



**STORMSHIELD**



GUIDE

# STORMSHIELD DATA SECURITY ENTERPRISE

## STORMSHIELD DATA SIGN

File signature

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd\_sign-user\_guide-v10



# Table of contents

Preface .....	3
1. Introduction .....	4
1.1 Authenticity and data integrity .....	4
1.2 Stormshield Data Sign key features .....	4
1.2.1 Multiple signatures .....	4
1.2.2 Active content detection .....	5
1.2.3 Compliance .....	5
1.2.4 Compatibility .....	5
1.2.5 Easy to use .....	5
1.3 A secured connection to Stormshield Data Security .....	6
2. Installing Stormshield Data Sign .....	7
2.1 Required configuration .....	7
2.2 Installing Stormshield Data Sign .....	7
3. Interacting with Stormshield Data Sign .....	8
3.1 Using the right-click .....	8
3.2 Using the drag-and-drop feature .....	8
3.3 Using the menu bar .....	8
4. Configuring Stormshield Data Sign .....	10
4.1 Displaying the configuration window .....	10
4.2 Configuring general settings .....	10
4.3 Configuring the active content detection settings .....	11
5. Using Stormshield Data Sign .....	12
5.1 Signing a file .....	12
5.1.1 Signing a file and signing and encrypting a file from the context-sensitive menu .....	12
5.2 Checking a signed file .....	13
5.3 Extracting the original file .....	16
5.4 Reading the content of a signed file .....	16
5.5 Signing a file that is already signed .....	17
5.6 Counter-signing a specific signature .....	18
5.7 Notifying by email .....	19
5.8 Removing a file from the Signature book list .....	19

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



## Preface

---

This document provides essential information on the use of Stormshield Data Sign. It describes the functions of Stormshield Data Sign in its default configuration. You can customize the installation of this component using Stormshield Data Authority Manager. The customization options are the most important in this guide. This guide is for

1. system administrators who want to install Stormshield Data Security.
2. users who want to protect confidential files.



# 1. Introduction

This chapter describes the features and characteristics of Stormshield Data Sign.

## 1.1 Authenticity and data integrity

Stormshield Data Sign is a digital signature software which allows you to digitally sign electronic documents and check signed documents. Digital signatures are based on Public Key Infrastructure (PKI) and are the result of a cryptographic operation.

Stormshield Data Sign allows thereby your organization to guarantee for any document the authenticity of its signatory and the integrity of its content.

In addition, signing a document with Stormshield Data Sign can be considered as a commitment, like a written signature does.

When you sign an electronic document using Stormshield Data Sign:

- the unique fingerprint of the document is created using a mathematical algorithm
- the document fingerprint is signed using your private key and is combined with your public key and certificate to create your unique digital signature which is appended to the document

Stormshield Data Sign then encloses the signed document in a new file, using the name of the original file and a specific file extension. The signed document is sealed and any changes made to it after it has been signed invalidates the signature, thereby protecting against signature forgery and information tampering.

When you check a signed document using Stormshield Data Sign:

- the signature of the sender is verified using the public key of the sender and the original document fingerprint is extracted. Then Stormshield Data Sign calculates the fingerprint of the received data and compares it to the original one previously extracted. If both fingerprints are the same, the document integrity is validated
- the authenticity of the signatory is then validated using the certificates and Certificate Revocation Lists (CRLs)

## 1.2 Stormshield Data Sign key features

Stormshield Data Sign provides the following key features:

### 1.2.1 Multiple signatures

Stormshield Data Sign allows multiple levels of signatures on the same document. You can therefore:

- co-sign a document by adding your own signature to a document already signed, independently from other signatures (already present)

For example, a contract between two parties requires both party signatures. Stormshield Data Sign allows each party to sign the contract independently from each other and in any order.

- counter-sign a signed document by adding your own signature on someone else's signature.

For example, the payment of an invoice must be first signed by the person who places the order to validate the invoice, then counter-signed by the accountant. Payment requires both



signatures; the accountant waits for the validation of the person who places the order, and actually counter-signs the validation.

- over-sign by signing the envelope containing an already signed file.

For example, a transporter guarantees the integrity of the document which must be delivered by placing the signed document in an envelope and signing this envelope. No co-signature or counter-signature can then be added or removed from the transported document. The over-signer does not know the content of the envelop.

### 1.2.2 Active content detection

In addition to supporting various types of documents, Stormshield Data Sign provides PDF and Microsoft Word document analysis and can detect macros or dynamic fields (for example, the current date) that could later modify the appearance or contents of a document after it has been signed. Stormshield Data Sign warns you of potential risks but lets you make your own decision.

If an active content is detected by Stormshield Data Sign during the signature operation, an error message and a warning icon are displayed in the summary window. However, the signature is not forbidden.

If an active content is detected during the signature check, the signature is considered as suspicious and a warning icon is displayed. Refer to [Section 5.2, "Checking a signed file"](#) for more information.

#### NOTE

Active content detection requires Microsoft Word to be installed on the computer and is only available for .doc documents. The .docx and .docm documents cannot be processed.

### 1.2.3 Compliance

Stormshield Data Sign implements CMS Standard: Cryptographic Message Syntax – RFC 2630.

### 1.2.4 Compatibility

Stormshield Data Sign allows you to save the signed files using two different file type extensions: .p7f and .p7m.

.p7m signed files can be sent to and validated by parties who do not run Stormshield Data Sign but run a software conforming to signature format defined in the RFC 2630 instead.

### 1.2.5 Easy to use

Stormshield Data Sign is fully integrated in the Windows environment, which enables you to sign any files with a simple right-click.

Moreover, the way you use Stormshield Data Sign is quite similar to the way you use a signature book. First, you temporarily put the documents awaiting signature in the Security BOX Sign-Signature book. Then you sign the documents. In addition, Stormshield Data Sign allows you to check the signature[s] of signed documents and extract the original file content of signed documents.

**i NOTE**

In the guide, the Security BOX Sign-Signature book is often simply referred to as the Signature book

### 1.3 A secured connection to Stormshield Data Security

Access to your keys is protected: to be able to use your keys, you must connect to Stormshield Data Security, a process which involves self-authentication, i.e. proving that you are actually the owner of the keys.

Stormshield Data Security provides two authentication methods:

- by password: you enter an identifier and a password,
- by smart card or USB token: you enter the secret code of the card – that is the Personal Identification Number (PIN).

Storage of keys will be defined to meet the required level of signature. Signatures demanding a high level of security require the use of enhanced-security devices such as smart cards and USB tokens. These devices provide a strong authentication and password management by generating and storing users' personal credentials such as private keys, passwords and digital certificates inside the protected environment of the smart card chip. Users' private keys cannot be lost, read or used by a third party. For more formal signatures, a password can be sufficient.

For further information, handling user accounts is described in the *Installation and Implementation guide*.



## 2. Installing Stormshield Data Sign

This chapter provides information on Stormshield Data Security requirements and installation.

### 2.1 Required configuration

For the required configuration, refer to the section **Compatibility** of the Stormshield Data Security 10.1 Release Notes.

200 MB of disk space are needed for the installation of all the Stormshield Data Security components.



#### IMPORTANT

Stormshield Data Security is not compatible with the **Fast User Switching** feature.

### 2.2 Installing Stormshield Data Sign

Stormshield Data Sign is a component of Stormshield Data Security.

Stormshield Data Security installation is global. The delivered product contains all the components of the software suite and allows you to install the applications and components you choose, according to the rights contained in the license key.

The installation procedure is described in the *Installation and Implementation guide*. Refer to this guide for further information.



## 3. Interacting with Stormshield Data Sign

This chapter describes the different ways of interacting with Stormshield Data Sign from Windows Explorer or from the Security BOX Sign-Signature book.

Stormshield Data Sign is fully integrated into Windows and the Windows Explorer and the Stormshield Data Sign functions can be launched using:

- a right-click after selecting a file in Windows Explorer
- the drag-and-drop feature to the Security BOX Sign-Signature book window.

When the Security BOX Sign-Signature book window is opened, functions can be launched from the menu bar.

### 3.1 Using the right-click

From Windows Explorer or from the Signature book window, select a file and right-click on it to select options from the context sensitive menus.

In the following chapters, we describe the use of right click in priority, as it is the easiest and safest to use.

### 3.2 Using the drag-and-drop feature

When the Signature book is already started, you can select a file to drag and drop in the Signature book window. From the Signature book window, the various functions can be launched from the context-sensitive menus or the menu bar.

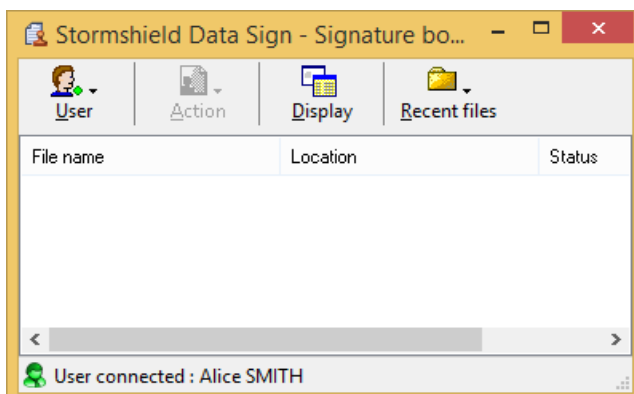
### 3.3 Using the menu bar

This section describes how to launch Stormshield Data Sign functions from the Signature book menu bar.

Open the Signature book window by selecting from the Start menu All programs > Stormshield Data Security > Stormshield Data Sign.

#### NOTE

The Signature book can also be launched from the General tab of the Stormshield Data Sign configuration window by clicking Start Stormshield Data Sign Signature book, as explained in [Section 4.2, "Configuring general settings"](#).



Four different menus are available from the Signature book window. These are described below.





From the User menu, you can:

- lock or unlock a Stormshield Data Security session
- connect to or disconnect from Stormshield Data Security
- access the configuration window
- create new Stormshield Data Security user accounts
- exit the Signature book

The Actions menu provides the same options as the ones available from the context-sensitive menu after selecting a file from the list. If no file is selected, the Actions menu is not available. Available options are:

- Remove to remove the selected file from the list. The file is not deleted from the disk.
- Extract to extract the content of the selected signed file after removing one level of signature (refer [Section 5.3, "Extracting the original file"](#) to for further information)
- Read to run the default action associated with the file type of the selected signed file. It generally opens the default application associated with the selected file.
- Sign to sign the selected file
- Signatures to display the signatures contained in the selected file and check the associated certificates
- Properties to display the properties of the selected file

The Display menu allows you to modify the file display mode:

- Tiles
- Icons
- List
- Details

The display mode options are similar to the ones available from Windows Explorer.

The Recent files displays the list of the files recently processed by Stormshield Data Sign. If you select a file from the list, the selected file is automatically added to the file list displayed in the Signature book window.



## 4. Configuring Stormshield Data Sign

This chapter describes how to configure general and advanced settings.

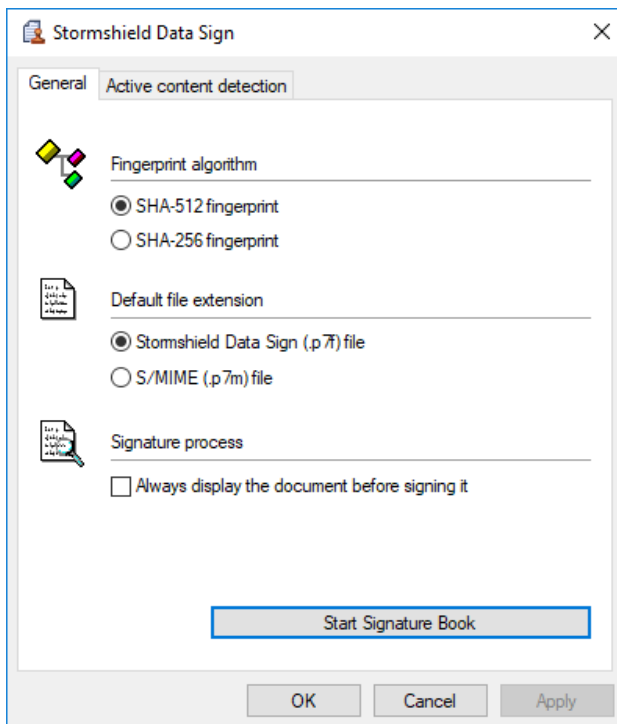
### 4.1 Displaying the configuration window

To display the configuration window:

1. From the system tray, right-click the Stormshield Data Security icon and select Properties.
2. Go to the Configuration tab and double-click the Sign icon. The Stormshield Data Sign configuration window is displayed.
3. Select the General or Active content detection tab according to your needs.

### 4.2 Configuring general settings

The general configuration window is shown below:




From the general configuration window, you can:

- Select the Fingerprint algorithm (hash algorithm) which Stormshield Data Sign will use to compute a fixed-length digital representation of a selected file when signing this file. Select one of the two possible choices:
  - SHA-512,
  - SHA-256.
- Specify the default signed file extension that will be used to identify the new file created when signing a file. The original file name is kept. Only the file extension is different. Select one of these:
  - Stormshield Data Sign (.p7f) file
  - S/MIME (.p7m) file

**i NOTE**

It is recommended to select the *.p7f* file extension to avoid conflicts with any other tool with *.p7m* files.

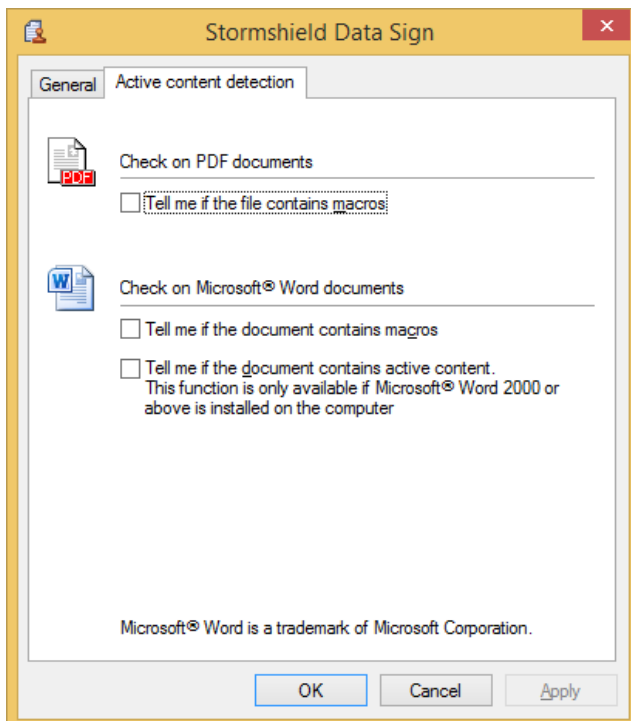
When you select the *.p7f* file extension:

- The icon shown below will be displayed over the right top bottom of the original file icon in the explorer. 
- The file cannot be used by a third party using another signature tool.
- Request for a systematic display of any document before signing it. If the Always display the document before signing it option is selected, you must first display the document before being able to sign it.
- Start the Signature book by clicking **Start Stormshield Data Sign Signature book**. The Signature book can also be started by selecting from the **Start** menu **All programs** > **Stormshield Data Security** > **Stormshield Data Sign**.

### 4.3 Configuring the active content detection settings

PDF and Microsoft Word documents can contain macros and active content, i.e. dynamic fields, which can later modify the appearance or the contents of the document without your intervention. If you sign such a document, there is a risk that the document layout or contents be later modified after you signed it, hence resulting in document integrity issues.

Before you sign a document, Stormshield Data Sign can check it in order to detect macros or active content in it. To do so, select the appropriate boxes in the Active content detection window, shown below:





## 5. Using Stormshield Data Sign

This chapter describes the tasks you can perform with Stormshield Data Sign.

### 5.1 Signing a file

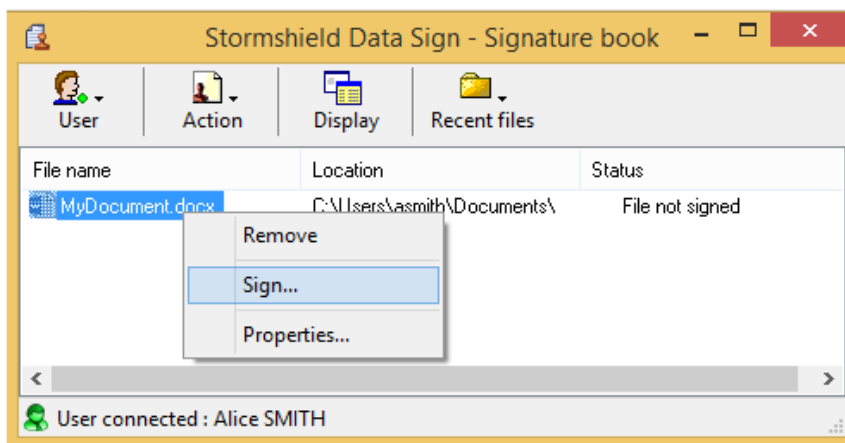
To sign a file:

1. In Windows Explorer, select the file you want to sign and right-click to select Send to > Stormshield Data Sign from the context-sensitive menu. The file is then dropped in the Signature book window.

#### NOTE

If the Signature book window is already open, you can select the desired file, and drag and drop it in the Signature book window.

2. Right-click on the file to select Sign from the context-sensitive menu.



3. Follow the instructions displayed on the screen. When prompted, enter your password or PIN code (if you use a smart card).

If you are about to sign a Microsoft Word or a PDF document, Stormshield Data Sign can analyze this document and warn you of the presence of macros or active content which could dynamically modify the appearance and content of the document after you signed it (refer to [Section 4.3, “Configuring the active content detection settings”](#)). It is then up to you to sign or not the document.

Displaying the document before signing it is optional unless you previously checked the Always display the document before signing it option (refer to [Section 4.2, “Configuring general settings”](#)). In this case you must display the document before you can further proceed.

#### NOTE

When you click on Display, the default program that opens the file is automatically launched.

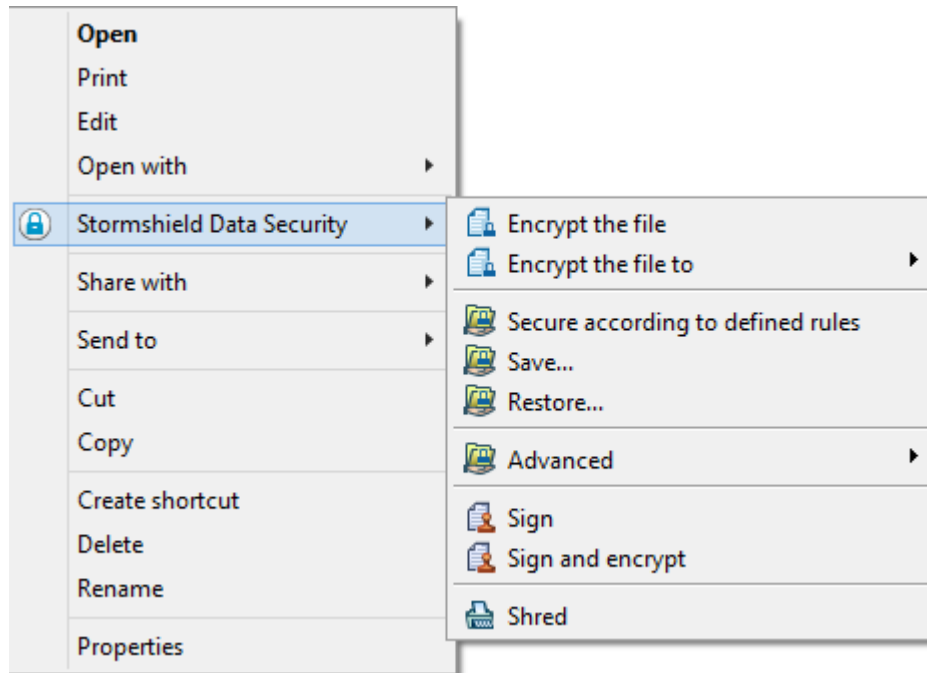
After successfully signing a file, Stormshield Data Sign does not modify the original file. It generates a new file with the same file name and the file extension based on the options previously set (refer to [Section 4.2, “Configuring general settings”](#)).

#### 5.1.1 Signing a file and signing and encrypting a file from the context-sensitive menu

To sign a file from the contextual menu:



1. Select the file to sign and right-click to choose Stormshield Data Sign > Sign from the context-sensitive menu:



2. Follow the instructions displayed on the screen. When prompted, enter your password or PIN code (if you use a smart card) and click on Leave to end the procedure.

To sign and encrypt a file from the context-sensitive menu:

1. Select the file to sign and right-click to choose Stormshield Data Sign > Sign and encrypt from the context-sensitive menu.

#### **NOTE**

This menu is available only if the Stormshield Data Sign module is installed.

2. Follow the instructions displayed on the screen. When prompted, enter your password or PIN code (if you use a smart card) and click on Leave.
3. When the window Choose your correspondents opens, select the correspondents for which you want to operate an encryption and click on OK.

## 5.2 Checking a signed file

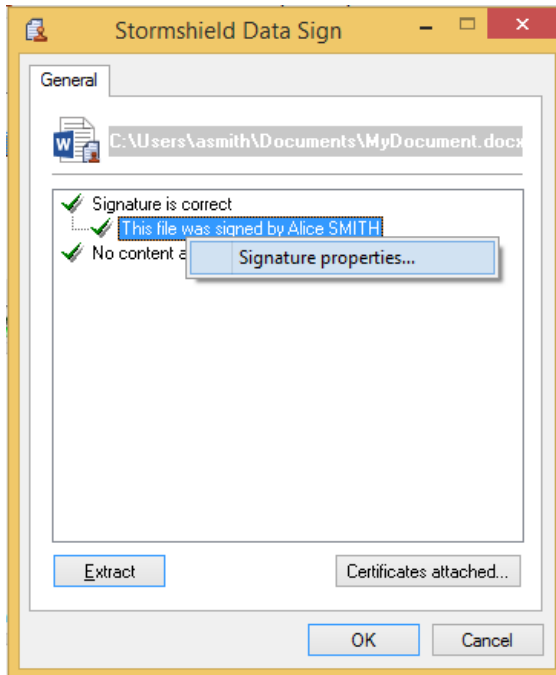
Use the following procedure to check a signed file. The file must have the .p7f or .p7m file extension.

1. In the Windows Explorer, double-click or right-click on the desired file and select Send to > Stormshield Data Sign from the context-sensitive. The Signature book window automatically opens and the file is dropped in it.

**NOTE**

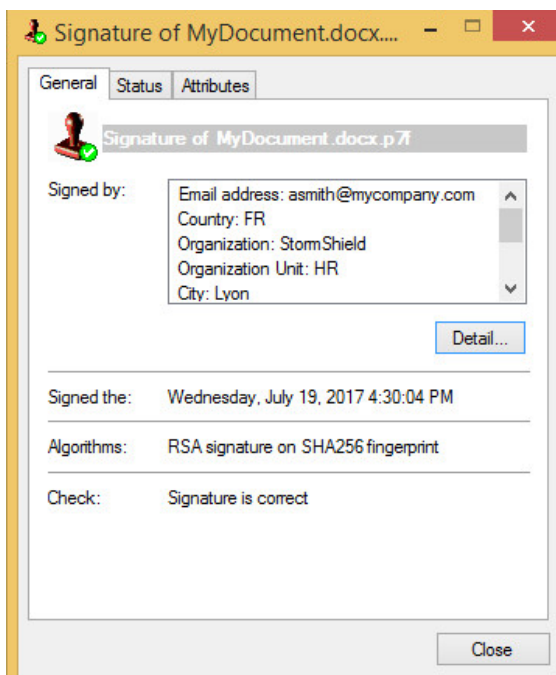
If the Signature book window is already open, you can also drag and drop the desired file in the Signature book window.

2. Right-click on the file to select Signatures from the context-sensitive menu. The signatory's certificate is then displayed, as shown below. Only the primary level of signatures that includes the signature, co-signature(s) and counter-signature(s), is displayed. The second level of signatures, i.e. the over-signature(s), is not shown.



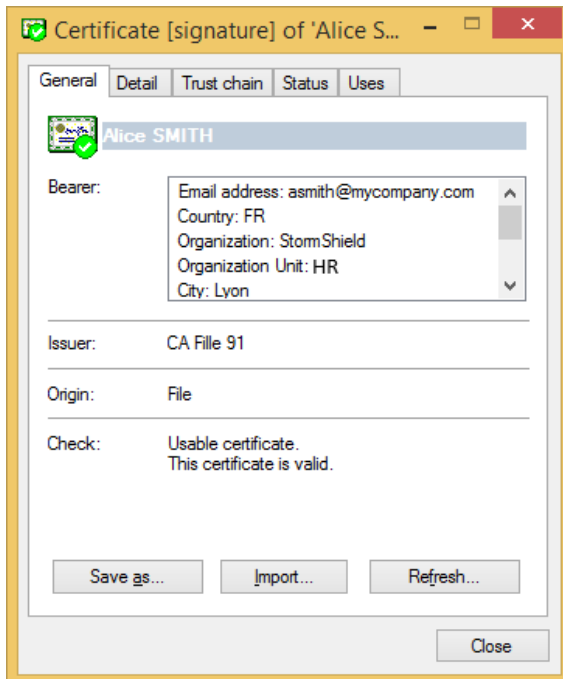
If you click Certificates attached, Stormshield Data Sign displays the certificates attached to the file when it was signed. These certificates cannot be considered as reliable and must be checked with your trusted address book or the LDAP directory.

3. Right-click on a signature and select Signature properties from the context-sensitive menu. The following window is displayed.





4. Click on Detail to display the signatory's certificate, as shown below.



Stormshield Data Sign checks:

- The file content and signature authenticity: Stormshield Data Sign verifies the signature and gets the original document fingerprint. Then Stormshield Data Sign calculates the document fingerprint of the signed document and compares it to the original document fingerprint. If they are the same, the signed document has not been altered.
- The signature certificate validity: Stormshield Data Sign checks the validity of the certificate which guarantees the authenticity of the signer. In case of multiple signatures, each individual signature is checked: all of the certificates needed to validate the digital signatures are verified.

In order to validate the certificate, the most recent Control Revocation Lists (CRLs) are used. As the CRLs are regularly updated, the result of the verification may be different each time you request a verification.

Click Import to import user certificate into your trusted address book.

Click Refresh to dynamically update the signature information with new data including new certificates or CRL input.

When the verification is complete, Stormshield Data Sign displays, next to the icon of the checked file, an icon that shows the result:



Signature is correct and the signatory's certificate is valid.



An anomaly was found.



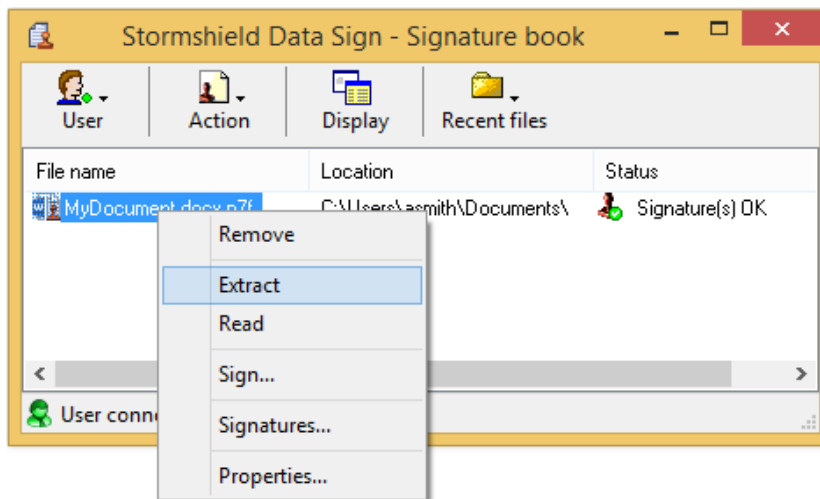
A serious error was found.



### 5.3 Extracting the original file

Use the following procedure to extract the original content of the signed file and save it into a new file.

1. Do one of the following:
  - From the Signature book window, right-click on the file and select Extract from the context-sensitive menu, as shown below:



- From the next window displaying the file signature, click Extract.
2. Type in the file name under which the extracted and original file will be saved.

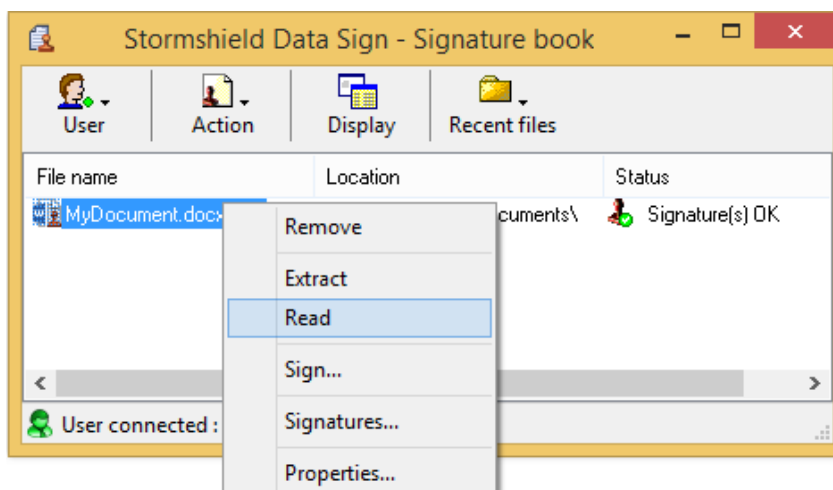
#### **i** NOTE

If you extract an over-signed file, the resulting extracted file contains the primary signature but does not contain the over signature. The file extraction removes only one level of signatures.

### 5.4 Reading the content of a signed file

Use the following procedure to open a signed file without extracting the original file and saving it onto your disk.

1. From the Signature book window, right-click on the desired file to select Read from the context-sensitive menu.







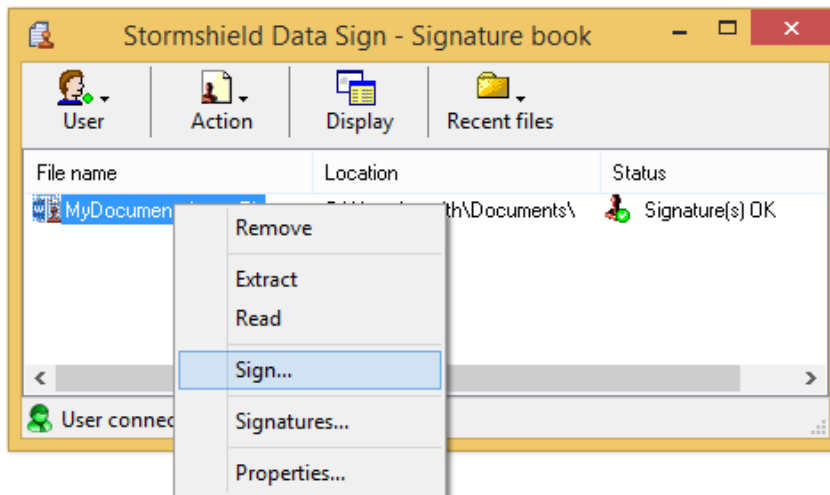
The signature report displays.

2. Click on Read. The default action associated with the type of the file is automatically run. Generally, the file is opened by the appropriate application.

## 5.5 Signing a file that is already signed

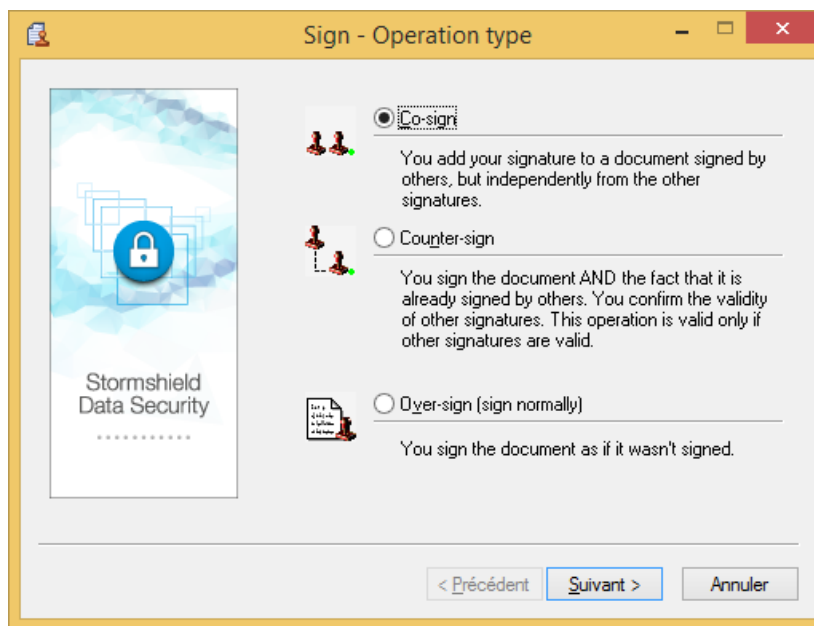
To sign a file which is already signed:

1. In Windows Explorer, right-click on the desired file to select Send to > Stormshield Data Sign from the context-sensitive menu. The Signature book window automatically opens and the file is dropped in it.
  - If the Signature book window is already open, you can drag and drop the desired file in the Signature book.
  - You can double-click on a .p7f file. The Signature book window automatically opens and the file is displayed in it.
2. From the Signature book window, right-click on the file to select Sign as shown below:



3. Follow the instructions displayed on the screen. When prompted for it, enter your password or PIN code (if you use a smart card).

The Operation type window is displayed.



4. Select one of the options according to your needs:

- Co-sign to add your own signature to the file, independently from any other signature already present and whether they are correct or not.
- Counter-sign to add your signature and counter-sign all the other signatures already included (and possibly other counter-signatures). Other signatures must be first successfully checked to ensure the counter-signature validity.

**i NOTE**

You can either counter-sign:

- all the signatures of a signed document (as described above)

or

- only one given signature. For further information, refer to [Section 5.6, "Counter-signing a specific signature"](#).
- Over-sign to over-sign a document. When you over-sign a document, you actually create a new file using the same file name and an additional .p7f extension.

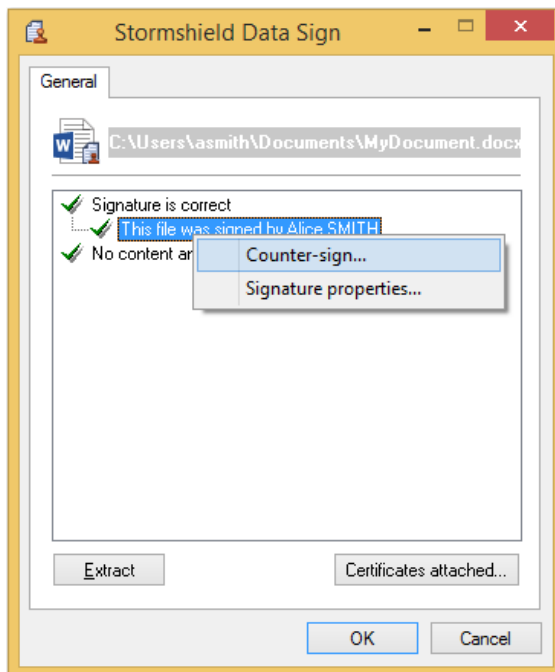
**i NOTE**

Each time a file is over-signed, the .p7f extension is added to the new file generated. It is then possible to find files with several .p7f file type extension.

## 5.6 Counter-signing a specific signature

To counter-sign a specific signature in an already signed file:

1. In Windows Explorer, right-click on the desired file to select Send to >Stormshield Data Sign from the context-sensitive menu: the file is dropped in the Signature book window.
2. From the Signature book window, right-click on the desired file and select Signatures from the context-sensitive menu.
3. Stormshield Data Sign displays a signature and counter-signature tree contained in the file.
4. Right-click on the signature you want to counter-sign and select Counter-sign. Enter your PIN code or password:



Your counter-signature is added to the original signed file. This modification will be effective as soon as you close the window.

## 5.7 Notifying by email

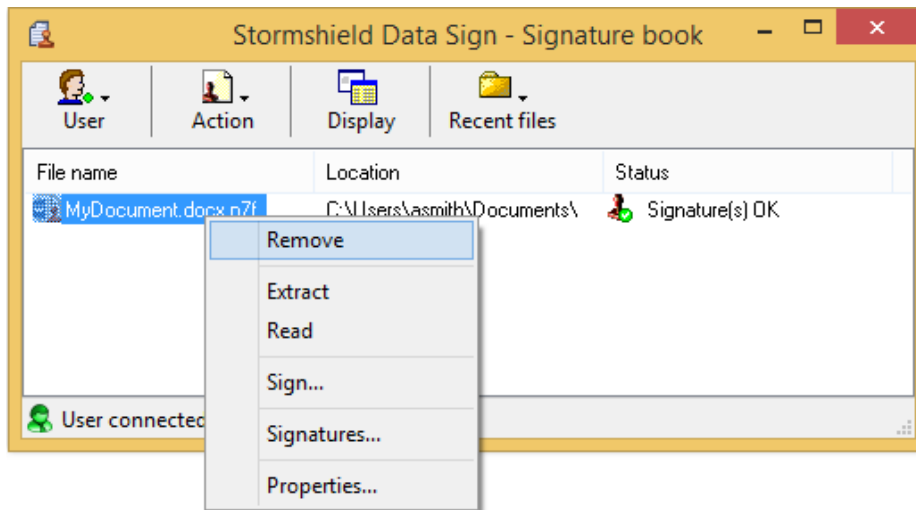
On the last window of the wizard, there are two notification options:

- **Notify coworkers by email:** Stormshield Data Security prepares an email intended to coworkers to notify them the document has been signed. If the document was previously signed, the recipients list is pre-filled with the co-signatories email addresses;
- **Request for a signature by email:** Stormshield Data Security prepares an email intended to coworkers to notify them they must sign the document.

It is possible to check these options by default. Refer to the *Stormshield Data Security Administration guide* for more information on the parameters `MailToNotifyCoWorkers` and `MailToAskForSignature` in the [Sign] section of the `Sbox.ini` configuration file.

## 5.8 Removing a file from the Signature book list

1. From the Signature book window, right-click on the desired file to select Remove.



2. Confirm your choice.

The file is then removed from the list but is not deleted from the disk.

**i NOTE**

Another quick way to remove a file from the list is to select the file and click the Delete key on your keyboard.



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*All images in this document are for representational purposes only, actual products may differ.*

*Copyright © Stormshield 2022. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.*