GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

INSTALLATION AND IMPLEMENTATION GUIDE

Version 10.1.1

Document last update: February 08, 2023

Reference: sds-en-sds_suite-installation_guide-v10

Table of contents

In the documentation, Stormshield Data Security Enterprise is referred to in its short form: SDS.

Preface

About this guide

This document provides essential information on the use of Stormshield Data Security Enterprise.

Audience

This guide is intended for:

- system administrators who want to install Stormshield Data Security Enterprise
- software users who wish to protect confidential files

1. Use environment

To use Stormshield Data Security Enterprise under the conditions of the Common Criteria evaluation and of the french qualification at standard level, it is essential to observe the following guidelines.

1.1 Recommendations on security watch

1. Regularly check security alerts provided on https://advisories.stormshield.eu/.
2. Always apply the software update if it contains a security breach correction. These updates are available on your customer area MyStormshield.

1.2 Recommendations on keys and certificates

1. RSA keys of users and certification authorities must be a minimum size of 4096 bits, with a public exponent strictly greater than 65536.
2. The certificates and CRLs must be signed with the SHA-512 algorithm.

1.3 Recommendations on algorithms

1. Stormshield Data Security supports several algorithms but recommends using AES 256, RSA 2048 and SHA 512.
2. Triple DES, RC4 and RC5 algorithms are supported too.
3. RC2 and DES algorithms are supported for compatibility but we recommend not using them because of known weaknesses.

1.4 Recommendations on user accounts

1. The user accounts must be protected by the AES encryption algorithm and SHA-256 cryptographic hash standard.
2. Passwords should be subject to a security policy preventing weak passwords.
3. Appropriate organizational measures must ensure the authenticity of templates from which the user accounts are created.
4. In case of using a hardware key ring (smart card or hardware token), this device protects the confidentiality and integrity of keys and certificates that it contains.

1.5 Recommendations on workstations

1. The workstation on which Stormshield Data Security is installed must be healthy. There must be an information system security policy whose requirements are met on the workstations. This policy shall verify the installed software is regularly updated and the system is protected against viruses and spyware or malware (firewall properly configured, antivirus updates, etc.).

2. The security policy should also consider that the workstations not equipped with Stormshield Data Security do not have access to shared confidential files on a server, so that a user can not cause a denial of service by altering or removing inadvertently or maliciously, files protected by the product.
3. Access to administrative functions of the workstation system is restricted only to system administrators.
4. The operating system must manage the event logs generated by the product in accordance with the security policy of the company. It must for example restrict read access to these logs to only those explicitly permitted.
5. The user must ensure that a potential attacker can not see or access the workstation when the Stormshield Data Security session is open.

1.6 Recommendations on files encryption

The files encryption algorithm must be AES.

1.7 Recommendations on administrators

1. The security administrator responsible for defining the security policy on the workstation or via Stormshield Data Authority Manager is considered as trusted.
2. The system administrator responsible is considered as trusted. He/She is responsible for the installation and maintenance of the application and workstation (operating system, protection software, PKCS#11 interface library with a smart card, desktop and engineering software. He/She applies the security policy defined by the security administrator.
3. The product user must respect the company's security policy.

1.8 Certification and qualification environment

The software modules evaluated in the context of the EAL 3+ Common Criteria Certification and of the qualification of Stormshield Data Security are:

1. The component "Transparent encryption" (Stormshield Data Team), including the definition of security rules, the encryption of files according to these rules, and the encryption of the system exchange file (swap).
2. The "Stormshield Data kernel", common to all Stormshield Data Security modules, including the authentication of the user, monitoring the inactivity of the workstation, managing a reliable certificates directory and controlling the non-recovation of used certificates.
3. The internal software cryptographic module (Stormshield Data Crypto), managing the user keys which are stored in a file (software implementation) or on a smart card.

However the following modules are beyond the evaluation scope:

1. Stormshield Data Authority Manager administration tool.
2. The possible smart card and its middleware PKCS#11.

2. Installing Stormshield Data Security

This chapter describes how to install and uninstall Stormshield Data Security.

2.1 Required configuration

For the required configuration, refer to the section **Compatibility** of the Stormshield Data Security 10.1.1 Release Notes.

> **NOTE**
> The product installation while connected to Windows with a domain user account is impossible for a domain user if the User Account Control is enabled because the elevation of privilege does not work.

2.2 Downloading Stormshield Data Security

Stormshield Data Security products are distributed through our Customer area. This area allows you to view and download:

- different software versions and patches of Stormshield Data Security;
- footprint installation packages to verify their authenticity.

To read the documentation of the product, please visit our Stormshield Technical Documentation website.

2.3 Checking Stormshield Data Security authenticity

Stormshield Data Security software is available in two formats:

- a Windows Installer package (.msi)
- or a self-extracting executable file (.exe)

To check the authenticity of one of these packages:

- calculate the SHA-256 using a tool of your choice
- verify that the fingerprint is identical to that published on the Customer Area

The self-extracting file can also be verified using digital signature:

1. In the Explorer, right-click on the file .exe and select Properties.
2. Click Digital signatures and select the line Stormshield.
3. Click Details.

2.4 Installing Stormshield Data Security

You should have a license key, given to you depending on the acquired user's rights when the product was ordered. This license key is requested during setup.

To run the installation of Stormshield Data Security, you must have administrator rights on the PC and this operation can be done from an *.exe* or *.msi* file. To install from the *.msi* packet, use a command line window. For more information, refer to next section.

NOTE
You cannot install Stormshield Data Security 10.1.1 over a version strictly previous to Security BOX 8.0.3. In this case, first uninstall the old version before installing 10.1.1 version.

Before installing the Stormshield Data Mail component, please install or update the desired version of Microsoft Outlook.

To update the version 8.0.5 of Security BOX Suite to the version 10.1.1 of Stormshield Data Security, the version 8.0.5 must be completely uninstalled with a dedicated script before installing version 10.1.1. This script is available from the Stormshield Data Security support. For more information, please contact Stormshield Data Security support.

2.5 Files requested for the installation procedure

The basic installation procedure comprises the following files available from the customer area MyStormshield.

TIP
x86 : 32-bit package
x64 : 64-bit package

SDS_Suite_10.0.000xx_ENU_Release_x86_setup SDS_Suite_10.0.000x_ENU_Release_x64_setup	Standalone packages to install the product and the prerequisites.
SDS_Suite_10.0.000xx_ENU_Release_x86 SDS_Suite_10.0.000xx_ENU_Release_x64	msi packages to install the product. These packages require the “SQL Server Compact Edition” prerequisite.
SSCERuntime-ENU	msi 32/64 bits packages of SQL Server Compact Edition 4.0 prerequisite.
VSTO Runtime 40 x86 Office 2010 VSTO Runtime 40 x64 Office 2010	*exe* 32/64-bit packages of Visual Studio 2010 Tools for Office Runtime prerequisite. This package is necessary only for the installation of Stormshield Data Mail Outlook Edition component.

Two modes of installation are available for each 32 and 64-bit version:

- Interactive mode: the standalone mode using the setup. Click on the file *xxx setup.exe* to launch the installation in interactive mode. It is Stormshield Data Security 10.1.1 default installation mode.
  Once you entered the license key and accepted the license contract, you can install all the components allowed by the license key.
- Silent mode: there is no user interaction. This mode uses the *msi* package. The installation of the SSCE (SQL Server Compact Edition) package and, for Stormshield Data Mail Outlook Edition component, of the VSTO Runtime 4.0 Office 2010 package is required. It is then possible to install the package as administrator with Windows Installer commands. If the product is not installed with administrator's rights, the installation will fail (error 1925).

For example:

```
msiexec /qn /i "<path>Stormshield Data Security 10.X"
LICENCENUM=<licensenumber>
```

where `<license number>` shall be ABCDEFGHABCDEFGH (16 attached characters).

You must launch this command in a command line window open as administrator.

The possible variants are:

- `/qn` installation with no screen
- `/qn+` same `/qn` with a final confirmation screen
- `/qb` installation with a screen with a progress bar and the estimate remaining time
- `/qb+` same `/qb` with a final confirmation screen

In silent mode, the procedure installs all the applications authorized by the license. Thanks to the private property `REMOVE` (refer to section Setting the applications preselection), it is possible to limit the applications installed.
Once the installation finished, Stormshield Data Security automatically starts each time you start Windows.

NOTE
The `/norestart` command is not supported. To prevent the computer from restarting, create a *.mst* with the relevant options.

2.6 Setting the applications preselection

Thanks to the private property REMOVE, it is possible to limit the applications installed by the user, even if the license key authorizes others.

For example, you can create several installation profiles with only one license key and one installation package.

Below is the list of possible values:

Code	Deleted product
SBoxFile	Stormshield Data File
SBoxDisk	Stormshield Data Virtual Disk
SBoxShredder	Stormshield Data Shredder
SBoxMailOutlookAddIn	Stormshield Data Mail Edition Outlook
SBoxMailNotes	Stormshield Data Mail Edition Notes
SBoxTeam	Stormshield Data Team
SBoxExtCarte	Stormshield Data Card Extension
SBoxSign	Stormshield Data Sign
SBoxConnector	Stormshield Data Connector

When defining the value of the REMOVE property, the different components whose installation is not authorized must be separated by a comma and there is no space.

The <SBOXLICENCENUM> license key allows the installation of all Stormshield Data Security components. The following command line deletes Stormshield Data File and Stormshield Data Virtual Disk.

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

IMPORTANT
You must launch this command in a command line window open as administrator.

2.7 Uninstalling Stormshield Data Security

1. Open the **Control Panel**.
2. Select **Programs and features**.
3. From the list of programs, select Stormshield Data Security.
4. Click on **Uninstall**.
5. Follow the on-screen instructions.

You can also use the Setup command of the installation pack which gives you the choice to install, uninstall and modify the list of components installed on your PC.

2.8 Applying a patch

A patch of Stormshield Data Security 10.1.1 presents itself as a major release of the product. Stormshield Data Security uses the mechanism of a "major upgrade" of Windows Installer. Therefore, installing a patch is identical to installing the original version.

Example:

1. Installing 9.1xxxx Release version

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

2. Installing 9.1yyyy patch version

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

2.9 Stormshield Data Security installation information

Once you have completed the Stormshield Data Security installation, you can view a summary of your installation from the About Stormshield Data Security window.

To view the information, right-click the Stormshield Data Security icon in the system tray and select the About Stormshield Data Security item.

Use the scroll bar to view all the Stormshield Data Security components installed on your PC.

3. Getting started with Stormshield Data Security

This chapter is intended to user accounts protected by password. If you use a smartcard or USB token to identify and connect to Stormshield Data Security, refer to chapter **Installing the card extension (smart card and USB token)**.

3.1 Introduction

After installation, Stormshield Data Security will start automatically every time you start Windows.

In order to use any of the components of Stormshield Data Security you will need to log on to Stormshield Data Security, and to have an "account" which contains your configuration parameters, your access key, as well as the trusted address book containing your contacts with their public keys. When you connect (or "log on") to Stormshield Data Security, your account is opened, which allows you to use any installed component in the software suite either simultaneously or alternately.

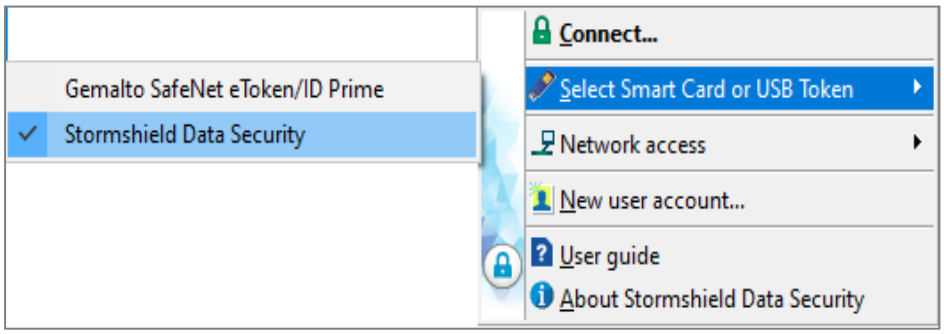
Stormshield Data Security software is multi-user software. However, only one user may use the software per open session. Several users can use the same computer maintaining individual and secured configurations insofar as the user environment is concerned. If the user wishes to create different profiles, they must be linked to different Stormshield Data Security accounts.

3.2 Stormshield Data Security menu

Right-click the Stormshield Data Security icon on the right of your Windows system tray to see the menu Stormshield Data Security.

This icon is grayed out when you are not connected, red when the Stormshield Data Security session is locked or green when you are connected.

Right-click this icon to open the Stormshield Data Security menu.



The Stormshield Data Security menu items displayed depends on the different parameters set up during configuration, such as actions for connecting/disconnecting, locking/unlocking, etc.

3.3 You already have a Stormshield Data Security account

All software products in the Stormshield Data Security product line use the same encryption engines. You only need to log on once: you may then use any of the software components without changing from one user account to another.

If you already have an account from another component in Stormshield Data Security, you do not need to create another account.

Your Stormshield Data Security account is not deleted when you uninstall an version of Stormshield Data Security older than 7.2 version.

This file must however typically be moved to: C:\ProgramData\Arkoon\Security BOX\Users.

If you are migrating from a previous version, the user accounts are automatically migrated to the new folder. However, if you later want to add an old account, you must put it into the new folder manually.

3.4 Creating an account

You can create a Stormshield Data Security account either:

- by creating or generating a key or two keys;
- by importing a PKCS#12 key.

If you are creating an account with two keys, according to the security and certification policies set up by administrators, you can use both methods (one for each key).

3.4.1 Creating a key

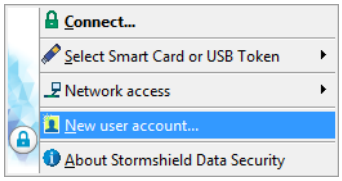
To create an account, you must create a key, which will be used, for example, to secure your files and messages. The key created is self-certified, so that it can be used immediately by the software. However, it is not automatically trusted by the correspondents and it may be certified by a certification authority later.

You can create two separate keys to encrypt and sign. You will have to follow the procedure below twice.

If you want to retrieve a security key saved to a file (in PKCS12 or PFX format), refer to Section 3.4.2, "Importing a PKCS#12 key".

To create a key:

1. Open the Stormshield Data Security menu, and choose **New User Account**.



2. Select **Account with password**.
3. Choose the type of account you want to create from the drop-down menu:

- use two different keys for encryption and signing (we advise that you use this setting if you use another Stormshield Data Security component for your electronic signature)
- use same key for encryption and signing
- use one key to encrypt only
- use one key to sign only

The rest of this procedure explains how to create an account that uses just one key for encryption and signing (a personal key). If you want to use two different keys, the steps described below apply to both the encryption key and the signing key.

4. Click **Create an account**, and skip the welcome screen.
5. Enter your identifier and your password, which are both requested before you can connect to Stormshield Data Security.

The number of characters used for the identifier creation is limited to 28.

You can check the password you entered by clicking the eye icon next to your password.

6. Proceed to the next screen.
7. Select the **Generate your personal key** radio button, and select the type and length of your key.
8. Click **Next**.
9. From the following window, you can generate your security key using a random number.

To generate this random number, do one of the following:

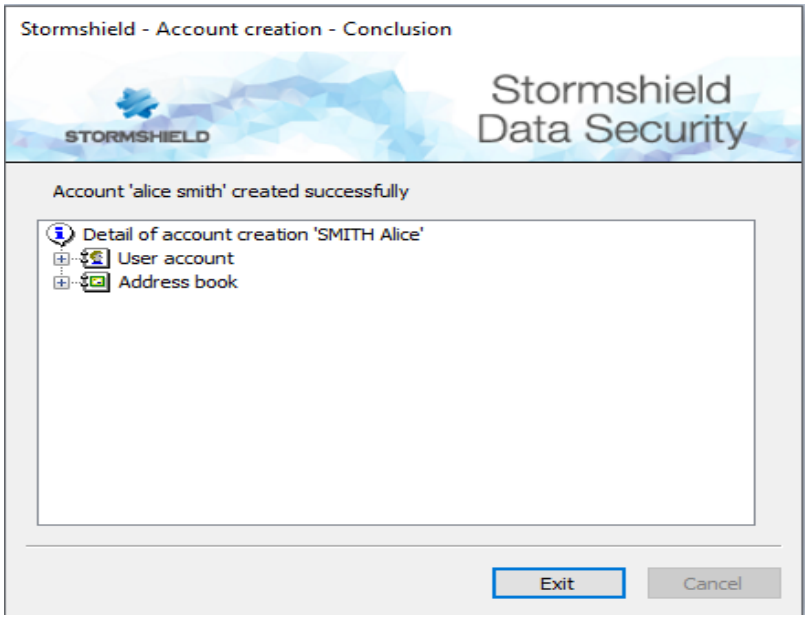
- Click in the square and move the mouse at random.
- Press F10 and move the mouse at random or type any random keys on your keyboard.

If you want to generate two separate keys for encryption and signing, you will need to repeat the last two steps (select Generate or, Import Generate Random).

10. Once the random number has been captured, proceed to the next screen.

Enter the personal details as you wish them to appear on your self-certified certificate. Only the fields with an asterisk are mandatory.

11. Proceed to the next screen.
12. Enter an optional Security Officer (backup) password. You will be asked for this password if you forget your main password or if you block your account by entering too many incorrect codes consecutively (see Section 8.8, "Unblocking your account").
13. Proceed to the next screen and check over the operation summary before creating your account. If necessary, return to any of the previous screens to edit incorrect information.
14. Click **Finish**. Stormshield Data Security generates your personal key and creates your account.



Your account can now be used.

NOTE

Your account folder name is your Stormshield Data Security account identifier (the identifier you provided previously under "Account creation, identification"). Since this folder contains your "keystore" (a file containing your keys and configuration settings) and your trusted address book, it is important that this folder be protected from potential deletion.

User accounts are stored in the path listed on the final window, as shown above. The path is typically something like:

C:\ProgramData\Arkoon\Security BOX\Users

Your account includes a personal "self-certified" certificate. Since you created this certificate yourself, it may not be trusted by some of your correspondents who only consider certificates created by known authorities as trustworthy. If you wish to have your key certified, or if such certification is required professionally, you may have your key certified by a certification authority (refer to section Certifying your key).

3.4.2 Importing a PKCS#12 key

This section explains how to create your account by retrieving a security key and certificate saved in a PKCS#12 file (with P12 or PFX extension).

This allows you to use a key (and associated certificate) that was generated previously or centrally by a PKI using a high grade random generator, or to store the private keys in order to perform recovery operations.

1. Open the Stormshield Data Security menu and choose New user account.
2. Select Account with password.
3. Choose the type of key you want to create from the drop-down menu:

- Use two different keys for encryption and signing (we advise that you use this setting if you use another Stormshield Data Security component for your electronic signature).
- Use same key for encryption and signing.
- Use one key to encrypt only.
- Use one key to sign only.

The rest of this procedure explains how to create an account that uses just one key for encryption and signing (a personal key). If you want to use two different keys, the steps described below apply to both the encryption key and the signing key.

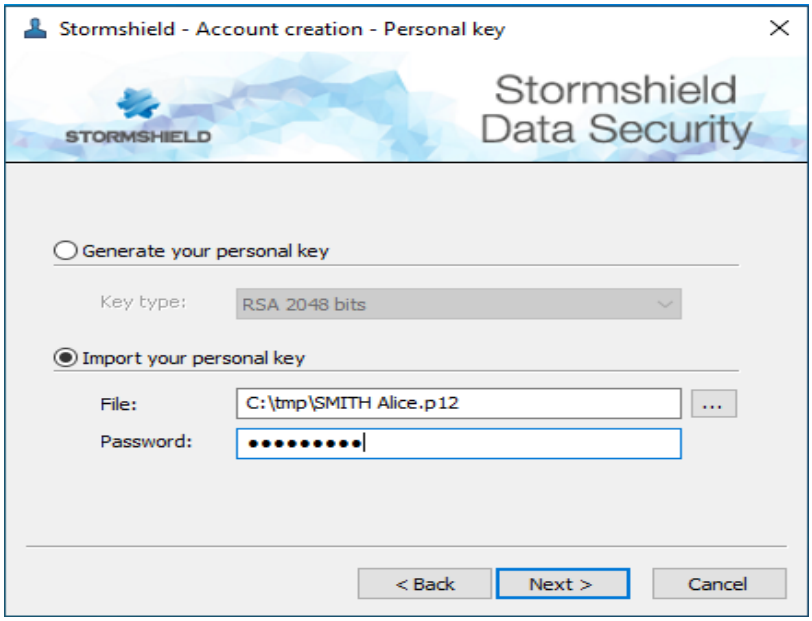
4. Click Create an account, and skip the welcome screen.
5. Enter your identifier and your password, which are both requested before you can connect to Stormshield Data Security.

You can check the password you entered by clicking the eye icon next to your password.

Click Next to proceed to the next screen.

6. Select Import your personal key, and:

- select the file. The whole path to the file containing the key and the associated certificate must be entered (format PKCS#12 with P12 or PFX extension).
- the password which protects the key stored in this file.



7. Proceed to the next screen.

If the file contains several keys or certificates, select the key to be imported and the certificate associated with this key.

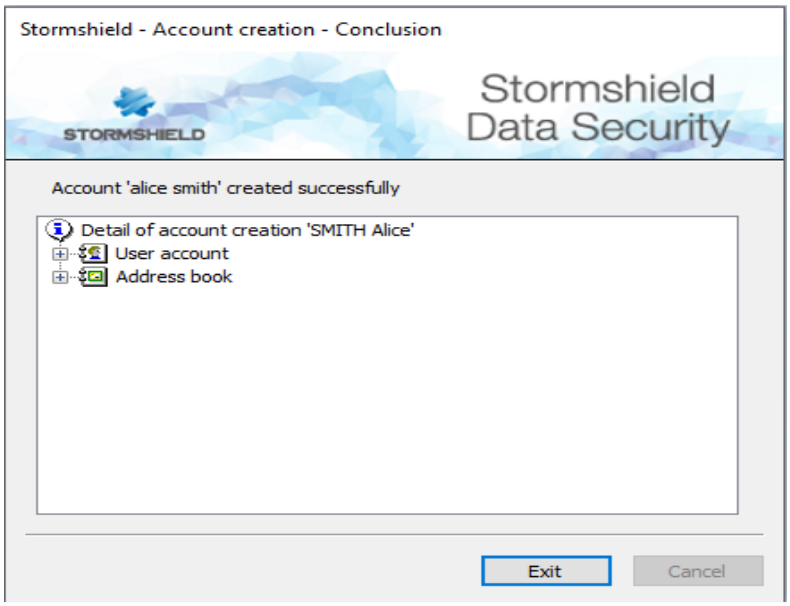
To display the certificate information, click on it, in the bottom pane.

To return to the list of certificates contained in the file, click .

- If the PKCS#12 file contains more than one key, Stormshield Data Security sorts them out to use the one which has a certificate compatible with the required uses (encryption, signature or both) according to the type of account to create.
- If more than one key is compatible, Stormshield Data Security displays them all in the bottom pane, and you must select the one you want to use. By default, Stormshield Data Security will choose the certificate which has the latest expiration date.
- If no key is compatible, Stormshield Data Security displays that no keys are available. You must create new keys. See Section 3.4.1, "Creating a key".

8. Click Next.
9. Enter an optional Security officer (backup) password. You will be asked for this if you forget your main password or if you block your account by entering too many incorrect codes consecutively (see Section 8.8, "Unblocking your account").
10. Proceed to the next screen and check the summary of your account. If necessary, return to any of the previous screens to edit incorrect information.
11. Click Finish.

Stormshield Data Security generates your personal key and creates your account. Your account may now be used.



CAUTION
Your account folder name is your Stormshield Data Security account identifier (the identifier you provided previously under "Account creation, identification"). Since this folder contains your "keystore" (a file containing your keys and configuration settings) and your trusted address book, it is important that this folder be protected from potential deletion.

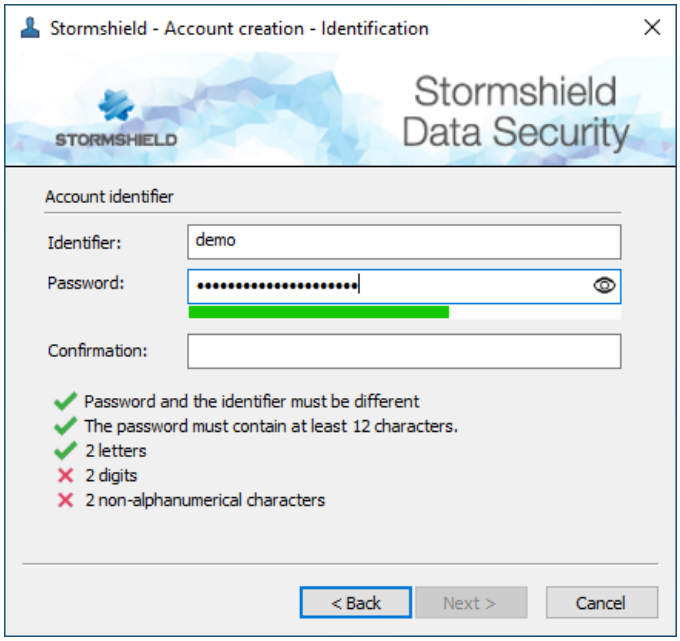
3.5 Information about your password

To ensure the confidentiality of your data, your password must comply with some rules:

- it should be reasonably long;
- it must be made up by a variety of characters (special characters and alphanumerical).

These rules are set in Stormshield Data Authority Manager. For more information, please refer to the section *Customizing the installation* in Stormshield Data Authority Manager guide.

When creating the account, Stormshield Data Security displays to rules to follow:



3.6 Connecting to Stormshield Data Security

When you connect to Stormshield Data Security, your identity is verified and your configuration settings are retrieved.

If several Windows sessions are opened at the same time, only one user can connect to Stormshield Data Security.

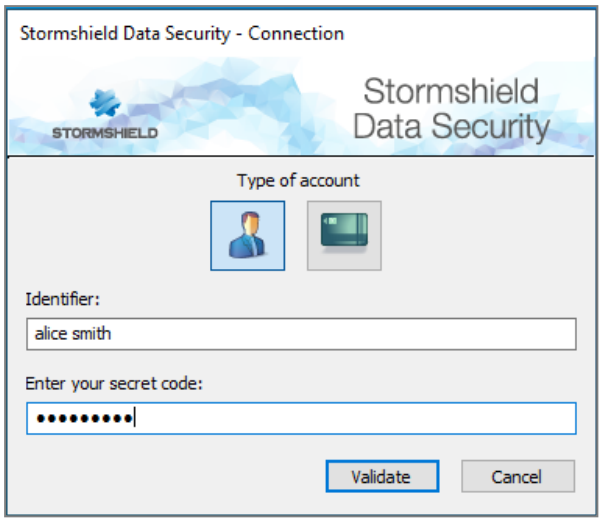
In smart card mode, insert the card to open the Stormshield Data Security menu. The connection window (step 2) directly opens if the card is already inserted in the reader. If you are using a virtual smart card, connect as shown below.

To connect to Stormshield Data Security:

1. Open the menu **Stormshield Data Security**.
2. Choose **Connect.**
3. Select the **Account type** with which you want to connect.

For a password account:

a. Enter your login and password:



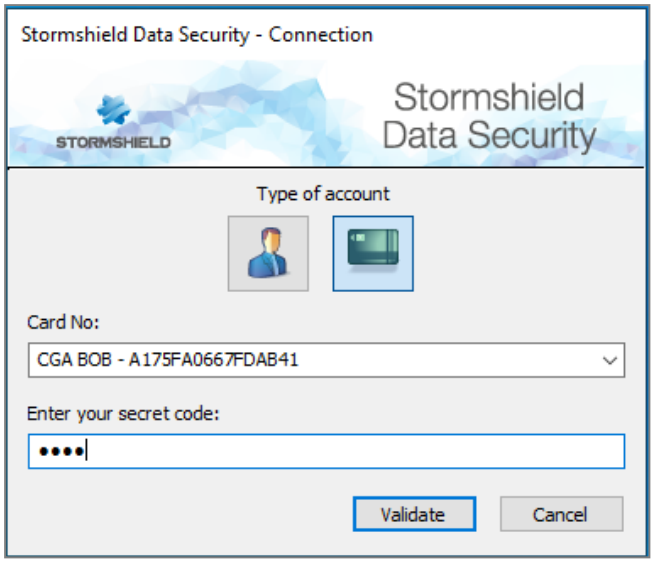
b. Click on **OK**.

c. If the login does not match any existing account, the password field and OK button remain disabled. In this case, refer to Creating an account.

By default, Stormshield Data Security suggests the login of the last connected user.

For a smart card account:

a. Select the card or token and enter your PIN:



b. Click on **OK**.

c. If the login does not match any existing account, <NO SDS ACCOUNT> will be added before it. Create an account in this case. Refer to Creating an account.

NOTE
If you enter your password incorrectly too many times (default is three tries), your account will be blocked. To unblock, refer to section Unblocking your account.

The person icon to the left of the user identifier field is only displayed once Stormshield Data Security finds the account corresponding to the identifier.

Once your connection has been validated, the Stormshield Data Security icon in the system tray turns green: .

You have just opened a Stormshield Data Security session. As long as you remain connected, you may access the Stormshield Data Security software components installed on your desktop (such as File, Virtual Disk, Shredder, Sign, Mail).

On a workstation, if no user has never been connected to Stormshield Data Security and if no Stormshield Data Security account exists, Stormshield Data Security provides a prior step to create a user account when run for the first time.

If you leave your workstation for some time, do not let your working session open. To do so, lock your Stormshield Data Security session (refer to the section Locking your session) or disconnect (refer to the section Disconnecting).

3.7 Disconnecting

Disconnection can be performed when the Stormshield Data Security account is available (green icon) or locked (red icon).

Disconnection involves completely closing your account.

You can set Stormshield Data Security to disconnect automatically, as described in Section 8.1.4, "Setting screen saver options".

Disconnecting could affect certain Stormshield Data Security components. Refer to the specific component documentation for more information.

The disconnection procedure is the same for both the password and card modes. After you disconnected, if you reinsert the card or token, you will access the connection screen.

To disconnect:

1. Open the Stormshield Data Security menu and select Disconnect.
2. The Stormshield Data Security icon in the system tray turns gray: 

> **NOTE**
> Closing the Windows session and stopping the system involves closing and stopping Stormshield Data Security.

3.8 Locking your session

Locking your session prevents access to your keys.

You can set Stormshield Data Security to lock automatically. See Section 8.1.4, "Setting screen saver options".

> **IMPORTANT**
> Locking your session could affect certain Stormshield Data Security components. For example, Access to data contained in encrypted files may no longer be possible. Refer to the specific component documentation for more information.

> **NOTE**
> The locking procedure is the same for both the password and card modes. Removing the card from the drive also permits to lock your session. By reinserting the card or token, you will directly access the unlocking screen.

To lock your Stormshield Data Security session:

1. Open the Stormshield Data Security menu and select Lock.
2. The Stormshield Data Security icon in the system tray turns red: 

It is now impossible to access your account.

3.9 Unlocking your session

> **NOTE**
> The unlocking procedure is the same for both the password and smart card modes. Reinsert the card in the drive to go to step 2 of the procedure.

To unlock your session:

1. Double-click on the red icon to open the Stormshield Data Security menu.
2. Enter your password or PIN.
3. Click on **Unlock**.
4. The Stormshield Data Security icon becomes green: 

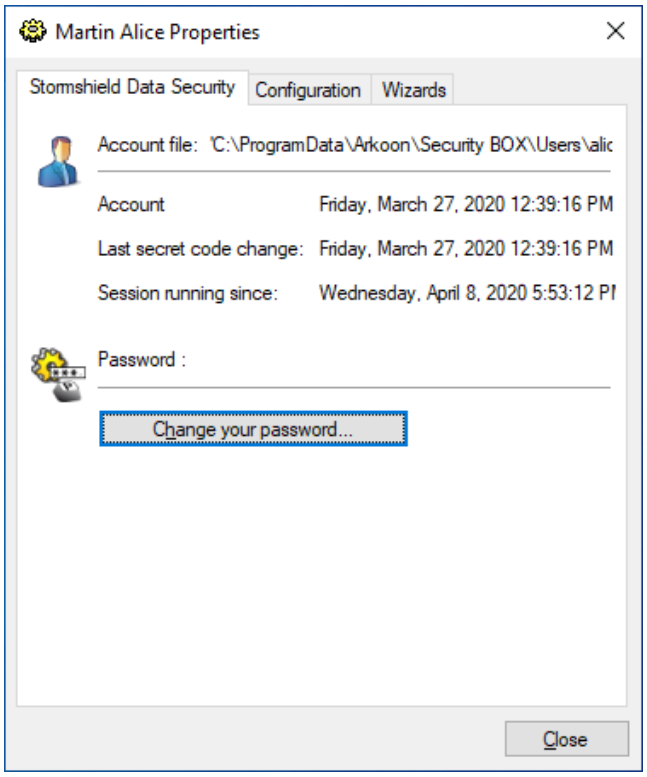
If your Stormshield Data Security account is blocked due to failed attempts to enter your password or PIN, a window appears to inform you that your account is blocked. You must first

log out from your account before trying to unblock it. An account cannot be unlocked if it is blocked. For instructions on unblocking the account, see Unblocking your account.

3.10 Changing your password

To change your password:

1. Open the **Stormshield Data Security** menu.
2. Select **Properties**.
3. Select the **Stormshield Data Security** tab.



4. Click **Change your password.**
5. In the following window, enter your current password and twice your new password.

If you click the eye icon in the New password field, you will see the password in plain text. It must comply with the rules displayed under the fields.

NOTE
Stormshield Data Security passwords are case sensitive.
For example, the secret code Smith-1 is not the same as smith-1.
Stormshield Data Security analyzes your password and estimates the strength. For more information, see section Information about your password.

4. Installing the card extension (smart card and USB token)

Although the basic version of Stormshield Data Security uses password authentication, you can use smart cards or USB tokens for stronger authentication. This chapter describes how to install Stormshield Data Security smart card extension to use these cards or tokens.

Not all USB keys can be used with Stormshield Data Security, namely USB keys that do not have active security functions cannot be used. The keys that can be used have security functions similar to smart cards. When referring to USB keys in this documentation, it implies keys with this level of security. This type of key will be referred to as a USB token.

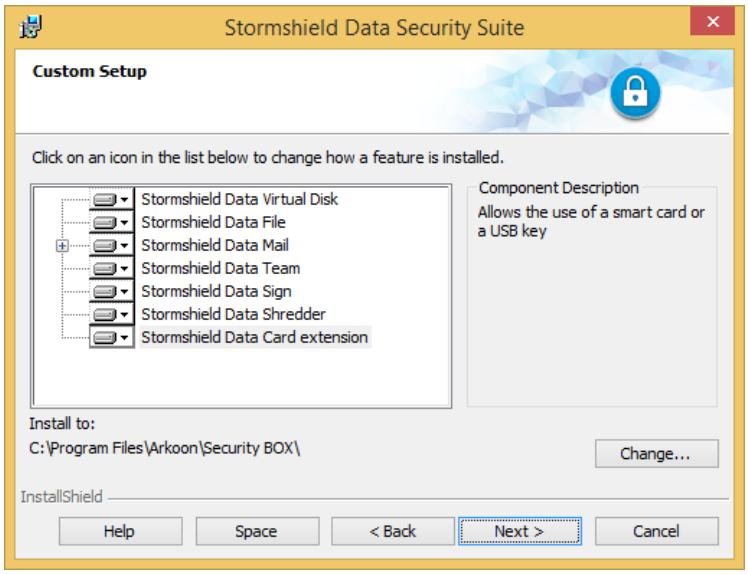
4.1 Installing the smart card extension

The smart card kit, associated reader and application must be installed and configured beforehand. If this is not the case, the smart card will not be automatically detected and will need to be run manually later. The Stormshield Data Security middleware is installed by default and can be used with plug-and-play cryptographic media. For more information, refer to the *Administration Guide*.

The Stormshield Data Security extension for smart cards and USB keys can be installed at the same time as the other components. Follow the procedure below for subsequent installations.

To install the Stormshield Data Security extension for smart cards and USB keys:

1. Open the **Start** menu in the task bar.
2. Open the **Control panel** and select **Add/Delete programs**.
3. From the list of programs, select the line that corresponds to Stormshield Data Security.
4. Click on **Change**. You will be in **Maintenance** mode.
5. Select **Modify** then go through the screens that follow.

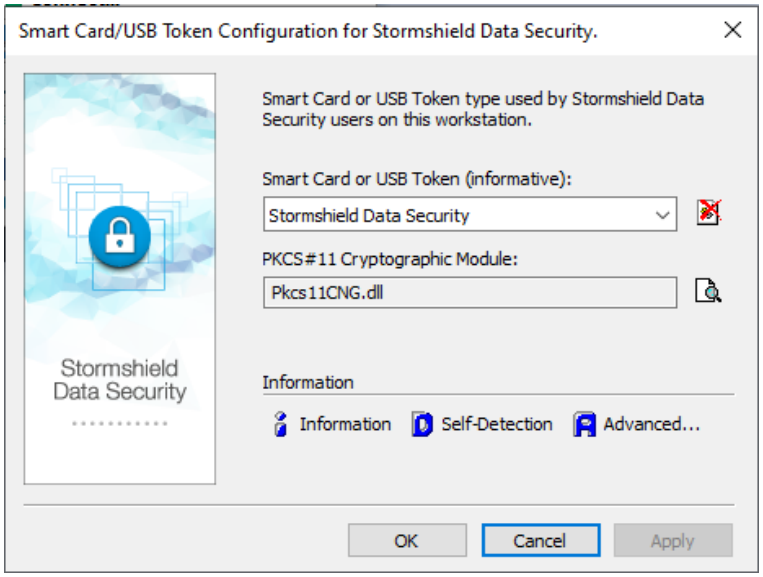


6. Select the Stormshield Data Security extension component for smart cards that you wish to install.

4.2 Configuring the smart card extension

You can specify in Stormshield Data Security the exact smart card or USB key model to use. To do so:

1. In the Windows task bar, select **Start** > **Stormshield Data Security**.
2. Open the **Card extension configurator**.
3. Click on **Self-Detection** so that Stormshield Data Security will automatically detect the right cryptographic module, then select your type of smart card or USB key from the pre-configured values:



4. If you do not find the middleware associated with your type of card from the list:

a. Enter the name of your smart card in the upper field. Click on the arrow on the right to see the list of supported readers/smart cards and select one.

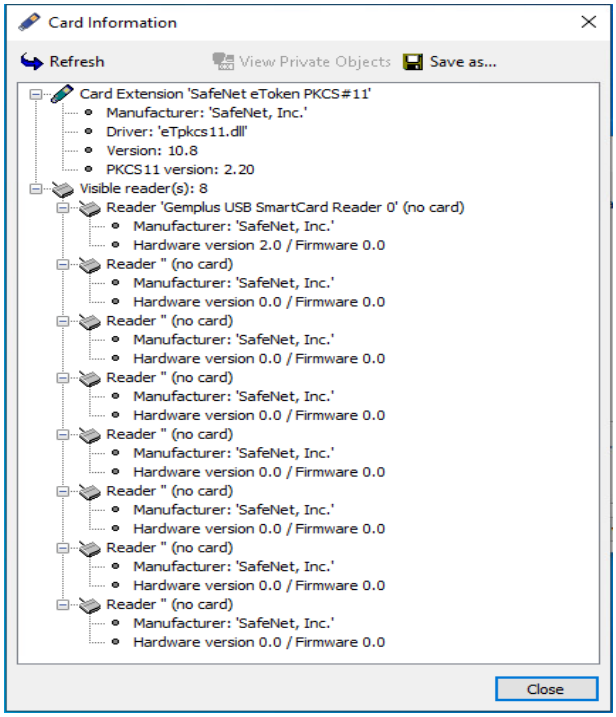
b. Enter the name of the DLL of the associated *PKCS#11* cryptographic interface module. The DLL must be accessible from any application on the system. So either an absolute path must be provided or the DLL must be located in the Windows system32 folder. The name of this `DLL PKCS#11` depends on the application that accesses the smart card/key and its version number. Refer to the vendor's documentation to find out this name.

Otherwise, you can use the Stormshield Data Security middleware offered in the list with all the cryptographic media compatible with Microsoft's CNG technology (plug-and-play).

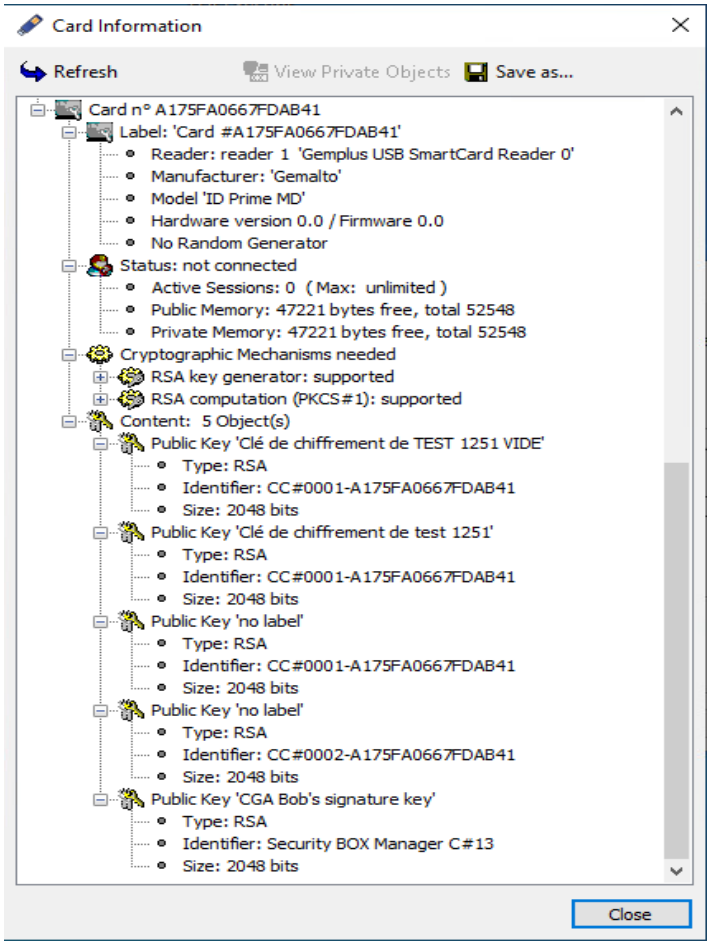
For the full list of smart cards and keys that Stormshield Data Security supports, get in touch with Stormshield Data Security's support department.

5. Click on **Information** to test the *PKCS#11* interface module: the number of readers detected is indicated. If the *PKCS#11* DLL cannot be reached, an error message will indicate it. In this case, simply verify the name and path of the DLL and verify whether the required items for this DLL are present (especially other DLLs).

- The following screen capture shows that the card extension exists and is configured for Gemalto smart cards. However, there are no actual USB keys;



- The following screen capture shows that a USB key is inserted and presents the key's characteristics as well as public objects such as public keys and certificates.



4.3 Viewing private objects

It is possible to view private objects (in particular private keys):

1. Click Information.
2. Select the line Status: not connected on the information window.
3. Click View private object. This button is not available if the previous line is not selected.
4. Enter the PIN code.

The Information window allows analyzing problems of access to cards.

The Save button allows saving the information listed in this window in a file. This file is often asked by the Support in case of problem of access to the smart card/USB key.

4.4 Creating an account for smart card or USB token

With a smart card or a USB token:

- your security key is embedded in the card (private key and public key);
- the calculations that operate your private key are carried out by the card (signing, decryption).

Creating your account involves creating your main key(s), which will be used for securing your files, volumes and messages, and self-certifying the key so that you can use it immediately.

To create an account, Stormshield Data Security can:

- certify a key created by your card or token
- re-use a key and certificate already present in the card or token
- create a new key and write it to the card or token, with its certificate

1. Right-click the Stormshield Data Security menu and choose **New user account**.
2. Select a **Smart Card/USB Token** account.
3. Select the smart card or USB token you wish to use.
4. From the drop-down menu select:
    - Use two different keys to encrypt and sign
    - Use same key to encrypt and sign
    - Use one key only to encrypt
    - Use one key only to sign

    For more information, see section "Creating an account".
5. Click **Create an account**, then skip the welcome screen.
6. Insert your card or token in the reader, type your PIN and click **Connect**.

Stormshield Data Security reads the card and displays its contents: the card is either empty or it contains all the required information (public key, private key, certificate). If the card contains old information, you can choose to delete it.

If you select to delete existing keys, only the keys that are not used at the end of the process will be deleted.

> **CAUTION**
> If the card contains old keys, do not request to delete objects not reused because it would delete the old keys.

6. When creating an account with two keys, complete the following steps once for each key.

On the next screen, you can either generate a new key, or re-use an existing one.

- To generate a new key, click Generate your personal key, select the type and length of the key.

If you are generating two keys and you do not want to save both keys on the card, you can uncheck Put your encryption key in the card. In this case, the key will be saved in the local Stormshield Data Security account. However, you cannot save both keys to the Stormshield Data Security account, otherwise it would not be a card account.

Click Next.

Go to Step 7.

- The option Reuse a key on the card is only available if a reusable key is found on the card or token.

If you choose to re-use an existing key, and click Next, the following screen is displayed.

You can select the key to use.

7. Your security key will be calculated from a random number. To do this, click in the middle of the screen and move the mouse at random: a random number will be generated to protect your account. Click Next.

The key is generated locally on the PC before being imported on the card or token. The generation of a key by the card is possible for certain cards; see the *Administration Guide* for more information.

8. If you created at least one key locally, enter the information required to create your identity. This identity will be shown on your self-certified certificate.

For an account with two keys, you only need to complete this step once.

Click Next.

9. If you created at least one key locally, it is possible to save a copy of your keys in a PKCS#12 file, in your "account" file if you want to save it, or to export it later.

Saving a copy of the key in your Stormshield Data Security account allows you to later export the key (in PKCS#12 format), for example if the card or token does not allow a private key to be exported.

Saving a copy of the private key (and associated objects) allows you to create a Stormshield Data Security account with the same keys and certificates, particularly if ever your card or token are lost or destroyed.

10. Proceed to the next screen and review the summary of your account. If necessary, return to previous screens to modify any information.
11. Click Finish. Stormshield Data Security generates your personal keys and creates your account with a summary of the generated key(s) and the tree associated to it.

The Stormshield Data Security account created using a card or token has the serial number of the card or token as an identifier.

Even when the keys are stored only on the card, it is recommended to save the Stormshield Data Security account to ensure that you recover all the information linked to the account and keys.

4.5 Renewing your keys

You can renew your keys to be used with smart card or USB token as follows:

- Import a new key from a P12 file. This method is recommended as it bypasses the certification phase. The process is identical to the one used for password accounts. Refer to Section 3.4.2, "Importing a PKCS#12 key".

Make sure to destroy the P12 files using Stormshield Data Shredder, once the import is complete.

- Generate the keys on the user's PC. The process is identical to the one used for password accounts. Refer to Section 3.4.1, "Creating a key".
- Generate a key by the card. The process is identical to the one used for card accounts creations. Refer to Section 4.4, "Creating an account for smart card or USB token".

> **CAUTION**
> If you have changed your key with a smart card or USB token account, it may not be possible to unblock your Stormshield Data Security account. It is mandatory to keep the previous encryption key (or personal key for an account with one key) in the card in order to access your Stormshield Data Security account. The new encryption key will be automatically taken into account when the certificate of the previous one reaches its end of validity.

In any case, it is recommended to keep your existing keys on your smart card or USB token, to be able to decrypt existing files. You can delete the signature keys after renewal, as they no

longer have a use.

4.6 Using old encryption keys

In order to decrypt files encrypted with an old key, you can save the old keys and associated certificates on the new smart card or token. These old keys will automatically be used for decryption, without having to import them as a decryption key into the account. It is always possible to import the old keys as decryption keys in the Stormshield Data Security account.

Make sure to save the certificates with the old encryption keys, otherwise you will not be able to use the old encryption key.

5. Certifying your key

To use Stormshield Data Security, you must have certified key(s). This chapter describes how to certify your key, including requesting a certificate, and adding or exporting a certificate.

5.1 Introduction

When Stormshield Data Security creates a key, it also creates a self-certified certificate. As self-certified certificates are not created by an authority, they are not automatically recognized by other recipients.

For a self-certified certificate to be recognized by a recipient, it must be sent with a verification of the origins of the certificate. In the case of an exchange with a large number of recipients, this method can be quite painstaking.

To ensure that a certificate is automatically recognized by a recipient, it is necessary to have a certificate distributed by an authority recognized by the recipient. The Stormshield Data Authority Manager guide describes how to set up an infrastructure to manage keys, which may or may not include a PKI or external service. You can also use other products or services that implement PKI (Public Key Infrastructure), as long as they manage keys with the X.509 V3 standard.

When importing a PKCS#12 file or one present on a smart card, certification is rarely necessary as the card generally includes a certificate from a recognized authority.

Certifying your key with an authority involves two steps:

1. First, you need to submit a certificate request to the authority.
2. Then you have to add the certificate issued by the authority to your account.

Stormshield Data Security supports all authorities that accept certificate requests PKCS#10 format and issue binary certificates (.cer), PEM certificates (.crt) or certificate chains (.p7b or .p7c).

Stormshield Data Security does not handle the transfer of authority requests and replies. These transfers are not standardized and vary according to the authority involved: they can be made by disk, mail, using a Web interface, etc. Contact the certifying authority for details on the preferred procedure.

However, using the Internet browser extension of Stormshield Data Security you can interact with PKI providing a Web interface. This extension enables you to submit certificate requests to an external PKI using the specific features of your Internet browser without manipulating PKCS#10 requests. The supported browsers are Microsoft Internet Explorer (through a CSP interface) and Netscape/Mozilla (through a PKCS#11 interface).

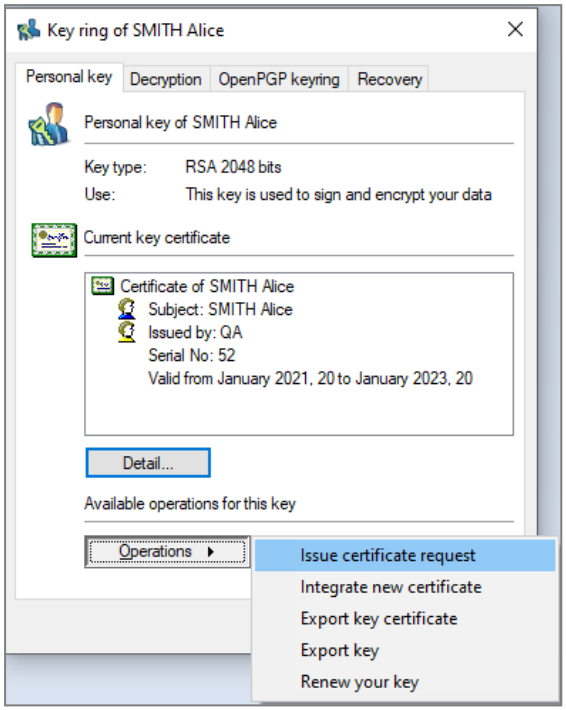
5.2 Requesting a certificate

To generate a certificate request:

1. Open the Stormshield Data Security menu, select Properties.
2. Click the Configuration tab.
3. Select the keyring icon.
4. If you have two keys, choose the Encryption key or Signing key tab.

If you are only using one key, choose Personal key.

5. Click Operations and select Issue certificate request.



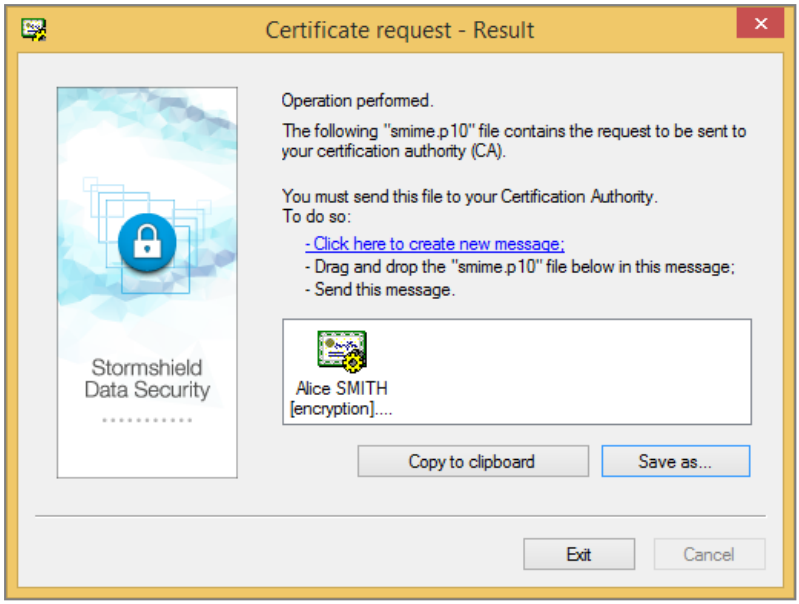
6. Click Next to proceed.
7. Enter all the requested parameters. These constitute your identity and will be used by the certification authority to build the certificate. However, the authority may change these values.

Click Next to proceed.

8. Check the summary of your request. If necessary, return to any previous screens to edit incorrect information.
9. The Result window allows you to get the certificate in PKCS#10 format.

You can either:

- Click Copy to clipboard. You can then paste the request into a window connected to the PKI (using an Internet browser for example).
- Save it to a file by clicking the Save as button. The file containing the request can then be transferred to the certification authority.
- Click the Click here to create a new message link. This will open your default mail messenger. You must then type in the mail address of the authority, copy the request into the message (for example you can drag and drop it into the e-mail), and complete the text of your e-mail request.



When the certificate request has been transferred to the authority or saved into a file, you can close the window by clicking Exit.

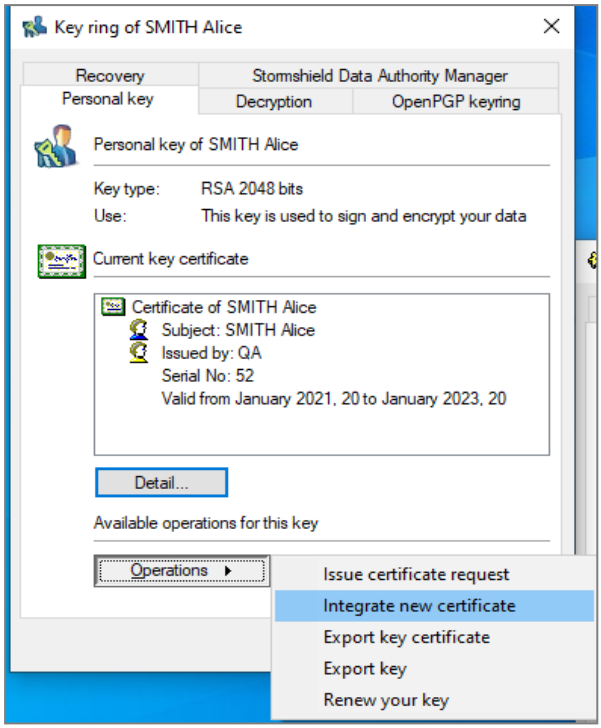
5.3 Adding a certificate

To add a certificate issued by your authority:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Select the Configuration tab.
4. Select the keyring icon.
5. If you have two keys, select the Encryption key or Signing key tab.

If you are only using one key, choose Personal key.

6. Click Operations and choose Integrate new certificate, and skip the introductory screen.

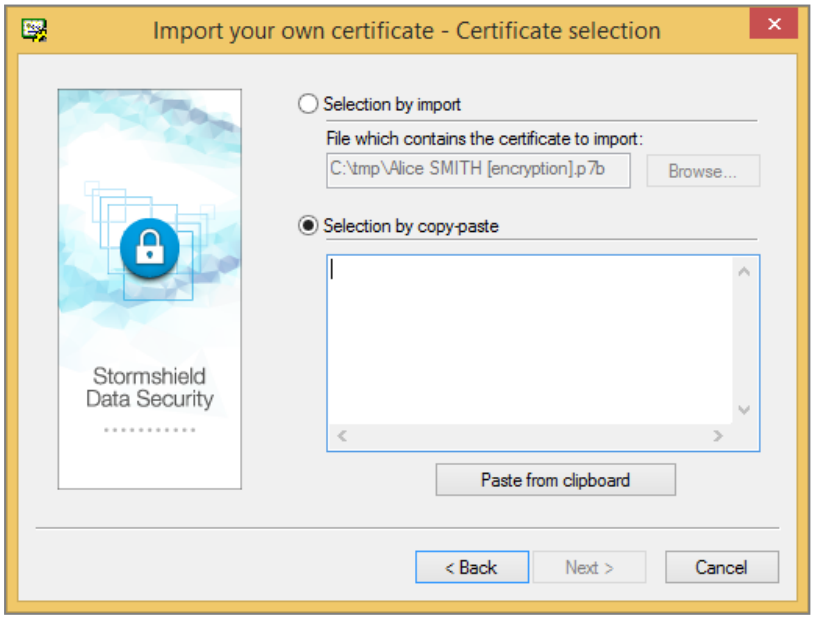


7. Provide your certificate (in X509 format) in one of the following ways:

- Select Selection by import and select a file using Browse. The file should be .CER (binary format), CRT (PEM format), p7b or p7c (certificate chains).
- Choose Selection by copy-paste and copy the certificate, as long as it is coded in Base 64.

In this case, make sure to add the following tags:

===== BEGIN CERTIFICATE ===== and ===== END CERTIFICATE ====



Click Next to proceed to the next screen.

8. If the file (with p7b or p7c extension), contains several certificates, select the certificate that you want to import.

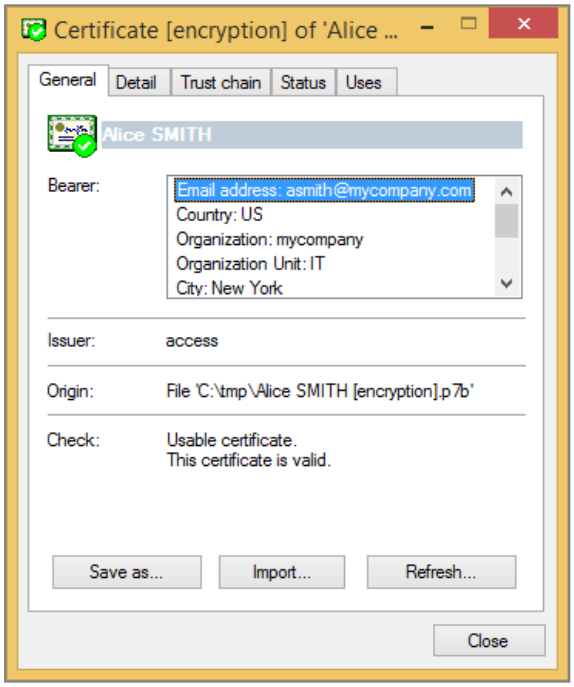
The certificates are listed in a tree structure. The user certificates are the main branch, while the authorities branch from the user certificate. Click the + sign next to the user certificate name to view the certificate hierarchy.

The certificate that has a check mark is the one that is selected, and that will be imported. The certificate of the current user is automatically selected. The certificates of authorities and other users are not selected by default.

Once you select a certificate, a confirmation window will appear. The external certificates (not the certificate of the current Stormshield Data Security user) that you select are added to your trusted address book, and will now be considered as coming from an authorized source.

9. Next to the name of the certificate, an icon indicates the status of the certificate, where green is OK, yellow is a warning, and red indicates an error. To understand the reason for the warning, view the certificate status.

To display a certificate, click it:



The Check section defines the reason for the status.

To return to the list of certificates, click Close.

10. Proceed to the next screen and check the summary for the certificate that you are going to add to your account.
11. Click Finish once you have selected the certificate(s) you want to add, and verify the summary.

You may now send this new certificate to your contacts. However, if you are sharing your certificate with co-workers, then this may not be necessary, if you are using a LDAP directory for your public key infrastructure (PKI). In this case, they will automatically have access to your certificate. Otherwise, you can send a signed message informing them that you will provide your new certificate (which is included in your signature).

5.4 Exporting a certificate

You can export your certificate and if necessary, its trust chain, to a file. This allows you to send your certificate directly to your contacts or to deposit it in an LDAP directory.

The file containing your certificate is generated using one of the following formats:

- Certificate only:
- binary format (extension .cer)
- binary base 64 format (extension .crt)
- Certificate with trust chain:
- PKCS#7 format (extensions .p7c or.p7b)

To export the self-certified certificate or the one issued by your authority:

1. Open the Stormshield Data Security menu.
2. Choose **Properties**.
3. Click the Configuration tab.
4. Select the keyring icon.
5. If you have two keys, select the Encryption key or Signing key tab.

If you are only using one key, choose Personal key.

6. Click **Operations**, then select **Export key certificate**, and pass the introductory screen.
7. Choose between **Export certificate only** and **Export certificate and trust chain**.

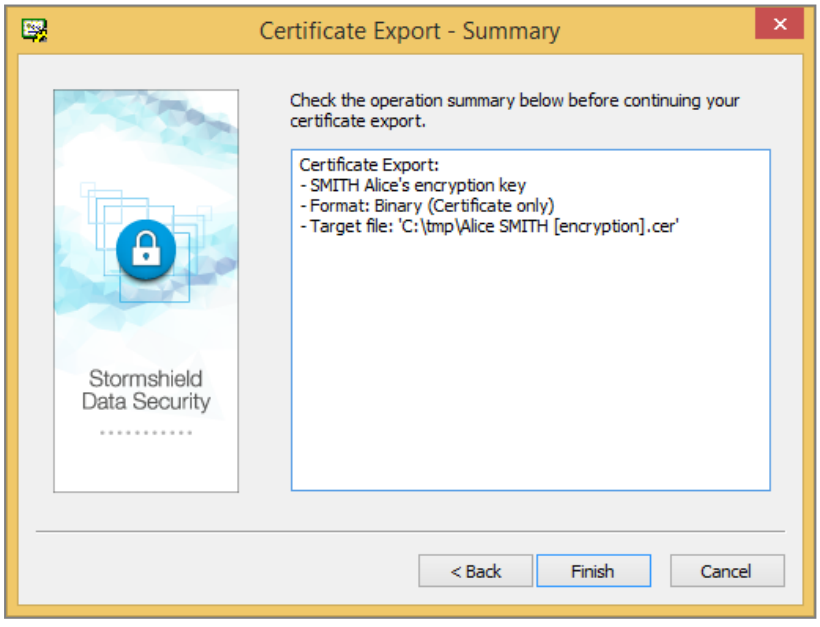
Click **Next** to continue.

8. In the following screen, indicate the file name to export.

If you click **Save as**, the name of the file you want to export will be saved, but the file will not be immediately exported.

Click **Next** to continue.

9. Review the summary, and click **Finish**.



Your certificate has been exported into the appropriate file.

6. Using certificates

Certificates in X509 format contain, in addition to other information, data concerning the holder and the holder's public key. This public key will be used to vehicle confidential information between correspondents, specifically in order to send data encryption keys.

This chapter explains how to:

- implement a centrally located address book in LDAP protocol
- consult and manage your trusted address book
- exchange certificates by sending a message

IMPORTANT
The only accepted certificates are the self-signed certificates included in the user trusted address book and the certificates whose kinship is in the trusted address book.

6.1 Using an LDAP directory

If Stormshield Data Security cannot find a recipient's certificate in your trusted address book, it can automatically search for it on an LDAP server. LDAP directories are also used to search certificates in order to import them into the trusted address book or as a target for contacts declared in the trusted address book.

Contrary to the certificates issued from the trusted address book, certificates returned from an LDAP directory are not automatically treated as trustworthy. However, before being used by Stormshield Data Security components, all certificates are entirely checked, regardless of their origin.

If the trust chain of the certificates from the LDAP directory cannot be checked, an error is reported and the process is blocked. If the certificates come from your trusted address book, a warning is reported and the process continues.

To install an LDAP directory, you must configure an LDAP search engine and declare an LDAP directory.

You can declare LDAP directories that will not be used for automatic searches, but for manual ones (for example, to import certificates).

NOTE
All LDAP directories declared for automatic searches must be accessible and operational at all times. Do not declare a server that cannot be reached but does not indicate this clearly due to a firewall; otherwise Stormshield Data Security may block waiting because of a reply that will never arrive (up to the timeout). For example, there should not be a firewall which intercepts the IP connections between the Computer and the LDAP server.

6.1.1 Configuring an LDAP search engine

Two search engines are available to search the LDAP directories for peers:

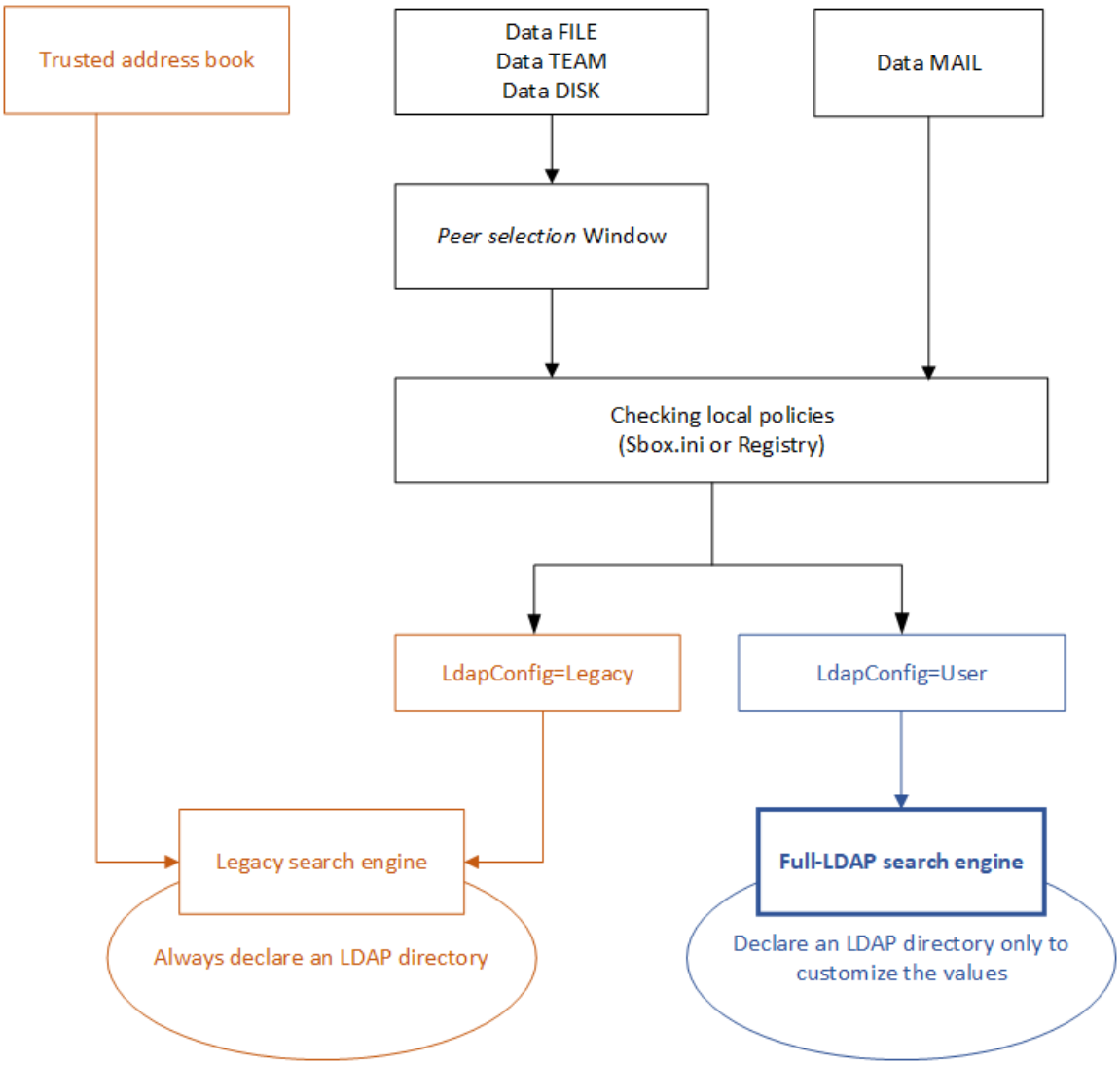
- The legacy search engine. It can be used by all the Stormshield Data Security components and it is used by the trusted address book,

- The search engine dedicated to LDAP searches. It can be used by the Stormshield Data File, Disk, and Team components, through the coworker selection window and by the Stormshield Data Mail component. This engine is not used by the trusted address book.

The parameter `LdapConfig` in local policies (*Sbox.ini* file) allows to select the engine to be used. The possible values are:

- `LdapConfig=Legacy`: legacy search engine (by default),
- `LdapConfig=User`: search engine dedicated to LDAP searches.

The diagram below explains which search engine is used depending on the components in which the LDAP search is performed and on you level of customization.



Customizing the full-LDAP search engine

If you want to use a different LDAP server and/or different attributes, you can customize the search engine.

1. In the [Directory] section of the *SBox.ini* file, set the `LdapConfig` parameter to *User*. For more information, refer to section Local Policies in the Stormshield Data Security *Administration guide*.

2. Declare an LDAP directory as described in section Declaring an LDAP directory :
   a. Specify the LDAP server to be used,
   b. Specify the attributes that you wish to use.

Using the legacy search engine

1. In the [Directory] section of the *Sbox.ini* file, set the `LdapConfig` parameter to *Legacy*. For more information, refer to section Local Policies in the Stormshield Data Security *Administration guide*.
2. Declare an LDAP directory as described in section Declaring an LDAP directory.

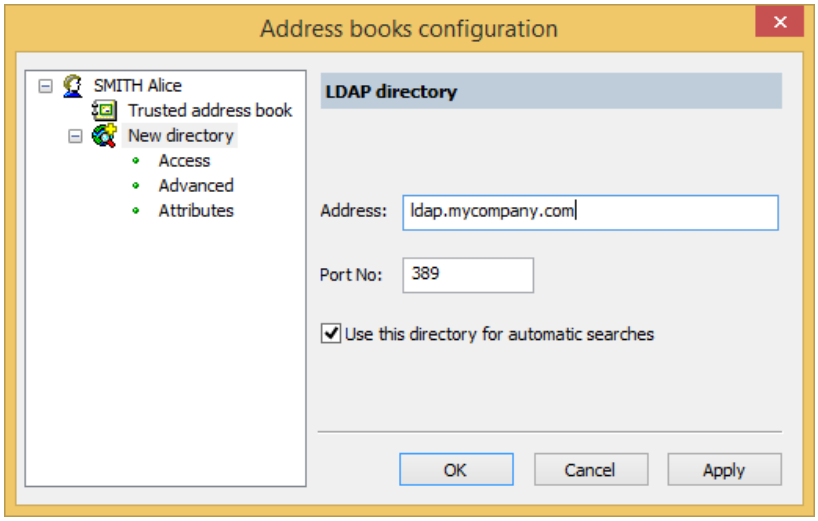
6.1.2 Declaring an LDAP directory

Declare an LDAP directory to perform LDAP searches with the trusted address book or to customize the LDAP server and/or the attributes in Stormshield Data File, Disk, Team ou Mail.

1. Open the **Stormshield Data Security** menu, and select **Properties**.
2. Click the *Configuration* tab.
3. Select the **Address Book** icon.
4. Choose the **File > Configuration** menu.
5. Open your root address book, and then the **LDAP Directory** category.

The LDAP directory is the second directory, just below your trusted address book. If you do not yet have an LDAP directory, then it will be listed as a **New directory**.

6. Enter the server name and its port number if required (the standard value is 389). An SSL connection is established if the specified port is 636.

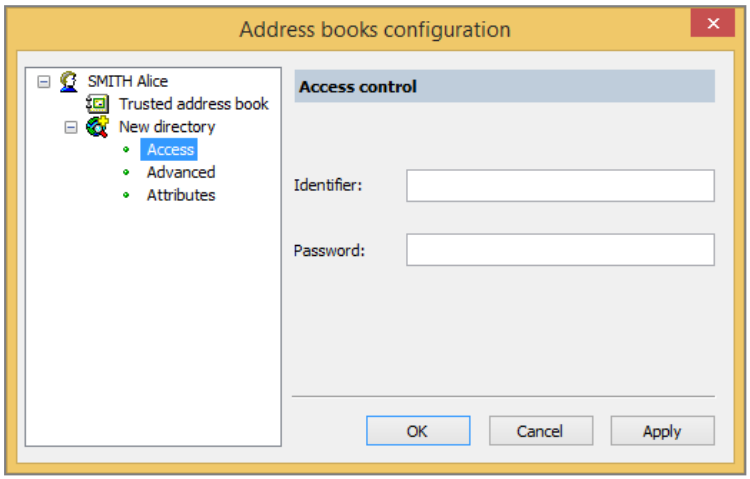


6.1.3 Setting access information

Two authentication mode are possible to access your LDAP directory:

- NTLM (Windows identification mechanism, the identifier and password do not go through the network).
  To use the Windows domain authentication, you must add to the configuration the following keyword `<MySelf>` into **Identifier** and **Password**.

- Simple (universal identification mechanism, the identifier and password are sent to the network in clear mode).
  If the first authentication mode fails, Stormshield Data Securitytries the second mode.
  Use the Access control screen in the LDAP directory folder to enter the identifier and password that you were given by the LDAP directory administrator.



NOTE

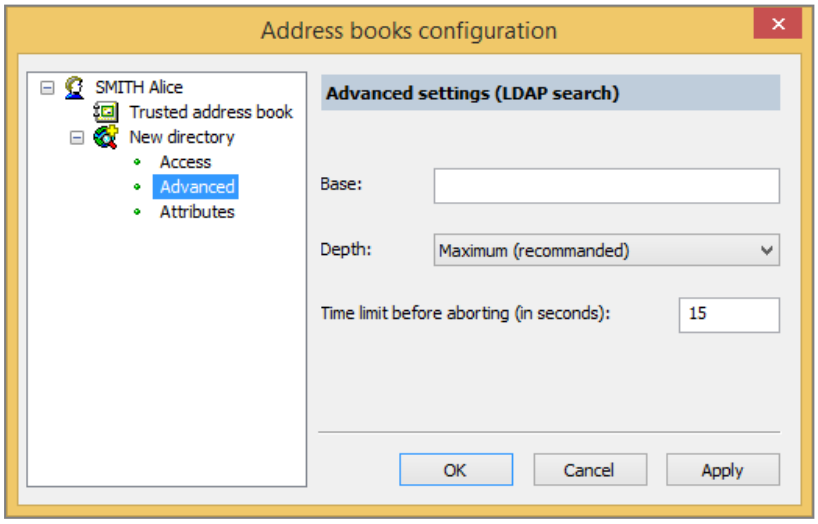
Kerberos authentication is not supported.

6.1.4 Setting LDAP searches

You can define a number of the LDAP search attributes, as described in the following sections.

Advanced folder

This screen allows you to narrow down searches performed in the directory tree structure.



Base field: Indicate which branch of the directory tree ("dn" for Distinguished Name) Stormshield Data Security is to start the search.

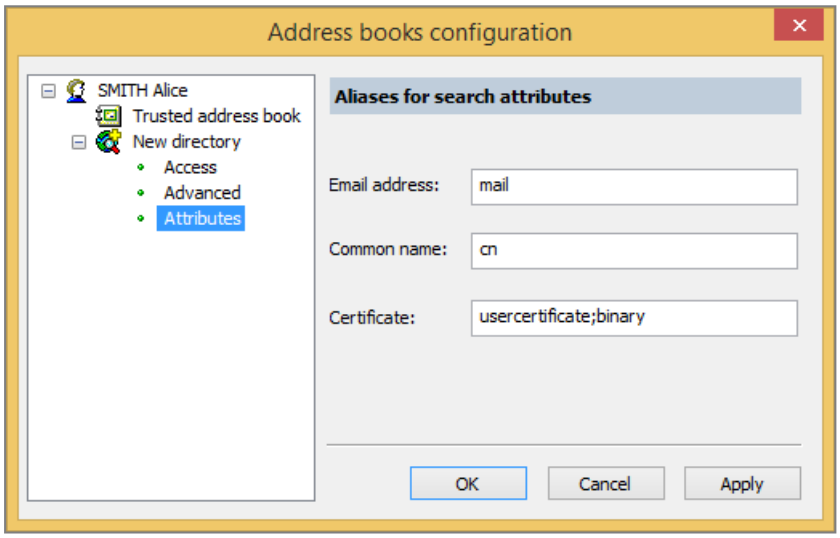
Depth field: indicates how many levels will be searched:

- Choose Minimum to search only the base specified.
- Choose One level to search only on the level immediately below the search base but not in the base itself.
- Choose Maximum to search all levels below the search base, as well as the search base.

Time limit before aborting: increase the time limit if your LDAP directory takes a long time to respond to your searches. Do not put too large a value, otherwise you will block your searches if the directory does not respond.

Attributes folder

Stormshield Data Security can carry out LDAP searches on the following attributes: e-mail address, user name and certificate.



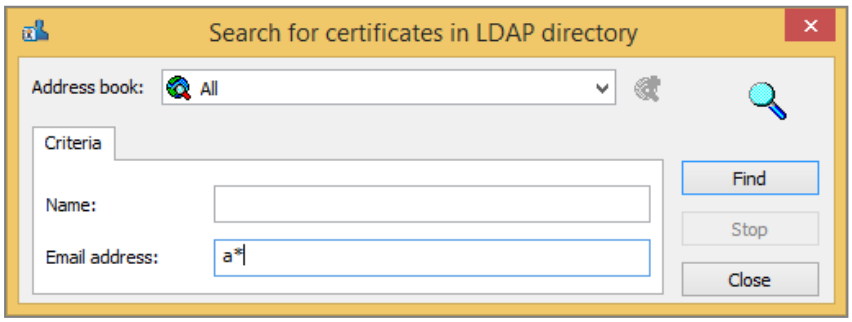
This screen allows you to enter the names of these attributes from your LDAP directory: mail, cn and usercertificate;binary, as shown in the screen above are the default values.

6.1.5 Importing a certificate from an LDAP directory

Stormshield Data Security allows you to import a correspondent's certificate into your trusted address book from any LDAP directory.

To do so:

1. Open the Stormshield Data Security menu, choose Properties.
2. Click the Configuration tab.
3. Select the Address Book icon.
4. Choose Edit / Find:



5. Enter the address of the LDAP server to be searched and the search parameters: name and/or e-mail address. You can include generic characters such as "*" or "?" in your search parameters if the directory you are searching accepts them.
6. Click Search now to launch the search. The results are displayed. Stormshield Data Security only displays certificates that are present in the directory, that are valid (according to the validity period) and which can be used for encryption or electronic signatures.
7. To display the details of a certificate, select it and click Preview.
8. To import one or more certificates into your trusted address book, select the certificate(s) and click Import.

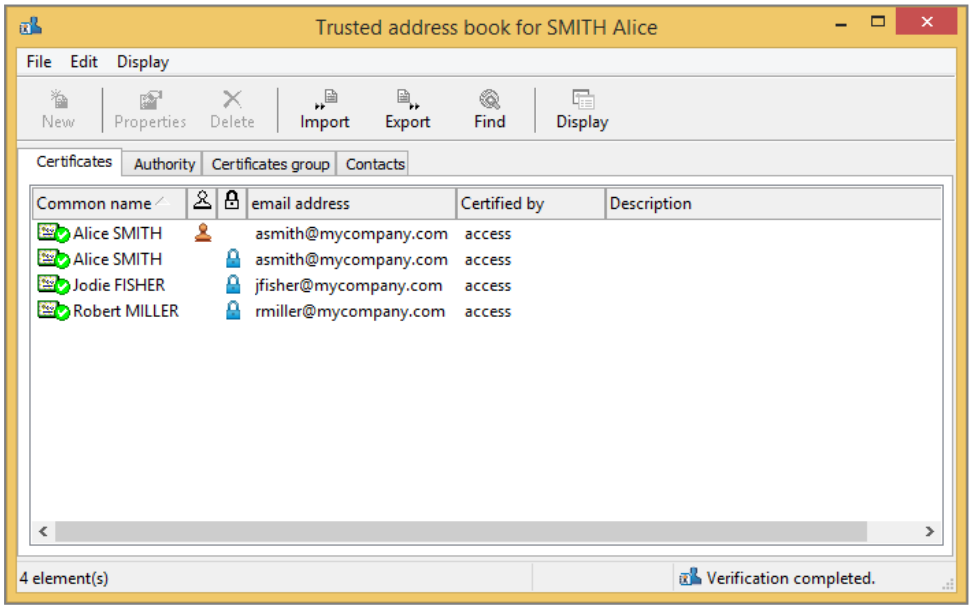
6.2 Managing your trusted address book

Your trusted address book allows you to save and use certificates from your correspondents (and authorities). This address book is protected and can only be modified by you. It is said to be “trusted” because all the certificates that you added are considered valid by Stormshield Data Security.

6.2.1 Opening your trusted address book

To open your trusted address book:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Select the Configuration tab.
4. Click the Address Book icon. The following window is displayed.



The Certificates tab displays the personal certificates of your correspondents, i.e. certificates that are not issued by a certification authority.

The Authority tab displays authority certificates; i.e. certificates that have the X.509 extensions indicating that it is an authority certificate (see Note below on X.509 v1 certificates).

The Certificates group tab displays certificates which regroup several certificates at once, i.e. encrypt for a group of persons with a single certificate.

The Contacts tab allows you to create shortcuts towards certificates located in an LDAP directory.

The validity of a certificate is shown by the icon on the left. All icons are shown in the following table.

	valid	expired, not yet valid, or self created	invalid
user certificate			
authority certificate			

For non-authority certificates, two columns show whether the certificate has been authorized for signing and/or encryption:

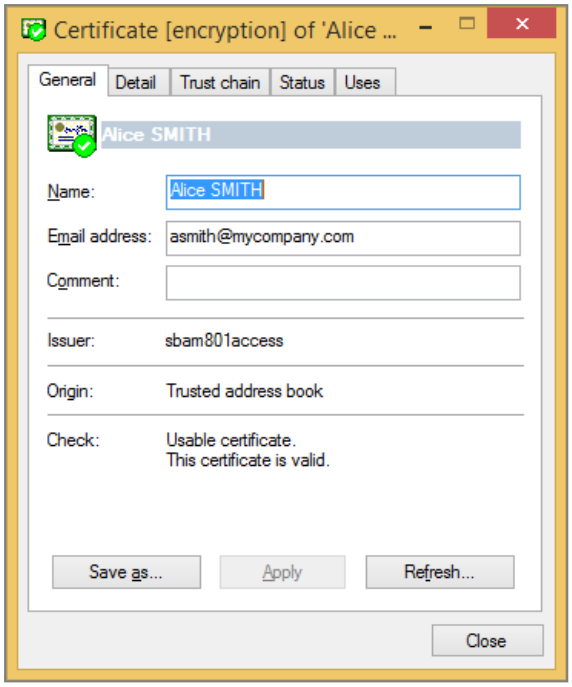
- the certificate is authorized for encryption
- the certificate is authorized for signing

To change the display of certificates, click the Display button or select the Display>Presentation menu.

- a X.509 v3 certificate is an authority certificate if it has a specific extension ("BasicConstraint"). This extension can include the full length of the certification chain belonging to this certificate.
- some authorities use root X.509 v1 certificates (Verisign for example), a version that does not support the above extension. Stormshield Data Security treats all auto-certified X.509 v1 certificates as an authority certificate. These certificates can be used by the various Stormshield Data Security components. However, it is recommended not to use certificates of this type.
- Stormshield Data Security does not use X.509 v2 certificates.

6.2.2 Displaying certificates

To display a certificate, double-click it or select it from the list and click the Properties button. The following screen is displayed:



The General tab displays a summary of the certificate's content

- the name and e-mail address of the holder
- a description that you can update as required (it is not part of the certificate)
- the name of the certification authority
- the origin of the certificate (trusted address book, LDAP, e-mail)
- the state after a verification check. If needed, a message indicates the error or warning

From this window, you can also export the certificate, using the Save as button.

The Detail tab displays the contents of the certificate.

For information on the different fields displayed, see the X.509 v3 standards, or the RFC 3280.

In case of error or warning after the check, the message will be displayed after the first line.

The Trust Chain tab rebuilds and displays the certification chain, and shows the results of checks carried out on the chain.

> **NOTE**
> The parent certificates are only researched in the trusted address book. No LDAP searches are performed for this chain.

You can click the certificates in the chain to see their content.

6.2.3 Importing certificates

You can import certificates into your trusted address book:

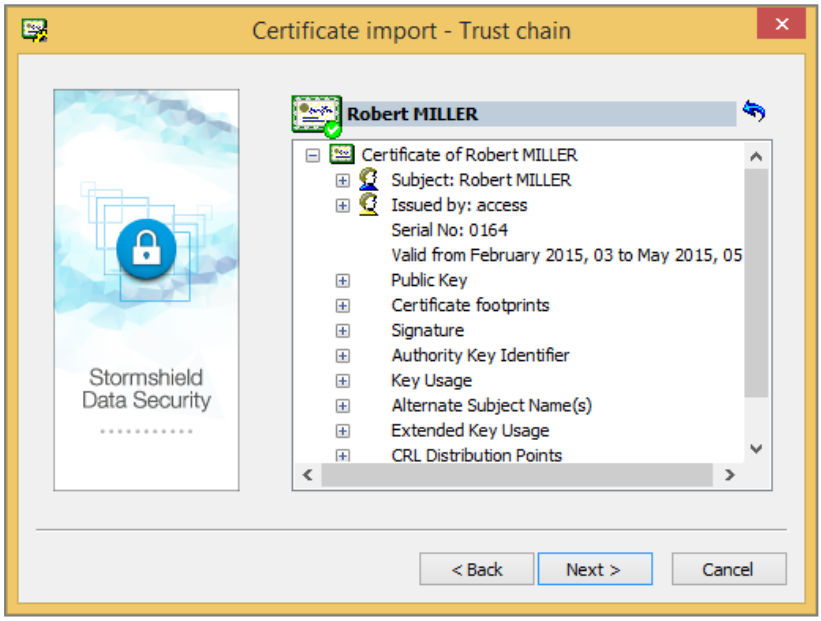
- as a certificate only, saved as a binary file (extension .cer) or a base 64 file (extension .crt),
- as a list of certificates saved in PKCS#7 format (extension .p7b or .p7c),
- as a complete backup of your address book (extension .p7z).

NOTE

If a customized certificate is imported whereas it already exists in the trusted address book, there will be both customized certificate and certificate without customization in the address book.

To import certificates, use the assistant or drag and drop them.

1. Click **Import** in the trusted address book main window, or drag and drop a certificate or list of certificates from the Desktop or the Windows Explorer.
2. Enter the name of the file that contains the certificate(s) you want to import, and proceed to the next screen. Stormshield Data Security displays all the certificates held in the file.
3. To view a certificate from the list, click on it:



During certificate import, these are checked. The check results in a green, yellow or red mark in the certificate icon. Regardless of the status, the result does not block the import; it is possible to import invalid certificates.

4. To return to the list of certificates, click .
5. To verify that a certificate belongs to your correspondent, contact him and check the displayed footprint.
6. To import one or more certificates from the list, select them and click **Next**; check the summary, and click **Finish**.

6.2.4 Exporting certificates or the trusted address book

If you have certificates in your trusted address book that you want to share with your correspondents, you can send them these certificates by exporting them.

You can export certificates using the assistant, or by using drag and drop, as described below.

If you want to export certificates groups, see section Exporting a certificates group.

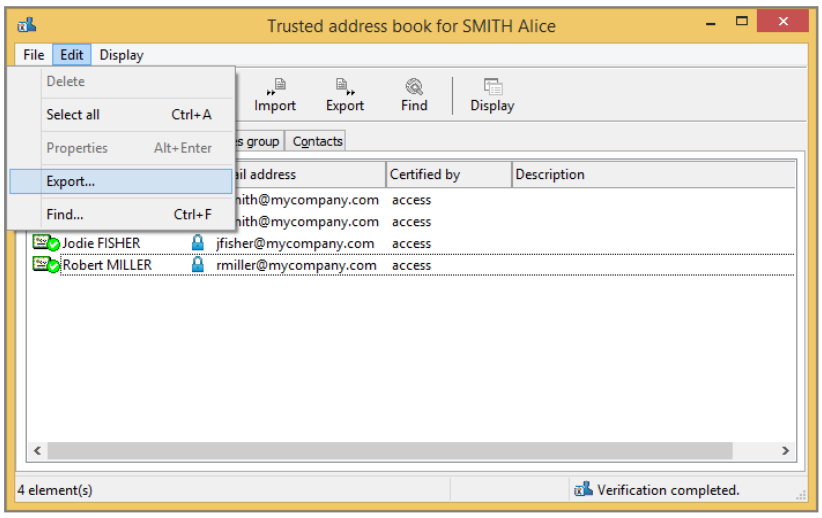
You can also export all the information in your trusted address book in a Stormshield Data Security file with the extension *.p7z*.

The export will include all the certificates, their customization if any, the certificates groups and the contacts certificates.

Using the assistant

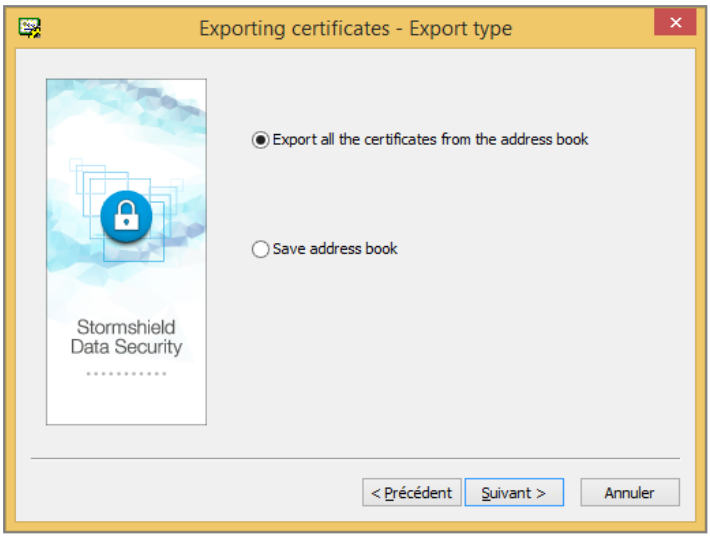
To export one or more certificates from your trusted address book:

1. Select them in your trusted address book.
2. Click the **Export** button or select the **Edit > Export** menu.



Continue to the next screen.

3. Choose the export type.



According to the elements you have selected in the address book, the text of the first option changes:

- **Export all the certificates from the address book**: this option is available when no certificate is selected in the address book. In this case all the certificates will be exported in a *.p7b* or *.p7c* file.
- **Export the selected certificates**: this option is available if several certificates or groups are selected in the address book. In this case only the selected certificates will be exported in a *.p7b* or *.p7c* file.
- **Export the selected certificate**: this option is available when only one certificate is selected in the address book. In this case the selected certificate will be exported in a *.cer* or *.crt* file.

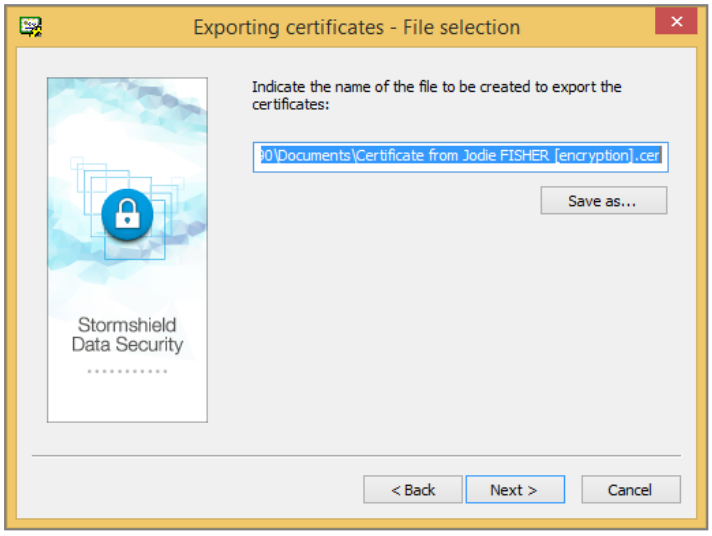
The **Save address book** option allows in any case to save all the certificates of the address book with their customized information if any.

4. If you have selected the first option of the **Export type** window and only in this case, the **Options** window opens. Additional elements can be added to the export file:
   - **Include parent-child relationship**: allows exporting the certificate's trust chain. In this case, any authority certificates that are shared are not duplicated.
   - **Include groups and contacts**: allows including groups and contacts certificates in the export file. If you want to export groups, see section Exporting a certificates group.

     NOTE
     This check box is checked by default when groups are selected in the address book. It is also unavailable to avoid unchecking it and generating an empty export file.

     NOTE
     If this option is checked whereas no group is selected in the address book, all the groups will be exported.

5. Enter a name and location for the export file. The assistant provides a default name, according to the selected export type. You can also directly type the information in the edit box or click the **Save as** button.



NOTE
The file extension is automatically changed if the extension chosen is not the right extension for the selected export type.

6. Check the information on the summary page before starting exporting.
7. The selected certificates have been exported in the indicated file. You can send the resulting file as you prefer (e-mail, USB token, shared files, etc.) or use it to restore the content of your address book (*.p7z* extension).

Using drag and drop

You can also export certificates using the drag and drop feature in your trusted address book.

1. Select the certificate(s) you want to export.
2. Keeping your left mouse button down, drag the certificates to your desktop, or to a folder in Windows Explorer, or to an application that can receive such a file.

If only one certificate is exported, the file will be named <CommonName>.cer. It is not possible to select another name or another format. The name does not distinguish between signature certificates or encryption certificates.

If several certificates are exported with drag and drop, the resulting file will be named *Certificate_List.p7b*. It is not possible to select another name or another format.

6.2.5 Deleting certificates

Select it from the list and click the Delete button.

It is possible to select several certificates to delete using CTRL key.

6.2.6 Creating a certificates group

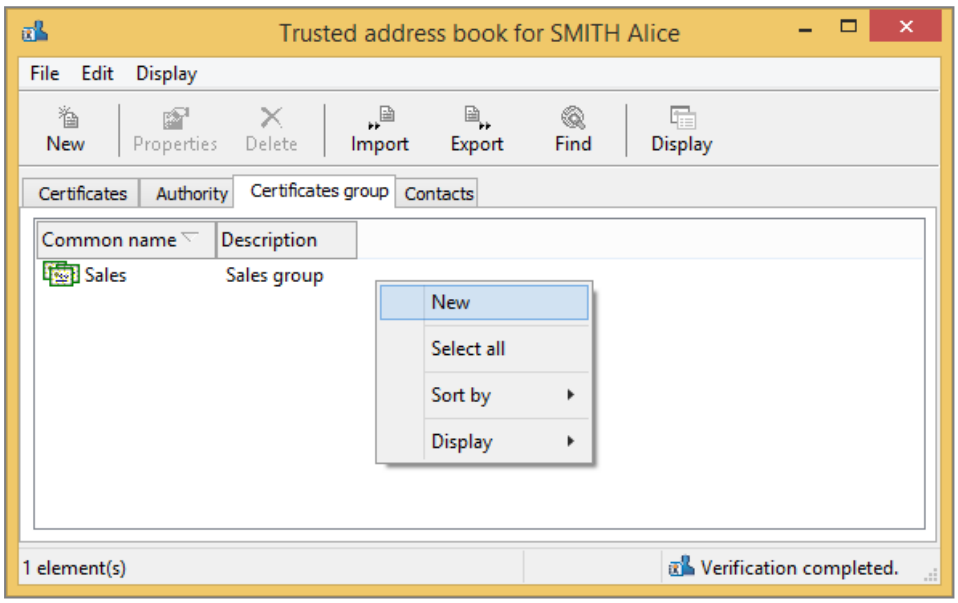
Creating a group of certificates simplifies the encryption for fixed groups of recipients. Instead of selecting each recipient, you can select a predefined group. If you use a group to encrypt a

document, the document will be encrypted for every member of the group that has a valid certificate.

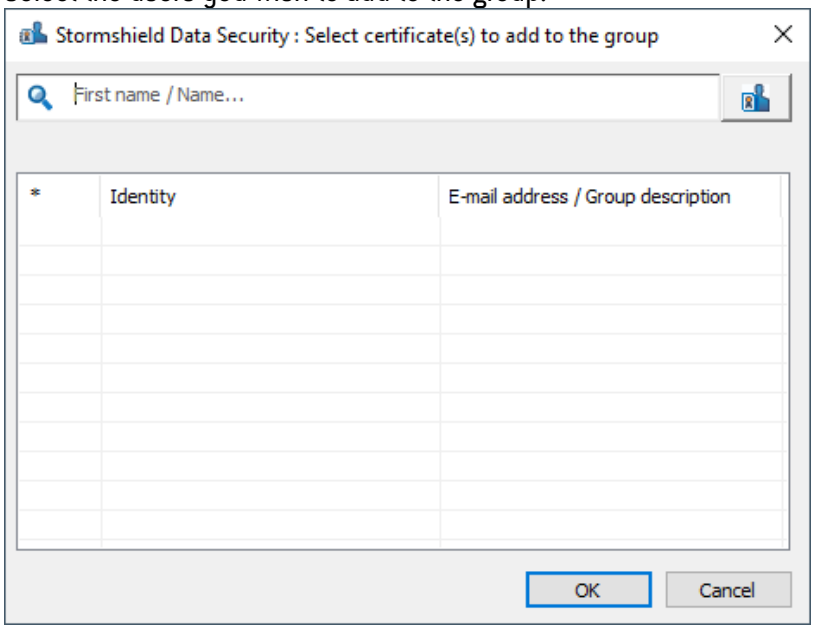
Groups that are supported by Stormshield Data Security are those saved in your trusted address book. You cannot use or import groups from an LDAP directory.

1. To create a group of certificates, choose the tab *Certificates Group* in your trusted address book.
2. Right-click in the window and choose **New**.

Do not click on an existing group, or you will get another menu.



3. Enter the information on the group and click **Add** to add certificates.
4. Select the users you wish to add to the group.

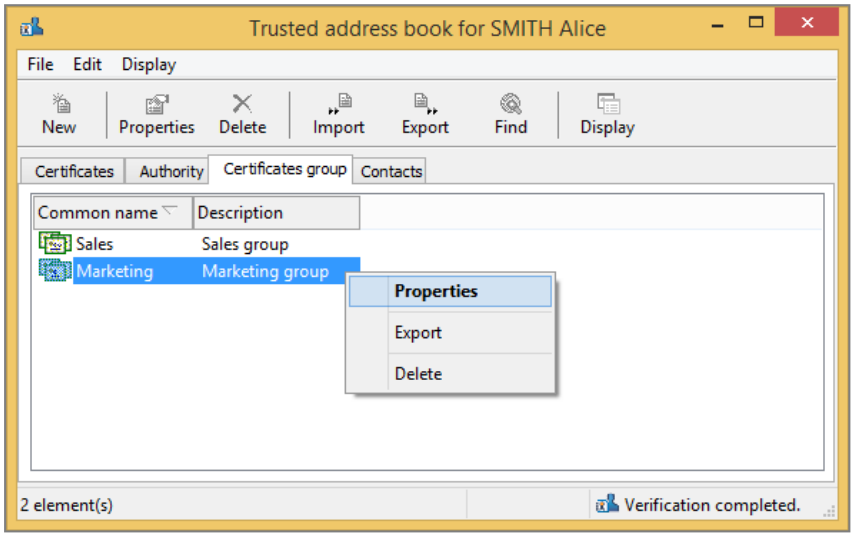


5. Click **OK** when you are done.
6. Click **OK** to close the window.

6.2.7 Modifying a certificates group

To modify a group of certificates,

1. Choose Certificates group in your trusted address book:
2. Right-click the group you wish to modify and choose Properties.



3. Add or remove certificates.

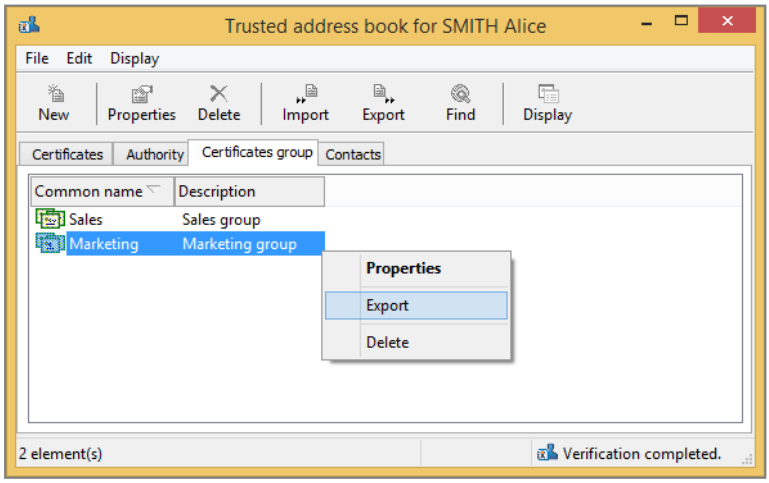
You can also modify the group name and description.

4. Click OK to confirm your changes.

6.2.8 Exporting a certificates group

To export a certificates group:

1. Right-click the certificates group(s) you want to export and select Export.



You can select and export several groups at once. In this case, all the certificates in the groups will be exported. If the same certificate appears in more than one group, it will only be exported once.

2. The following steps are the same for exporting certificates. Refer to the section Exporting certificates or the trusted address book.

> **NOTE**
>
> When exporting certificates groups, the **Exporting groups and contacts** check box in the wizard **Options** window is checked by default and not available.

6.2.9 Deleting a certificates group

To remove a group of certificates,

1. Choose Certificates group in your trusted address book.
2. Right-click the group you wish to remove and click Delete.

It is possible to select several certificates groups to remove using CTRL key.

Moreover, it is possible to remove all the certificates groups by right-clicking outside of the group and selecting Select All and clicking the Delete button of the menu bar.

6.3 Exchanging certificates using Stormshield Data Mail

Exchanges of certificates between users are infrequent because typically LDAP directories are used to share certificates between coworkers. Manual exchanges are used when sharing certificates with colleagues outside a company, or for test purposes.

Certificate exchange procedures differ depending on whether you use Stormshield Data Mail.

If you do not have Stormshield Data Mail and you want to export your certificate, you will need to use the certificate export/import procedure (see Section 6.2, "Managing your trusted address book"), and then send the certificate file by any appropriate means of communication.

6.3.1 Sending your certificate with Stormshield Data Mail

The easiest way to send your certificate to correspondents is by sending them a signed message via Stormshield Data Mail. If you own this software component, refer to the appropriate chapter in the Stormshield Data Mail documentation for a detailed procedure.

With standard S/MIME V3 secured mail, messages sent or received contain the sender's signature, which contains the sender's certificate. Any time a message is sent, it is possible to send a certificate to a correspondent. To send an encrypted message to a correspondent, you (the sender) must first have added the correspondent's certificate in your trusted address book (or the certificate must be available in the LDAP directory).

These are added manually when messages are received, since an acknowledgement indicates the information contained in the certificate and you must confirm that the certificate originates from a trusted source; it is then added to the trusted address book. Once this manual operation is performed, access to certificates for encrypted/signed messaging is automated.

In its standard configuration, Stormshield Data Mail sends signature and encryption certificates with a signed message. If you own Stormshield Data Mail, refer to its documentation for more details.

If you do not own Stormshield Data Mail, refer to section Exporting certificates.

6.3.2 Receiving a certificate with Stormshield Data Mail

The signed/encrypted electronic messages generally contain sender certificates (but it is not mandatory by the S/MIME standard). These certificates are signing certificates, encryption certificates, and authority certificates.

Stormshield Data Mail enables you to import these certificates into your trusted address book. To do so:

- If you have Stormshield Data Mail installed on your PC, please refer to the Stormshield Data Mail documentation, section *Exchanging certificates*.
- If you do not have Stormshield Data Mail installed on your PC, use your e-mail software to extract the certificate in PKCS#7 format. Use the procedure describing import from certificates file in section Importing certificates.

6.4 Working off-line

Stormshield Data Security monitors the network connection (LAN, Wifi, GPRS/UMTS card, etc).

When you are connected to the network (on-line), every time you search the LDAP directory for a certificate, certificates found as a result of the search are saved in a local temporary file.

When you are disconnected from the network (off-line), Stormshield Data Security detects that the network is missing and searches for certificates in this local cache.

This allows you to encrypt files and e-mail for your correspondents even when you are disconnected from your corporate network, as long as you have previously used a given contact's certificate at least once while connected.

Certificate revocation lists are also cached locally while you are on line to allow for verification when you are working off-line.

You can force Stormshield Data Security to work in off-line mode if necessary, for example if you are having local network problems:

1. Right-click the Stormshield Data Security icon in the task bar.
2. Activate Network access > Work offline.
3. De-activate Network access > Reconnect Automatically.
4. When you re-enable Reconnect Automatically, Stormshield Data Security automatically detects the network connection and switches back to on-line mode.

7. Setting revocation control

Revocation control is essential in using certificates since it is the only efficient way to send an alert to indicate that a certificate should no longer be used (for example if the bearer is no longer part of the group, suspects the key was compromised, or simply has a new key, etc.).

Revocation control can be performed either thanks to a Certificate Revocation List (CRL) or thanks to the OCSP protocol. In this case, the OCSP responder's URL address must be specified in the certificate.

This chapter describes Certificate Revocation Lists (CRL), and how they are used with Stormshield Data Security.

7.1 About certificate validation

Certificate validation is done by checking the following points:

- the certificate itself: format, validity dates, signature, extension, etc.
- the parent chain: It must be possible to establish a complete chain, up to the certificate from a trusted authority. Each certificate must meet the same level of security as the original certificate being checked. When a certificate in a chain cannot be validated, another chain is verified, until a valid chain is found.
- revocation control. This check ensures that each certificate in the chain (including the original certificate) is not on a certificate revocation list supplied by the certification authority (or a third party that has the delegation to create CRLs). Since CRLs are also signed by a certificate, the control also checks the certificates applied at the level of the CRL.

Therefore, to validate a certificate, access to several CRLs is required.

7.2 About revocation lists

CRL verification is described in the certificate standards and in CRL standard (X.509, RFC 3280 and RFC 5280). Basically, all the certificates used by Stormshield Data Security are controlled before being used, unless revocation control is deactivated, or if it is your own certificate.

The locations of the CRLs that must be downloaded are obtained in one of the following ways:

- from the certificates, using the distribution point extension
- from the configuration of the revocation controller, which indicates eventually the personalized distribution points of each authority of the revocation controller configuration.

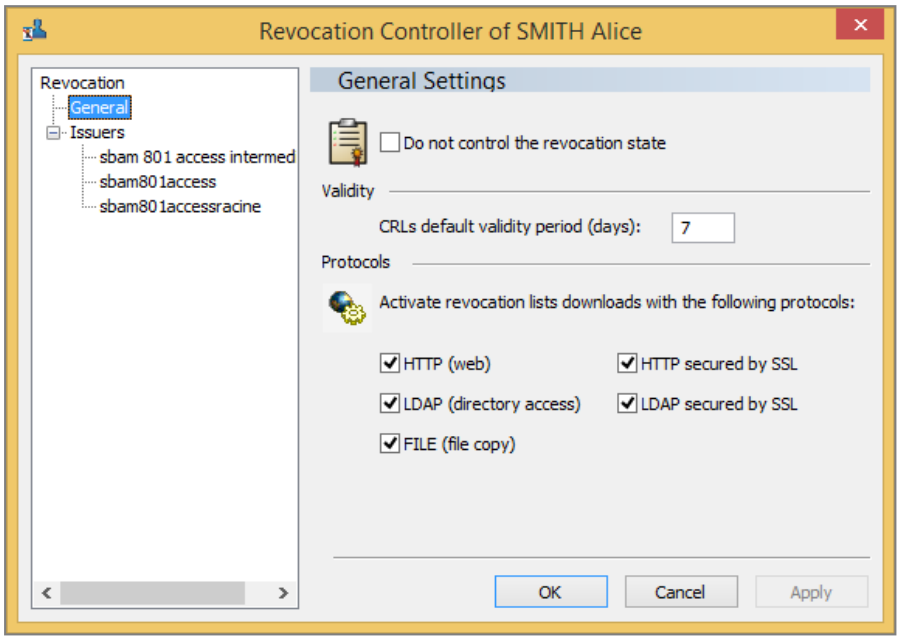
Stormshield Data Security integrates a full control of certificates in use with, if necessary, a (configurable) automated download of CRLs, with the following protocols FILE, HTTP, LDAP, HTTPS (HTTP with SSL 2), LDAPS (LDAP with SSL 2). CRL distribution points, possibly indicated in certificates, are managed by Stormshield Data Security and it is possible to define customized distribution points.

Users can configure several download criteria for each certification (authority) supplier. Received revocation lists are stored locally in a secured base.

It is possible to request explicitly "not to control certificate revocation" or to limit certificate validity to a customized number of days. You can choose between several protocols to load revocation lists.

7.3 General configuration

From the Revocation Controller screen, you can set how you want Stormshield Data Security to treat revocation control.



- If you check Do not control the revocation state, you can use all certificates as the revocation state will not be checked. This means that if a certificate has been revoked because it is corrupt, Stormshield Data Security will still use the certificate.

Only check this option if the network access to the CRLs is unavailable, and this is blocking your use of Stormshield Data Security.

- In the Validity section, you can set the number of days CRLs are valid for. CRLs contain the date of the next release, which is generally later than the date of the next publication. Use this setting to indicate the delay since the CRL generation at which the newer CRL version should be downloaded, or the number of days after which the CRL should not be used. The CRL downloading does not reset this period because it takes into account the CRL generation date and the delay, not the download date. If no CRL is generated after the delay expiration, a CRL download is performed for each certificate check involving it.

This value will be copied in each known authority, when the authority is created. If you modify the value in this configuration screen after the authority is created, the value will not be modified in the authority.

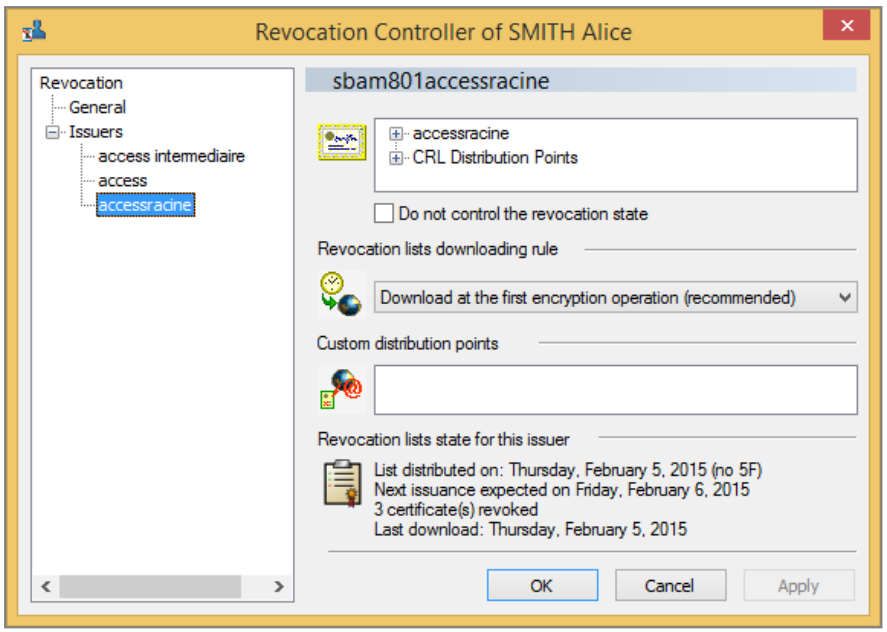
The special value 0 disables this functionality. In this case, the next release date of the CRL is used.

- In the Protocols section, select the protocols of the CRLs. Only the protocols selected will be used.

7.4 Adding authorities

When a certificate is correctly configured and it contains valid distribution points, the authority is automatically created in the Revocation Controller, and the distribution point issued by the certificate is taken into account. This authority will be listed in the Issuers list of the Revocation Controller window, shown below.

The name of the authority corresponds to its CommonName (as defined in the Issuer field of the child certificate).



For the complete identity of the authority, click the + sign next to the authority name in the top right.

For a list of the distribution points of the certificate, click the + sign next to Access point. This list corresponds to the URL used to find the latest CRL. This list is filtered upon execution, using only the protocol authorized (even if all the URL are listed here).

NOTE

The distribution points for the CRL of the authority are not present in the certificate of the authority, but rather in the certificate produced. The distribution points present in the certificate of the authority allow the CRL of the parent authority to be downloaded.

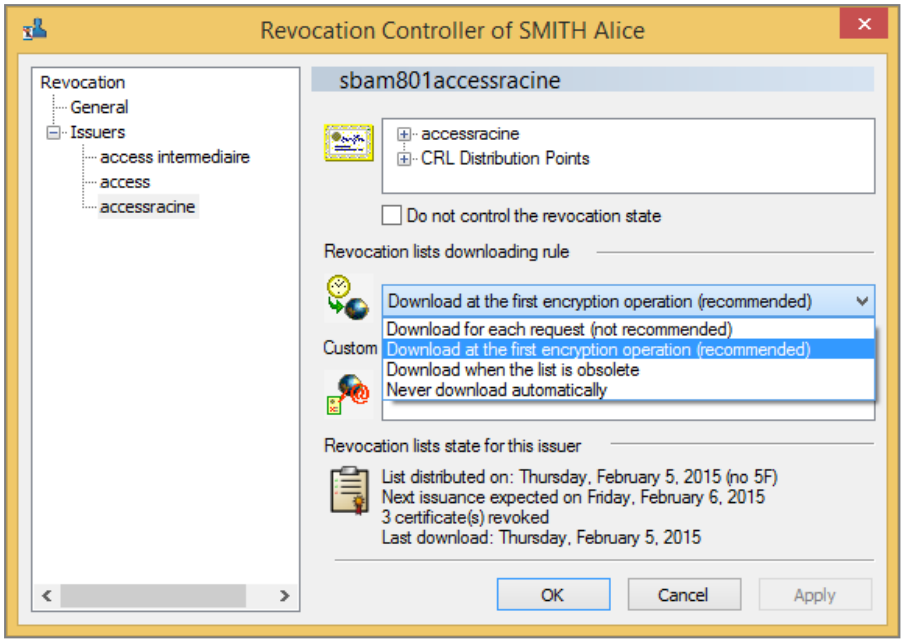
7.4.1 Deactivation

If you check Do not control the revocation state, you can use all certificates as the revocation state will not be checked. This means that if a certificate has been revoked because it is corrupt, Stormshield Data Security will still use the certificate.

Only check this option if the network access to the CRLs is unavailable, and this is blocking your use of Stormshield Data Security.

7.4.2 Download rules

You can set the download rules for the CRLs of each authority.



Select one of the following items from the drop-down menu:

NOTE

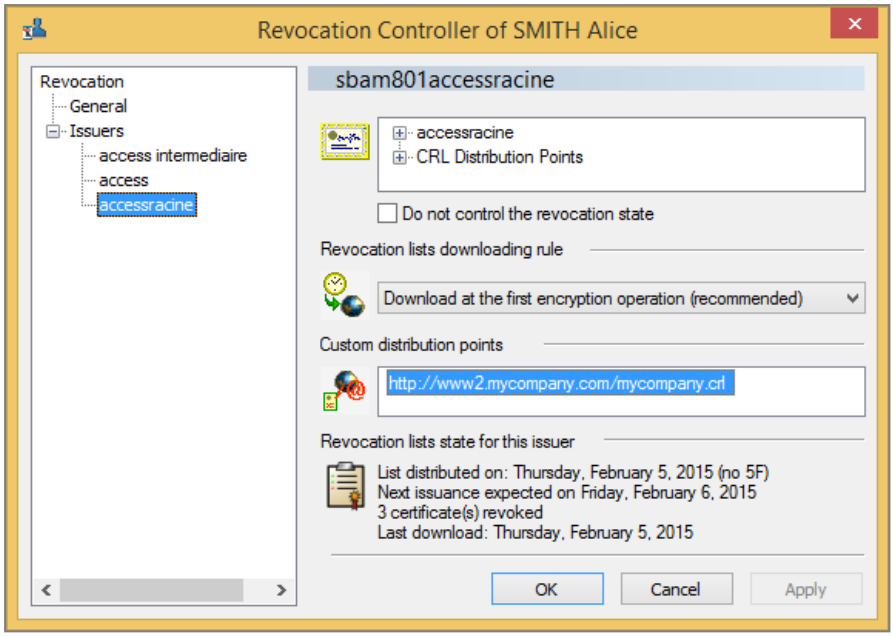
Regardless of the option selected, the download will be done automatically at the date of the next issue of the CRL. See the summary of the revocation list state for this information.

- Download for each request. It is not recommended to use this option, as Stormshield Data Security often needs to use CRLs. Only use this option in a high-security environment where you only occasionally use Stormshield Data Security for encryption.
- Download once after login (recommended). The CRL will be downloaded for its first use after the user connects to Stormshield Data Security.
- Download when the list is obsolete. The CRL will be downloaded when the date of creation and the validity date (set during configuration) are reached. Make sure that the CRL downloaded is more recent that the CRL currently used, otherwise the CRL will be downloaded each time it is used.
- Never download automatically. If you select this option, the user must manually download the CRLs. Only select this option for experienced users who are well trained or technical, and who only need to download CRLs occasionally.

7.4.3 Distribution points

In addition to the distribution points automatically listed with the certificates, you can manually add distribution points, in the section Custom distribution points. This is useful when an authority did not define its distribution points in the certificates, when certificates have changed or when they are not accessible in some environments.

1. In the Custom distribution points field, click after the last URL listed (or simply in the field if there are no URLs present).
2. Press F2.



3. Enter the URL of the CRL to be downloaded, and indicate the protocol to be used.
4. Press Enter to exit.

To edit an existing distribution point, select the URL and press F2.

NOTE
About the LDAP protocol, a SSL connection is established if the protocol specified is ldaps:// or if the port specified in the URL is 636.

7.4.4 CRL information

For each authority listed in the revocation list, the details of the last CRL download are listed in the section Revocation list state.

The following information is listed:

- List distributed on: This is the date the current CRL was created.
- Next issuance expected on: This indicates the date the next version of the CRL will be expected. This is often also referred to as the expiration date.
- the number of certificates that have been revoked.
- the date the CRL was last downloaded. The frequency of the downloads is set during configuration. The same CRL can be downloaded many times, especially if the recommended configuration is used (download once after login).

7.5 CRL download

To manually download a CRL, right-click the name of the authority under Issuers, and select Download.

NOTE
Manual downloads are generally used for users that only rarely have access to the company's network. In this case, they need to download the CRLs when they can.

7.6 Deleting an authority

You can delete authorities from the issuer list.

To do so, right click the authority and select Remove.

This does not affect the performance of Stormshield Data Security. This is only used to clean up the list of authorities.

8. Advanced functions

This chapter describes a number of advanced functions that you will need only exceptionally.

8.1 Managing your Stormshield Data Security connection

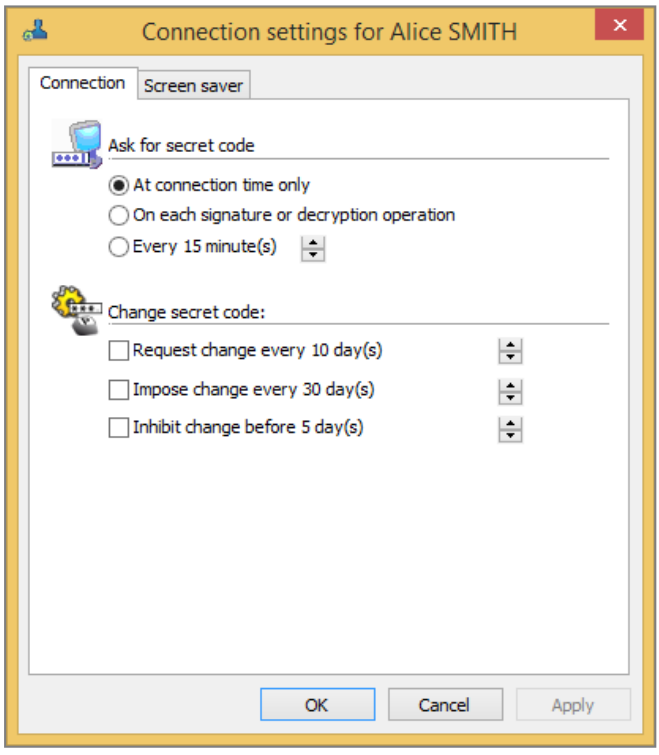
To modify the management rules of your Stormshield Data Security connection:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Click the Configuration tab.
4. Click the Connection icon.

8.1.1 Setting secret code requests

NOTE
This section applies to both password-protected accounts and card accounts.

On the Connection tab, you can configure when you must enter the secret code entry.



At connection time

You can configure Stormshield Data Security to request a secret code only when connecting to Stormshield Data Security.

This option is recommended in most situations.

CAUTION
Be sure to disconnect from Stormshield Data Security or lock your session before leaving your computer. Otherwise, third parties could use your workstation to sign messages with your key or decrypt confidential messages addressed to you.

To prevent people who are not authorized from using Stormshield Data Security, it is recommended that you set up an automatic de-connection or lock on a PC when not in use. For more information, see Section 8.1.4, "Setting screen saver options".

For each signature or decryption operation

In order to guarantee the highest level of security, you can configure Stormshield Data Security to ask for a secret code each time your private key is used (signature, decryption).

This option is recommended for occasional use of Stormshield Data Security only.

At a user-configurable interval

You can configure Stormshield Data Security to request secret code entry at user configurable intervals, i.e. every "x" minutes.

If you choose this option, your session will be kept open for the indicated time. After this period has elapsed, you will be asked to re-enter your secret code if you try to carry out any operations. This option is a compromise between entering the code at launch only and entering it systematically for all operations.

8.1.2 Changing your password

CAUTION
This section only applies to password-protected accounts. If you use a physical identification device (smart card, USB token...), refer to section Creating an account for smart card or USB token.

The more regularly you change your secret code (every X days), the less likely it is it will become detected by someone else. You will thus be better protected.

Select the option you prefer, and using the spin box, set the time after which you will need to enter your secret code. The options are described below.

- **Request change every x day(s).**

This option makes it possible to ensure the highest confidentiality of your password. By changing it every X days, the risk someone else steals the password is limited.

- **Impose change every x day(s).**

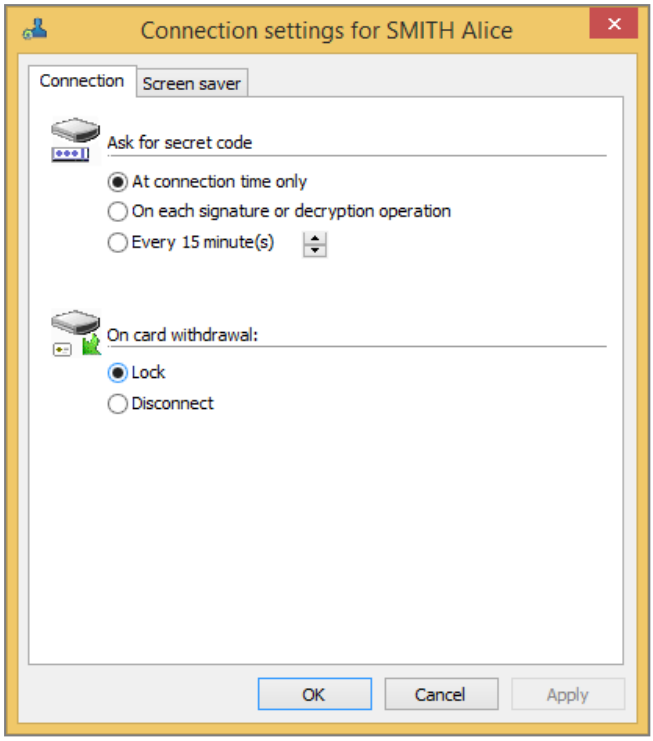
Unlike the previous option, this option forces users to change their password.

- **Inhibit change before x day(s).**

This option stops users from changing their password before a certain period. This is typically useful to ensure that the user does not change the password once, and then quickly change it a second time, to the value of the original password. This is to avoid that subsequent changes could result in the user using the same password, and thereby lowering the security.

8.1.3 Setting action on card or token withdrawal

If you are using a smart card or a USB token, you can configure the behaviour of Stormshield Data Security when the card is removed.



Select one of the radio buttons:

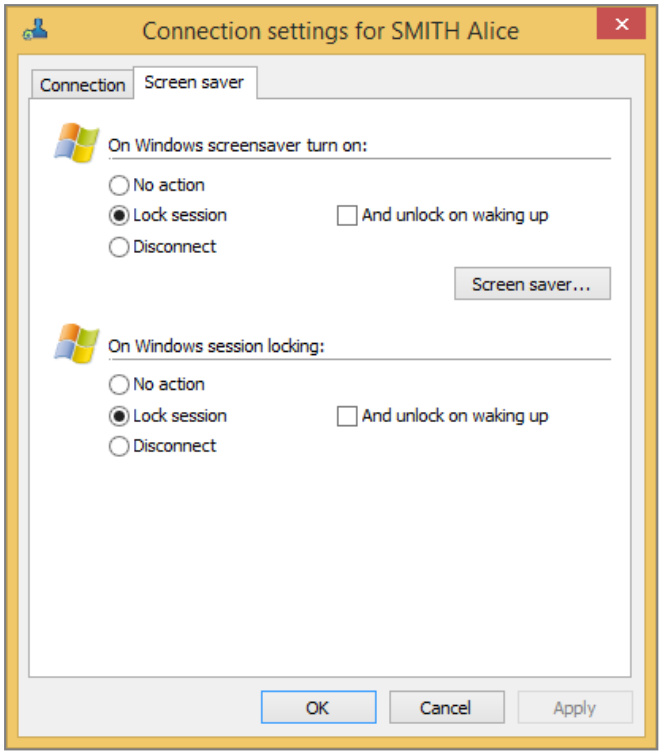
- Lock
- Disconnect

When you lock the Stormshield Data Security session, the private keys and the user configuration are inaccessible, but some of the components may still be accessible (though not all). In addition, when a session is locked, it is not possible for another user to log on to Stormshield Data Security on the same PC without disconnecting the current user.

When a session is disconnected, all the components are closed and inaccessible.

8.1.4 Setting screen saver options

On the Screen saver tab, you can set the behaviour of Stormshield Data Security when the screen saver is activated, or Windows is locked.



Select No action

You can configure Stormshield Data Security so that when your system goes on standby this has no effect on your Stormshield Data Security session. Select No action.

CAUTION
This option is not recommended for security reasons.

Select Lock session

You can configure Stormshield Data Security so that when your system goes on standby, your Stormshield Data Security session is locked. Select Lock session.

- If you check the box **Unlock on waking up**, you must enter your password or when the system wakes up or is unlocked.
- If you do not check this box, you will be asked to enter your secret code the first time you try to access information protected by Stormshield Data Security.

Locking takes effect five seconds after the system enters standby mode.

Select Disconnect

You can configure Stormshield Data Security so that you are disconnected from Stormshield Data Security when your system enters standby mode. Select Disconnect.

Disconnection occurs five seconds after the system enters standby mode.

8.2 Decryption key (delegated decryption)

This section describes how to configure and use decryption keys, either using a co-worker's key (delegation) or a former key.

8.2.1 Overview

With Stormshield Data Security, you can use decryption keys to decrypt files or messages that have been encrypted by a key other than your current key.

Stormshield Data Security allows two types of decryption keys:

- former private keys. When you renew your private encryption key, your former key is automatically moved to a location where all your former keys are kept.
- delegation keys. These are keys that another user has shared with you, to allow you to decrypt documents that were encrypted for their use.

While a delegation key only allows decryption, by using a former key you can also transcipher documents, for example towards your new key.

Delegation decryption allows you to give another co-worker (for example, your secretary), permissions to decrypt messages for you (for example, during your holidays). In order to do so, you must give your co-worker your private key (if you are using only one key for encryption and signature), or your bi-key (if you use two different keys for encryption and signature).

With your decryption key, your co-worker will only be able to decrypt message. To ensure that your co-worker does not sign in your place, you must use separate keys for encryption and signature. In this case, you will export the key used for encryption, which will be imported by your co-worker (delegate).

Keys imported this way cannot be exported by the person who received the key. In other words, the delegated people cannot transmit the delegation.

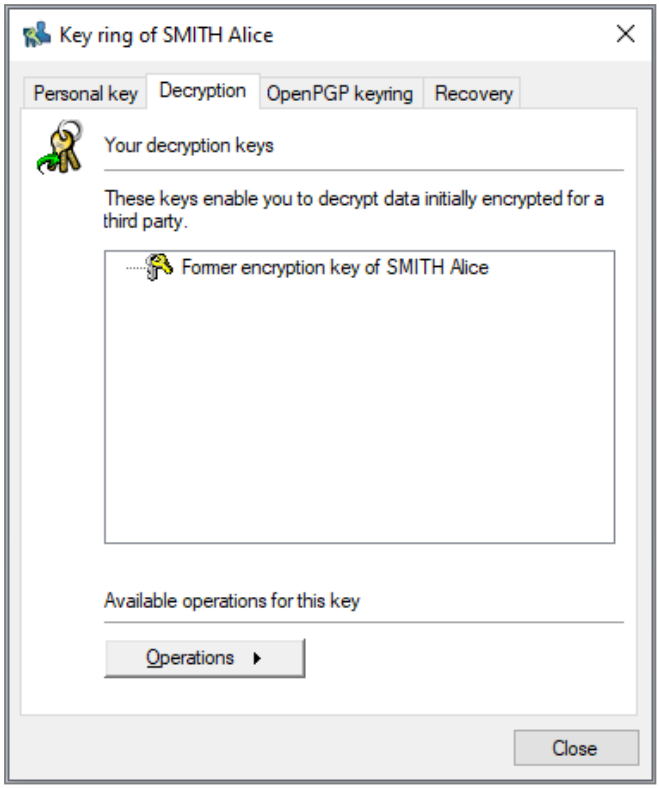
To export your security key, refer to Section 8.6, "Exporting your security key". You obtain a password-protected .p12 or .pfx file containing your key. This file can be used as an import function in another account.

> **NOTE**
> It is not recommended to own one bi-key (for signature and encryption) to use decryption delegation.

8.2.2 Importing a decryption key

To import a decryption key:

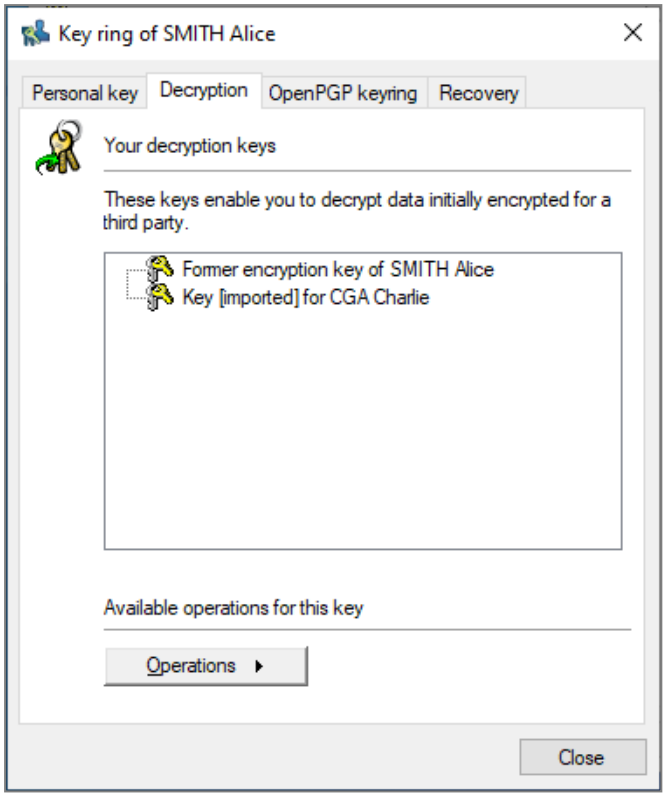
1. Open the **Stormshield Data Security** menu.
2. Choose **Properties**.
3. Go to the *Configuration* tab.
4. Click on the key ring icon.
5. Go to the *Decryption* tab:



6. Click **Operations** and choose **Import a key** and pass the introductory screen.
7. Indicate the name of the .p12 or .pfx file containing the key to be imported and enter the password. Stormshield Data Security displays a list of certificates present in the file, that is the certificate associated with the key contained in the file and its trust chain.
8. To view a certificate from the list, click it.

To return to the list of certificates, click the **Close** button.

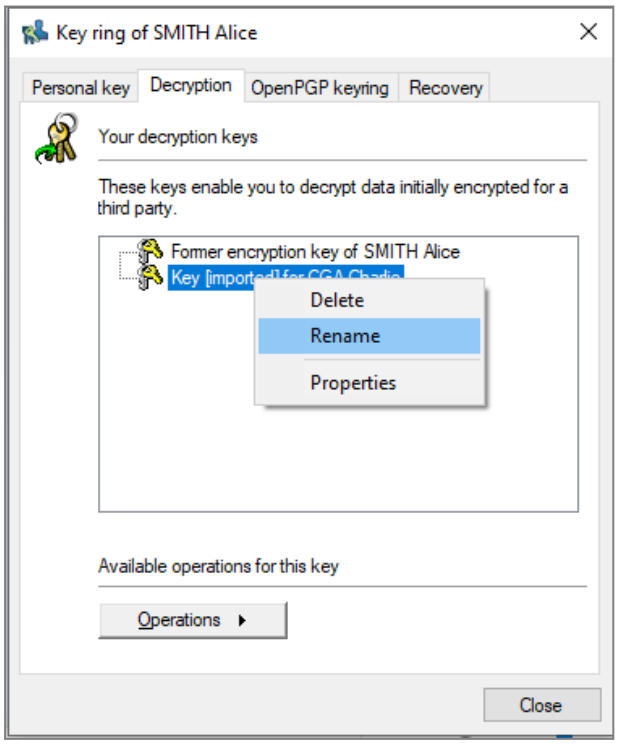
9. Select the trust chains that you wish to import into your address book, then proceed to the next screen.
10. Choose the type of key:
    - For delegation select **This key is that of a co-worker**.
    - For former key select **This is a former key of yours**.
11. Review the summary, click **Finish** and verify the result of the operation. The imported key should now appear in the list:



8.2.3 Renaming a decryption key

Once imported, Stormshield Data Security automatically creates a name for decryption keys. You can modify this name as follows:

1. Go to the *Decryption* tab.



2. Right-click the key for which you want to modify the name and select **Rename**.

You can also select the key and then click the **Operations** button.

3. Enter the new name of the key.
4. Validate the change by pressing Enter.

To cancel, press Escape.

8.2.4 Viewing properties

If you want to view information on a decryption key:

1. Go to the Decryption key tab.
2. Right-click the key you want to the view the properties for and select Properties.

You can also select the key and then click the Operations button.

The certificate of the key is displayed.

8.2.5 Deleting a decryption key

If a decryption key is no longer used (for example, you no longer have delegation tasks), you can delete the decryption key from your account. To do so,

1. Go to the Decryption tab.
2. Right-click the key you want to delete and select Delete.

You can also select the key and then click the Operations button.

3. Confirm the deletion.

8.3 Recovery certificate

This section describes how to use a recovery certificate.

8.3.1 Overview

The recovery certificate secures the use of a strong encryption software. If a user loses their Stormshield Data Security account (for example, by losing the password) and has not saved the encryption key, a recovery certificate ensures that the user can still decrypt the data.

Also, if a user leaves without sharing the Stormshield Data Security password to access his account, the recovery then allows to decrypt the data from this person.

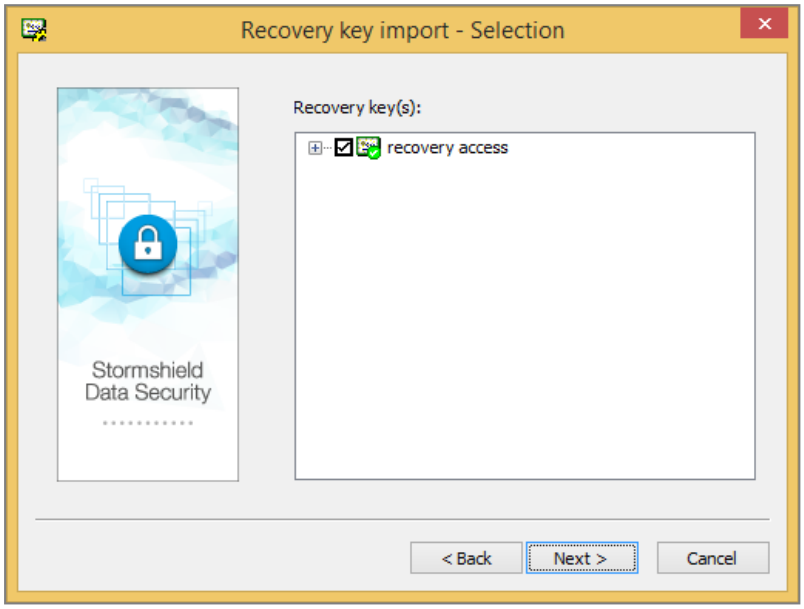
The recovery certificate may come from another Stormshield Data Security account from which the public encryption certificate will have been exported from. Due to the fact that this recovery key is highly sensitive and because of the use of this key, it is essential that this recovery account be protected.

8.3.2 Importing a recovery certificate

To import a recovery certificate:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. click the Configuration tab.
4. Choose the Key-holder icon.

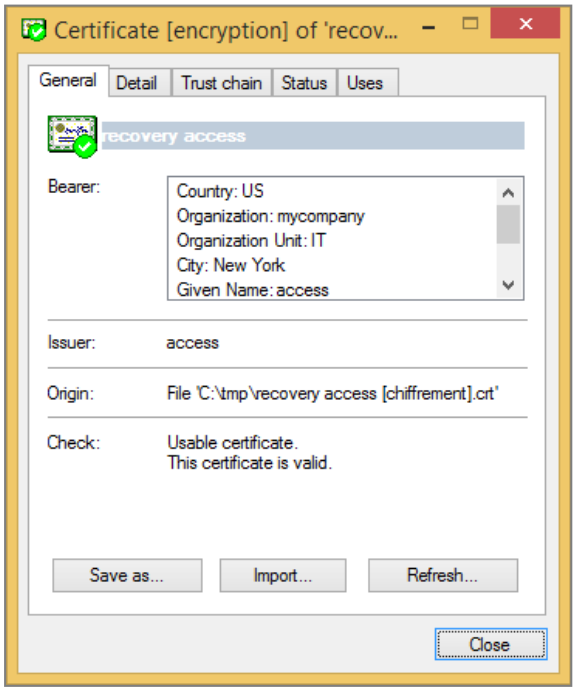
5. click the Recovery tab.
6. Click Operations and choose Import a key, then pass the introductory screen.
7. Fill in the name of the .p7b or.p7c file containing the certificates to import or the name of the .cer or .crt file containing one certificate. Stormshield Data Security displays the list of certificates present in the file, with its parenthood:



The selected certificates must be allowed to use the encryption key.

NOTE
It is possible that a recovery certificate needed is indicated as not trustworthy (red or yellow check mark), particularly if it were created in a third party environment.

8. You can create different levels of certificates, for example, to mirror the structure of your company in order to distinguish several levels of recovery.
9. To visualize a certificate from the list, click on it:



To come back to the list of certificates, click the Close button.

10. Proceed to the next screen and select for which components the recovery certificate will be used.

As you can import several recovery certificates, you can also associate different components with each certificate.

11. Check the summary, click Finish and check the result of the operation. The imported certificate then appears in the list.

8.3.3 Using a recovery certificate

You can either use recovery certificates for a Stormshield Data Security account that exists, or from an external source, as described below.

- If the recovery certificate comes from a Stormshield Data Security account, use the originator's Stormshield Data Security account to decrypt information.
- If the recovery certificate comes from another source, export or ensure you get the private key from this source, along with the certificate, in the format PKCS#12 (.p12).

Create a Stormshield Data Security account using the .p12 file at the associated password, as described in Section 3.4.2, "Importing a PKCS#12 key". Use the account you created to decrypt information.

You can create an account with only the decryption function.

You can use the recovery certificate to decrypt all information encrypted by the original owner of the certificate, or encrypted for the original user by a co-worker using the same certificate. However, you cannot decrypt information received from an external source (for example e-mails).

8.3.4 Renaming a recovery certificate

Stormshield Data Security automatically assigns the name of a recovery certificate. You can modify the name as follows:

1. Go to the Recovery tab.
2. Right-click the certificate you want to modify the name of and select Rename.

You can also select the certificate and click the Operations button.

3. Enter the new name.
4. Validate the change by pressing Enter.

To cancel, press Escape.

8.3.5 Recovery certificate properties

You can view the properties of a recovery certificate as follows:

1. Go to the Recovery tab.
2. Right-click the certificate and select Properties.

You can also select the certificate and click the Operations button.

The details are displayed.

8.3.6 Deleting a recovery certificate

You can delete old recovery certificates, as follows:

1. Go to the Recovery tab.
2. Right-click the certificate you want to delete and select Delete.

You can also select the certificate and click the Operations button.

3. Confirm the deletion.

8.4 Exporting a Stormshield Data Security account

You may export your user account in a Windows Installer file which will contain all the information and files from your account.

Once your account is exported, you can either store this file to save it, or install it on another computer where Stormshield Data Security is installed.

To export your account:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Select the Wizards tab.
4. Click Account export, and skip the introductory screen.
5. In the File selection window, enter the absolute pathname of the account you want to export.

You can also find the file by clicking on the icon to the right of the field. This will open a window from which you can navigate to the location of the file.

6. A summary of the file you selected is displayed. Check that the summary corresponds to the account you want to export, and click Finish.

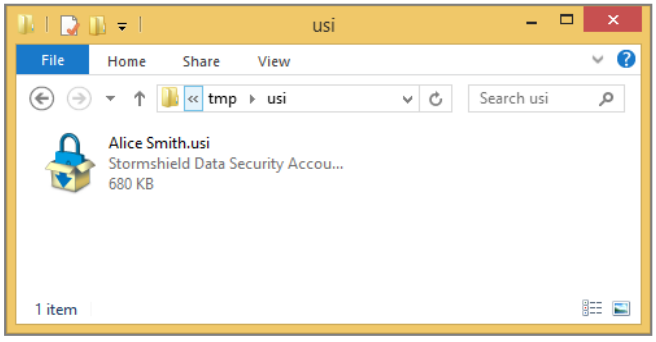
Stormshield Data Security creates a *.usi* file in the location you indicated, and provides a final summary.

8.5 Installing a user account

You can install an existing account (either exported or created using Stormshield Data Authority Manager) on another computer.

To install an account:

1. From Windows explorer, double click the *.usi* file which contains your account:

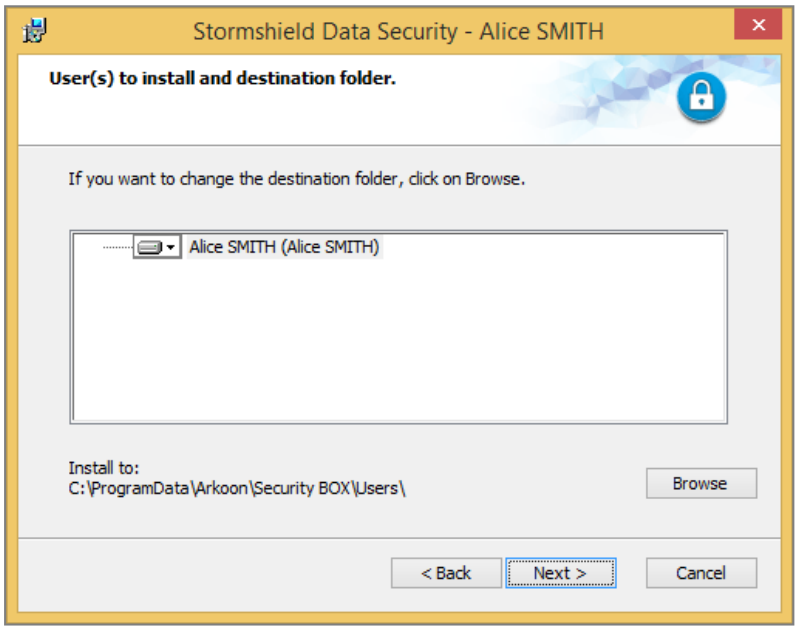


2. The installation procedure process starts, and the following window is displayed. From this window, you must:

a. Choose the user account you want to install. For an export, only the exported account will be listed.

b. Choose the location where you want to install the account, using the Browse button.

> **NOTE**
> It is strongly recommended that you keep the default location, otherwise you will not be able to use the account directly. You will first have to enter the full path of your account in the connection window or modify the account default location. For more information, refer to the *Administration Guide*.



3. Click Next to start the installation.

Once the account is installed you can directly connect to your user account; provided that you used the default location for the installation.

8.6 Exporting your security key

You can create a file to export your security key (public key and private key), with its certificate and any trust chain.

For an account with two keys, you can export each key individually.

By saving this file, you can:

- create a new account using your current key.
- use this key in all applications that are capable of importing security keys.

This will be used for decryption keys (see Section 8.2, "Decryption key (delegated decryption)"). This is also useful if you want to decrypt files or information previously encrypted with this key.

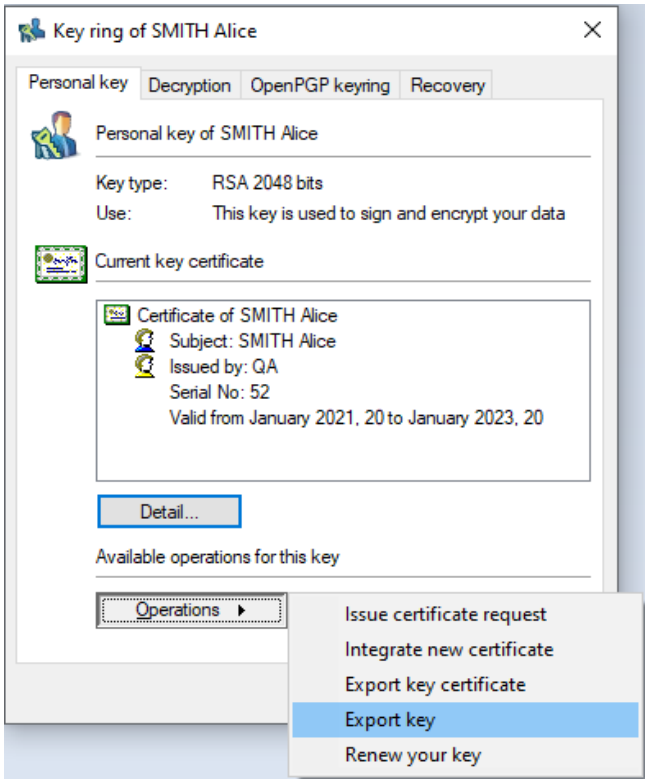
The file containing your key is generated in PKCS#12 format (extension .p12 or .pfx). If you have two keys, each will be exported in a separate.

To export your key:

1. Open the Stormshield Data Security menu.
2. Choose **Properties**.
3. Go to the *Configuration* tab.
4. Select the key ring icon.
5. If you have two keys, choose the *Encryption* or *Signature* tab.

If you are only using one key, choose the *Personal* tab.

6. Click **Operations** and choose **Export key**, then skip the introduction screen.



7. Select the option:

- your certificate trust chain if you wish to join the certificate of the authorities that certified your key.

Only the certificates present in your trusted address book will be listed. No LDAP search will be performed.

- your former key certificates if you made one or several certificates renewals and wish to decrypt documents which were encrypted with the previous certificates.

You can select both options.

Click **Next** to proceed.

8. Enter the name of the file to be created, and proceed to the next screen.

The Save as button enables you to browse folders in order to set the target file. However, the keys are not yet exported.

9. Enter a password to protect the file: this will allow you to encrypt your key in the generated file.

The password must be 8 characters long, with at least one numerical character or one special character, otherwise the export will be refused.

10. Proceed to the next screen, check the summary, and click **Finish**.

Your key has been exported into the indicated file.

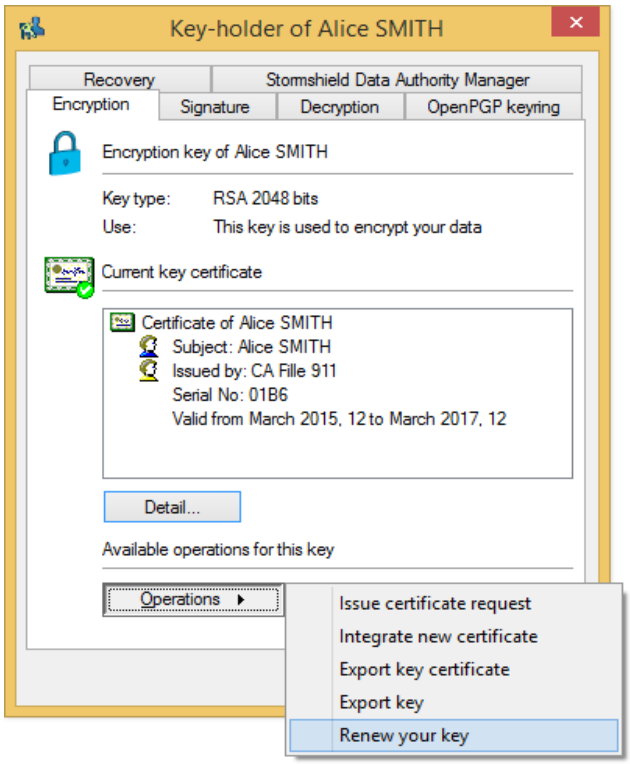
8.7 Key renewal

You may renew your keys as follows:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Click the Configuration tab.
4. Choose the Key-holder icon.
5. If you have two keys, choose the Encryption or Signature tab.

If you are only using one key, choose Personal tab.

6. Click Operations and choose Renew your key.



Skip the introduction screen.

7. Select how you want to create the encryption key:

- To create a new key, select the Generate your x key radio button, where x can be encryption, signature, or personal, depending on the type of key you want to import, and select the type and length of your key.

To complete the creation, see Step 8 onwards in Section 3.4.1, "Creating a key".

- To import an encryption key, select Import your x key.

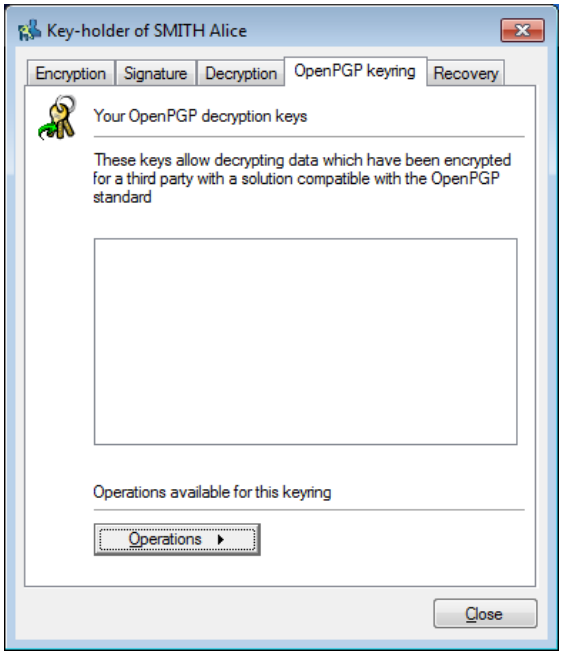
To complete, see Section 3.4.2, "Importing a PKCS#12 key".

8. Click Finish. Stormshield Data Security generates or /imports your key and uses your former key as a decryption key for your old documents, in the case of a personal key or encryption key (the signature keys are not kept).

8.8 OpenPGP decryption keys

Stormshield Data Security manages message decryption keys in OpenPGP format. These keys are used by the Stormshield Data Mail Outlook Edition add-in to read messages secured by PGP and GnuPGP applications and any other applications compatible the OpenPGP format.

When the Stormshield Data Mail Outlook Edition add-in is installed on the machine, the options in the *OpenPGP keyring* tab in the properties of the user account will allow managing these keys.



8.8.1 Importing an OpenPGP keyring

1. Open the **Stormshield Data Security** menu.
2. Select **Properties**.
3. Go to the *Configuration* tab.
4. Select the **key ring** icon.
5. Select the *OpenPGP keyring* tab.
6. Click on **Operations** then on **Import a keyring**.
7. Select a file in OpenPGP format (*.gpg*, *.pgp*or *.asc*). The file may contain several keys.
8. Enter the password that protects the file.

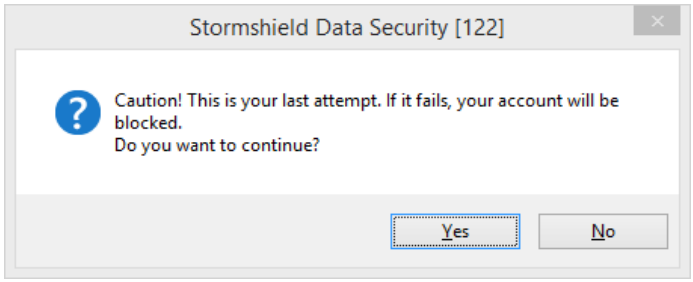
8.9 Unblocking your account

If you forgot your password, or if your account has been locked after entering too many incorrect codes consecutively, you can unblock your account using 2 different procedures:

- Using the Security Officer (backup) password you created when setting up your account.
- If you do not know the Security Officer (backup) password: contact your administrator to provide him with the characters suite to unblock your account.

The number of logins is typically set to three, however, this can be modified; see the *Administration Guide*.

Before the last login attempt, the following window will be displayed. If you click **No**, the login attempt will not be counted, and you can check your password carefully before your next attempt. Remember that the secret code is case-sensitive.

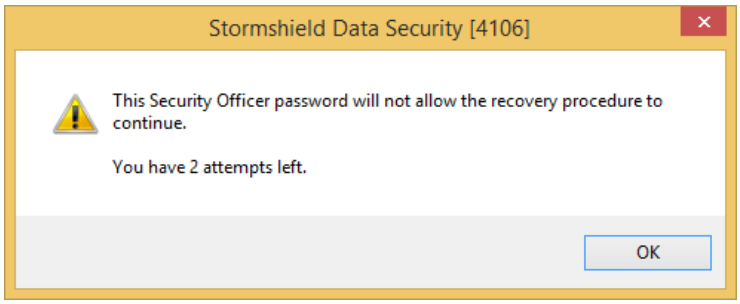


If your account is locked, the following error window will be displayed. This window will be displayed as soon as your account is blocked, and on all subsequent log in attempts, regardless if you are using the correct password or not.

8.9.1 To unlock the account if you know the Security Officer Password:

1. Right click the system tray, and select **Unlock**.
2. Skip the introduction message, then select **You know the Security Officer password**.
3. Enter the Security Officer password, then click **Next**.

If you did not enter the correct Security Officer password, the following message will be displayed:



IMPORTANT
If you block the Security Officer password, you will not longer be able to unlock the account.

4. Enter a new user password according to the criteria displayed and confirm it.
5. Click **Finish**. The account is now operational again. You must connect to Stormshield Data Security using the new password.

8.9.2 To unlock the account if you do NOT know the Security Officer Password:

1. Right click the system tray, and select **Unlock**.
2. Skip the introduction message, then select **You do not know the Security Officer password**.
3. Provide the administrator with the series of characters displayed on the screen.

The number of characters can vary depending on how the account was created and can be up to 126 characters:

IMPORTANT
Do not close the password recovery window until your administrator contacts you.

4. Enter the characters your administrator provided and click **Next**. The account is unblocked.
5. Enter a new user password according to the criteria displayed and confirm it.
6. Click **Finish**. The account is now operational again. You must connect to Stormshield Data Security using the new password.

9. Functional errors

NOTE
In the following tables, the term Log means an event has been saved in Microsoft Windows Event Logs.

The PIN code is wrong.	
Circumstance	You entered an incorrect PIN code in the account creation wizard.
Consequence	Displaying the message: “Incorrect confidential code. Please enter it again.” Requested to enter a new one.
Log	Yes

The card is blocked.	
Circumstance	The inserted card is blocked.
Consequence	Displaying the message: “Your card is blocked”.
Log	Yes

You do not have the authorizations on the accounts storage folder.	
Circumstance	You do not have the authorizations on the folder in which the user accounts are created.
Consequence	In this case, the Stormshield Data kernel does not launch and displays the message: “The values of DefaultyPath1 and/or DefaultPath2 parameters present in *sbox.ini* are not valid. Stormshield Data Security cannot start. Please contact your administrator.”
Log	Yes

The content of the card does not allow you to create the account.	
Circumstance	The content of the card/token (number and type of keys) does not match the automatic creation policy defined in the *sbox.ini* file.
Consequence	Displaying the message: “The content of your card does not allow you to use the automatic account creation”. The account has not been created.
Log	Yes

The template is blocked.	
Circumstance	The template used to create the account is password-protected: it is blocked after too many attempts to log on to the account.

Consequence	Displaying the message: “The template is blocked (too many attempts)”. The account has not been created.
Log	Yes

The template account cannot be accessed.	
Circumstance	The template cannot be found, is not accessible or does not correspond to the type of account you request (*sbox.ini* or permissions on the template file are not set correctly).
Consequence	Displaying the message: “Failed to copy template” The account has not been created.
Log	Yes

The list of trusted certificates cannot be accessed.	
Circumstance	The list of certificates cannot be found or cannot be accessed following a bad setting of *sbox.ini* or permissions on the certificats file(s).
Consequence	Displaying the message: “Failed to copy template”. The account has not been created.
Log	Yes

A user is already logged on to Stormshield Data Security in another Windows session.	
Circumstance	You are not logged on to Stormshield Data Security in a Windows session, open a second Windows session and try to log on to Stormshield Data Security.
Consequence	Connection denied with the message “A user is already logged on”.
Log	Yes

The PIN code is wrong.	
Circumstance	You entered an incorrect password or PIN.
Consequence	Displaying the message ”The secret code is wrong”. Displaying the number of remaining attempts. Requested to re-enter the password or PIN code.
Log	Yes

The entered identifier or the inserted card do not match any Stormshield Data Security account.	
Circumstance	You entered an identifier for which there is no Stormshield Data Security account. You inserted a card for which there is no Stormshield Data Security account.

Consequence	Displaying the message: “This user does not exist”. Requested to re-enter a new identifier.
Log	Yes

The card used to unlock is not the card expected.	
Circumstance	The account has been locked after you removed a card and a different card has been inserted to unlock Stormshield Data Security.
Consequence	Displaying the message: “The card in the drive is not the card of xxxxx, or it is not the correct card.” The account is not locked.
Log	Yes

The secret code is incorrect.	
Circumstance	You entered an incorrect password or PIN code.
Consequence	Displaying the message: "The secret code is incorrect". Displaying the number of remaining attempts. Requested to re-enter the password or PIN code.
Log	Yes

Appendix A. Credits

The software Stormshield Data Security uses the freeware component BouncyCastle.Net. Here is the license:

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

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

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

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

documentation@stormshield.eu