire.

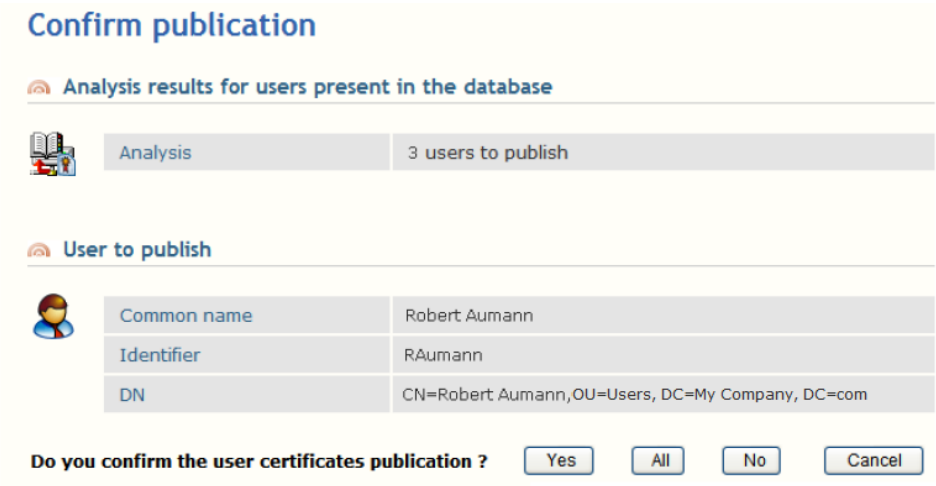
La date de la dernière publication des certificats est affichée dans la page **Utilisateurs** (section Page Utilisateur).

2. Lancez cette publication à partir de la page principale de la synchronisation avec un annuaire LDAP (section Synchronisation avec un annuaire LDAP) :

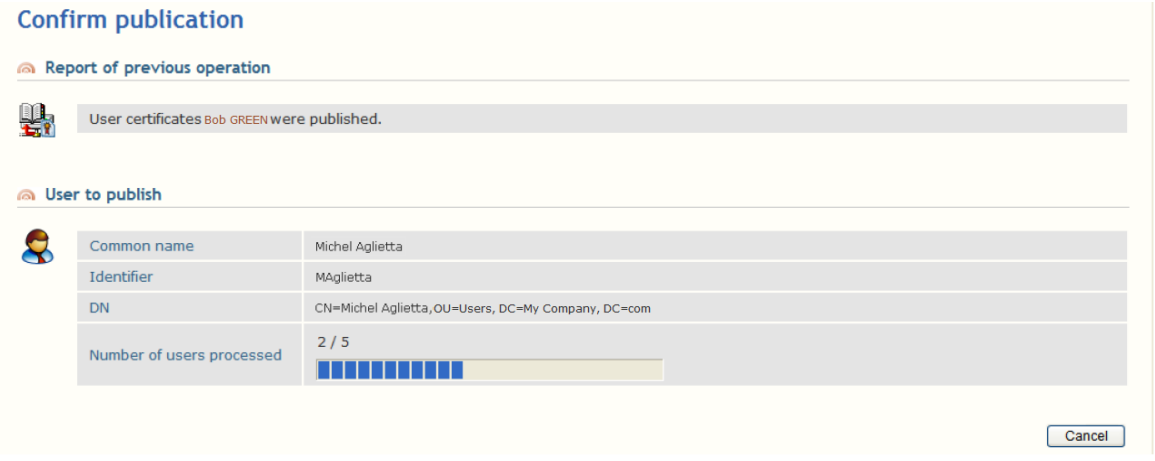
- soit en cliquant sur le lien **Tous les certificats** : pour chaque certificat d'un utilisateur associé à une entrée, Stormshield Data Authority Manager écrit dans l'entrée un attribut contenant la valeur du certificat ;
- soit en cliquant sur le lien **Les certificats qui ne sont pas déjà publiés** : pour chaque certificat d'un utilisateur associé à une entrée, dont les certificats n'ont pas déjà été publiés, Stormshield Data Authority Manager écrit dans l'entrée un attribut contenant la valeur du certificat.

Dans les deux cas, la présentation et l'enchaînement des pages sont identiques.

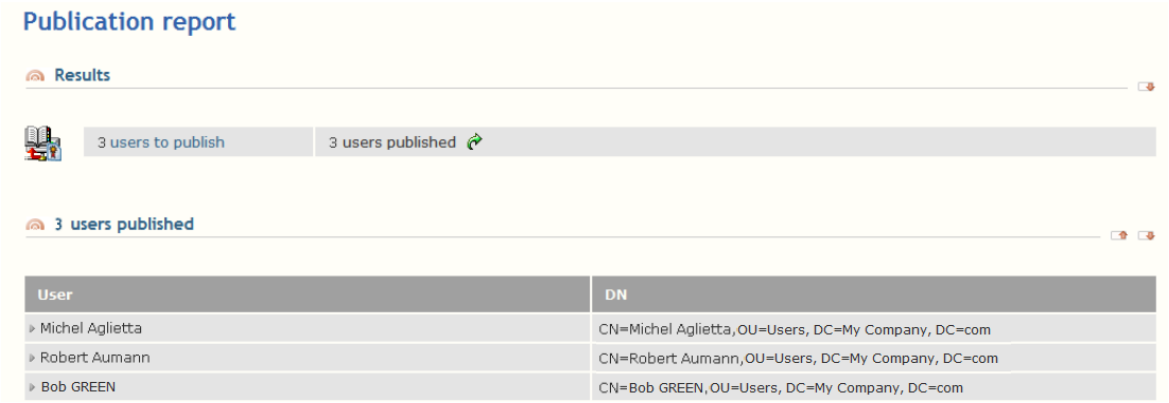
3. Après chaque publication, Stormshield Data Authority Manager affiche un compte rendu et demande une confirmation pour la publication suivante.



4. Évitez ces demandes de confirmation en activant la publication automatique par appui sur le bouton **Tous** :



Lorsque tous les utilisateurs ont été traités, Stormshield Data Authority Manager affiche une page de compte rendu.



Cette page affiche la liste des utilisateurs pour lesquels au moins un certificat a été publié, et éventuellement la liste des utilisateurs pour lesquels la publication a échoué. Afin de limiter le temps d'affichage de la page, ces deux listes sont limitées à 100 utilisateurs. Les listes complètes sont téléchargeables en cliquant sur l'icône .

11. Configuration des composants

Cette section décrit comment configurer les composants de Stormshield Data Security en utilisant Stormshield Data Authority Manager.

11.1 Présentation

Stormshield Data Authority Manager permet de fournir aux utilisateurs une configuration pour chaque composant de Stormshield Data Security. Il permet :

- de configurer chaque composant comme il est possible de le faire à partir du panneau de configuration de Stormshield Data Security (cases à cocher, listes déroulantes, listes…) ;
- de configurer en plus des paramètres qui restreignent le fonctionnement des composants ;
- d'imposer cette configuration à l'utilisateur en limitant ses choix ou en interdisant son accès aux contrôles, aux boutons, etc.

Les configurations par défaut proposées par Stormshield Data Authority Manager sont les mêmes que celles proposées par défaut par les composants de Stormshield Data Security. Elles ne contiennent aucune restriction pour l'utilisateur.

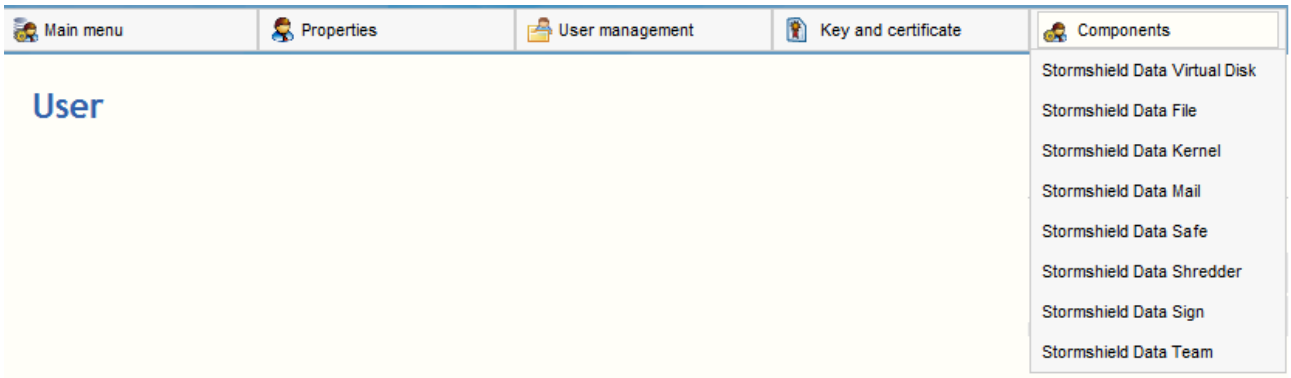
Les modifications apportées aux configurations ne sont prises en compte que lors de la diffusion du compte de l'utilisateur.

Vous pouvez modifier les configurations des composants après une diffusion à l'aide d'un fichier de mise à jour (section Fichier de mise à jour de la politique de sécurité (.usx)).

11.2 Accès aux configurations d'un utilisateur

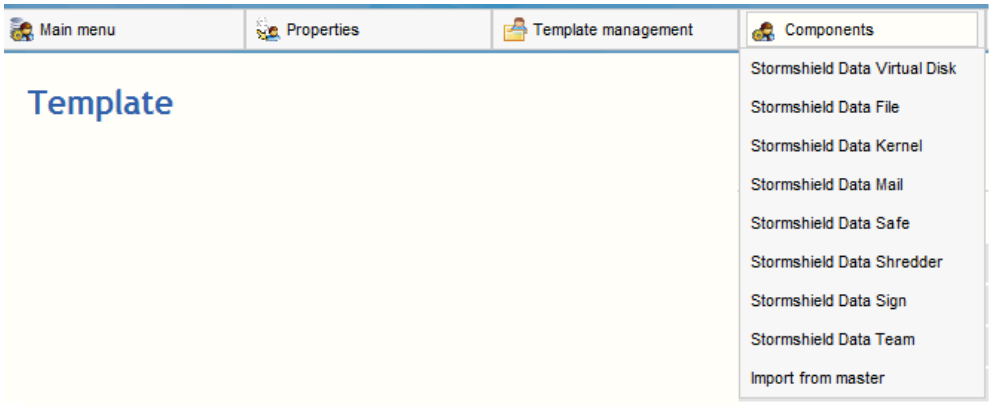
Vous accédez à la configuration des composants pour un utilisateur à partir de la page **Utilisateur** (section Page Utilisateur).

- L'utilisateur peut avoir ses propres configurations :



Chaque lien affiche la page principale de la configuration d'un composant (section Configuration d'un composant).

- Ou bien hériter des configurations d'un modèle (section Modèle) :

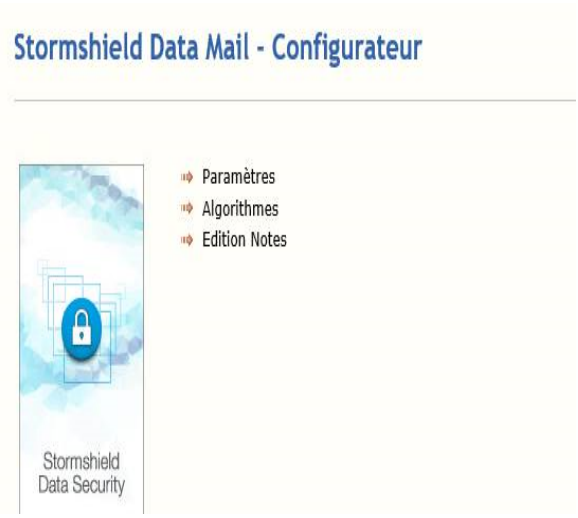


L'identifiant du modèle, dont hérite l'utilisateur, est affiché sous forme d'un lien dans la ligne **Modèle** de la section Utilisateur. En cliquant sur ce lien, vous accédez à la page du modèle, et ainsi à sa configuration des composants.

Pour changer de modèle, reportez-vous à la section Choix du modèle .

11.3 Configuration d'un composant

Stormshield Data Authority Manager propose pour chaque composant une page principale présentant un menu.

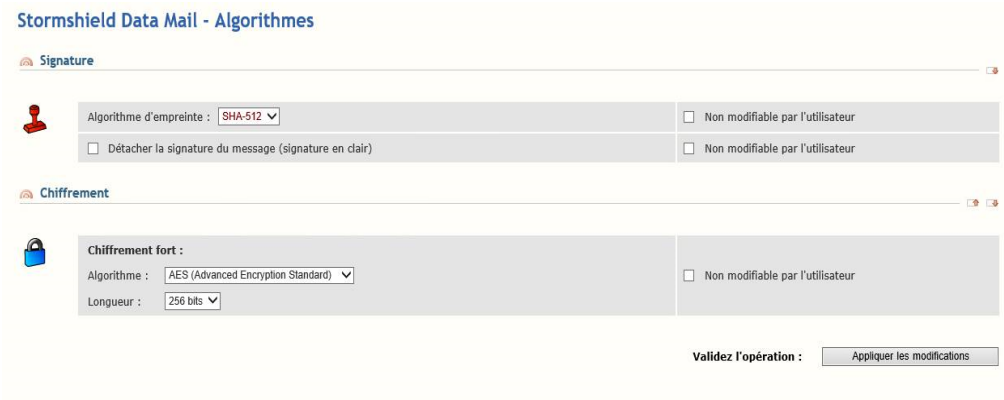


Pour les composants Stormshield Data Virtual Disk, Stormshield Data File, Stormshield Data Mail, Stormshield Data Shredder et Stormshield Data Sign, le lien **Paramètres** permet de configurer des paramètres généraux qui restreignent le fonctionnement du composant. Ces paramètres ne sont pas accessibles à partir du panneau de configuration de Stormshield Data Security.

Les autres liens des menus correspondent à un onglet de la fenêtre de configuration du composant, qui est accessible à partir du panneau de configuration de Stormshield Data Security.

Ainsi chaque page correspondant à un onglet contient :

- une colonne gauche proposant les mêmes paramètres à configurer que ceux proposés dans la fenêtre de configuration Stormshield Data Security. Pour obtenir des explications sur ces paramètres vous devez vous référer au manuel associé au composant ;
- une colonne droite contenant des restrictions pour l'utilisateur (section Restriction d'accès à l'utilisateur). Le texte de cette colonne est écrit en noir.



11.4 Restriction d'accès à l'utilisateur

Les pages de configuration des paramètres des composants contiennent une colonne droite proposant de restreindre l'accès de l'utilisateur aux onglets, aux boutons, aux menus déroulant, et aux contrôles (cases à cocher, etc.).

11.4.1 Descriptif des principales restrictions

Chaque restriction s'applique au(x) contrôle(s) situé(s) en vis-à-vis dans la colonne de gauche :

☐ Cannot be modified by the user	Le contrôle sera visible dans la fenêtre de configuration, mais il sera en grisé, c'est-à-dire non accessible donc non modifiable.
☐ Not visible	Le bouton ou le choix du menu sera en grisé donc non accessible par l'utilisateur.
☐ Element not visible	L'élément sélectionné dans la liste n'apparaîtra pas dans la liste proposée à l'utilisateur.
☐ The user is not allowed to add items	Le composant ne proposera pas à l'utilisateur d'ajouter un élément à la liste.
☐ The user is not allowed to modify the selected item	L'utilisateur ne pourra pas modifier les propriétés de cet élément de la liste.
☐ Not visible	L'onglet n'apparaîtra pas dans la fenêtre de configuration.

11.4.2 Limitation de la liste des algorithmes proposés

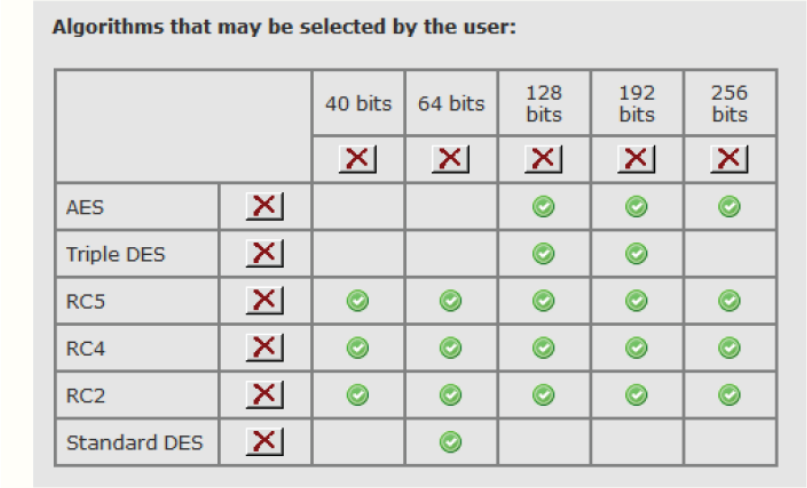
Pour les composants Stormshield Data Virtual Disk, Stormshield Data File, et Stormshield Data Mail, vous pouvez masquer des algorithmes afin qu'ils ne soient pas proposés à l'utilisateur.

Chaque algorithme est défini par un nom et une force. Il est matérialisé par une boule associant une ligne et une colonne :

- La coche verte indique que l'algorithme sera accessible.
- La croix rouge indique que l'algorithme ne sera pas accessible.

En cliquant sur le symbole, on change l'état de l'algorithme. Il est possible d'agir sur toute une ligne ou sur toute une colonne avec le bouton .

L'algorithme proposé par défaut à l'utilisateur doit être accessible, donc associé à une boule verte.



11.5 Configuration avancée

11.5.1 Paramètres de Stormshield Data Kernel

Configuration du composant Téléchargement des politiques de sécurité

Les points de distribution saisis dans la configuration de ce composant peuvent contenir les tags suivants :

- un point de distribution LDAP doit être une URI LDAP valide, dans laquelle vous pouvez inclure les tags `<LdapHost>`, `<LdapPort>`, `<LdapDn>`, `<UserId>` ;
- un point de distribution HTTP doit être une URI valide, dans laquelle vous pouvez inclure le tag `<UserId>`.

Exemples d'URI :

```
ldap://<LdapHost>:<LdapPort>/<LdapDn>?SboxPolicyUpgrade;binary
```

```
http://server/SecurityPolicies/<UserId>.usx
```

Lors de la diffusion, les tags sont remplacés par :

- le paramètre LDAP correspondant (voir la section Configuration LDAP) ;
- le DN LDAP de l'utilisateur ou du modèle diffusé ;
- l'identifiant de l'utilisateur ou du modèle diffusé.

Ces remplacements sont effectués selon les règles suivantes :

1. Pour un modèle :

- lors de la diffusion d'un fichier master .usr (c'est-à-dire avec une configuration de connexion mode mot de passe ou avec une configuration de connexion mode carte, section Diffusion d'un master), et lors de la diffusion d'un fichier de mise à jour *.usx* "générique" (voir la section Diffusion d'un fichier de mise à jour de la politique de sécurité (.usx)), les tags sont remplacés par les données du modèle diffusé ;

- lors de la diffusion d'un fichier master .msr (c'est-à-dire avec toutes les configurations, section Diffusion d'un master), les tags ne sont pas remplacés, afin que les points de distributions soient conservés lors de leur importation dans le nouveau modèle (voir la section Importation de configuration des composants à partir d'un master (fichier .msr)).

2. Pour un utilisateur, que ses configurations des composants dérivent d'un modèle ou non, les tags sont toujours remplacés par les données de l'utilisateur diffusé (voir la section Diffusion des comptes utilisateurs).

Des masques de résolution de point de distribution peuvent être saisis dans les paramètres généraux afin d'être proposés automatiquement dans la page de configuration du composant (voir la section Paramètres de la configuration des composants).

Configuration du compte utilisateur

Quatre configurations "Code secret et connexion" sont proposées :

- deux pour le mode "mot de passe" : une pour la version 5 et inférieure, plus une pour la version 6 et supérieure de Stormshield Data Security ;
- deux pour le mode "carte" : une pour la version 5 et inférieure, plus une pour la version 6 et supérieure de Stormshield Data Security.

Un utilisateur standard ne peut pas avoir deux modes de connexion ou un nombre de clés variable. Il est donc inutile de renseigner les pages ne correspondant pas à son profil. Pour le mode de connexion utilisé, renseignez la page correspondant à la version de Stormshield Data Security installée sur le poste de l'utilisateur.

Un modèle est susceptible d'être appliqué à des utilisateurs nécessitant ces différents profils. Vous pouvez donc avoir besoin de renseigner toutes ces configurations pour un même modèle.

La diffusion de ces configurations est décrite section Diffusion des comptes utilisateurs .

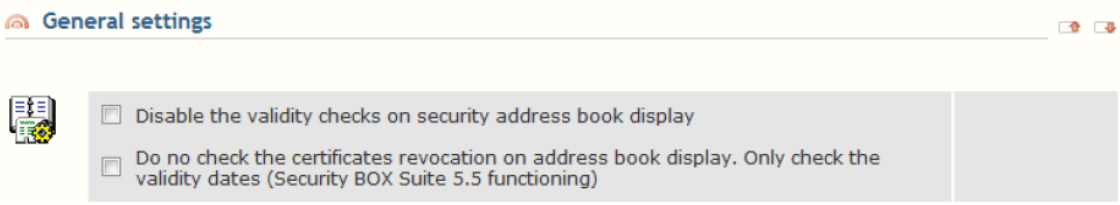
Composition du code secret

La syntaxe que vous définissez dans la section **Composition du code secret** de la page **Connexion et code secret** intervient lors d'un changement de mot de passe.

Configuration de l'annuaire

Dans la page **Annuaire**, dans la section **Paramètres généraux**, vous pouvez effectuer les paramétrages suivants :

- Ne pas effectuer les contrôles de validité à l'ouverture de l'annuaire de sécurité. Par défaut, les contrôles sont activés.
- Ne pas contrôler la révocation des certificats lors de l'affichage de l'annuaire, afin d'accélérer cet affichage. C'est-à-dire que seules les dates de validité sont contrôlées (fonctionnement Security BOX Suite 5.5). Par défaut les dates et la révocation sont contrôlées.



Configuration de la mise à jour automatique de l'annuaire

Dans la page **Annuaire**, dans la section **Mise à jour automatique de l'annuaire**, vous pouvez effectuer les paramétrages suivants :

Concernant l'activation et l'exécution :

- Activer la mise à jour automatique de l'annuaire, qui est désactivée par défaut, en indiquant la fréquence d'exécution des traitements (en heures).
- Lancer le traitement de mise à jour de l'annuaire lors de la connexion de l'utilisateur Stormshield Data Security. Par défaut, il n'est pas lancé lors de la connexion.
- Autoriser l'exécution manuelle des opérations de mise à jour (interdite par défaut). Ce paramètre est pris en compte uniquement si la fonctionnalité **Mise à jour de l'annuaire** est activée.

Concernant la mise à jour automatique des certificats :

- Activer la mise à jour automatique des certificats présents dans l'annuaire local avec des certificats plus récents trouvés sur un annuaire LDAP (désactivé par défaut).

Ce paramètre est pris en compte uniquement si les fonctionnalités **Mise à jour de l'annuaire** et **Remplacement automatique** sont activées. La mise à jour ne fonctionne que si le certificat est valide.

- Préciser si cette mise à jour est effectuée sur les certificats valides, périmés et/ou révoqués.
- Préciser si vous voulez effectuer un import de certificats absents. Cette configuration est utilisée uniquement lors de l'envoi d'un e-mail via Outlook.
- Vous pouvez filtrer les autorités d'émission des certificats sur lesquels s'applique le remplacement automatique, en remplaçant le mot-clé **All** (par défaut) par la liste des CommonName des autorités ayant émis les certificats concernés par le traitement (séparés par un point-virgule).

Lors d'une recherche manuelle de collaborateur durant l'envoi d'un e-mail via Outlook, l'annuaire ne sera mis à jour que si l'autorité est connue, sans tenir compte du filtre défini dans le Stormshield Data Authority Manager.

NOTE
Le processus de mise à jour automatique de l'annuaire local ne se base que sur l'adresse e-mail contenue dans le certificat des utilisateurs pour faire la correspondance avec l'annuaire LDAP.

Concernant la suppression automatique des certificats périmés :

- Activer la suppression automatique des certificats périmés (désactivée par défaut). Ce paramètre est pris en compte uniquement si la fonctionnalité **Mise à jour de l'annuaire** est activée.
- Vous pouvez filtrer les autorités d'émission des certificats sur lesquels s'applique la suppression automatique à la date de péremption, en remplaçant le mot-clé **All** (par défaut) par la liste des CommonName des autorités ayant émis les certificats concernés par le traitement (séparés par un point-virgule).

Ce paramètre est pris en compte uniquement si les fonctionnalités **Mise à jour de l'annuaire** et **Suppression automatique** sont activées.

Concernant la suppression automatique des certificats révoqués :

- Activer la suppression automatique des certificats révoqués (désactivée par défaut). Ce paramètre est pris en compte uniquement si la fonctionnalité **Mise à jour de l'annuaire** est activée.

- Vous pouvez filtrer les autorités d'émission des certificats sur lesquels s'applique la suppression automatique sur révocation, en remplaçant le mot-clé **All** (par défaut) par la liste des CommonName des autorités ayant émis les certificats concernés par le traitement (séparés par un point-virgule).

Ce paramètre est pris en compte uniquement si les fonctionnalités **Mise à jour de l'annuaire** et **Suppression automatique** sur révocation sont activées.

11.5.2 Paramètres de Stormshield Data Team

Paramètres Restriction

Sur la page **Règles de sécurité**, dans la partie **Liste des dossiers à sécuriser**, le paramètre **Restriction** permet de définir la manière dont la règle est affichée dans la liste des règles de l'onglet Règles de sécurité du composant Stormshield Data Team, dans les propriétés de l'utilisateur.

Paramètre Mettre à jour la clé d'un collaborateur dans les règles Team connues après un renouvellement de clé (nécessite l'activation de la synchronisation LDAP)

Sur la page **Paramètres**, dans la partie **Paramètres généraux**, l'option **Mettre à jour la clé d'un collaborateur dans les règles Team connues après un renouvellement de clé (nécessite l'activation de la synchronisation LDAP)** permet de mettre à jour automatiquement les clés dans les règles Team. La synchronisation de l'annuaire de confiance avec un annuaire LDAP doit être activée (voir la section Synchronisation avec un annuaire LDAP).

Si cette option est activée, la mise à jour des règles Team se déclenche automatiquement à l'issue de la synchronisation de l'annuaire de confiance. Une nouvelle icône apparaît dans la zone de notification, signalant le début du traitement. Double-cliquez sur l'icône pour afficher la fenêtre d'avancement de la mise à jour.

Le traitement se déroule en deux étapes :

1. Les règles dont l'utilisateur est propriétaire sont mises à jour avec les nouveaux certificats récupérés dans l'annuaire. L'icône dans la zone de notification signale la fin de cette étape. La fenêtre d'avancement liste alors l'ensemble des règles concernées par cette mise à jour.
2. La nouvelle politique de sécurité est appliquée pour toutes les règles mises à jour. Cette étape doit être opérée manuellement par l'utilisateur.

Ouvrez la fenêtre d'avancement en double-cliquant sur l'icône de la zone de notification puis cliquez sur **Appliquer**. Cette action déclenche la mise à jour de la sécurité de chaque dossier dont la règle a été modifiée et le transchiffrement des fichiers du dossier (en accord avec la politique définie pour le transchiffrement dans le compte utilisateur).

Paramètre Comportement de Stormshield Data Security vis-à-vis des dates attachées aux fichiers lors des opérations de sécurisation/désécurisation

Sur la page **Paramètres**, dans la partie **Paramètres généraux**, l'option **Comportement de Stormshield Data Security vis-à-vis des dates attachées aux fichiers lors des opérations de sécurisation/désécurisation** offre trois possibilités d'action sur les dates de création, de modification et de dernier accès d'un fichier qui peuvent être combinées entre elles. Si aucune option n'est cochée, les dates restent inchangées en cas d'opération de sécurisation ou désécurisation.

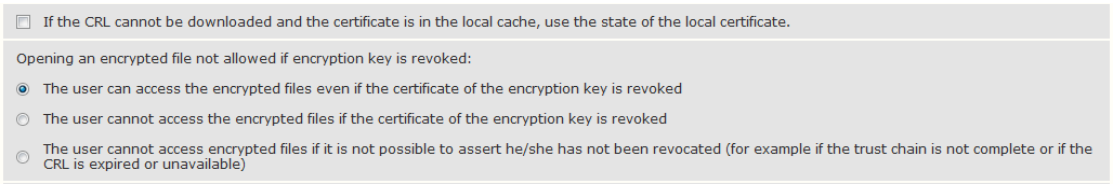
Lors de la synchronisation des fichiers d'un compte itinérant, Windows se base sur la date de modification des fichiers pour savoir s'il faut les synchroniser.

Par défaut, Stormshield Data Team conserve la date de modification des fichiers lorsque leur sécurité a changé (premier chiffrement, ajout d'un collaborateur, transchiffrement, désécurisation). Dans ce cas, des fichiers précédemment synchronisés ne sont pas synchronisés dans leur nouvel état. Ce paramètre permet de garantir la synchronisation des fichiers d'un compte itinérant.

Paramètres d'accès à un fichier chiffré si le certificat est révoqué

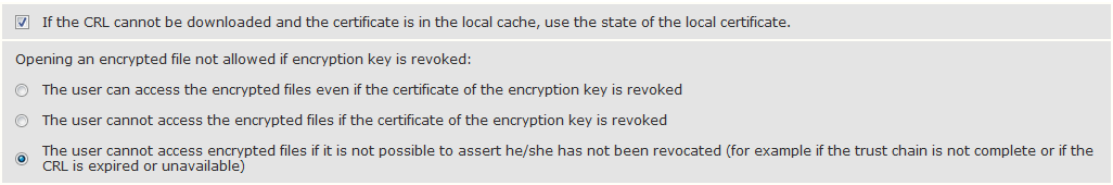
Sur la page **Paramètres**, dans la partie **Paramètres généraux**, les combinaisons d'options suivantes permettent de configurer deux modes d'accès à un fichier chiffré si le certificat de la clé de chiffrement de l'utilisateur est révoqué :

- Mode par défaut :



Ce mode permet à l'utilisateur d'accéder aux fichiers chiffrés même si le certificat de sa clé de chiffrement est révoqué.

- Mode sécurisé :



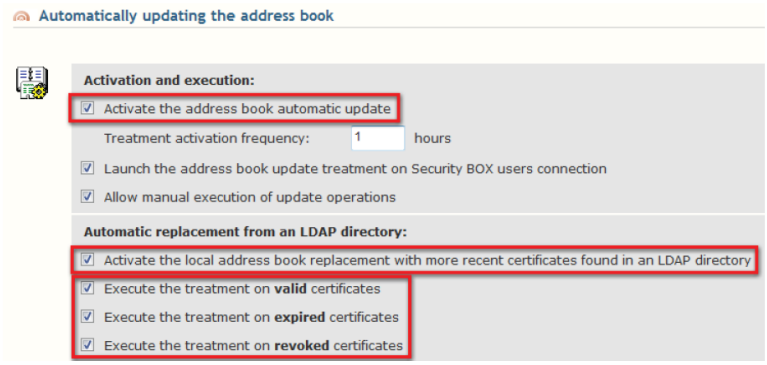
Ce mode permet à l'utilisateur d'accéder aux fichiers chiffrés à la condition que la CRL soit disponible en ligne (par téléchargement forcé) et que le certificat de sa clé de chiffrement ne soit pas révoqué.

NOTE
La vérification du certificat peut être longue, en particulier lorsque des time-outs réseaux sont en jeu si la CRL ne peut pas être téléchargée (par exemple si le serveur hôte n'est pas accessible) ou si la CRL devient volumineuse.

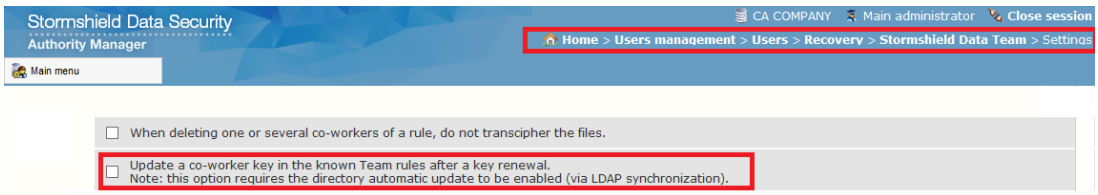
Mise à jour automatique des règles Team

Pour que les règles Team soient automatiquement mises à jour, il faut que la mise à jour automatique de l'annuaire (par synchronisation LDAP) soit activée. Suivez la procédure suivante :

1. Dans les paramètres Kernel d'un modèle, sélectionnez les options suivantes :



2. Dans les paramètres Team d'un modèle, activez la mise à jour automatique des règles :



11.5.3 Paramètres de Stormshield Data File

Fabrication des listes de fichiers

Vous devez fabriquer la liste d'exclusion (*.efp*), la liste de déchiffrement (*.dec*) et la liste de chiffrement (*.enc*) avec Stormshield Data File et ensuite les sélectionner dans les pages correspondantes.

Choix du format des fichiers

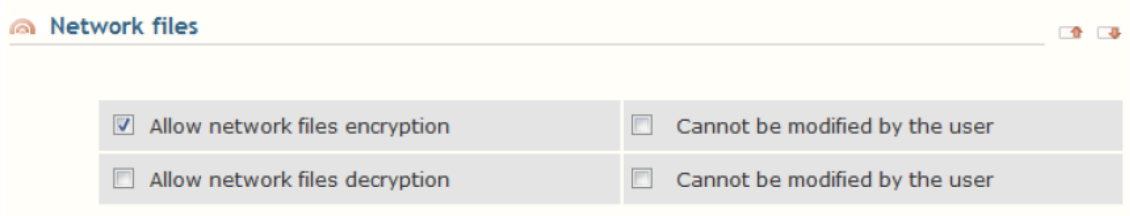
Par défaut, les fichiers chiffrés par SDS sont au format SBOX. Si vous souhaitez modifier le format de fichiers (SDSX), choisissez-le dans la section **Chiffrement et déchiffrement** de la page **Paramètres de Stormshield Data File**.

Interdiction de chiffrer (ou de déchiffrer) des fichiers

Dans la section **Chiffrement et déchiffrement** de la page **Paramètres de Stormshield Data File**, vous pouvez interdire le chiffrement et/ou le déchiffrement de tout fichier et/ou de tout dossier.

Chiffrement / déchiffrement des fichiers réseau

Dans la section **Fichiers réseau** de la page **Avancé**, vous pouvez autoriser ou non l'utilisateur à chiffrer ou déchiffrer des fichiers qui se trouvent sur un réseau.



11.5.4 Paramètres de Stormshield Data Shredder

Fabrication des listes de fichiers

Vous devez fabriquer la liste des fichiers à protéger (*.cfp*) et la liste des fichiers à supprimer (*.cln*) avec Stormshield Data Shredder, et ensuite les sélectionner dans les pages correspondantes.

Interdiction d'effectuer un effacement sécurisé

Dans la section **Chiffrement et déchiffrement** de la page **Paramètres de Stormshield Data Shredder**, vous pouvez interdire l'effacement de façon sécurisé de tout fichier et/ou de tout dossier.

11.5.5 Paramètres de Stormshield Data Mail Édition Outlook

Un utilisateur peut transmettre son certificat de chiffrement à un collaborateur en lui envoyant un e-mail signé. Le destinataire peut alors importer le certificat de chiffrement dans son annuaire de confiance pour le mettre à jour.

Cette procédure de mise à jour est applicable uniquement si la signature de l'e-mail reçu a pu être vérifiée par le destinataire.

Afin d'éviter des modifications de cette configuration de la part de l'utilisateur, cochez la case **Non modifiable par l'utilisateur**.

Mise à jour manuelle

Trois comportements sont possibles :

- **Non** : Aucune mise à jour de l'annuaire de confiance ne sera proposée.
- **Seulement pour une autorité connue** : L'import du certificat de l'émetteur ne sera proposé que s'il est issu d'une autorité dont le certificat est déjà présent dans l'annuaire du destinataire.
- **Quelle que soit l'autorité** : L'import du certificat de l'émetteur sera proposé même s'il est issu d'une autorité dont le certificat est absent de l'annuaire du destinataire.
  Pour cette option, l'import de certificats d'utilisateur et d'autorité doit être autorisé dans **Stormshield Data Kernel** > **Annuaire** > **Paramètres généraux**.

Ce mode requiert une intervention de l'utilisateur. Lors de la réception d'un e-mail signé dont les certificats de chiffrement sont absents de l'annuaire de confiance, l'utilisateur doit importer les certificats en cliquant sur le lien proposé en bas de l'e-mail.

Mise à jour automatique

Deux comportements sont possibles :

- **Non** : Aucune mise à jour de l'annuaire ne sera effectuée.
- **Seulement pour une autorité connue** : Le certificat de chiffrement de l'émetteur sera importé seulement s'il est issu d'une autorité dont le certificat est déjà présent dans l'annuaire de confiance du destinataire.

Ce mode ne requiert aucune intervention de l'utilisateur.

11.5.6 Configurer les modèles d'e-mails

Afin de modifier l'apparence des e-mails envoyés depuis le Stormshield Data Authority Manager, il est possible de modifier les fichiers de modèles d'e-mails qui sont créés dans le dossier \MailTemplates lors de l'installation du Stormshield Data Authority Manager.

Les fichiers suivants peuvent être modifiés dans tout éditeur de texte :

- template_expiration_mail
- template_request
- template_user_account
- template_user_account_mail_link
- template_validation_external_admin
- template_validation_external_user
- template_validation_internal_admin
- template_validation_internal_user

Modifiez le code HTML entre les balises <HTML> et </HTML> pour adapter l'apparence des e-mails.

Dans ces fichiers, toutes les variables comprises entre les drapeaux #D et #F ne doivent pas être supprimées ni modifiées.

12. Personnalisation de l'installation

Cette section décrit comment personnaliser Stormshield Data Security de deux façons différentes :

- en modifiant la configuration des fichiers *sbox.ini* et *cardchoice.ini*, qui sont spécifiques au poste sur lequel Stormshield Data Security est installée. Ainsi la personnalisation s'applique à tous les utilisateurs qui se connectent à Stormshield Data Security sur ce poste ;
- ou en modifiant la procédure d'installation de Stormshield Data Security, afin de créer un nouveau fichier d'installation *SDS_Suite_10.0.xxx.msi*.

Depuis Stormshield Data Authority Manager, il est possible de personnaliser le fichier d'installation d'une version équivalente ou d'une version antérieure encore supportée de Stormshield Data Security. L'inverse n'est pas possible.

12.1 Présentation

La personnalisation de l'installation de Stormshield Data Security est accessible à partir de la page d'accueil ou par le menu principal en cliquant sur le lien **Personnalisation de l'installation** (voir la section Page d'accueil).

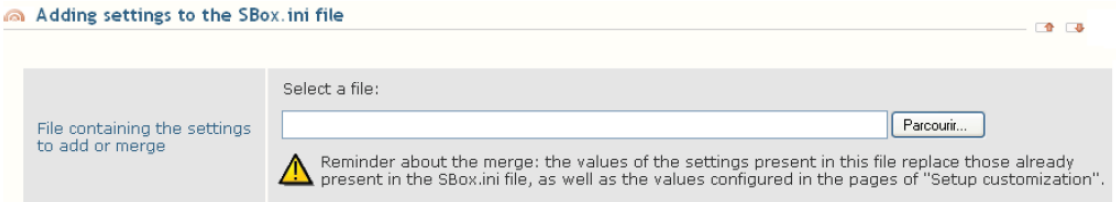
Cette personnalisation permet de :

- paramétrer une partie du fonctionnement de Stormshield Data Security sur le poste de l'utilisateur (connexion, création de compte, renouvellement de clé, voir la section Paramétrage du fonctionnement de Stormshield Data Security) ;
- paramétrer la procédure d'installation de Stormshield Data Security (voir la section Paramétrage de la procédure d'installation de Stormshield Data Security).

Elle modifie :

- le fichier *SDS_Suite_10.0.xxx.msi* qui contient la procédure d'installation ;
- les fichiers *sbox.ini* et *cardchoice.ini* qui configurent Stormshield Data Security.

Il est également possible d'ajouter ou de fusionner d'autres paramètres qui ne seraient pas gérés par les pages de la personnalisation de l'installation. Pour cela, allez sur la page **Paramètres Généraux** > section **Ajout de paramètres au fichier *SBox.ini*** :



Les paramètres ajoutés ici sont pris en compte uniquement lors de la génération du *.msi* personnalisé.

12.2 Paramétrage du fonctionnement de Stormshield Data Security

Paramétrer Stormshield Data Security s'effectue de deux façons complémentaires :

- lors de la configuration des composants qui est accessible depuis la page Utilisateurs (section Présentation). Ce paramétrage est propre au compte de l'utilisateur (pré-configuration, restrictions). Ces configurations des composants de Stormshield Data Security sont stockées dans le fichier compte (*.usr*) du compte utilisateur lors de la diffusion ;
- lors du paramétrage décrit dans cette section. Ce paramétrage est présent dans les fichiers *sbox.ini* et *cardchoice.ini* spécifiques au poste sur lequel est installé Stormshield Data Security. Ainsi, il s'applique à tous les utilisateurs qui se connectent à Stormshield Data Security sur ce poste.

Donc, deux utilisateurs qui se connectent à Stormshield Data Security sur le même poste, ont une configuration personnelle issue de leur compte utilisateur et une configuration commune apportée par les fichiers *sbox.ini* et *cardchoice.ini*.

La personnalisation de l'installation permet de configurer :

- les éléments relatifs à la connexion des utilisateurs ;
- les règles de création de compte avec une ou deux clés ;
- les règles du renouvellement de clé ;
- d'autres paramètres indépendants de tout utilisateur.

Les modifications apportées ne sont prises en compte qu'après la génération d'une nouvelle procédure d'installation (section Paramétrage de la procédure d'installation de Stormshield Data Security).

Les chapitres suivants présentent uniquement les paramètres qui nécessitent un complément d'information par rapport au contenu des pages HTML. La configuration des paramètres du fichier *sbox.ini* est décrite en détail dans le *Guide d'administration*.

12.2.1 Utilisation d'un master pour la création de compte

Vous pouvez définir un master pour chacune des créations de compte suivantes :

- Compte mot de passe avec une clé ;
- Compte mot de passe avec deux clés ;
- Compte carte avec une clé ;
- Compte carte avec deux clés.

Un master est composé :

1. d'un modèle à sélectionner parmi les modèles présents dans la base.

> **NOTE**
> L'utilisation d'un modèle pour la création d'un compte implique la saisie du mot de passe de ce modèle. Le processus de création de compte tente d'ouvrir le modèle avec un mot de passe vide, et si ce mot de passe vide est refusé, un écran demande alors à l'utilisateur de saisir le bon mot de passe. Il faut savoir qu'un essai est ainsi systématiquement consommé. L'utilisation d'un modèle avec un mot de passe vide permet d'éviter la saisie d'un tel mot de passe.

Lors de l'installation du produit, le fichier *SBox.ini* est automatiquement mis à jour : le paramètre `MasterPath` est renseigné dans la section correspondant à la création de compte concernée.

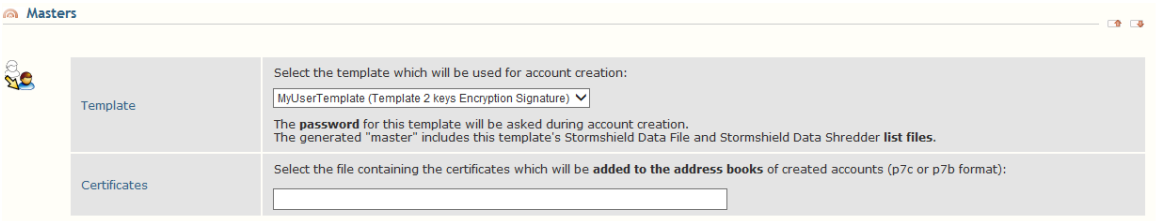
Lors de la création d'un utilisateur, celui-ci hérite des données suivantes du modèle :

- les configurations des composants de Stormshield Data Security ;
- les clés de recouvrement visibles ;
- les listes pour Stormshield Data File et Stormshield Data Shredder.

2. d'un fichier contenant des certificats à ajouter à l'annuaire des comptes créés (format pkcs 7).

Lors de l'installation du produit, le fichier *SBox.ini* est automatiquement mis à jour : les paramètres `DirectoryModel` et `DirModelIsFolder` sont renseignés dans la section correspondant à la création de compte concernée.

Lors de la création d'un utilisateur, son annuaire est automatiquement rempli avec les certificats contenus dans ce fichier.



12.2.2 Paramètres pour les comptes mot de passe

Paramétrage de la saisie du mot de passe

Les règles à appliquer aux mots de passe, qui sont définies dans cette page, s'appliquent lors d'une création de compte. Elles sont distinctes de celles définies dans la configuration de Stormshield Data Kernel (voir la section Composition du code secret) qui s'appliquent lors du changement de mot de passe.

Elles ne s'appliquent pas au mot de passe de secours.

Lorsque l'option **Ne pas afficher la fenêtre de saisie du mot de passe de secours** est cochée (section **Divers**), un mot de passe de secours est tiré aléatoirement. Puisqu'il n'est pas dévoilé, il ne peut pas être utilisé pour déverrouiller le compte utilisateur.

12.2.3 Paramètres pour les comptes carte ou clé USB

Définition du type de carte ou de clé USB utilisée

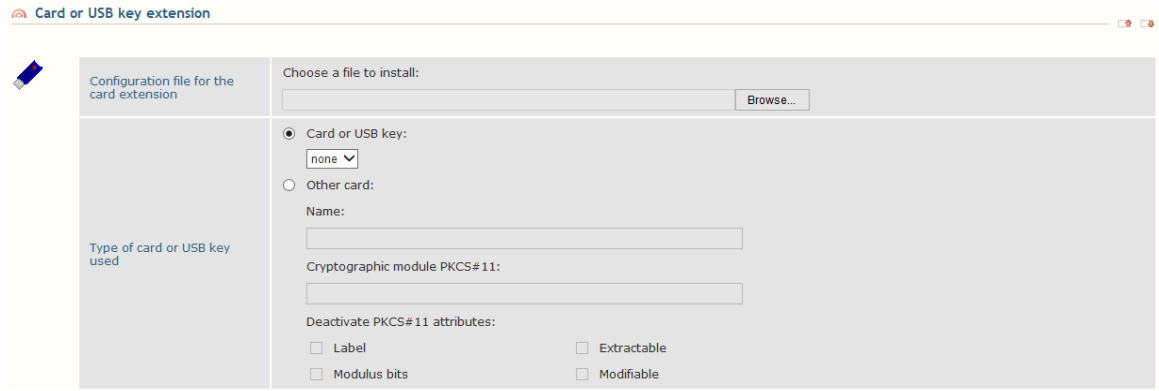
L'extension carte ou clé USB à utiliser est définie dans les paramètres généraux des comptes carte ou clé USB.

Il est possible de :

- sélectionner un fichier *.ini* qui contient le paramétrage d'une ou plusieurs extensions carte (par exemple le fichier *cardchoice.ini* de Stormshield Data Security présent sur votre poste). Vous pouvez ensuite sélectionner dans la liste déroulante, l'extension carte que vous souhaitez utiliser.

Lors de la génération de la procédure d'installation, le contenu du fichier *.ini* sélectionné est fusionné avec le contenu du fichier *cardchoice.ini* présent dans le fichier *SDS_Suite_10.0.xxx.msi* utilisé (voir la section Paramétrage de la procédure d'installation de Stormshield Data Security).

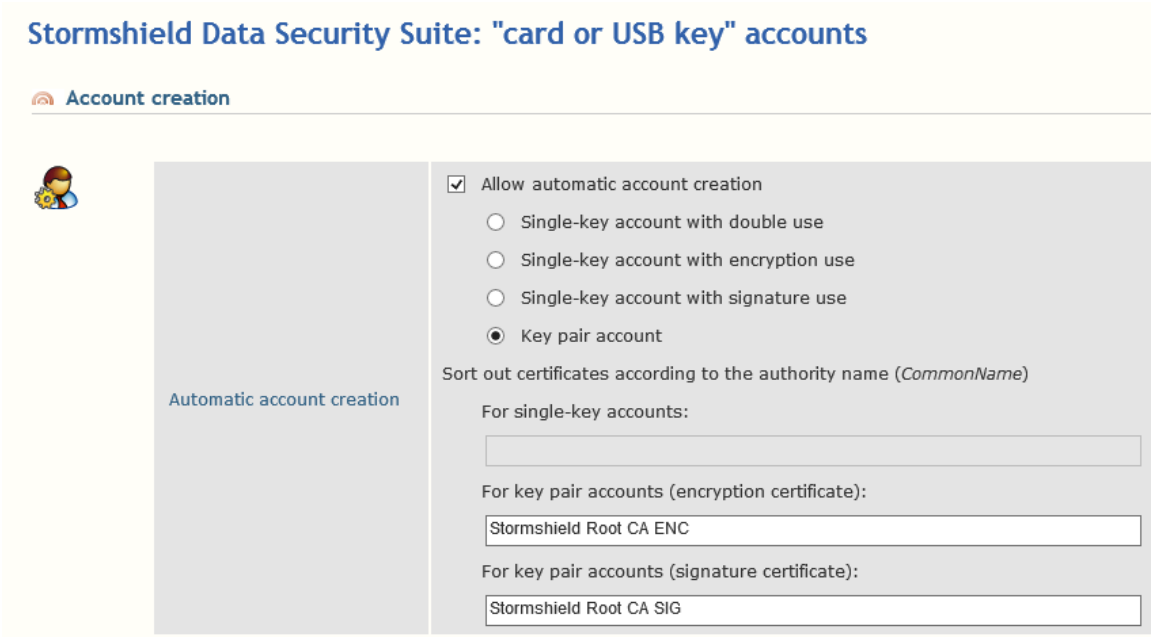
- choisir d'utiliser une extension carte non définie dans un fichier *.ini*. Elle doit être paramétrée dans la page. Elle sera écrite dans le fichier *cardchoice.ini* lors de la génération de la procédure d'installation.



Paramétrage de la création automatique de compte carte

La création de compte automatique se paramètre depuis la page **Personnalisation de l'installation > Paramètres pour les comptes "carte ou clé USB" > Paramètres généraux**.

Elle est activée lorsque la case **Autoriser la création de compte automatique** est cochée et qu'une des quatre options présentées ci-dessous est sélectionnée.



L'activation de la création de compte automatique positionne automatiquement certains paramètres sur les autres pages de la personnalisation de l'installation :

- **Autorisation de création** et **Usages réduits** dans la page **Création d'un compte "carte ou clé USB" avec une seule clé** ;
- **Autorisation de création** dans la page **Création d'un compte "carte ou clé USB" avec deux clés**.

Ces paramètres ne peuvent pas être modifiés tant que la création de compte automatique est activée.

Filtrage des autorités à la création automatique d'un compte carte

Si la création de compte automatique est activée, alors il est possible de définir un filtre sur les certificats à utiliser en se basant sur le nom de l'autorité de certification ayant délivré les certificats.

En fonction du type de compte (mono-clé, bi-clé), les champs correspondants sont accessibles pour renseigner le nom de la ou des autorités de certification.

Les certificats n'ayant pas été émis par l'autorité dont le nom est spécifié sur cette page, ne seront pas utilisés lors de la création de compte carte/token.

Filtrage des lecteurs

Si plusieurs lecteurs de carte sont connectés à un poste de travail, vous pouvez configurer un filtrage des lecteurs afin d'autoriser Stormshield Data Security à communiquer uniquement avec un lecteur spécifique et à ne pas afficher les autres.

Cochez la case **Si plusieurs lecteurs sont connectés au poste, ne prendre en compte que le lecteur suivant** et indiquez une description et le fabricant du lecteur.

Vous pouvez utiliser les caractères spéciaux "*" et "?" pour élargir le périmètre du filtre.

12.3 Paramétrage de la procédure d'installation de Stormshield Data Security

Paramétrez la procédure d'installation de Stormshield Data Security dans la page **Génération de la procédure d'installation**. Cette page est accessible à partir du menu **Opérations**, en cliquant sur le lien **Générer la procédure d'installation**.

Créez une procédure qui contient :

- un numéro de licence, ce qui permettra à l'utilisateur de ne pas le saisir ;
- la liste des composants qui seront présélectionnés lors de l'exécution de la procédure d'installation ;
- un dossier d'installation, si vous souhaitez installer Stormshield Data Security dans un dossier différent du dossier par défaut.

Saisissez :

- un nom complet pour le fichier *SDS_Suite_10.0.xxx.msi* source, accessible par le serveur hébergeant Stormshield Data Authority Manager. Ce nom complet doit être écrit « comme le serveur va l'interpréter ». Il peut contenir des espaces dans le nom du fichier mais pas dans le chemin, et ne peut excéder 256 caractères. Par exemple : **C:\SBMData\<base_id>\SDS_Suite_10.0.xxx.msi**
- un dossier cible existant situé sur ce serveur (ne sélectionnez pas un dossier partagé sur votre réseau). Il doit être écrit « comme le serveur va l'interpréter ». Par exemple : **C:\SBMData\<base_id>\MSITarget**

La génération crée un nouveau fichier *SDS_Suite_10.0.xxx.msi* dans le dossier cible.

Annexe A. Méthodologie de déploiement

Cette annexe énumère les opérations à effectuer pour installer Stormshield Data Authority Manager, et liste les fonctionnalités les plus couramment utilisées dans l'ordre dans lequel il est préférable de les effectuer.

Cette annexe a pour objectif d'aider à prendre rapidement en main le présent guide utilisateur. Elle n'est pas exhaustive et ne rentre pas dans les détails des fonctionnalités. Elle renvoie aux chapitres concernés où l'administrateur trouvera toutes les informations nécessaires pour faire les choix liés à son architecture.

A.1. Serveur

Sur le serveur, effectuez les opérations suivantes :

1. Installer Stormshield Data Authority Manager (voir la section Installation de Stormshield Data Authority Manager) ou mettre à jour Stormshield Data Authority Manager version 6 (voir la section Mise à jour de Security BOX pour une version supérieure à 6.x).
2. Configurer le serveur (voir les sections Configuration du serveur Web IIS puis Paramétrage du serveur Web IIS).
3. Mettre à jour la section WebServer du fichier *Manager.ini* (voir la section Serveur Web).
4. Positionner les droits de l'utilisateur réseau (voir la section Droits NTFS requis pour l'utilisateur réseau) pour :

- le fichier *bases.ini* ;
- le fichier *manager.exe* ;
- le dossier **c:\sbmdata** ;
- le dossier **c:\Windows\Temp** ;

5. Positionner les droits DCOM (voir la section « Assignation des droits DCOM pour le service Stormshield Data Authority Manager »).
6. Créer la base (voir la section Création d'une base de données) ou bien démarrer (voir la section Démarrage/Arrêt d'une base de données) et mettre à jour une base (voir Outil de mise à jour de base de données) ou mettre à jour une base d'une version antérieure.

A.2. Client

Sur le poste client, dans le navigateur Internet Explorer, effectuez les opérations suivantes :

1. Placer le serveur dans les sites de confiance et adoucir les restrictions concernant les ActiveX pour les sites de confiance (voir la section Configuration du poste administrateur) ;
2. Accéder à Stormshield Data Authority Manager (voir la section URL d'accès au serveur).

Dans Stormshield Data Authority Manager :

1. Initialiser la base (voir la section Initialisation d'une base de données) ;
2. Créer les administrateurs de la base (voir la section Définition des administrateurs et de leurs rôles) ;
3. Créer les autorités de certifications externes (voir la section Autorités de certification externes) ;
4. Créer les modèles de certificats (voir la section Modèles de certificats) ;

5. Faire certifier l'autorité de certification de la base (voir la section section Gestion de la clé de l'autorité de certification), qui comprend une demande de certificat (voir Demande de certificat) et l'importation du certificat (voir la section Importation d'un nouveau certificat) ;
6. Importer dans les certificats externes les certificats constituant la chaîne de parenté de la CA de la base (voir la section Autres certificats externes) ;
7. Configurer la synchronisation avec le serveur LDAP (voir la section Configuration LDAP) ;
8. Activer dans les paramètres généraux des utilisateurs :

- les publications des mises à jour de sécurité (voir la section Publication des mises à jour de politiques de sécurité et Publication et téléchargement des mises à jour de sécurité à l'aide d'un annuaire LDAP) ;
- la publication des fichiers d'installation (voir la section Gestion des utilisateurs).

9. Renseigner dans les paramètres généraux de l'autorité de certification (voir la section Listes de révocation (CRLs) :

- le point de distribution des CRLs dans lequel seront publiées les CRLs générées par l'autorité de certification. Ce point de distribution sera inclus dans tous les certificats générés par l'autorité de certification ;
- le DN de publication afin de lancer la fonctionnalité de publication des CRLs.
- la publication par fichier des certificats générés (voir la section Certificats générés) ;

10. Configurer le serveur SMTP (voir la section Serveur de courrier sortant) ;
11. Créer les modèles (voir la section Modèle et section Création d'un modèle d'utilisateur) ;
12. Définir pour chaque modèle les configurations des composants avec, entre autres, les points de distribution des mises à jour de sécurité (voir Publication et téléchargement des mises à jour de sécurité à l'aide d'un annuaire LDAP) ;
13. Créer le compte signataire de politiques de sécurité. (voir la section Création d'un signataire de politiques de sécurité) ;
14. Mise en place du recouvrement :

- créer le ou les comptes de recouvrement (voir la section Création d'un compte de recouvrement) ;
- et/ou importer le ou les certificats externes de recouvrement (voir la section Certificats externes de recouvrement) ;

15. Créer les utilisateurs à partir des modèles : à partir d'un fichier (voir la section Création d'un grand nombre d'utilisateurs à partir d'un fichier), à partir d'un annuaire LDAP (voir la section Création à partir d'un annuaire LDAP)
16. Publier une CRL (voir la section Génération d'une liste de révocation) ;
17. Diffuser les utilisateurs en créant des fichiers d'installation et en envoyant par mail, soit les fichiers eux-mêmes, soit des liens de téléchargement vers les fichiers publiés (voir la section Diffusion des comptes utilisateurs).

Annexe B. Configuration de Windows Server

La configuration du serveur s'effectue selon les étapes suivantes :

1. configurer le serveur Web ;
2. permettre à Stormshield Data Authority Manager d'accéder au réseau (cette étape ne vous concerne que si Stormshield Data Authority Manager est amené à accéder à des fichiers stockés sur une ressource réseau) ;
3. assigner les droits DCOM à l'utilisateur réseau pour le service Stormshield Data Authority Manager.

B.1. Configuration du serveur Web IIS

B.1.1. Déclaration du CGI

1. Cliquez sur **Démarrer**, **Panneau de configuration**, **Outils d'administration** puis ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Dans l'arborescence, placez-vous sur le nom du serveur.
3. Dans la page d'accueil, double-cliquez sur **Restrictions ISAPI et CGI**.
4. Cliquez sur **Ajouter...** situé en haut à droite de la page.
5. Sélectionnez le fichier **<sdam_install_dir>\Bin\MANAGER.exe** puis placez-le entre « » s'il contient des espaces.
6. Saisissez **Stormshield Data Authority Manager** comme description.
7. Cochez **Autoriser l'exécution du chemin de l'extension** puis validez.

B.1.2. Ajout du site Web

1. Effectuez un clic droit sur **Sites** dans l'arborescence puis sélectionnez **Ajouter un site Web...**
2. Saisissez **Stormshield Data Authority Manager** comme nom de site.
3. Sélectionnez **<sdam_install_dir>** comme chemin d'accès physique.
4. Saisissez une nouvelle valeur `<port>` pour le port puis validez.

> **NOTE**
> Vous devez contrôler la configuration du pare-feu présent sur le serveur. Il est certainement nécessaire d'ajouter une règle de trafic entrant dédiée au contrôle des connexions au port TCP local spécifique `<port>`.

Pour configurer des ports assignés (par exemple, le port sécurisé 443 pour le protocole https), consultez la Activation du protocole HTTPS sur Stormshield Data Authority Manager.

B.1.3. Définition des autorisations pour le site Web

1. Dans l'arborescence, placez-vous sur le site Stormshield Data Authority Manager.
2. Double-cliquez sur **Mappages de gestionnaire**.
3. Cliquez sur le lien **Modifier les autorisations de fonctions**.
4. Décochez toutes les cases puis validez.

5. Placez-vous ensuite sur le dossier **ActiveX** puis double-cliquez sur **Mappages de gestionnaires**.
6. Dans la colonne de droite, cliquez sur le lien **Modifier les autorisations de fonctions**.
7. Cochez **Lecture** puis validez.
8. Placez-vous ensuite sur le dossier **Htdocs** puis double-cliquez sur **Mappages de gestionnaires**.
9. Dans la colonne de droite, cliquez sur le lien **Modifier les autorisations de fonctions...**
10. Cochez **Lecture** puis validez.
11. Placez-vous ensuite sur le dossier **Bin**, puis double-cliquez sur **Mappages de gestionnaires**.
12. Dans la colonne de droite, cliquez sur le lien **Modifier les autorisations de fonctions...**
13. Cochez **Lecture**, **Script** et **Exécution**, puis validez.
14. Redémarrez le site web.

B.1.4. Configuration du fichier *manager.ini*

Configurez le fichier *manager.ini* pour que les liens des pages Web soient compatibles avec le paramétrage d'IIS (voir la section Serveur Web). Pour la configuration décrite précédemment, les valeurs à positionner dans la section WebServer sont :

```
ManagerRootUrl = http://<hostname>/bin/manager.exe
```

```
ManagerDocUrl = /
```

Où `<hostname>` est soit le nom de la machine hébergeant le serveur soit `<adresseIP>:<port>`.

B.2. Paramétrage d'accession au réseau pour Stormshield Data Authority Manager

Ce paragraphe ne vous concerne que si Stormshield Data Authority Manager est amené à accéder à des fichiers stockés sur une ressource réseau.

Vous devez dans ce cas :

1. Choisir ou créer à cet effet un utilisateur NT ayant le droit d'accéder à des ressources réseaux. Nous l'appellerons par la suite `Utilisateur réseau`.

Avec le serveur IIS, cet `Utilisateur réseau` est l'utilisateur `Invité Internet (IUSR)` sous lequel le serveur Web tourne.

Si nécessaire, pour créer l'utilisateur réseau, dans le menu **Démarrer** de Windows, sélectionnez **Outils d'administration**, **Gestion de l'ordinateur**, **Utilisateurs locaux**, **Utilisateurs**, puis cliquez sur le bouton droit et sélectionnez **Nouvel utilisateur**.

2. Paramétrez votre serveur Web pour qu'il utilise cet utilisateur (voir la section Paramétrage du serveur Web IIS).
3. Donnez à cet utilisateur les droits NTFS suffisants sur les dossiers utilisés par Stormshield Data Authority Manager (voir la section Droits NTFS requis pour l'utilisateur réseau).
4. Donnez à cet utilisateur le droit DCOM d'invoquer le service Stormshield Data Authority Manager (voir la section A.3, « Assignation des droits DCOM pour le service Stormshield Data Authority Manager »).

Utilisez la syntaxe UNC (Universal Naming Convention) pour désigner les ressources réseau dans Stormshield Data Authority Manager : **\\machine\dossier\fichier** est un chemin valide mais **Z:\dossier\fichier** ne l'est pas.

Si vous utilisez le SGBD Microsoft Access, la base de données créée ne doit pas être une ressource réseau.

B.2.1. Paramétrage du serveur Web IIS

Procédez comme suit :

1. Dans le **Gestionnaire des services Internet (IIS)**, placez-vous sur le répertoire **Bin** du site web de Stormshield Data Authority Manager.
2. Double-cliquez sur **Authentification**.
3. Sélectionnez **Authentification anonyme** dans la liste.
4. Dans la colonne de droite, cliquez sur le lien **Modifier…**.
5. Sélectionnez **Utilisateur spécifique**, cliquez sur le bouton **Définir…**, saisissez **IUSR** sans mettre de mot de passe. Ce sont les valeurs proposées par défaut.
6. Validez en cliquant deux fois sur **OK**.

B.2.2. Droits NTFS requis pour l'utilisateur réseau

L'utilisateur réseau doit avoir :

- Le droit d'exécution sur le fichier : **<sdam_install_dir>\Bin\Manager.exe** ;
- Le droit de modification sur le fichier : **<sdam_install_dir>\bases.ini** ;
- Le droit de modification sur le dossier de données de Stormshield Data Authority Manager, par défaut **<sdam_data_install_dir>\SBMData**, et ses sous-dossiers ;
- Le droit de modification sur le dossier temporaire de la machine, par défaut **C:\WINDOWS\TEMP**.

> **NOTE**
> Il faut que l'utilisateur réseau ait aussi le droit de modification sur le dossier temporaire utilisé par Stormshield Data Authority Manager. Par défaut, c'est le dossier défini par le paramètre `TempPath` de la section `[Path]` du fichier de configuration *manager.ini* (voir la section Dossier des fichiers temporaires). L'installation lui affecte la valeur **<sdam_data_install_dir>\SBMData\tmp**. Si vous choisissez de modifier cette valeur afin de travailler dans un autre dossier, veuillez donner le droit de modification sur le dossier utilisé.

Procédez comme suit :

1. Dans le menu **Démarrer** de Windows, sélectionnez **Exécuter**, puis saisissez **explorer**.
2. Allez dans le dossier **<sdam_install_dir>**.
3. Cliquez avec le bouton droit sur le fichier *bases.ini*, sélectionnez **Propriétés**, puis l'onglet *Sécurité*.
4. Appuyez sur [**Modifier** puis] **Ajouter**, saisissez le nom de l'utilisateur réseau, puis validez.
5. Donnez-lui le droit de modification puis validez.
6. Allez dans le dossier **<sdam_install_dir>\Bin**.
7. Cliquez avec le bouton droit sur le fichier *Manager.exe*, sélectionnez **Propriétés**, puis l'onglet *Sécurité*.
8. Appuyez sur [**Modifier** puis] **Ajouter**, saisir le nom de l'utilisateur réseau, puis validez.
9. Donnez-lui le droit de lecture et d'exécution puis validez.
10. Allez dans le dossier **<sdam_data_install_dir>**.

11. Cliquez avec le bouton droit sur le dossier **SBMData**, sélectionnez **Propriétés**, puis l'onglet *Sécurité*.
12. Appuyez sur [**Modifier** puis] **Ajouter**, saisir le nom de l'utilisateur réseau, puis validez.
13. Donnez-lui le droit de modification puis validez. Ensuite :
    - Cliquez sur le bouton **Avancé**, puis sélectionnez l'onglet *Autorisation*.
    - Cliquez sur le bouton **Modifier les autorisations…**.
    - Cochez la case **Remplacer toutes les autorisations [...]**, puis validez.
14. Allez dans le dossier **C:\WINDOWS**.
15. Cliquez avec le bouton droit sur le dossier **Temp**, sélectionnez **Propriétés**, puis l'onglet *Sécurité*.
16. Appuyez sur [**Modifier**] puis **Ajouter**, saisissez le nom de l'utilisateur réseau, puis validez.
17. Donnez-lui le droit de modification puis validez.

B.3. Assignation des droits DCOM pour le service Stormshield Data Authority Manager

Le service Stormshield Data Authority Manager est implémenté sous forme de composants COM. Il doit pouvoir être invoqué par l'utilisateur Windows sous lequel tourne le serveur Web.

Vous devez explicitement accorder à cet utilisateur Windows le droit d'invoquer Stormshield Data Authority Manager dans les cas suivants :

- le produit accède à des ressources réseau. Vous avez alors défini un `utilisateur réseau` sous le compte duquel le serveur Web tourne (voir la section A.2, « Paramétrage d'accession au réseau pour Stormshield Data Authority Manager ») ;
- vous utilisez le serveur IIS : le serveur Web tourne sous l'utilisateur `Invité Internet` qui est par défaut `IUSR`.

Pour positionner ce droit :

1. Dans le menu **Démarrer** de Windows, choisissez **Exécuter**, puis saisissez **dcomcnfg**.
2. Dans l'arborescence, choisissez : **Services de composants, Ordinateurs, Poste de travail, Configuration DCOM**.
3. Cliquez avec le bouton droit sur **Stormshield Data Authority Manager service**, puis choisissez **Propriétés**.
4. Dans l'onglet *Sécurité*, dans **Autorisations d'exécution et d'activation**, choisissez **Personnaliser**, puis cliquez sur **Modifier**.
5. Appuyez sur **Ajouter**, saisissez le nom de l'utilisateur réseau, puis validez.
6. Cochez les cases **Exécution locale, Exécution à distance, Activation locale, Activation à distance** dans la section **Autoriser**.
7. Validez deux fois par **OK**.

Annexe C. Migration de Microsoft Access vers Microsoft SQL Server

A l'aide des outils Microsoft, il est possible d'importer dans une base Microsoft SQL Server la totalité du contenu d'une base Microsoft Access.

C.1. Présentation

Cette annexe décrit l'importation dans une base version 10.1 Microsoft SQL Server du contenu d'une base version 10.1 Microsoft Access, à l'aide de l'outil SQL Server Import and Export Wizard présent dans le produit Microsoft SQL Server 2005.

Si la base Microsoft Access source *<base_id_source>.sba* est une base de version antérieure à la version 10.1, elle doit impérativement être mise à jour en version 10.1 (voir la section Outil de mise à jour de base de données).

Les composants suivants de Microsoft SQL Server ont été installés :

- Database Services ;
- Analysis Services ;
- Integration Services ;
- Client components.

Le mode d'authentification est mixte : identifiant `sa`, mot de passe `<Authentication_logon_password>`.

C.2. Procédure

C.2.1. Création de la base destination SQL Server

1. Ouvrez **SQL Server Management Studio**.
2. Dans l'arborescence du serveur, cliquez avec le bouton droit sur le dossier **Bases de données**, puis sélectionnez **Nouvelle base de données…**.
3. Dans **Nom de la base de données**, saisissez le nom de la base `<base_name>`, puis validez par **OK**. La base est créée.
4. Effectuez un clic droit sur la base créée et sélectionnez **Nouvelle requête**. Dans la partie droite de la fenêtre, faites ensuite un copier-coller du contenu du fichier *create_database_SqlServer_for_import.sql* présent dans le dossier.
5. Dans la barre d'outils, cliquez sur **Exécuter**. La base est peuplée.

C.2.2. Importation des données de la base source Access

1. Toujours dans SQL Server Management Studio, dans l'arborescence des bases, cliquez avec le bouton droit sur la base `<base_name>` nouvellement créée, sélectionnez **Tâches**, puis **Importer des données…**. L'**Assistant Importation et Exportation SQL Server** est lancé.
2. Dans **Source de données**, sélectionnez **Microsoft Access**.
3. Dans **Nom de fichier**, sélectionnez la base source Access `<base_id_source>.sba` à importer, laissez **Nom d'utilisateur** et **Mot de passe** vides, puis validez.

4. Sélectionnez le mode d'authentification SQL Server, saisissez `sa` dans le **Nom d'utilisateur** et le mot de passe `<Authentication_logon_password>` dans **Mot de passe**, vérifiez que la base sélectionnée dans **Base de données** est bien `<base_name>`, puis validez.
5. Validez la page suivante en laissant la sélection **Copier les données à partir d'une ou plusieurs tables ou vues**.
6. Sélectionnez toutes les tables en cochant la case présente à droite de **Source**, et décochez la ligne de la table COUNTERS si celle-ci est présente, puis validez.
7. Validez la page suivante en laissant la sélection **Exécuter immédiatement**.
8. Lancez l'exécution.
9. A la fin du traitement, vous pouvez fermer l'**Assistant Importation et Exportation SQL Server**, puis **SQL Server Management Studio**.

C.2.3. Déclaration de la base SQL Server dans Stormshield Data Authority Manager

Installation sur la même machine

Si la version précédente du logiciel Stormshield Data Authority Manager a été directement mise à jour avec la version 10.1 sur la même machine, il y a eu conservation du dossier d'installation et du dossier de données.

1. Editez le fichier *bases.ini* présent dans le dossier d'installation **<sdam_install_dir>** de Stormshield Data Authority Manager.
2. Dans la section de la base `<base_id_source>`, remplacez la valeur de la donnée `ConnectionString` par la chaîne de connection suivante :

```
Provider=SQLOLEDB;Data Source=<server name>;DataBase=<databasename>;
User Id=<user ID>;Password=<password>
```

Où

`<servername>`	est le nom du serveur (visible dans **Panneau de configuration**, **Système**, onglet *Nom de l'ordinateur*) ;
`<database name>`	est le nom de la base SQL Server `<base_name>` ;
`<user ID>`	est l'identifiant de connexion `sa` ;
`<password>`	est le mot de passe de connexion `<Authentication_logon_password>`.

3. Sauvegardez le fichier.

La base peut être démarrée.

Installation sur une nouvelle machine

Si le produit Stormshield Data Authority Manager version 10.1 a été installé sur une nouvelle machine :

1. Cliquez sur **Démarrer**, **Tous les programmes**, **Stormshield Data Authority Manager** puis **Créer une nouvelle base**.
2. Dans l'assistant, saisissez l'identifiant `<base_id_source>` de la base source afin de faire le lien avec le fichier keystore *<base_id_source>.mng*. Vous pouvez saisir un libellé différent de celui de la base source mais il faudra ensuite modifier celui sauvegardé dans la base afin de les harmoniser (voir la section Libellé de la base).
3. Dans la page suivante, saisissez le type de base Microsoft SQL Server.

4. Saisissez ensuite le nom du serveur, le nom de la base SQL Server `<base_name>`, l'identifiant de connexion sa et le mot de passe de connexion `<Authentication_logon_password>` en décochant la demande de mot de passe.
5. Testez la connexion. Si la connexion est établie, exécutez les dernières pages du wizard afin d'achever la déclaration de la base.
6. Copiez dans le dossier **<sdam_data_install_dir>/SBMData/Databases** le fichier keystore *<base_id_source>.mng* anciennement associé à la base source Access et qui est dorénavant associé à la nouvelle base SQL Server.
7. Création de l'arborescence :

- Si vous ne voulez pas conserver l'ancienne arborescence de la base, créez dans le dossier **<sdam_data_install_dir>/SBMData** l'arborescence décrite à la section Arborescence créée lors de l'initialisation en utilisant bien `<base_id_source>` comme identifiant pour la base. Il est vivement conseillé de dupliquer une arborescence existante, en vidant tous les dossiers à l'exception du dossier `MailTemplates`.
- Si vous souhaitez conserver l'ancienne arborescence de la base, copiez cette arborescence dans le dossier **<sdam_data_install_dir>/SBMData/<base_id_source>**.

La base peut être démarrée.

Une mise à jour des chemins présents dans les paramètres généraux est peut être nécessaire pour tenir compte de la nouvelle localisation du dossier de données `<sdam_data_install_dir>` (voir les paramètres généraux définis dans les sections Propriétés de la base de données, Gestion des utilisateurs, Paramètres de gestion des certificats et Autorités de certification externes).

Annexe D. Renouvellement d'un certificat

Cette annexe est un exemple de l'utilisation des fonctionnalités de Stormshield Data Authority Manager pour effectuer le renouvellement du certificat d'un utilisateur, qu'il ait un compte "carte" ou un compte "mot de passe". Elle décrit l'enchaînement des étapes, depuis la génération du nouveau certificat, jusqu'à son importation dans le compte de l'utilisateur sur son poste.

D.1. Activation de la notification par e-mail

Dans les paramètres de gestion des certificats, la notification par e-mail au demandeur lors de la validation d'une demande interne doit être activée (voir la section Notifications par e-mail).

D.2. Renouvellement du certificat

Dans Stormshield Data Authority Manager, le renouvellement du certificat d'un utilisateur s'effectue :

- de manière unitaire à partir de la page **Clé et certificat** de l'utilisateur (voir la section Renouvellement de certificat) ;
- de manière groupée à partir de la page **Liste des utilisateurs** (voir la section Renouvellement de plusieurs certificats).

Le nouveau certificat est généré par l'autorité de certification de la base, ce qui entraîne l'envoi d'un e-mail de notification à l'adresse contenue dans le sujet du certificat.

D.3. Importation du nouveau certificat dans le compte de l'utilisateur

L'utilisateur reçoit un e-mail de notification contenant un lien l'invitant à accéder à la page publique de la PKI présentant le certificat généré.

Cette page propose plusieurs fonctions de sauvegarde du certificat, dont sa copie dans Stormshield Data Security si elle est affichée avec Internet Explorer (voir la section Affichage de certificat).

L'utilisateur, en exécutant cette fonction, lance l'assistant d'importation du certificat de Stormshield Data Security, qui importe le certificat dans le compte. Il est aussi importé dans la carte si c'est un compte "carte".

Annexe E. Publication et téléchargement des mises à jour de sécurité à l'aide d'un annuaire LDAP

Stormshield Data Authority Manager permet de publier dans un annuaire LDAP des mises à jour des politiques de sécurité. Il permet aussi de configurer le composant « Mise à jour automatique » pour que Stormshield Data Security télécharge les mises à jour publiées.

E.1. Publication des mises à jour

Que ce soit pour un utilisateur (voir la section Diffusion des comptes utilisateurs) ou pour un modèle, la publication de la mise à jour dans l'annuaire LDAP est proposée lors de la diffusion de la mise à jour, si :

- un serveur LDAP est configuré (voir la section Configuration LDAP) ;
- l'option est cochée dans les paramètres généraux (voir la section Publication des mises à jour de politiques de sécurité).

Le DN `<LDAP_entry_DN>` de l'entrée LDAP dans laquelle la mise à jour est publiée, correspond à :

- dans le cas de l'utilisateur, au DN de l'entrée associée à l'utilisateur (voir la section Page Utilisateur et section Association d'un utilisateur à une entrée LDAP) ;
- dans le cas du modèle, au DN saisi spécifiquement pour cette opération (section Création d'un modèle d'utilisateur).

E.2. Configuration annuaire LDAP

L'annuaire LDAP doit supporter l'attribut `<security_policies_upgrade_attribute>` spécifique aux produits Stormshield Data Security. Dans le produit Stormshield Data Authority Manager, il est défini dans les paramètres du serveur LDAP (voir la section Nom des attributs). Il vaut par défaut `sboxPolicyUpgrade;binary`.

L'entrée LDAP dans laquelle la mise à jour est publiée doit dériver d'une classe supportant l'attribut `<security_policies_upgrade_attribute>`. Idéalement il faut créer une nouvelle classe `sboxPerson` qui dérive de `inetOrgPerson` et qui supporte l'attribut `<security_policies_upgrade_attribute>`. Exemple de fichier *sboxperson.schema* :

```
# This file can be used to support Security BOX
# security policies upgrade.
#
# Requires files : core.schema, cosine.schema, inetorgperson.schema,


# sboxPolicyUpgrade
# Must be transferred using ;binary
attributetype ( 1.2.250.1.63.1.6.1.2.3
NAME 'sboxPolicyUpgrade'
DESC 'Security BOX security policies upgrade'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.8)

# sboxPerson
Objectclass ( 1.2.250.1.63.1.6.1.1
NAME 'sboxPerson'
DESC 'Security BOX User'
```

```
SUP inetOrgPerson
STRUCTURAL
        MAY   ( sboxPolicyUpgrade)
        )
```

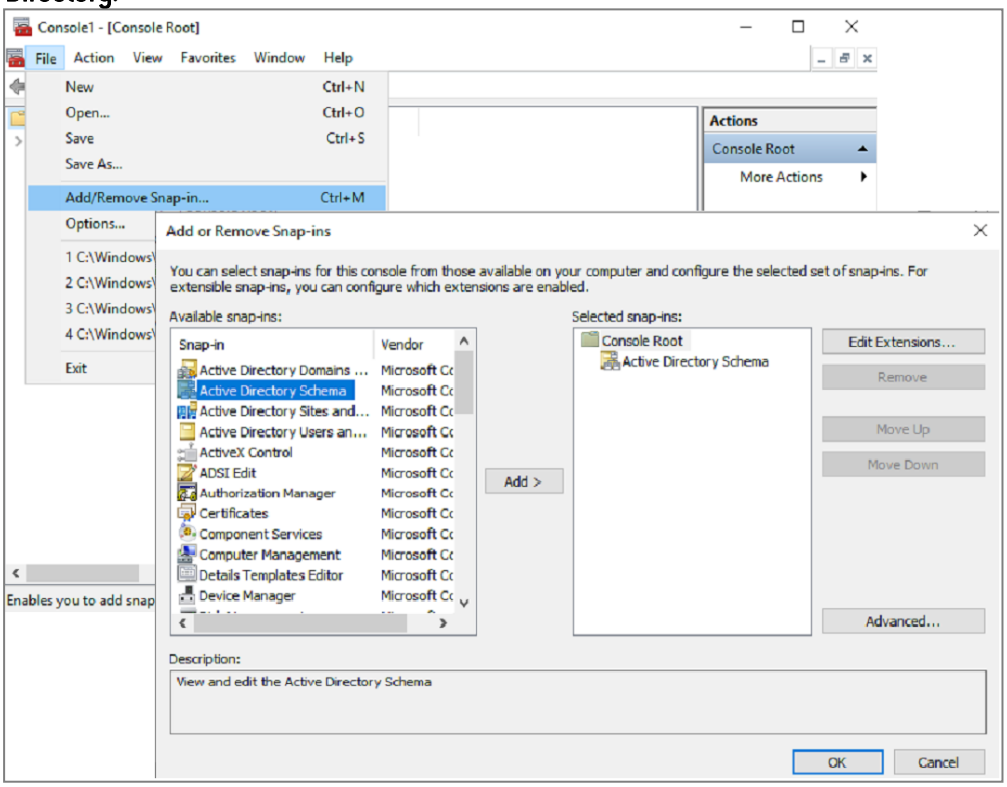
L'entrée LDAP doit dériver de cette classe.

Dans un annuaire existant, s'il n'est pas possible de faire dériver l'entrée existante à partir d'une nouvelle classe, il est toujours possible de mettre à jour une classe existante.

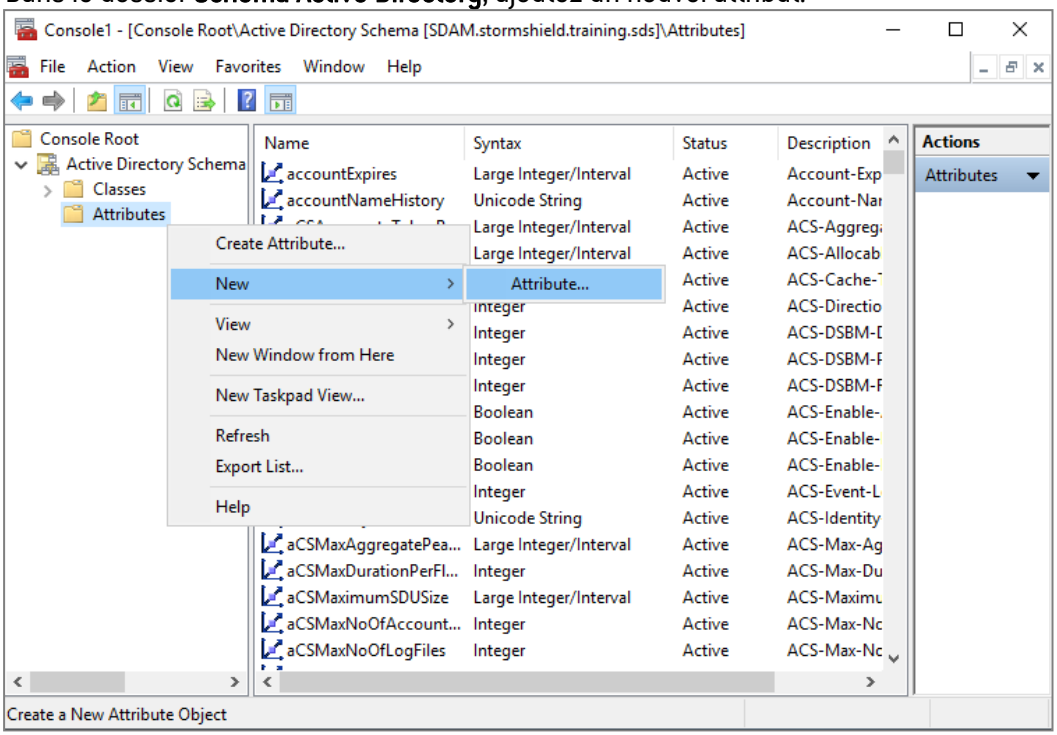
En conformité avec la norme RFC 2252, si la syntaxe définie dans le schéma se termine par `.8` (syntaxe du type Certificate), « `;binary` » doit être présent à la fin du nom de l'attribut dans sa définition dans Stormshield Data Authority Manager et dans le point de distribution. Si la syntaxe se termine par `.5` (syntaxe du type Binary) « `;binary` » ne doit pas être présent.

Exemple d'ajout de l'attribut `sboxPolicyUpgrade` à la classe `inetOrgPerson` sur Active Directory

1. Sur l'Active Directory, exécutez *MMC.exe* afin d'ajouter le composant logiciel **Schéma Active Directory**.

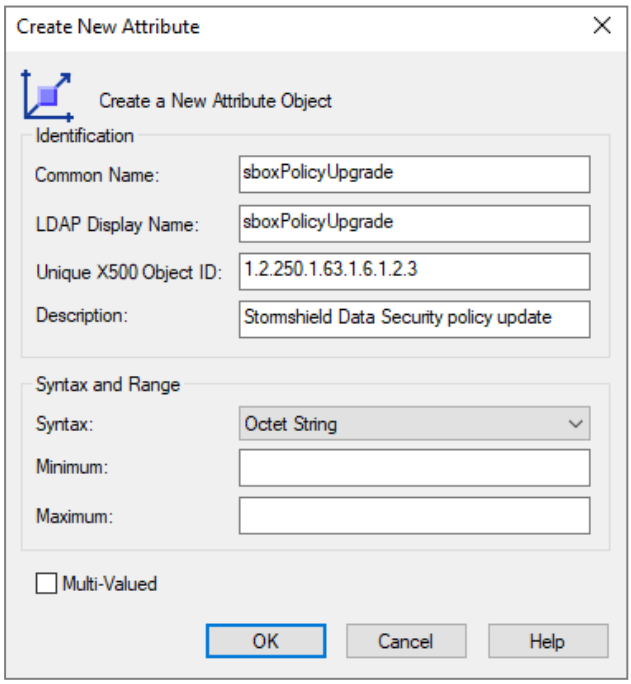


2. Dans le dossier **Schéma Active Directory**, ajoutez un nouvel attribut.

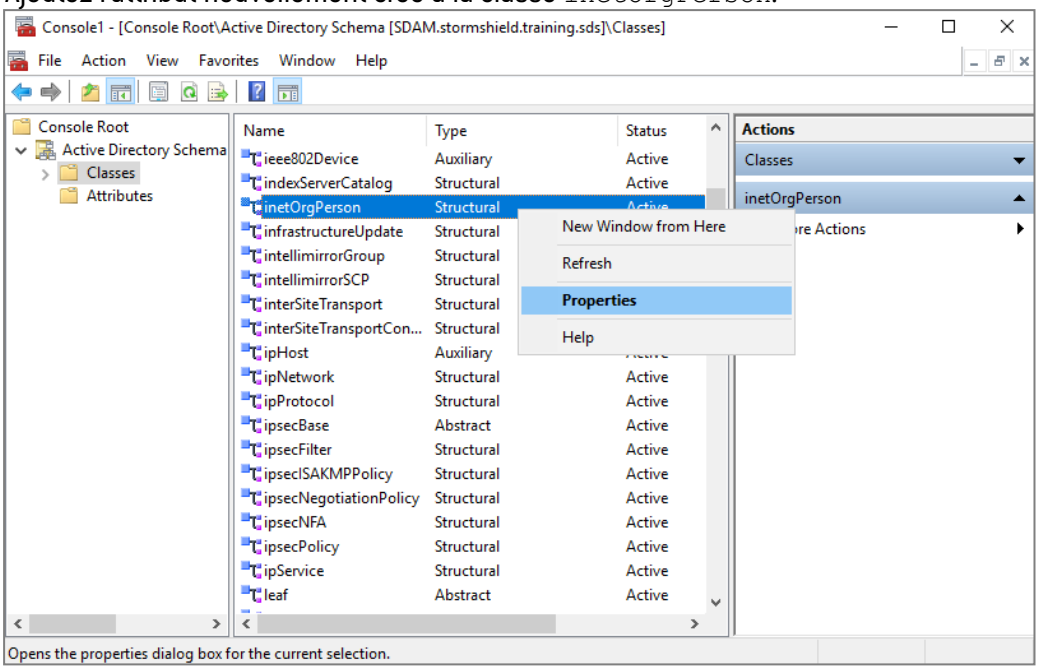


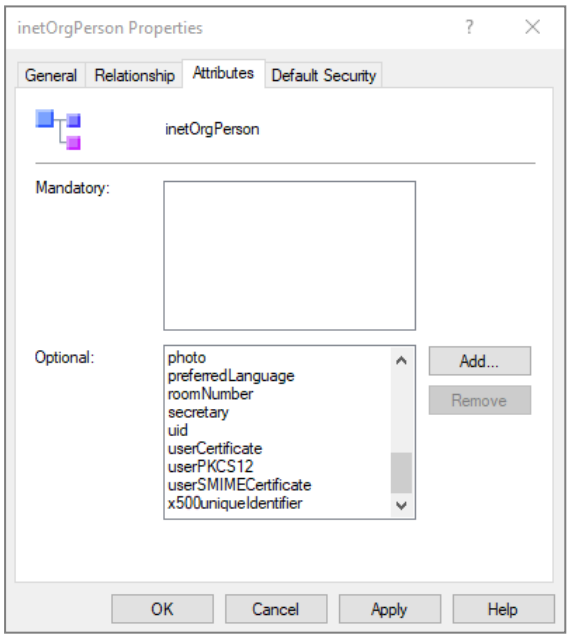
3. Remplissez les champs puis cliquez sur **OK**.

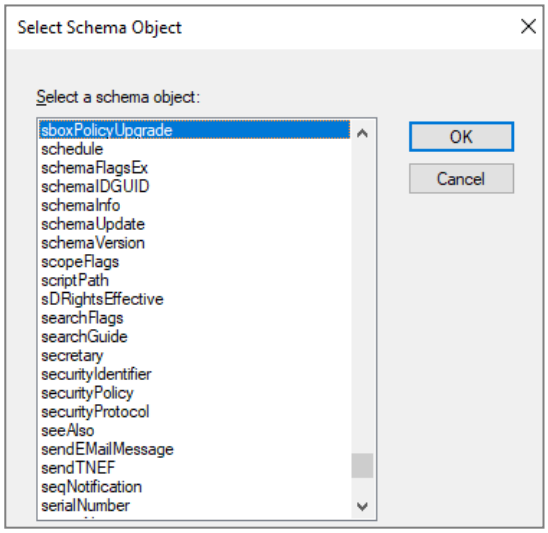
IMPORTANT
La création d'un attribut est définitive et un attribut ne peut être supprimé. Veillez donc à remplir correctement les champs.



4. Ajoutez l'attribut nouvellement créé à la classe `inetOrgPerson`.







E.3. Téléchargement des mises à jour

Le composant **Mise à jour automatique** doit être configuré pour télécharger automatiquement à la connexion une éventuelle mise à jour des politiques de sécurité. Dans Stormshield Data Authority Manager, la page de configuration de ce composant est disponible à partir de la page de configuration du composant Kernel, en cliquant sur le lien **Téléchargement des politiques de sécurité**.

Vous devez ajouter le point de distribution suivant :

```
ldap://<LDAP_server_name>:<LDAP_port>/<LDAP_entry_DN>?<security_policies_upgrade_attribute>
```

Où :

`<LDAP_server_name>`	est le nom du serveur LDAP (voir la section Serveur LDAP) ;
`<LDAP_port>`	est le port d'appel (voir la section Serveur LDAP) ;
`<LDAP_entry_DN>`	est le DN de l'entrée LDAP (défini plus haut) ;
`<security_policies_upgrade_attribute>`	est le nom de l'attribut dans lequel on publie (défini plus haut).

Annexe F. Publication et téléchargement des mises à jour de sécurité à l'aide du serveur Web

Stormshield Data Authority Manager permet de publier dans un dossier des mises à jour des politiques de sécurité. Il permet aussi de configurer le composant "Mise à jour automatique" pour que Stormshield Data Security télécharge les mises à jour publiées.

F.1. Publication des mises à jour

Que ce soit pour un utilisateur (voir la section Diffusion des comptes utilisateurs) ou pour un modèle, la publication par fichier de la mise à jour est proposée lors de la diffusion de celle-ci, si l'option est cochée dans les paramètres généraux (voir la section intitulée « Publication des mises à jour de politiques de sécurité »).

Le dossier **<USX_publication_dir>** dans lequel les fichiers de mises à jour sont copiés est défini dans les paramètres généraux.

F.2. Configuration du serveur Web IIS

Un serveur de fichier doit être configuré pour permettre le téléchargement des fichiers publiés dans le dossier **<USX_publication_dir>**.

1. Dans le **Gestionnaire des services Internet (IIS)**, déroulez l'arborescence du serveur puis celle des **Sites**.
2. Cliquez avec le bouton droit sur le site web créé pour le produit Stormshield Data Authority Manager ; sélectionnez ensuite **Ajouter un répertoire virtuel…**.
3. Dans l'assistant, saisissez un alias `<USX_publication_alias>` de préférence sans espace ; puis sélectionnez le chemin d'accès physique au dossier **<USX_publication_dir>**. Validez en cliquant sur **OK**.
4. Placez-vous sur le répertoire virtuel nouvellement créé, puis double-cliquez sur **Mappages de gestionnaires**.
5. Dans la colonne de droite, cliquez sur le lien **Modifier les autorisations de fonctions**.
6. Cochez **Lecture** puis validez.
7. Double-cliquez sur **Types MIME**.
8. Dans la colonne de droite, cliquez sur le lien **Ajouter…**, puis saisissez `usx` dans **Extension du nom de fichier** et `application/octet-stream` dans **Type MIME**. Validez en cliquant sur **OK**.

F.3. Téléchargement des mises à jour

Le composant **Mise à jour automatique** doit être configuré pour télécharger automatiquement à la connexion une éventuelle mise à jour des politiques de sécurité. Dans Stormshield Data Authority Manager, la page de configuration de ce composant est disponible à partir de la page de configuration du composant Kernel, en cliquant sur le lien **Téléchargement des politiques de sécurité**.

Vous devez ajouter le point de distribution suivant :

```
http://<hostname>/<USX_publication_alias>/<UserId>.usx
```

Où :

`<hostname>`	est soit le nom de la machine hébergeant le serveur, soit `<adresseIP>:<port>` en utilisant le port d'accès au site web créé pour le produit Stormshield Data Authority Manager ;
`<USX_publication_alias>`	est l'alias du répertoire virtuel (défini plus haut) ;
`<UserId>`	est l'identifiant de l'utilisateur.

Annexe G. Publication et téléchargement des CRL

Stormshield Data Authority Manager permet de publier des CRL dans un annuaire LDAP et/ou sur un serveur Web. Nous vous recommandons de configurer des points de distribution sur les deux types de serveurs.

Il permet aussi de configurer le composant « Contrôleur de révocation » pour que Stormshield Data Security télécharge les CRL publiées.

Les deux étapes suivantes sont nécessaires pour définir les points de publication des CRL :

1. Configurer l'annuaire LDAP et le serveur Web IIS,
2. Indiquer les points de distribution dans Stormshield Data Authority Manager.

IMPORTANT
Nous vous recommandons de générer les certificats des utilisateurs après avoir défini les points de distribution de CRL.

G.1. Configuration de l'annuaire LDAP et du serveur Web IIS

G.1.1. Annuaire LDAP

L'attribut CRL `certificateRevocationList` est standard : il est supporté par la classe `cRLDistributionPoint` (RFC 4523).

```
( 2.5.4.39 NAME 'certificateRevocationList'
           DESC 'X.509 certificate revocation list'
           EQUALITY certificateListExactMatch
           SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

( 2.5.6.19 NAME 'cRLDistributionPoint'
           DESC 'X.509 CRL distribution point'
           SUP top STRUCTURAL
           MUST cn
           MAY ( certificateRevocationList $
                 authorityRevocationList $ deltaRevocationList ) )
```

L'entrée LDAP dans laquelle la CRL est publiée doit donc dériver de cette classe.

Comme indiqué dans la norme, `;binary` doit être présent à la fin du nom de l'attribut dans sa définition dans Stormshield Data Authority Manager et dans le point de distribution.

Annuaire Active Directory

Ajoutez d'abord l'objet organizationalUnit dans le Schéma Active Directory afin de pouvoir stocker la CRL dans une unité organisationnelle (la procédure pour ajouter le composant logiciel Schéma Active Directory est indiqué dans l'annexe Publication et téléchargement des mises à jour de sécurité à l'aide d'un annuaire LDAP) :

1. Dans le Schéma de l'Active Directory, dépliez les classes,
2. Faites un clic droit sur la classe `cRLDistributionPoint` et ouvrez le menu **Propriétés**,
3. Affichez l'onglet **Relation**,
4. Cliquez sur **Ajouter une classe supérieure**,
5. Ajoutez organizationalUnit et validez,
6. Fermez le schéma Active Directory.

Ajoutez ensuite l'objet cRLDistributionPoint dans l'unité organisationnelle de l'Active Directory :

1. Dans **Démarrer**, **Outils d'administration**, sélectionnez **ADSI Edit**,
2. Dépliez l'arborescence de l'annuaire,
3. Dans l'unité organisationnelle choisie pour stocker la CRL, faites un clic droit et sélectionnez **Nouveau** > **Objet**,
4. Sélectionnez cRLDistribution Point,
5. Entrez un nom pour l'objet puis validez.

G.1.2. Serveur Web IIS

Configurez un serveur de fichier pour permettre le téléchargement des CRL publiées automatiquement dans le dossier **<CRL_publication_dir>** du serveur Stormshield Data Authority Manager.

1. Dans le **Gestionnaire des services Internet (IIS)**, déroulez l'arborescence du serveur puis celle des **Sites**.
2. Faites un clic droit sur le site web créé pour le produit Stormshield Data Authority Manager ; sélectionnez ensuite **Ajouter un répertoire virtuel…**.
3. Dans l'assistant, saisissez un alias `<CRL_publication_alias>` de préférence sans espace ; puis sélectionnez le chemin d'accès physique au dossier **<CRL_publication_dir>**.
4. Validez.
5. Placez-vous sur le répertoire virtuel nouvellement créé, puis double-cliquez sur **Mappages de gestionnaires**.
6. Dans la colonne de droite, cliquez sur le lien **Modifier les autorisations de fonctions**.
7. Cochez **Lecture**.
8. Décochez **Script** puis validez.

G.2. Configuration dans Stormshield Data Authority Manager

Pour plus d'informations sur les paramètres concernant les listes de révocation, reportez-vous à la section Listes de révocation (CRLs).

G.2.1. Publication des CRL

Dans le cas de l'utilisation d'un annuaire LDAP, pour que Stormshield Data Authority Manager publie automatiquement les CRL sur l'annuaire :

1. Dans Stormshield Data Authority Manager, cliquez sur **Paramètres** sur la page d'accueil,
2. Cliquez sur **Gestion des certificats**,
3. Dans le champ **DN LDAP de publication des CRLs** de la partie **Listes de révocation (CRLs)**, entrez le DN du point de distribution que vous venez de créer à l'étape précédente. Tant que ce paramètre est rempli et que l'annuaire LDAP est bien configuré, toute CRL générée par Stormshield Data Authority Manager est automatiquement publiée dans l'entrée LDAP correspondant au DN indiqué ici. Pour plus d'informations, reportez-vous à la section Configuration LDAP.

Dans le cas de l'utilisation d'un serveur Web IIS, la page de téléchargement a déjà été configurée à l'étape précédente.

G.2.2. Téléchargement des CRL

Inclusion automatique de la CRL dans les certificats

Le composant « Annuaire » du produit Stormshield Data Security permet de contrôler la validité des certificats des clés de l'utilisateur en téléchargeant automatiquement une éventuelle CRL pour chaque certificat de la chaîne de parenté des certificats à valider. Le résultat de ce contrôle de validité et de ces éventuels téléchargements de CRL est visible dans le composant « Contrôleur de révocation ».

Pour que ce travail soit possible, il faut que chaque certificat contienne un point de distribution de CRL permettant de vérifier sa validité.

Ainsi, dans Stormshield Data Authority Manager, pour chaque base, il faut que chaque certificat généré par l'autorité de certification de la base contienne le point de distribution dans lequel l'autorité de certification publie ses CRL.

- Ajoutez vos points de distribution dans le paramètre **Points de distribution des CRLs**. Dès qu'il est renseigné, ils sont automatiquement inclus dans le champ **CrlDistributionPoint** des certificats générés.

  Dans le cas d'une publication dans l'annuaire LDAP, le point de distribution est :

```
ldap://<LDAP_server_name>:<LDAP_port>/<LDAP_entry_
DN>?certificateRevocationList;binary
```

  Où :

`<LDAP_server_name>`	est le nom du serveur LDAP (voir la section Serveur LDAP) ;
`<LDAP_port>`	est le port d'appel (voir la section Serveur LDAP) ;
`<LDAP_entry_DN>`	est le DN de l'entrée LDAP (défini plus haut).

Configuration du composant Contrôleur de révocation

Pour pallier l'absence de point de distribution de CRL dans les certificats d'un utilisateur, le composant **Contrôleur de révocation** peut être configuré pour télécharger automatiquement des éventuelles CRL à la première utilisation après la connexion.

1. Dans Stormshield Data Authority Manager, cliquez sur **Gestion des utilisateurs** sur la page d'accueil,
2. Cliquez sur **Modèles**>Nom du modèle,
3. Dans le menu **Composants** du bandeau supérieur, cliquez sur **Stormshield Data kernel**,
4. Cliquez sur le lien **Contrôleur de révocation**.

Il est conseillé de définir dans la liste des émetteurs toutes les autorités constituant la chaîne de parenté, en définissant évidemment pour chacune au moins un point de distributions de CRL. Un bouton permet d'ajouter spécifiquement à la liste l'autorité de la base. Dans le cas d'une publication dans l'annuaire LDAP, le point de distribution est celui défini précédemment.

Annexe H. Autorité de certification racine

L'autorité de certification racine est certifiée par elle-même. Son certificat est "auto-certifié", sa gestion nécessite en conséquence quelques compléments d'information.

H.1. Renouvellement du certificat

Le renouvellement du certificat de l'autorité racine étant une opération rarement effectuée, Stormshield Data Authority Manager ne propose pas une fonctionnalité dédiée à cette tâche.

Le renouvellement peut être effectué de la manière suivante :

- générez une demande de certificat pour la clé de l'autorité de certification (pas de renouvellement du sujet) (voir la section Demande de certificat) ;
- déposez à cette autorité de certification sa demande de certificat (voir la section Dépôt d'une demande de certificat avancé) ;
- validez la demande de certificat (voir la section Demande de certificat) et exportez la valeur du certificat obtenu (voir la section Affichage de certificat) ;
- importez ce nouveau certificat pour la clé de l'autorité de certification (voir la section Importation d'un nouveau certificat).

H.2. Renouvellement du certificat avec modification de son identité

Il est possible de modifier l'identité de l'autorité de certification racine, c'est-à-dire de mettre à jour le sujet de son certificat.

NOTE
Cette opération est lourde de conséquences si vous n'avez pas positionné systématiquement un `AuthorityKeyIdentifier` dans tous les certificats générés, ou si le certificat de l'autorité ne possède pas de `SubjectKeyIdentifier`. En effet, dans ce cas, la relation de parenté entre les certificats émis et l'autorité est obtenue par comparaison du sujet de l'émetteur des certificats avec le sujet de l'autorité. Cette relation sera cassée si le sujet de l'autorité est modifié, et il sera alors nécessaire de :

- renouveler les certificats "fils". Un seul niveau est nécessaire, c'est-à-dire, le plus couramment, les certificats des sous-autorités certifiées par l'autorité racine ;
- diffuser la nouvelle chaîne de parenté auprès de tous les certificats émis par l'ensemble de "l'arborescence de certification" (des sous-autorités aux utilisateurs finaux).

Le renouvellement du certificat avec modification de l'identité peut être effectué de la manière suivante :

- générez une demande de certificat pour la clé de l'autorité de certification (pas de renouvellement du sujet) (voir la section Demande de certificat) ;
- déposez à cette autorité de certification sa demande de certificat (voir la section Dépôt d'une demande de certificat avancé) ;
- dans la page de validation de la demande (voir la section Demande de certificat), modifiez le sujet en saisissant dans le DN proposé la nouvelle identité ;
- validez la demande de certificat et exportez la valeur du certificat obtenu (voir la section Affichage de certificat) ;

- importez ce nouveau certificat pour la clé de l'autorité de certification (voir la section Importation d'un nouveau certificat)

A cette étape, le sujet du certificat contient la nouvelle identité, et l'émetteur du certificat contient l'ancienne identité. Il n'est pas considéré comme auto-certifié, il n'est donc pas utilisable en l'état.

Il suffit de le certifier à nouveau :

- générez une demande de certificat pour la clé de l'autorité de certification (pas de renouvellement du sujet) ;
- déposez à cette autorité de certification sa demande de certificat ;
- validez la demande de certificat sans modifier le sujet et exportez la valeur du certificat obtenu ;
- importez ce nouveau certificat pour la clé de l'autorité de certification.

Le nouveau certificat est bien considéré comme auto-certifié, le sujet et l'émetteur possédant tous les deux la nouvelle identité.

H.3. Révocation du certificat

Le certificat de l'autorité de certification racine apparaît dans la liste des certificats émis par l'autorité (voir la section Affichage et traitement des certificats émis).

A partir de la page de ce certificat, il est possible de le révoquer (voir la section Gestion des listes de révocations (CRL)).

IMPORTANT
Révoquer le certificat de l'autorité de certification racine invalide toutes les chaînes de parenté issues de cette autorité.

Annexe I. Contenu d'un certificat émis par la PKI

Cette annexe présente le contenu d'un certificat émis par la PKI de Stormshield Data Authority Manager. Tous les attributs et extensions proposés par la PKI sont présents.

```
SEQUENCE :
   SEQUENCE :
      CONTEXT SPECIFIC (0) :
         INTEGER : 2
      INTEGER : 5
      SEQUENCE :
         OBJECT IDENTIFIER : sha1withRSAEncryption [1.2.840.113549.1.1.5]
         NULL : ''
      SEQUENCE :
         SET :
            SEQUENCE :
               OBJECT IDENTIFIER : commonName [2.5.4.3]
               PRINTABLE STRING :
                  'CA ROOT'
         SET :
            SEQUENCE :
               OBJECT IDENTIFIER : localityName [2.5.4.7]
               PRINTABLE STRING :
                  'LYON'
         SET :
            SEQUENCE :
               OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
               PRINTABLE STRING :
                  'SI'
         SET :
            SEQUENCE :
               OBJECT IDENTIFIER : organizationName [2.5.4.10]
               PRINTABLE STRING :
                  'ARKOON'
         SET :
            SEQUENCE :
               OBJECT IDENTIFIER : countryName [2.5.4.6]
               PRINTABLE STRING :
                  'FR'
      SEQUENCE :
         UTC TIME : '0911191620582'
         UTC TIME : '1111191620582'

      SEQUENCE :
         SET :
            SEQUENCE :
               OBJECT IDENTIFIER : commonName [2.5.4.3]
               PRINTABLE STRING :
                  'Foureux Pierre'
         SET :
            SEQUENCE :
               OBJECT IDENTIFIER : surname [2.5.4.4]
               PRINTABLE STRING :
                  'Foureux'
```

```
      SET :
         SEQUENCE :
            OBJECT IDENTIFIER : givenName [2.5.4.42]
            PRINTABLE STRING :
               'Pierre'
      SET :
         SEQUENCE :
            OBJECT IDENTIFIER : localityName [2.5.4.7]
            PRINTABLE STRING :
               'LYON'
      SET :
         SEQUENCE :
            OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
            UTF8 STRING :
               'R&D'
      SET :
         SEQUENCE :
            OBJECT IDENTIFIER : organizationName [2.5.4.10]
            PRINTABLE STRING :
               'ARKOON'
      SET :
         SEQUENCE :
            OBJECT IDENTIFIER : countryName [2.5.4.6]
            PRINTABLE STRING :
               'FR'
      SET :
         SEQUENCE :
            OBJECT IDENTIFIER : emailAddress [1.2.840.113549.1.9.1]
            IA5 STRING :
               'pfoureux@arkoon.net'
   SEQUENCE :
      SEQUENCE :
         OBJECT IDENTIFIER : rsaEncryption [1.2.840.113549.1.1.1]
         NULL : ''
      BIT STRING UnusedBits:0 :
         SEQUENCE :
            INTEGER :
               00B36AE27B97D69E490A438AB355666233A9ADFE94
               D28389C0B5F468BD5DAC2FBD5A9EC18730C52C320B
               6B41136A552045922338C6F6C580234A0572ABCA10
               28B14D39CF05E81A49892155BF65FAF7898BF7B313
               A0FEEB1A3E58C23F6C06383A5E610951B6D62D1478
               E4FAD37D57767B74F28869F32CD1CCF176810E88C6
               1E04E7
            INTEGER : 65537
   CONTEXT SPECIFIC (3) :
      SEQUENCE :
         SEQUENCE :
            OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
            OCTET STRING :
               SEQUENCE :
                  CONTEXT SPECIFIC (0) :
                     C2B7D055F0CC0B2545D813CE26A7011967AD
                     13C6
   SEQUENCE :
      OBJECT IDENTIFIER : subjectKeyIdentifier [2.5.29.14]
      OCTET STRING :
         OCTET STRING :
            ECD1033DA6AE8411303B6A78826AE0F9E8CDF73
            7
   SEQUENCE :
      OBJECT IDENTIFIER : keyUsage [2.5.29.15]
      BOOLEAN : 'ÿ'
      OCTET STRING :
         BIT STRING UnusedBits:7 :
            FF80
```

```
            SEQUENCE :
               OBJECT IDENTIFIER : subjectAltName [2.5.29.17]
               OCTET STRING :
                  SEQUENCE :
                     CONTEXT SPECIFIC (1) :
                        'test@'
                     CONTEXT SPECIFIC (2) :
                        'pFoureux'
                     CONTEXT SPECIFIC (7) :
                        0A0A0A0A
                     CONTEXT SPECIFIC (0) :
                        OBJECT IDENTIFIER : szOID_NT_PRINCIPAL_NAME [1.3.6.1.4.1.311.20.2.3]
                        CONTEXT SPECIFIC (0) :
                              UTF8 STRING :
                                    'ID44712'
            SEQUENCE :
               OBJECT IDENTIFIER : basicConstraints [2.5.29.19]
               BOOLEAN : 'ÿ'
               OCTET STRING :
                  SEQUENCE :
                     BOOLEAN : 'ÿ'
                     INTEGER : 6
            SEQUENCE :
               OBJECT IDENTIFIER : extKeyUsage [2.5.29.37]
               OCTET STRING :
                  SEQUENCE :
                     OBJECT IDENTIFIER : emailProtection [1.3.6.1.5.5.7.3.4]
                     OBJECT IDENTIFIER : clientAuth [1.3.6.1.5.5.7.3.2]
                     OBJECT IDENTIFIER : serverAuth [1.3.6.1.5.5.7.3.1]
             SEQUENCE :
                OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
                OCTET STRING : ''
                   SEQUENCE :
                      SEQUENCE : ''
                         CONTEXT SPECIFIC (0) :
                            CONTEXT SPECIFIC (0) :
                               CONTEXT SPECIFIC (6) :
                                  'ldap://Srv2k3.lyon2k3.labs:'
                                  '389/cn=CRL,dc=test,dc=Arkoo'
                                  'n?certificateRevocationList'
                                  ';binary'
                      SEQUENCE :
                         CONTEXT SPECIFIC (0) :
                            CONTEXT SPECIFIC (0) :
                               CONTEXT SPECIFIC (6) :
                                  'file:server/sharing/folder/'
                                  'file.crl'
SEQUENCE :
   OBJECT IDENTIFIER : sha1withRSAEncryption [1.2.840.113549.1.1.5]
   NULL : ''
BIT STRING UnusedBits:0 :
   2CDA469A61040735433422DA2DAE860877BE0959FD18FF3B648DBF
   9477773931 10C765D1FC0D82CA7E6DC9BB0A50EAC3A02C8810663D
   06DC9A752A72285CAD662DCC48CA50D7EFDF583AC24FA05BAADE9A
   A990A2F2347955AF9DBE98E02BE87744321B707253C2AC38CA43BC
   1E5953E1D09455D0BCBCFB1946E95223FCF78DAF2E7096ABFEB1F7
   2DF8791469A458AF0F3C7A433E92A6FD1523C28B3F7310FD396031
   14FEE8616FA2432354586D5FC228C6DAD29C7DE45B4B3F71B9C411
   576A4E8CFD3352FA26B9724A4B3F4DCBD273E90101279B709F1EC7
   0F58D009B22D6F635FA3618029C3CB922637FD4CFE37ABCCA689CE
   F2C53B8D8A24BCC462CC27991B
```

Annexe J. Démarrage d'une base de données avec PowerShell

L'outil *SBMSTART.EXE* contenu dans le dossier **Outils** du dossier d'installation de Stormshield Data Authority Manager permet de démarrer et d'arrêter une base de données. Dans certains cas, vous devrez utiliser un script PowerShell pour contrôler la commande *SBMSTART.EXE*. C'est le cas si le mot de passe de la base contient des caractères non ASCII par exemple.

1. Créez un fichier portant l'extension *.ps1* et contenant la commande suivante :

```
& "C:\Program Files\Arkoon\Security BOX Authority
Manager\Tools\SBMSTART.exe" "/O" "-b" "<id_de_base>" "-p" "<mot_
de_passe>"
```

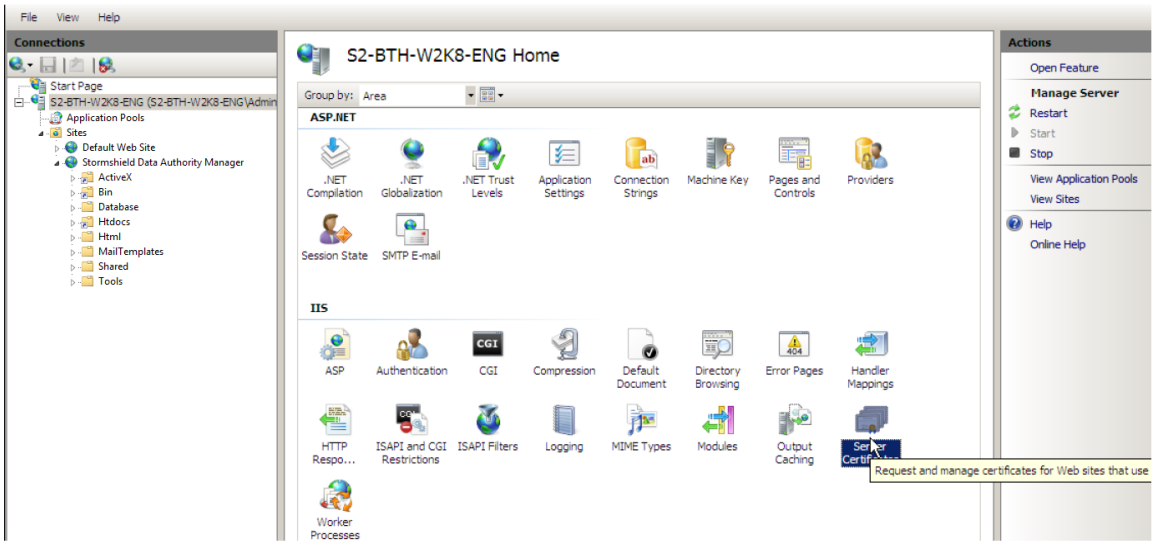
   - Le caractère "&" en début de commande indique à PowerShell que la chaîne de caractères qui suit est une commande à exécuter.
   - Chaque paramètre est entouré de guillemets pour éviter une mauvaise interprétation des paramètres PowerShell.

2. Avant la première exécution du script, entrez la commande suivante dans PowerShell : `Set-ExecutionPolicy Unrestricted`. Elle permet d'autoriser l'exécution du script sur la machine pour tous les utilisateurs. Cette autorisation peut être restreinte à l'utilisateur courant en ajoutant l'argument `-Scope CurrentUser` à la commande.
3. Pour lancer l'exécution du script, il existe deux possibilités :
   - Faites un clic droit sur le fichier et sélectionnez **Exécuter avec PowerShell**.
   - Ouvrez PowerShell et renseignez le chemin vers le script (par exemple : "C:\Users\foobar\Desktop\sbmstart.ps1") ou bien glissez-déposez le fichier, puis appuyez sur Entrée.

Annexe K. Activation du protocole HTTPS sur Stormshield Data Authority Manager

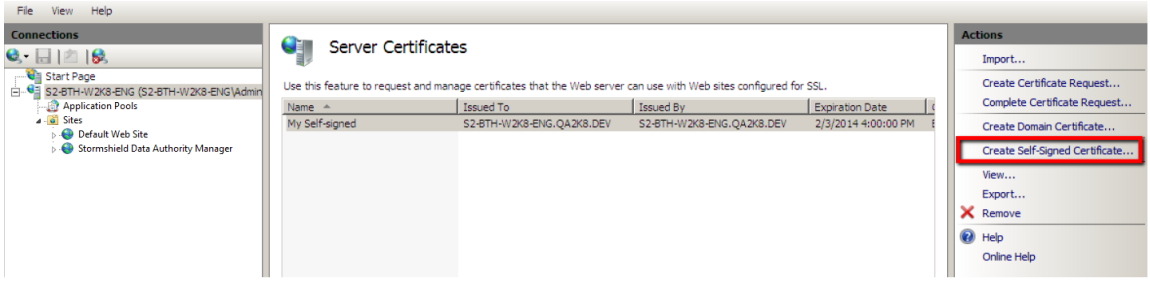
Pour activer le protocole HTTPS sur Stormshield Data Authority Manager, suivez la procédure suivante :

1. Cliquez sur **Démarrer, Panneau de configuration, Outils d'administration** puis ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Il est nécessaire d'indiquer un certificat à utiliser. Pour cela, cliquez sur **Certificats de serveur** sur la page d'accueil.

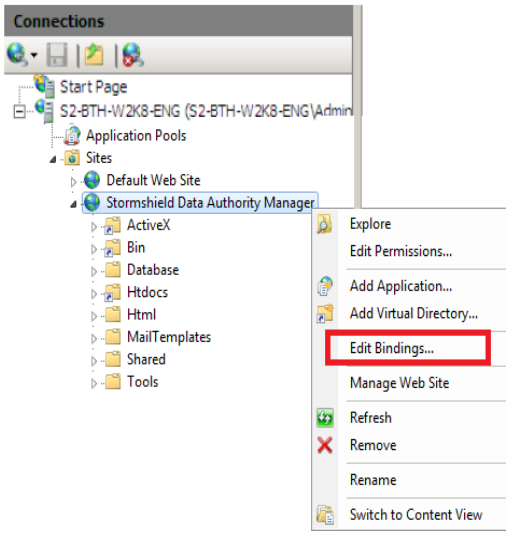


3. Pour créer un certificat, cliquez sur le lien **Créer un certificat auto-signé** sur le panneau de droite. Cette option permet de ne pas avoir à générer un certificat sur une PKI externe et à l'importer dans IIS avec sa parenté. Une fois créé, le certificat est visible dans la liste **Certificats de serveur**.

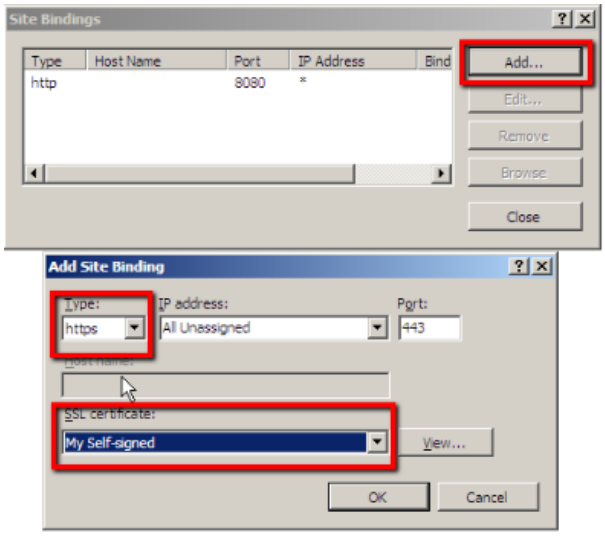
Si l'on souhaite générer le certificat avec une PKI externe, il faut créer un modèle de certificat SSL qui aura pour usages Chiffrement de clé (éventuellement Chiffrement de données également) et Authentification serveur.



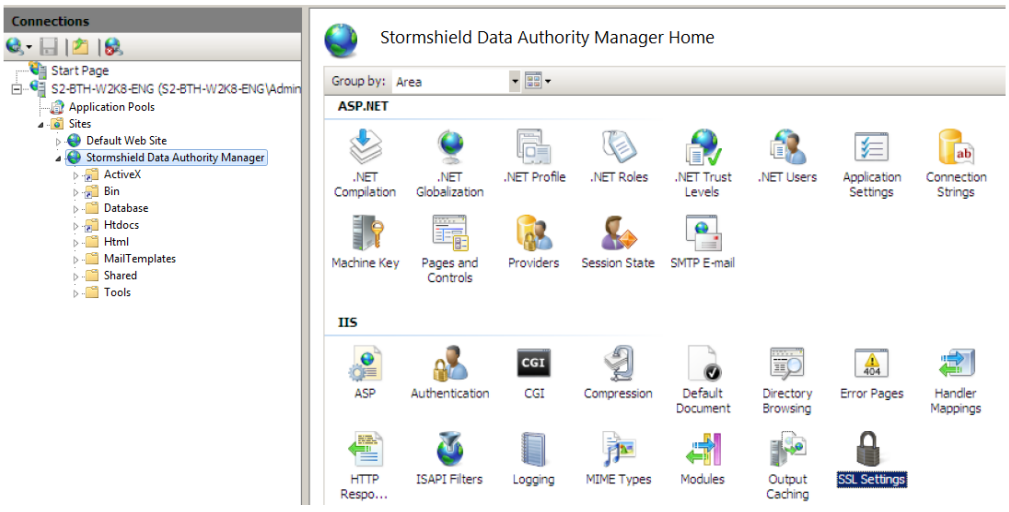
4. Ensuite, il faut signaler que le site Stormshield Data Authority Manager doit pouvoir être atteint en HTTPS. Faites un clic droit sur le site dans l'arborescence de gauche et sélectionnez **Modifier les liaisons**.



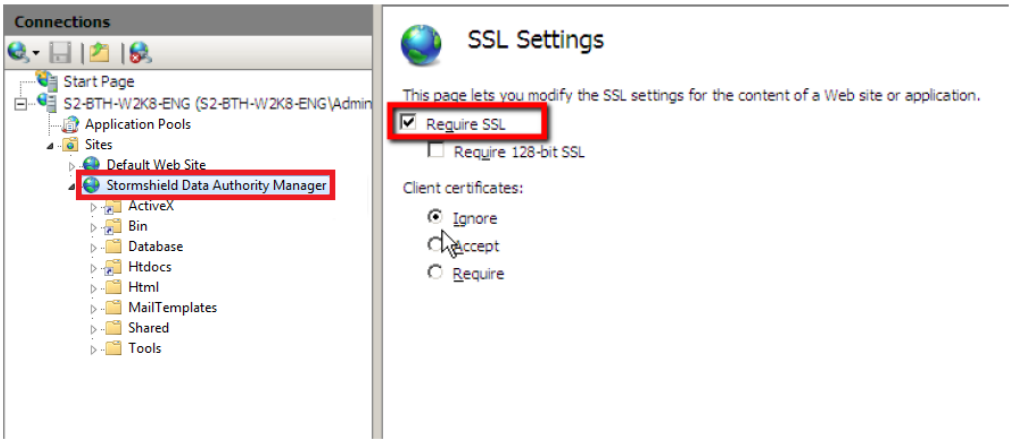
5. Dans la fenêtre **Liaisons de sites**, cliquez sur **Ajouter**. Dans la fenêtre suivante, sélectionnez **https** dans le champ **Type** et choisissez le certificat généré précédemment dans le champ **Certificat SSL**. Cliquez sur **OK**.



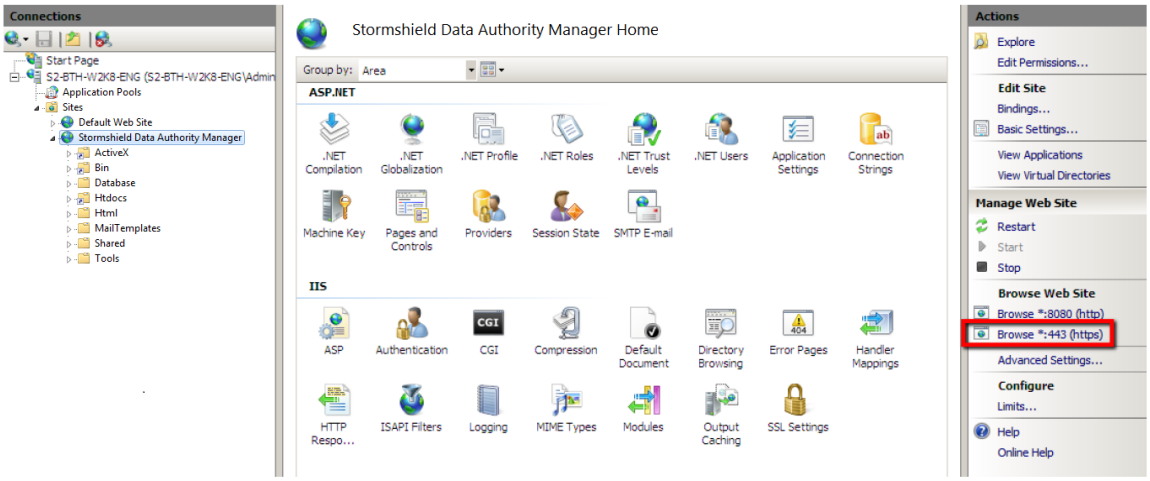
6. De retour sur la page d'accueil, sélectionnez **Paramètres SSL**. Le site Stormshield Data Authority Manager doit être sélectionné dans l'arborescence à gauche.



7. Cochez la case **Exiger SSL**.

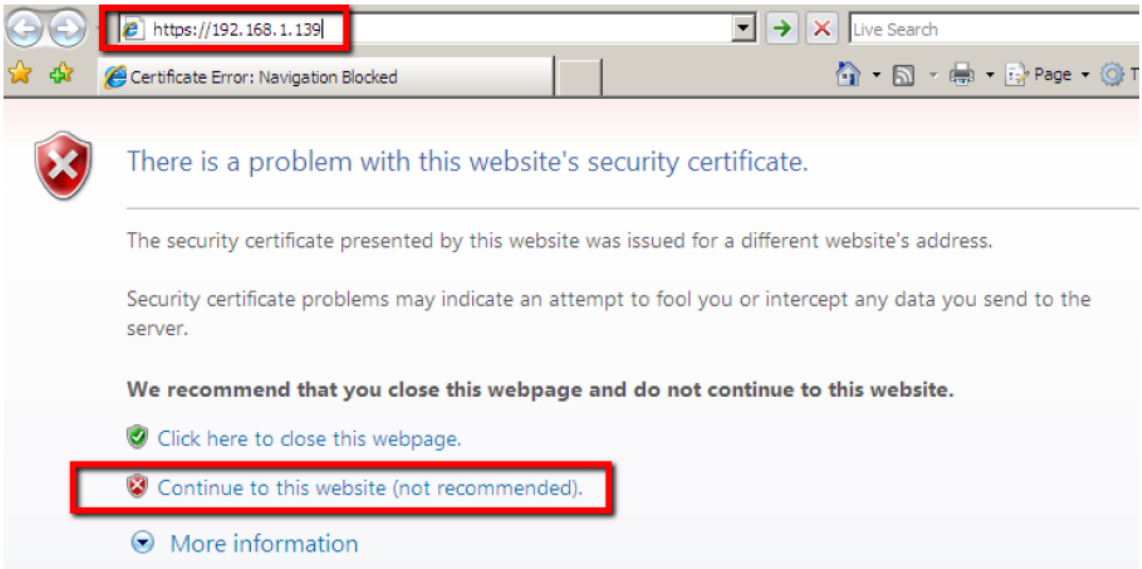


8. Pour tester que la procédure a fonctionné, dans le panneau de droite **Actions** cliquez sur **Parcourir *:443 (https)**.



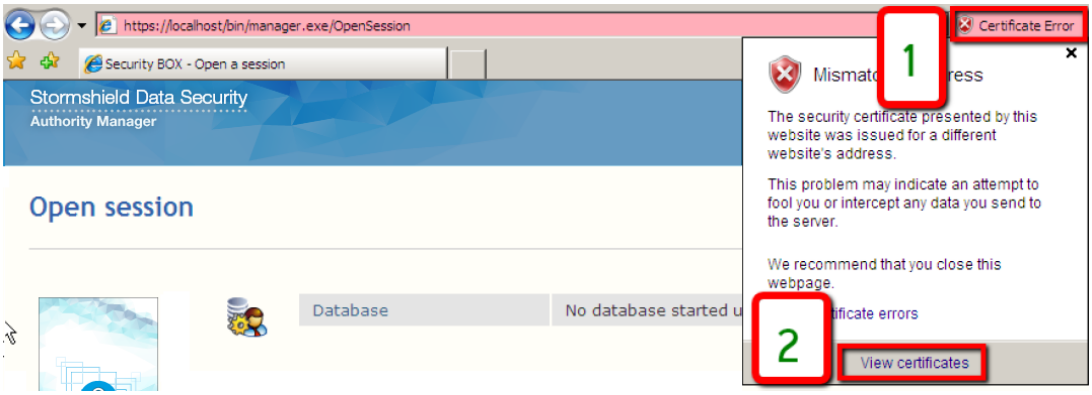
9. Le navigateur Internet Explorer s'ouvre. Attention, l'adresse https dans la barre d'adresse est incomplète. Il faut y ajouter **/bin/manager.exe/Opensession**.

Le nouveau certificat n'étant pas dans le magasin de certificats d'Internet Explorer, l'avertissement suivant s'affiche :

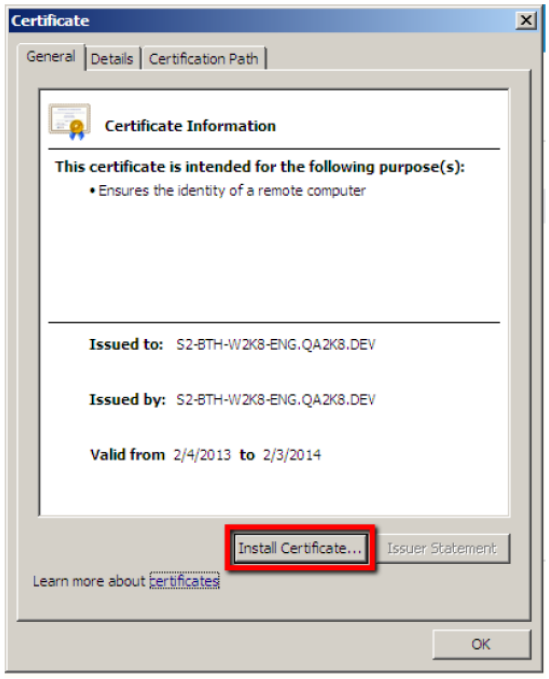


Cliquez sur **Poursuivre avec ce site Web (non recommandé)**.

10. Pour que cet avertissement ne s'affiche plus, importez le certificat au préalable ou bien cliquez sur **Erreur de certificat** puis sur **Afficher les certificats**.



11. Installez le certificat.



Annexe L. Sauvegarde/restauration des bases de données

Suivez les procédures suivantes pour sauvegarder et restaurer vos bases de données.

L.1. Sauvegarde

1. Arrêtez toutes les bases de données et le service sbasrv (avec la commande `net stop sbasrv`).
2. Sauvegardez le fichier **<sdam_install_dir>\SBMData**.
3. Sauvegardez le dossier **<sdam_data_install_dir>\SBMData**.

L.2. Restauration

1. Arrêtez toutes les bases de données et le service sbasrv (avec la commande `net stop sbasrv`).
2. Restaurez le fichier *bases.ini* dans le dossier **<sdam_install_dir>**.
3. Restaurez le dossier **<sdam_data_install_dir>\SBMData**.
4. Démarrez le service sbasrv (avec la commande `net start sbasrv`) et toutes les bases.

Si le chemin **<sdam_data_install_dir>** n'est pas identique à celui défini lors de la sauvegarde, il faudra mettre à jour les chemins définis dans le fichier **<sdam_install_dir>\bases.ini** (données BasePath et KSPath). Il faudra également vérifier la configuration de Stormshield Data Authority Manager car le chemin <sdam_data_install_dir> peut être référencé dans les paramètres (par exemple dans la page **Paramètres > Gestion des utilisateurs**). Il est donc conseillé de garder le même chemin pour le dossier **<sdam_data_install_dir>** lors de la restauration.

documentation@stormshield.eu