



**STORMSHIELD**



GUIDE

**STORMSHIELD DATA SECURITY  
ENTERPRISE**

# STORMSHIELD DATA AUTHORITY MANAGER

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd\_authority\_manager-user\_guide-v10



# Table of contents

Preface .....	8
About Stormshield Data Security Enterprise .....	8
Applicability .....	8
Audience .....	8
1. Use environment .....	9
1.1 Recommendations on security watch .....	9
1.2 Recommendations on keys and certificates .....	9
1.3 Recommendations on algorithms .....	9
1.4 Recommendations on user accounts .....	9
1.5 Recommendations on workstations .....	9
1.6 Recommendations on administrators .....	10
1.7 Recommendations on files encryption .....	10
1.8 Certification and qualification environment .....	10
2. Introduction .....	11
2.1 Description .....	11
2.2 Architecture .....	11
3. Administrative procedure .....	14
3.1 Defining a Security Policy .....	14
3.2 Need for a certification authority .....	14
3.3 Rollout Phases .....	14
4. Installation/Start-up .....	16
4.1 Required configuration .....	16
4.1.1 Server .....	16
4.1.2 Client .....	16
4.2 Installing and Configuring Web IIS Server .....	16
4.3 Installing Stormshield Data Authority Manager .....	17
4.4 Directory Structure Created during Installation .....	17
4.5 URL Access to Server .....	18
4.6 Configuring the Administrator Workstation .....	18
4.7 Configuring the manager.ini File .....	19
4.7.1 Web Server .....	19
4.7.2 Hardware Security Module .....	19
4.7.3 Internet Access .....	21
4.7.4 Session .....	21
4.7.5 Automatic Processing .....	21
4.7.6 Algorithms .....	22
4.7.7 Disabling PKCS#11 Attributes .....	22
4.7.8 Attributes of Private Keys in User Keystores .....	23
4.7.9 Temporary Files Folder .....	24
4.8 Using a Hardware Security Module (HSM) .....	24
4.8.1 Configuring the hardware security module .....	25
4.8.2 Enabling and Disabling a Container .....	25
4.8.3 HSM Password Management .....	25
5. Creating and configuring a database .....	27
5.1 Introduction .....	27



5.1.1 Link between Certification Authority and Database .....	27
5.1.2 Certification Authority Keys .....	28
5.1.3 Main Administrator and Other Administrators .....	28
5.1.4 Starting an Authority and an Associated Database .....	28
5.1.5 Start-up Password .....	29
5.2 Creating a Database .....	29
5.2.1 Database Creation Wizard .....	29
5.2.2 Bases.ini File .....	30
5.3 Initializing a Database .....	31
5.3.1 Selecting the Database to be Initialized .....	31
5.3.2 Entering the Start-up Password .....	31
5.3.3 Selecting the Security Module .....	32
5.3.4 Creating the Encryption Key .....	32
5.3.5 Entering the Password for the Main Administrator .....	33
5.3.6 Creating the Certification Authority Signature Key .....	33
5.3.7 Initialization Report .....	37
5.3.8 Directory Structure Created during Initialization .....	37
5.4 Starting and Stopping a Database .....	37
5.5 Updating Stormshield Data Authority Manager .....	38
5.5.1 On the same machine .....	38
5.5.2 On a New Machine without Preserving the Tree Structure .....	39
5.5.3 On a New Machine and Copying the Tree Structure .....	39
5.5.4 Running the Database Update Tool .....	40
5.6 Populating a 10.1 database .....	41
5.6.1 Presentation .....	41
5.6.2 Use .....	42
5.7 Opening and Closing a Session on a Database .....	44
5.7.1 Opening a Session on a Database .....	44
5.7.2 Homepage .....	44
5.7.3 Closing a Session on a Database .....	45
5.8 Entering the Operating Settings for the Database .....	46
5.8.1 Settings Page .....	46
5.8.2 Database Page .....	46
5.8.3 Database properties .....	47
5.8.4 Modifying the Start-up Password .....	48
5.8.5 Modifying the Main Administrator Password .....	48
5.8.6 LDAP Configuration .....	48
5.8.7 Outgoing Mail Server .....	51
5.8.8 User Management .....	52
5.8.9 Component Configuration Parameters .....	56
5.8.10 Certificate Management Parameters .....	56
5.8.11 Certificate Templates .....	62
5.8.12 External Certification Authorities .....	63
6. Defining Administrators and Their Roles .....	66
6.1 Introduction .....	66
6.2 Authorizations .....	66
6.3 Administrators List Page .....	67
6.4 Administrator Page .....	68
6.5 Adding an Administrator .....	69
6.5.1 Adding an External Administrator to the Database .....	69
6.5.2 Adding an Internal Administrator to the Database .....	69



7. Certification authority operation .....	70
7.1 Introduction .....	70
7.1.1 Services Provided .....	70
7.1.2 Public Access and Authenticated Access .....	70
7.2 Homepage .....	71
7.2.1 Public Access Page .....	71
7.2.2 Authenticated Access Page .....	71
7.3 Managing the Certification Authority Key .....	72
7.3.1 Authority Certificate and Key Page .....	72
7.3.2 Making a Certificate Request .....	74
7.3.3 Importing a New certificate .....	74
7.3.4 Exporting the Key .....	74
7.4 Requesting a Certificate .....	74
7.4.1 Requesting a Standard Certificate .....	75
7.4.2 Requesting an Advanced Certificate .....	78
7.4.3 Displaying the Status of a Certificate Request .....	80
7.5 Displaying and Processing Certificate Requests .....	81
7.5.1 List of Pending Requests .....	81
7.5.2 Processing a Certificate Request .....	82
7.6 Displaying and Processing Issued Certificates .....	85
7.6.1 Finding a Certificate .....	85
7.6.2 List of Certificates Issued .....	86
7.6.3 Displaying a Certificate .....	87
7.6.4 Publishing a Certificate .....	88
7.6.5 Revoking a Certificate .....	89
7.7 Managing Certificate Revocation Lists (CRL) .....	90
7.7.1 Displaying the Revocation List .....	90
7.7.2 Generating a Revocation List .....	91
7.7.3 Generating Revocation Lists Automatically .....	91
8. User management .....	92
8.1 The different Types of Users .....	92
8.1.1 Template .....	92
8.1.2 Recovery Account .....	92
8.1.3 Security Policy Signatory .....	93
8.1.4 Standard User .....	93
8.2 Users Management Page .....	94
8.3 List of Templates Page .....	94
8.3.1 Creating a User Template .....	95
8.3.2 Template Page .....	97
8.3.3 Template Properties Page .....	98
8.3.4 Distributing a Master .....	98
8.3.5 Importing Component Configurations from a Master (.msr file) .....	99
8.3.6 Distributing a Security Policy Update File (.usx) .....	100
8.3.7 Creating a Template by Duplicating an Existing Template .....	101
8.4 Users List Page .....	101
8.4.1 Operations Available .....	101
8.4.2 Searching for users .....	102
8.5 Creating Users .....	104
8.5.1 Advanced Creation .....	104
8.5.2 Creating a User from a Template .....	106
8.5.3 Creating a Large Number of Users from a File .....	107
8.5.4 Creating a User from a Smart Card .....	109





8.5.5 Creating a User from a PKCS#12 File .....	110
8.5.6 Creating a User from a user File .....	112
8.5.7 Creating a User from an LDAP Directory .....	113
8.6 Creating a Recovery Account .....	115
8.7 Creating a Security Policies Signatory .....	116
8.7.1 Renewing a Security Policies Signatory .....	116
8.7.2 Re-creating a Security Policies Signatory .....	116
8.8 Users Page .....	117
8.8.1 Changing the Identity .....	118
8.8.2 Changing Passwords .....	119
8.8.3 Changing the Properties of a Recovery Account .....	119
8.8.4 Removing a User's Association with an LDAP Entry .....	120
8.8.5 Choosing a Template .....	120
8.8.6 Associating a Smart Card or Token .....	121
8.9 Distributing User Accounts .....	121
8.9.1 Installation File (.usi) .....	122
8.9.2 Security Policy Update File (.usx) .....	123
8.9.3 Configuring Stormshield Data Kernel .....	124
8.9.4 Sending by Email .....	124
8.9.5 Distributing an Account .....	125
8.9.6 Distributing More than One Account .....	125
8.10 Remote Account Unblocking .....	126
8.10.1 Managing SO Passwords .....	126
8.10.2 Distributing an Account .....	126
8.10.3 Unblocking an Account Generated by Stormshield Data Authority Manager .....	127
8.10.4 Unblocking an Account Generated by Stormshield Data Security .....	128
8.11 Deleting Users .....	128
8.11.1 Deleting a User .....	129
8.11.2 Deleting More than One User .....	129
8.12 Revoking users .....	129
8.12.1 Revoking a single user .....	130
8.12.2 Revoking several users .....	130
8.13 Synchronizing with an LDAP Directory .....	131
8.14 Associating a User with an LDAP Entry .....	131
9. Managing User Keys .....	133
9.1 Key and Certificate Page .....	133
9.2 Key Properties Page .....	134
9.3 Renewing Keys .....	135
9.3.1 Renewing a key .....	135
9.3.2 Renewing several keys .....	137
9.4 Exporting Keys in a PKCS#12 File .....	139
10. Managing Certificates .....	140
10.1 About External Certificates .....	140
10.1.1 External Recovery Certificates .....	140
10.1.2 Other External Certificates .....	141
10.2 Email notification for a certificate expiry .....	141
10.3 Creating PKCS#10 Certificate Requests .....	142
10.3.1 "Binary"/"base 64" Formats .....	142
10.3.2 Creating a Request .....	142
10.3.3 Creating Multiple Requests .....	143
10.3.4 Having a Request Signed by a Physical Smart Card .....	145



10.3.5 Submitting a Request to a Remote Stormshield Data Authority Manager Server .....	145
10.3.6 Cancelling Requests .....	146
10.4 Renewing Certificates .....	146
10.4.1 Renewing one Certificate .....	146
10.4.2 Renewing More than One Certificate .....	147
10.5 Importing Certificates .....	149
10.5.1 Importing Internal Certificates .....	149
10.5.2 Importing External Certificates .....	153
10.6 Exporting Certificates .....	154
10.6.1 Exporting Internal Certificates .....	154
10.7 Publishing Certificates in an LDAP Directory .....	157
11. Configuring Stormshield Data Authority Manager Components .....	159
11.1 Description .....	159
11.2 Accessing Users' Configurations .....	159
11.3 Configuring a Component .....	160
11.4 Imposing a Configuration on a User .....	161
11.4.1 Description of Main Restrictions .....	161
11.4.2 Limiting the List of Proposed Algorithms .....	161
11.5 Advanced configuration .....	162
11.5.1 Stormshield Data Kernel Parameters .....	162
11.5.2 Stormshield Data Team Parameters .....	165
11.5.3 Stormshield Data File settings .....	167
11.5.4 Stormshield Data Shredder Parameters .....	167
11.5.5 Stormshield Data Mail Outlook Edition settings .....	167
11.5.6 Configuring e-mail templates .....	168
12. Customizing the Installation .....	169
12.1 Description .....	169
12.2 Configuring Stormshield Data Security Operation .....	170
12.2.1 Using a master to create an account .....	170
12.2.2 Parameters for Password Accounts .....	171
12.2.3 Parameters for Smart Card or USB Token Accounts .....	171
12.3 Configuring the Stormshield Data Security Installation Procedure .....	174
Appendix A. Deployment methodology .....	175
A.1. Server .....	175
A.2. Client .....	175
Appendix B. Configuring Windows Server .....	177
B.1. Configuring an IIS Web Server .....	177
B.1.1. Declaring CGI .....	177
B.1.2. Adding Website .....	177
B.1.3. Defining authorizations for Web site .....	177
B.1.4. Configuring manager.ini file .....	178
B.2. Giving Stormshield Data Authority Manager Access to the Network .....	178
B.2.1. Configuring IIS Web Server .....	179
B.2.2. Assigning the NTFS Rights Required for the Network User .....	179
B.3. Assigning DCOM Rights for the Stormshield Data Authority Manager Service .....	180
Appendix C. Migrating from Microsoft Access to Microsoft SQL Server .....	181
C.1. Presentation .....	181
C.2. Procedure .....	181



C.2.1. Creating the SQL Server Destination Database .....	181
C.2.2. Importing the Access Source Database Data .....	181
C.2.3. Declaring the SQL Server database in Stormshield Data Authority Manager .....	182
Appendix D. Renewing Certificates .....	184
D.1. Activating Email Notification .....	184
D.2. Renewing the Certificate .....	184
D.3. Importing the new Certificate in the User Account .....	184
Appendix E. Publishing and Downloading Security Updates Using an LDAP Directory .....	185
E.1. Publishing Updates .....	185
E.2. Configuring the LDAP Directory .....	185
E.3. Downloading Updates .....	188
Appendix F. Publishing and Downloading Security Updates using the Web Server .....	190
F.1. Publishing Updates .....	190
F.2. Configuring the IIS Web Server .....	190
F.3. Downloading Updates .....	190
Appendix G. Publishing and Downloading CRLs .....	192
G.1. Configuring the LDAP directory and the IIS Web server .....	192
G.1.1. LDAP directory .....	192
G.1.2. IIS Web server .....	193
G.2. Configuring in Stormshield Data Authority Manager .....	193
G.2.1. Publishing CRLs .....	193
G.2.2. Downloading CRLs .....	193
Appendix H. Root Authority Certification .....	195
H.1. Renewing the Certificate .....	195
H.2. Renewing the Certificate after Modifying its Identity .....	195
H.3. Revoking the Certificate .....	196
Appendix I. Content of a Certificate issued by the PKI .....	197
Appendix J. Starting a database with PowerShell .....	200
Appendix K. Activating HTTPS protocol on Stormshield Data Authority Manager .....	201
Appendix L. Database Backup/Restoration .....	206
L.1. Backup .....	206
L.2. Restoring .....	206

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



# Preface

## About Stormshield Data Security Enterprise

Stormshield Data Security Enterprise is a software set that includes:

- Stormshield Data Security
- Stormshield Data Authority Manager

**NOTE**

You need to install Stormshield Data Security to use Stormshield Data Authority Manager.

## Applicability

The documentation describes the Stormshield Data Authority Manager functions.

Stormshield Data Authority Manager:

- is a client/server software
- runs on Server operating systems
- manages users who have different rights
- gives you the opportunity to use HSM (Hardware Security Module)
- allows you to use large DBMS such as Microsoft SQL Server

## Audience

This guide is intended for security administrators who define the security policy and who may create user accounts.

This guide should be used in conjunction with Stormshield Data Security *Administration Guide*.



# 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 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.

## 1.7 Recommendations on files encryption

1. The files encryption algorithm must be AES.
2. We recommend transciphering files when deleting co-workers (Stormshield Data Team module).

## 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-recovery 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. Introduction

This chapter presents the Stormshield Data Authority Manager tool in relation to the Stormshield Data Security components, and describes its software architecture.

### 2.1 Description

Stormshield Data Security Enterprise is a workstation security product running on Windows. Its features include:

- file encryption
- irreversible deletion
- electronic signature
- ensuring the confidentiality and integrity of exchanges using messaging systems or on a network

Stormshield Data Authority Manager is an administration tool whose main purpose is to create and manage Stormshield Data Security user accounts. As such it carries out:

- key generation and account creation
- definition and distribution of security policies
- key certification functions

Stormshield Data Security's key certification functions are not restricted to Stormshield Data Authority Manager. It can also certify any other key, for example the key for an SSL server or for another certification authority.

This certificate management includes the usual Public Key Infrastructure (PKI) functions:

- make a certificate request
- confirm or reject a request
- publish the issued certificates on an LDAP server
- revoke a certificate and publish a Certificate Revocation List (CRL)

### 2.2 Architecture

Stormshield Data Authority Manager can be installed on a Windows Server platform and it is controlled via an HTTP server (IIS or Apache). There can be several administrators with different rights. Stormshield Data Security 10.1 product must be installed on each administrator's workstation to ensure it is securely authenticated. Authentication can be carried out using a smart card or USB token.

The key for the certification authority is drawn and stored by one of the following:

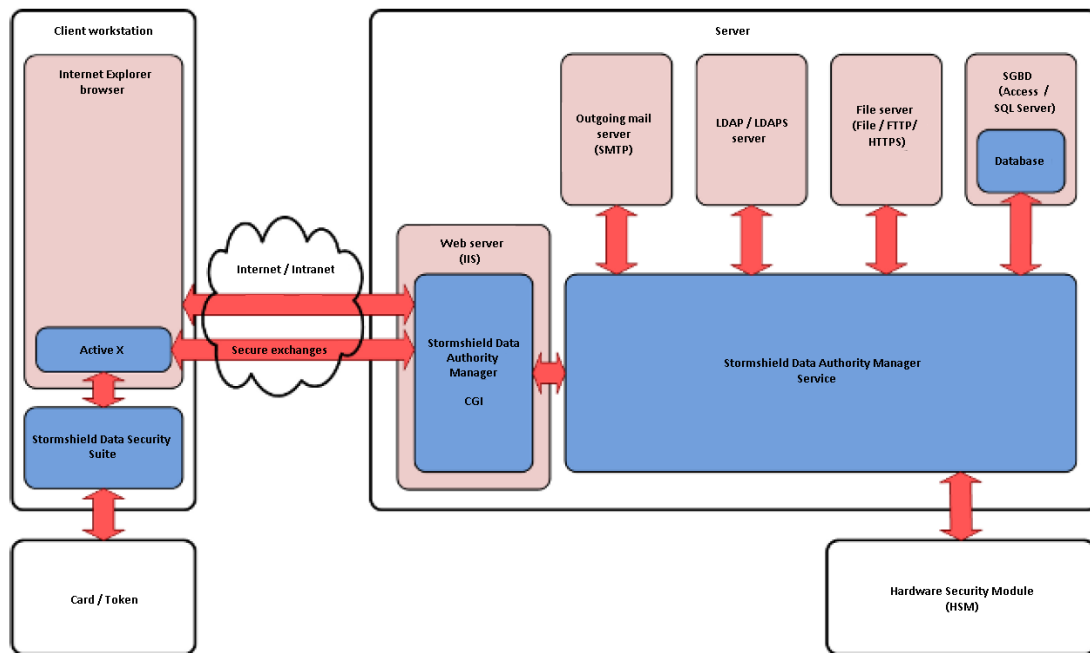
- the Stormshield Data Crypto software security module;
- a Hardware Security Module.

User accounts are stored in a database and the generated certificates are published on an LDAP server. Notifications are sent to the end user by messaging.

#### **i** NOTE

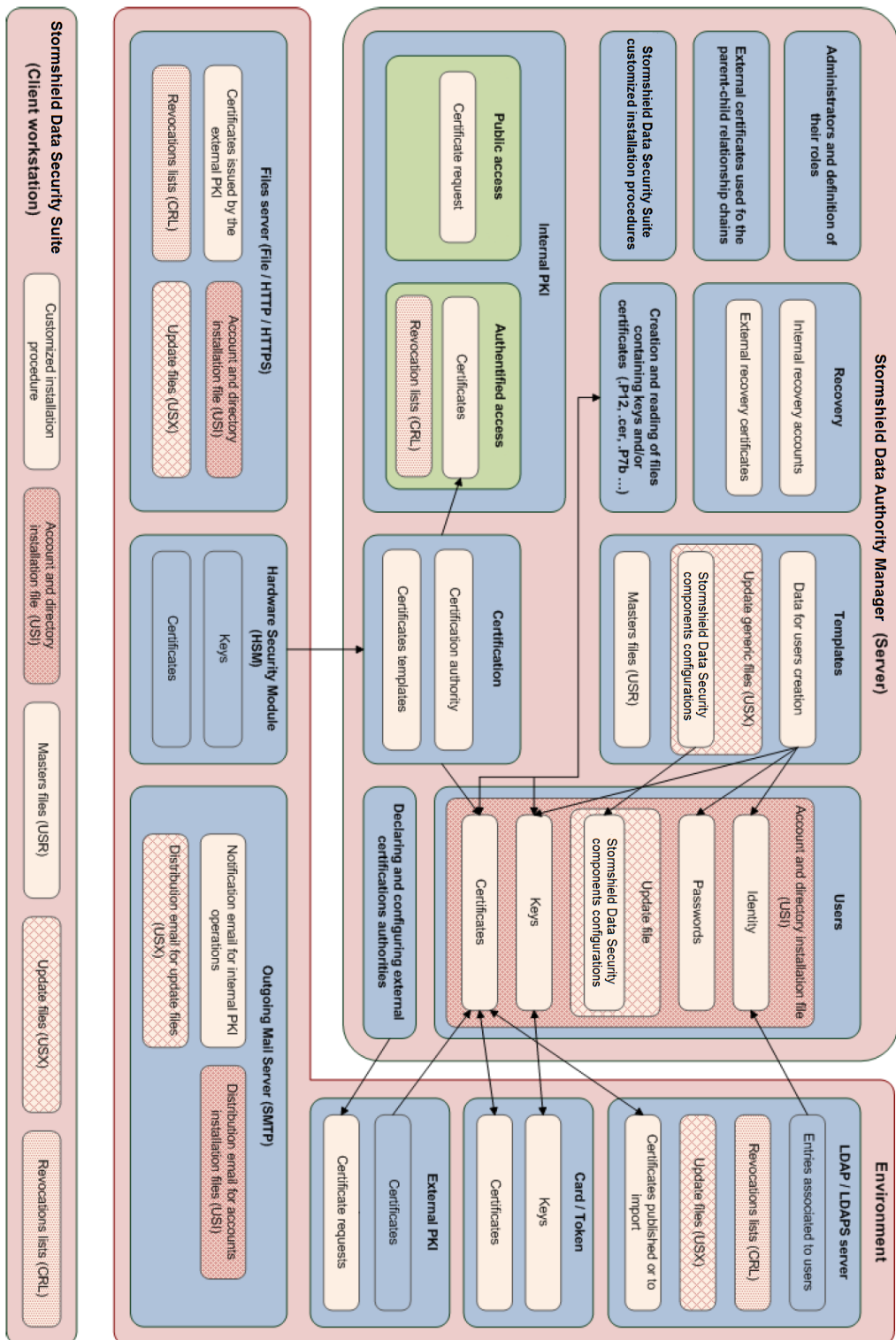
The auxiliary "server" software (HTTP, LDAP, SMTP) are not provided with Stormshield Data Authority Manager.







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





## 3. Administrative procedure

This chapter gives conceptual information on security policy and how to implement it with Stormshield Data Authority Manager, following the step-by-step overall procedure given in a flowchart.

### 3.1 Defining a Security Policy

In order to implement a logical security system in a company, you must define a security policy.

Before starting implementation or rollout, the security manager must:

- identify the risks for the company and their impact on the organization.
- classify information and how it is processed.
- specify the roles and rights of users or groups of users regarding access to information and systems.

Implementing Stormshield Data Security requires you to define:

- how to use numeric certificates, their authority, lifetime and distribution
- how they are made available to users and components
- how to protect the keys and their distribution within hardware devices (cards or tokens)

The security policy must not only set the rules for production and management of numeric certificates (PKI), but also the rules for applying and implementing this security policy on the workstations.

Stormshield Data Authority Manager is a Stormshield Data Security administration tool, which facilitates its rollout within the company, enables the company's security policy to be applied and puts in place an infrastructure based on confidence.

### 3.2 Need for a certification authority

The role of the certification authority is to check certification requests and produce certificates, needed by the security products, in accordance with your company's defined security policy.

According to requirements, rollout within the company can be one of the following options:

- Using self-certified certificates for each user. These are either created and distributed by the owners, or centralized and made available in a directory.
- Creating an authority internal to the company with or without sub-authorities.
- Using an external authority that produces and distributes the certificates and/or smart cards.

To create an authority internal to a company, and so produce and manage certificates, you can use one of the following:

- proprietary PKI software.
- Stormshield Data Authority Manager, which provides the functions required for the rollout of Stormshield Data Security.

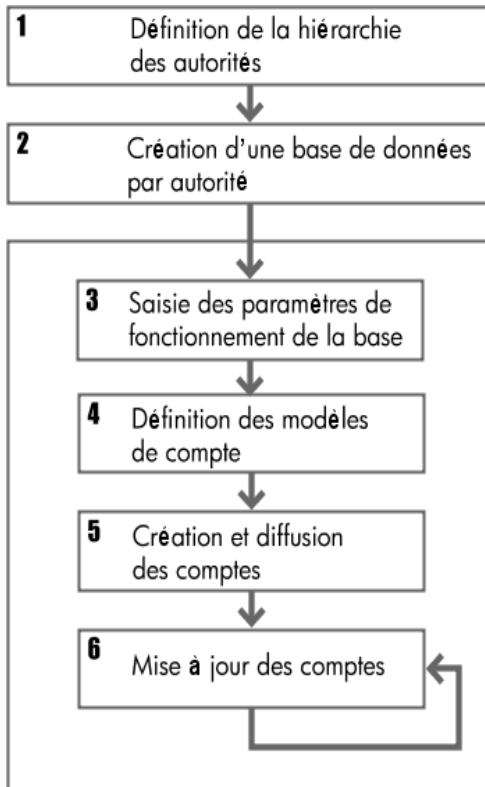
### 3.3 Rollout Phases

Before creating user accounts, you must establish your rollout procedure.



In addition to the rollout of the software itself and its future upgrades, this procedure consists of defining authorities, classifying users using templates and defining the parameters for each template.

The administrator rolling out Stormshield Data Security components must carry out the tasks shown in the diagram below, in the following order:





## 4. Installation/Start-up

This chapter describes how to install Stormshield Data Authority Manager, including: configuration required, server installation and configuration, and HSM (Hardware Security Module) configuration, if any.

A step by step install and start-up procedure for Stormshield Data Authority Manager is provided in [Appendix A, Deployment methodology](#).

### 4.1 Required configuration

#### 4.1.1 Server

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

#### 4.1.2 Client

Stormshield Data Authority Manager requires the following on the client workstation:

- Microsoft Internet Explorer 32 bits version 11 (using the Compatibility View) for “authenticated access pages”.
- Google Chrome 41 or under or Mozilla Firefox 36 or under or Internet Explorer 11 or under for “public access pages”.

#### **i** NOTE

To use the Compatibility View on Internet Explorer 11, select **Tools** and **Compatibility View settings**. Add Stormshield Data Authority Manager website to the Compatibility View list.

- Stormshield Data Security 10.1 for the administrator profile (authenticated access); Security BOX Suite 8.0.x, 9.3.x, Stormshield Data Security 9.3.x or 10.0 for users (public access).
- A user (either power user or administrator) for the installation of ActiveX controls. Once the ActiveX controls have been installed, a standard user can logon.

### 4.2 Installing and Configuring Web IIS Server

To install the IIS Web server:

1. Open the **Server Manager**.
2. Open the **Manage** menu and click **Add roles and features**.
3. In the **Add Roles** assistant, move after the first page and keep **Role-based or feature-based installation** selected. Go to the next window.
4. Select the server on which you will install the role.
5. Check **Web Server (IIS)** and then **Management tools** if needed, and click **Add features**. Then click **Next**.
6. On the **Select features** page, click **Next**.



7. In the **Role Services** page, select the following branches:
  - **Application Development**, then select: **ISAPI Extensions**, **ASP** and **CGI**.
  - **Common http Features**, then select **Static Content**.
  - **Security**, then select **Request Filtering**.
8. Click **Next** and then **Install**.
9. Close the wizard and the **Server Manager** once the installation is finished.

### 4.3 Installing Stormshield Data Authority Manager

Use the *Stormshield Data Authority Manager .msi* file and enter the following command line in a command prompt in administrator mode: `msiexec /i <msi file full path>`.

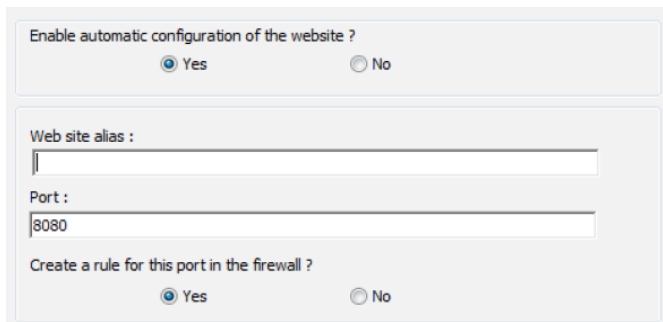
The installation program asks for:

- the license key, provided with the product. For an evaluation version, contact Stormshield commercial department ([sales@stormshield.eu](mailto:sales@stormshield.eu)).
- the installation folder.
- the folder where the databases are to be stored.

Once the installation is finished, the sbasrv service is created and started.

The configuration can be done automatically during the installation:

1. Select **Yes** for **Enable automatic configuration of the Web site?**



2. Provide the Web site alias and the port (or leave the pre-filled values).
3. Select **Yes** for **Create a rule for this port in the firewall?**

The automatic configuration of the IIS Web server is not compatible with ports assigned to protocols. To use these ports (for example the secure port 443), configure manually IIS (to do so, refer to [Section A.1, “Configuring an IIS Web Server”](#) and to [Section J.1, “Activating HTTPS protocol on Stormshield Data Authority Manager”](#)) or configure IIS manually after the automatic configuration on non-assigned ports (refer to [Section J.1, “Activating HTTPS protocol on Stormshield Data Authority Manager”](#)).

### 4.4 Directory Structure Created during Installation

The installation procedure assigns the following default values:

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

Both paths can be changed during installation.

If you want to use DBMS Microsoft Access, the folder `<sdam_data_install_dir>` must not be networked.



The following directory structure is created when Stormshield Data Authority Manager is installed:

- installation folder:

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

- data folder:

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

## 4.5 URL Access to Server

The root URL to access the IIS Web server is:

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

Where <hostname> is the name of the machine hosting the server or <IPAddress>:port>.

In this document, this URL is also known as <manager\_root\_url>.

For instance, from the administrator's workstation, you can access Stormshield Data Authority Manager through the URL: <manager\_root\_url>/OpenSession.

## 4.6 Configuring the Administrator Workstation

Firstly, Stormshield Data Security 10.1 must be installed on the administrator's workstation.

Certain operations carried out by Stormshield Data Authority Manager require that ActiveX components are executed on the administrator's workstation.

You must therefore:

- Add your server to the "trusted sites".
- Authorize execution of ActiveX components that are not marked as trusted on these trusted sites.

To do this:

1. From the Internet Explorer Tools menu, select Internet Options.
2. Select the Security tab, Trusted sites field, click Sites.
3. Enter <manager\_root\_url>, where <manager\_root\_url> is the address of the web server hosting Stormshield Data Authority Manager.
4. Click Add followed by OK.
5. Select Custom Level in ActiveX controls and plug-ins.
6. Change Initialize and script ActiveX controls not marked as safe by selecting Enable.
7. Confirm by clicking OK twice.

To download and install ActiveX, the user must be either an authorized user or an administrator.





Once the ActiveX are installed, a standard user can use the client workstation to connect to Stormshield Data Authority Manager.

## 4.7 Configuring the manager.ini File

The *manager.ini* configuration file, located in the Stormshield Data Authority Manager installation folder <sdam\_install\_dir>, contains parameters that are database-independent.

For changes to certain parameters to be taken into account, the Stormshield Data Authority Manager service needs to be restarted. Proceed in one of the two following ways:

- In the command window, type `net stop sbasrv` then `net start sbasrv`.
- In the Windows services window, right-click Stormshield Data Authority Manager service and select **Restart**.

### 4.7.1 Web Server

Use the [WebServer] section to configure the various paths, which are dependant on your Web server configuration.

If you later change the configuration of your Web server, remember to change these parameters so that Stormshield Data Authority Manager can work correctly.

#### [WebServer]

ManagerRootUrl	Root URL <manager_root_url> used to access the Stormshield Data Authority Manager server, as defined in <a href="#">Section 4.5, "URL Access to Server"</a> . This URL is used to build the links in the notification emails. Default value: determined automatically.  For technical reasons this automatic resolution may not be reliable so it is essential that you enter this parameter.
ManagerCgiUrl	URL added as prefix to names of actions related to the links present in Stormshield Data Authority Manager pages. Must be specified when using absolute links. Default value: blank, meaning links are relative.
ManagerDocUrl	URL prefixed to links to resources (images, ActiveX, etc.) used in the pages. If you use an IIS web server with the configuration given in <a href="#">Appendix B. Configuring Windows 2008 Server [R2]</a> , the parameter value is "/". Default value: blank, meaning links are relative.

### 4.7.2 Hardware Security Module

If you are installing a hardware security module (HSM), you must declare it in the [HSM] section.

One or more "containers" must then be defined. This generic term describes a physical component in the module: a slot or a token according to the type of module.

#### [HSM]

Name	Descriptive name for the module.
------	----------------------------------



DllName	Full path for the PKCS#11 DLL associated with the module.
ContainerIdentification	<p>Must only be specified if the HSM has more than one "container". Means of differentiating between "containers". Possible values are:</p> <ul style="list-style-type: none"> <li>TokenSerialNumber: the "container" is a token identified by a serial number</li> <li>TokenLabel: the "container" is a token identified by a label</li> <li>SlotId: the "container" is a slot identified by its identifier</li> </ul>

If your HSM only has a single "container", add a [ContainerIfUnique] section with a Login key.

#### [ContainerIfUnique]

Login	<p>Means of logging in to the "container". Possible values for this key are:</p> <ul style="list-style-type: none"> <li>none: a login is not requested</li> <li>null: a null pointer is sent</li> <li>empty: an empty string is sent</li> <li>gui: a secret code is requested from the user when the container is activated (see <a href="#">Section 4.8, "Using a Hardware Security Module (HSM)"</a>)</li> <li>any other string</li> </ul> <p>Default value: gui</p>
-------	--

If your HSM has several "containers", add a [Container\_XXX] section for each "container" you want to use. The section names must be unique. They are used as identifiers for tokens and slots (see [Section 4.8.2, "Enabling and Disabling a Container"](#)).

#### [Container\_XXX]

Name	Descriptive name for the "container".
TokenSerialNumber, TokenLabel or SlotId	Value identifying the "container".
Login	<p>Means of connecting to the "container". The possible values for this key are:</p> <ul style="list-style-type: none"> <li>none: no login is required;</li> <li>null: a null pointer is transmitted;</li> <li>empty: an empty chain is transmitted;</li> <li>gui: a secret code is required for the user during the container activation (see <a href="#">Section 4.8, "Using a Hardware Security Module (HSM)"</a>);</li> <li>any other chain.</li> </ul> <p>By default: gui</p>

#### Examples:

For an HSM with a single "container":

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

[ContainerIfUnique]
Login = gui
```



For an HSM with more than one "container":

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

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

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

### 4.7.3 Internet Access

Requesting a certificate from a remote Stormshield Data Authority Manager server (see [Section 10.3.5, "Submitting a Request to a Remote Stormshield Data Authority Manager Server"](#)) requires that Stormshield Data Authority Manager sends an HTTP request to the remote server. If the remote servers are not located on the local intranet but on the Internet, it is possible that the HTTP requests will be sent via a proxy, depending on how your network is configured.

In order for these HTTP requests to be sent via a proxy, the proxy must be specified in the [Internet] section. If it is not specified, the requests will be sent directly to the remote servers.

[Internet]	
ProxyName	Name or address of the proxy machine and its port separated by ":".
ProxyBypass	Addresses for which the proxy will not be used, separated by ";".

### 4.7.4 Session

To use Stormshield Data Authority Manager, each administrator must open a session beforehand on the database concerned.

The [Ctx] section deals with the management of work sessions.

[Ctx]	
LifeTime	Period beyond which an unused session is closed, in seconds. Default value: 900 seconds (15 minutes).
ScanTime	Polling interval for sessions, in seconds. Every ScanTime seconds, the software checks that the sessions have not expired. Default value: 60 seconds.

### 4.7.5 Automatic Processing

Stormshield Data Authority Manager lets you carry out certain processes using batch processing: user creation, certificate requests, certificate exports, etc.



In "automatic" processing, an HTML page displays the results of the last operation carried out and runs the next operation.

#### [Auto]

ProcessPeriod	The ProcessPeriod parameter is the elapsed time between displaying this page and starting the next operation (submit) in milliseconds. Default value: 200 milliseconds. This value should be increased on a slow server.
---------------	--

### 4.7.6 Algorithms

The [Algo] section defines the various algorithms used by Stormshield Data Authority Manager.

#### [Algo]

HashStartKey CryptStartKey	Algorithms used to derive and encrypt the start-up password. Default value: AES 256 bits / SHA-1.
KeyGenSecretKey	Algorithm for generating the secret encryption key. Default value: AES 256 bits.
CryptBase	Encryption algorithm for sensitive data in the database. Default value: AES 256 bits.
IterationCountKeystore HashKeystore CryptKeystore	Derivation and encryption algorithms for protecting authority keys when stored in a keystore file. Default value: 10000 / SHA-1 / AES 256 bits.
GroupDH HashDH CryptDH	Diffie-Hellman group and hashing and encryption algorithms used to protect exchanges between an administrator's workstation and the server. Default value: 14 / SHA-256 / AES 256 bits.

The values for the encryption algorithms are: DES Simple 64 bits, DES Triple 128 bits, DES Triple 192 bits, AES 128 bits, AES 192 bits, AES 256 bits, RC5 40 bits, RC5 64 bits, RC5 128 bits, RC5 256 bits, RC4 40 bits, RC4 64 bits, RC4 128 bits, RC4 256 bits, RC2 40 bits, RC2 64 bits, RC2 128 bits and RC2 256 bits.

The values for the hashing algorithms are: SHA-1, MD5 and MD2.

The values for the Diffie-Hellman group are 5, 14, 15, 16, 17 and 18.

### 4.7.7 Disabling PKCS#11 Attributes

Certain HSMs do not support the PKCS#11 attributes used by Stormshield Data Authority Manager.

If this is the case, it is possible to disable the use of PKCS#11 attributes when certain objects are created.

To disable a PKCS#11 attribute:

1. Declare a section with the name of the object for which this attribute is to be disabled.
2. Add a key with the name of the attribute to be disabled (from the list below) and with value set to 0.



Section	PKCS#11 Object Concerned
[CA_Public_Key_HSM]	Public certification key drawn by the HSM
[CA_Private_Key_HSM]	Private certification key drawn by the HSM
[CA_Public_Key_P12]	Public certification key imported from a PKCS#12 file
[CA_Private_Key_P12]	Private certification key imported from a PKCS#12 file
[WK_Public_Key_HSM]	Public encryption key drawn by the HSM
[WK_Private_Key_HSM]	Private encryption key drawn by the HSM
[WK_Public_Key_P12]	Public encryption key imported from a PKCS#12 file
[WK_Private_Key_P12]	Private encryption key imported from a PKCS#12 file

You can disable the following attributes:

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

#### Example:

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

This means you do not want the PKCS#11 attribute CKA\_LABEL to be declared when the HSM draws the public encryption key.

#### 4.7.8 Attributes of Private Keys in User Keystores

Stormshield Data Authority Manager creates a keystore file for each user, which is a PKCS #11 token.

As such, each object created in this token will have PKCS#11 attributes.

The sections below let you define the value of two sensitive attributes relating to private user keys:

Section	Operation type
[SBox.NewUserWizardExKS1]	Password account with a single key



[SBox.NewUserWizardExKS2]	Password account with two keys
[SBox.NewUserWizardExGP1]	Card account with a single key
[SBox.NewUserWizardExGP2]	Card account with two keys

**[SBox.NewUserWizardExXXX]**

NoExtractableK	The private key can be exported: 0: Yes 1: No Default value 0.
KModifiable	Indicates if the keys can be changed, i.e. if they have the PKCS#11 attribute CKA_MODIFIABLE set. 0: the keys cannot be changed. 1: the keys can be changed. Default value 0.

**Example:**

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

This means that the password account key cannot be exported by the user.

**4.7.9 Temporary Files Folder**

Stormshield Data Authority Manager creates and deletes temporary files. This parameter allows to specify the folder in which temporary files are created. The product installation gives the <sdam\_data\_install\_dir>\SBMData\tmp value to this parameter.

If you modify this value, select an existing folder and gives the network user the right to modify the folder.

It is advised to fill in this parameter.

**[Path]**

TempPath	Folder into which Stormshield Data Authority Manager creates and deletes temporary files. Value by default: <sdam_data_install_dir>\SBMData\tmp
----------	--

**4.8 Using a Hardware Security Module (HSM)**

As a reminder, the key for the certification authority is drawn and stored by one of the following:

- a Stormshield Data Crypto software security module
- a hardware security module

This section explains how to use a HSM.



### 4.8.1 Configuring the hardware security module

To use a hardware security module, you must declare it beforehand and define any "containers" (token or slot) it has in the *manager.ini* file (see [Section 4.7.2, "Hardware Security Module"](#)).

### 4.8.2 Enabling and Disabling a Container

Activating a "container" (token or slot) consists of logging in Stormshield Data Authority Manager to this container. Disabling consists of logging out.

On your server, several authorities can store their keys in the same container. In this case, this container must be enabled once only: all authorities will thereafter be able to use their keys.

Activation and deactivation is carried out using the command line program SBMHSM.EXE installed in the Tools folder in Stormshield Data Authority Manager installation folder <sdam\_install\_dir>.

You can open a console directly on this folder from the Start menu by selecting All Programs, Stormshield Data Authority Manager , then Open a shell console].

Note that

To enable a token or a slot:

```
SBMHSM /A [-c <identifier>] [-p <password>] [-s]
```

---

-c: token or slot identifier

---

-p: password (see [Section 4.8.3, "HSM Password Management"](#) below)

---

-s: silent mode: no messages are displayed

To disable a token or a slot:

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

---

-c: token or slot identifier

---

-s: silent mode: no messages are displayed

To display the status of tokens or slots defined in the *manager.ini* file:

```
SBMHSM /L
```

### 4.8.3 HSM Password Management

Stormshield Data Security can work with different HSMs with different hardware configurations depending on the security and confidence levels they provide.

For an HSM made up of a secure database, security token and special keyboard ("PIN pad"), the HSM may be initialized using the "PIN pad" directly linked to the basic device to enter the Token access password.

PIN entry is activated via a call to a standard Login function.

For other devices, and depending on the PKCS#11 middleware implementation provided by the manufacturer of the HSM, you must specify the type of PIN passed as a parameter to this Login





function in the *manager.ini* file (see [Section 4.7.2, “Hardware Security Module”](#)). This Login parameter may take the following values:

- None: the Login function is not called (Login was carried out when the server was started and is valid for all products running on the server).
- Null: a null pointer is sent.
- Empty: an empty string is sent.
- Gui: a secret code is required to validate start-up (default value). In this case, the secret code can be:
- Passed from the SBMHSM.EXE command line (see [Section 4.8.2, “Enabling and Disabling a Container”](#) below).
- Requested interactively by this program.
- Any other string which could for example be a keyword identifying a login profile.



## 5. Creating and configuring a database

This chapter presents the links between a CA (certification authority) and a database, and it describes all the necessary steps to create, initialize, configure and start a database and open a session.

### 5.1 Introduction

#### 5.1.1 Link between Certification Authority and Database

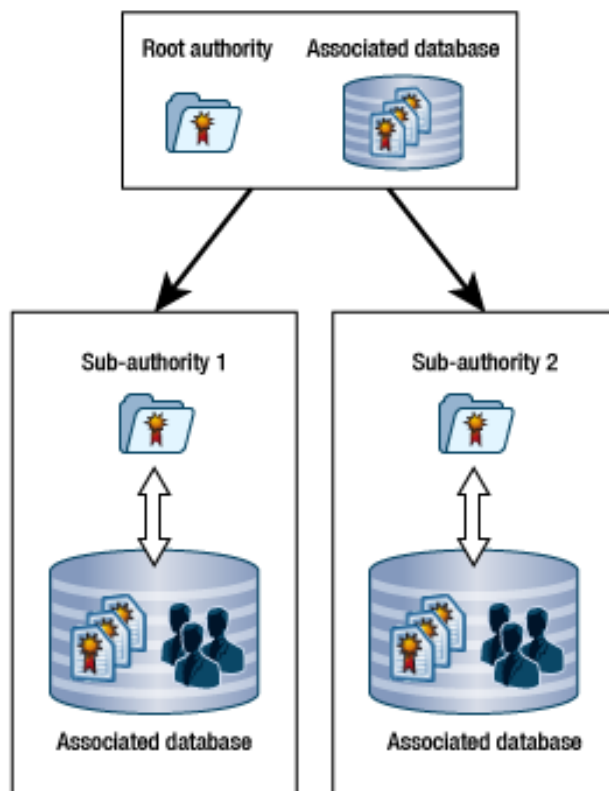
Each certification authority (or sub-authority) controls its own database, which contains:

- the user accounts it manages.
- and/or the certificates it generates.

The Key Management Infrastructure to be implemented depends on a company's technical and organizational constraints according to whether it wants centralized or decentralized certificate management and users managed by entity.

After defining the list of authorities in your infrastructure, their respective roles and hierarchy, you have to declare a database for each authority. These two operations correspond to step 1 and step 2 of the rollout procedure, and they are grouped into a unique procedure.

The following diagram illustrates a simplified two-level hierarchy comprising a root authority and two sub-authorities:





### 5.1.2 Certification Authority Keys

A certification authority works using two keys:

- The "certification authority" key itself is used to sign certificates generated by this authority. This key identifies the authority publicly.
- The "encryption" key, which is used to encrypt users' confidential data held in the database (their private keys, password, etc.).

This key is internal to Stormshield Data Authority Manager.

Both these keys are of the same type (RSA two-key) and are stored in the same security module:

- either Stormshield Data Authority Manager's internal module (i.e. a keystore file).
- or a Hardware Security Module (HSM).

It is important to note that no database recovery mechanism is implemented. This is why it is essential to backup both keys:

- If the internal module is used by backing up the file keystore and the database after the initialization procedure described below.
- If an HSM is used by using the token duplication methods it offers.

### 5.1.3 Main Administrator and Other Administrators

A database can be managed and administered by several physical administrators, each administrator possibly having a different role (see section [Defining Administrators and Their Roles](#)).

Such an administrator is authenticated automatically and securely through the Stormshield Data Security account (password account or smart card/USB token account).

The main administrator can authenticate using a simple password (without a secure mechanism using a Stormshield Data Security account), which the other users cannot do. The *bases.ini* file located in Stormshield Data Authority Manager installation folder <sdam\_install\_dir> defines the main administrator's rights:

- all rights.
- only the right to manage administrators.
- no rights (which is equivalent to disabling the main administrator).

Refer to [Section 5.2.2, "Bases.ini File"](#) for a definition of the main administrator.

### 5.1.4 Starting an Authority and an Associated Database

The order of operations for preparing an authority or a database is defined in the following procedure:

1. First create your database (see [Section 5.2, "Creating a Database"](#)). This will be the physical support for managing the authority and the user accounts.
2. Then initialize this database, which mainly consists of generating certification and encryption keys for the authority (see [Section 5.3, "Initializing a Database"](#)).

Your database is now operational.

To use this database you must:



3. Start it up (see [Section 5.4, “Starting and Stopping a Database ”](#)). The authority associated with the database can:
  - Receive certificate requests.
  - Automatically and periodically update the Certificate Revocation List (CRL).
4. Open a session on this database (see [Section 5.7.1, “Opening a Session on a Database ”](#)) either using the "main administrator" password or with your Stormshield Data Security account: you will then have access to all the functions for which you are authorized.

Note that if you were using a previous version of Stormshield Data Authority Manager, you must import the data from your old database.

### 5.1.5 Start-up Password

Starting and stopping a database requires the use of a special password.

This "start up password" may be granted to a user; it does not give authorization to use Stormshield Data Authority Manager services.

The procedure for defining the start-up password is in [Section 5.3.2, “Entering the Start-up Password ”](#).

## 5.2 Creating a Database

Stormshield Data Authority Manager supports two DBMS: Microsoft Access and Microsoft SQL Server.

The database creation wizard allows you to:

- Create and populate a database, if the administrator chooses to work with Microsoft Access.
- Take an existing populated database into account, if the administrator chooses to work with Microsoft SQL Server.

#### **i** NOTE

For Microsoft SQL Server databases, before using the creation tool, you must:

- create the bases: one Microsoft SQL Server base per desired Stormshield Data Authority Manager base.
- populate these bases beforehand with the script `create_database_SqlServer.sql` provided in the folder `<sdam_install_dir>\DataBase`.

Detailed information are provided in [Appendix C, Migrating from Microsoft Access to Microsoft SQL Server](#).

### 5.2.1 Database Creation Wizard

1. Run SBMCB.EXE by selecting All Programs, Stormshield Data Authority Manager, Create a new database from the Windows Start menu.

#### **i** NOTE

The tool must be launched with administration rights in order to avoid the base creation process to stop because of a lack of privileges.

2. On the first page, enter:



- The database identifier using only lower case letters without accents or digits. This identifier is mainly used internally by Stormshield Data Authority Manager.
  - The database label. This label is used in all Stormshield Data Authority Manager pages to refer to the user database.
3. In the second page, you can select the database type:
- If Microsoft Access is selected, the database is created, and you can access the administrator's rights main page directly.
  - If Microsoft SQL Server is selected, you can access a form to connect to an existing Microsoft SQL Server database:

If the Ask for connection password every time check box is not checked, then you must enter the password in this page. You can control the parameters by testing the connection when clicking the Test button.

4. The main administrator's rights page: select the permissions (see [Section 6.2, "Authorizations"](#)) that will be granted to the main administrator. Choose between:
- granting all rights.
  - granting only the right to manage administrators (Permissions administrator).
  - disabling the main administrator (No rights). In this case, a session will only be able to be opened by a secure authentication (see [Section 5.7.1, "Opening a Session on a Database"](#)) after the database has been initialized (see [Section 5.3, "Initializing a Database"](#)). You must then create at least one Permissions administrator just after the database has been initialized (see section [Defining Administrators and Their Roles](#)).
5. In the last page, confirm the database configuration by clicking the Finish button.

The link to a physical database has now been established. You must now initialize it as described in the next section.

## 5.2.2 Bases.ini File

The *bases.ini* file, located in Stormshield Data Authority Manager installation folder <sdam\_install\_dir>, has one section per database.

This section, which has the same identifier as the associated database, is automatically created and filled in by the database creation wizard SBMCB.EXE.

Each section contains the following data:

[<BaseId>]	
BaseName	Common name of database
ConnectionString	Connection string to the DBMS. For Microsoft Access: Provider=Microsoft.Jet.OLEDB.4.0; Data Source=<sdam_data_install_dir>\SBMData\DataBases\<baseid>.sba For Microsoft SQL Server: Provider=SQLOLEDB;Data Source=<server name>; DataBase=<database name>; User Id=<user ID>; Password=<password>



AskSqlPwd	<p>Password request when connecting to the database.</p> <ul style="list-style-type: none"><li>0: The password is not requested to the user when connecting to the database. If you do not use Microsoft Access, you must ensure that the password is filled in the <code>ConnectionString</code> section.</li></ul> <div><p><b>! IMPORTANT</b></p><p>This means the password is visible in the <i>bases.ini</i> file.</p></div> <ul style="list-style-type: none"><li>1: The password is requested to the user when connecting to the database. It is added to the connection string. You must ensure that the Password field is not filled in the <code>ConnectionString</code> section: <code>Password=</code> must be included at the end of the chain, but not its value <code>&lt;password&gt;</code>.</li></ul> <p>If you use Microsoft Access, the parameter value must be equal to 0.</p>
KSPath	<p>Full pathname of the keystore file containing the authority keys. This field is not relevant when the keys are stored in an HSM. Default value: <code>&lt;sdam_data_install_dir&gt;\DataBases\&lt;baseid&gt;.mng</code></p>
MainAdmin	<p>Rights granted to the "main administrator": All: all rights Admin: only the right to manage administrators None: no rights (which means that authentication by simple password is disabled)</p>

## 5.3 Initializing a Database

Initializing a database consists of:

- generating the authority keys (certification key, encryption key).
- defining protection passwords.
- if necessary, having the certification key certified by another authority.

### **i** NOTE

A database that has not been completely initialized cannot be used. If the initialization is interrupted for some reason, it cannot be restarted. An unused session has a limited period of life. It is then advised to initialize a database without any significant stop.

### 5.3.1 Selecting the Database to be Initialized

Go to the initialization page by entering the URL `<manager_root_url>InitBase`, where `<manager_root_url>` is the root URL as defined in [Section 4.5, "URL Access to Server"](#).

It gives the list of existing databases that have not been started up.

Run initialization on the selected database by clicking the Initialize button.

### 5.3.2 Entering the Start-up Password

The first part of the page displays the database identifier and label entered when it was created (see [Section 5.2.1, "Database Creation Wizard"](#)).



Identifier	caroot
Label	CA ROOT

A link in the banner of the page allows you to return to the selection page for the databases to be initialized.

Enter the start-up password for the database that will later be used to start up and shut down the database (see [Section 5.4, "Starting and Stopping a Database"](#)).

A database must be started up prior to being used. The startup procedure requires a password to be presented. It must contain between 8 and 64 characters.

Password	<input type="password"/>
Password confirmation	<input type="password"/>

### 5.3.3 Selecting the Security Module

Select the security module in which the encryption key and certification authority key will be stored. They may be stored in the internal security module or in a hardware security module (HSM). The security module is declared in the *manager.ini* file (see [Section 4.7.2, "Hardware Security Module"](#)). Only enabled containers (see [Section 4.8.2, "Enabling and Disabling a Container"](#)) are shown in the list.

Key storage

☐ Store keys in the **internal** cryptographic module

☒ Store keys in a **hardware** cryptographic module

Slot / Token: HSM

### 5.3.4 Creating the Encryption Key

To create the encryption key, you can:

- Have the security module draw the key. If you use the internal security module, you can create an RSA key of 1024, 2048 or 4096 bits. Certain of these key sizes, although shown as possible options, may not be supported by a particular hardware security module.
- Import a key from the PKCS#12 file into the security module.

Enter the complete file pathname together with its password.

Encryption key

Confidential data managed by Stormshield Data Authority Manager are encrypted using a secret key, itself wrapped with an encryption key.

Key creation

☒ Draw an encryption key RSA 2048 bits

☐ Import an encryption key from a PKCS#12 file:

File name Browse...

Password

In all cases, you can choose to create an exportable key, that is, a key which can later be "output" from its security module.





To create an exportable key, Stormshield Data Authority Manager sets the attribute CKA\_EXTRACTABLE to TRUE, and the attribute CKA\_SENSITIVE to FALSE for the private key. For a non-exportable key, it sets the attribute CKA\_EXTRACTABLE to FALSE, and the attribute CKA\_SENSITIVE to TRUE.

**i NOTE**

This property may not be supported by a particular hardware security module.

If you use a hardware security module that does not support all of the PKCS#11 standard, you can disable some PKCS#11 attributes in the *manager.ini* file (see [Section 4.7.7, “Disabling PKCS#11 Attributes”](#)).

If you are importing the key, the showing the contents page of the PKCS#12 file is displayed in which you confirm the import.

### 5.3.5 Entering the Password for the Main Administrator

The first part of this page displays a report of the encryption key creation operation.

Enter the password for the main administrator (see [Section 5.8.5, “Modifying the Main Administrator Password”](#)). This password will be requested when a session on the database is opened by password.

Main administrator's password

The main administrator is the only administrator authenticated through a password.

Password

Password confirmation

### 5.3.6 Creating the Certification Authority Signature Key

Select the creation mode for the certification authority signature key:

- Do not create a certification authority in the database. The database is now initialized. You are taken directly to the database initialization report page (see [Section 5.3.7, “Initialization Report”](#)).
- Have the security module Draw a new key (see [the section called “Generating the Certification Authority Key”](#)).
- Import a key from a PKCS#12 file (see [the section called “Importing the Certification Authority Key”](#)).
- Use a key already present in the hardware security module (see [the section called “Using a Key already Present in the Hardware Security Module”](#)).

Database certification authority

Certification authority

☐ Do not create an authority

☒ Draw an authority key

☐ Import an authority key from a PKCS#12 file

☐ Use an authority key present in the hardware cryptographic module



## Generating the Certification Authority Key

Generating the certification authority key

This page lets you choose the size of the RSA key to be drawn by the security module. If you use the internal security module, you can create an RSA key of 1024, 2048 or 4096 bits. Some of these key sizes, although shown as possible options each time may not be supported by all hardware security modules.

**Certification authority's key**

Key size	RSA 2048 bits
Exportable key	<input type="checkbox"/> Mark key as exportable

You can choose an exportable key. But this property may not be supported by all hardware security modules.

If you use a hardware security module, you can choose not to set certain PKCS#11 attributes when the key is drawn (see [Section 4.7.7, "Disabling PKCS#11 Attributes"](#)).

Generating the key certificate

The first part of this page displays a report of the encryption key generation operation.

1. Enter the identity of the certification authority:

**Authority identity**

Common name	
Organization	
Organization unit	
City	
State or province	
Country	France (FR)
DN	

2. To generate the certificate for the certification authority key, you can choose to:

- Have the key certified by an external certification authority. You are taken to the certificate request page, which offers you several request options (see [Section 10.3.2, "Creating a Request"](#)).

If you choose to request a certificate to a remote Stormshield Data Authority Manager, you must enter:

- The root URL <manager\_root\_url> of the remote Stormshield Data Authority Manager (see [Section 4.5, "URL Access to Server"](#)).
- The identifier of the database present on the server. It contains the certification authority to be used.
- The label of the certificate template, which is present in this database, and that must be used to generate the certificate.



Remote Stormshield Data Authority Manager server

The certificate request is automatically submitted to a remote Stormshield Data Authority Manager certification server.

Server's URL:

Database identifier:

Certificate template name:

After the request is confirmed, the database initialization report page is displayed (see [Section 5.3.7, "Initialization Report"](#)).

#### **i** NOTE

The certificate generated by the external authority must later be imported (see [Section 7.3.3, "Importing a New certificate"](#)). Until imported, the certification authority cannot generate any certificates.

- Have the certification authority certify the key itself. The authority then becomes a self-certified root authority. You are taken directly to the database initialization report page (see [Section 5.3.7, "Initialization Report"](#)).

Authority certification

☒ Key certified by an external authority

☐ Self-certified (root) key

Validity period: 10 years  
The certificate will be valid until Sunday, April 08, 2018.

Algorithm: Certificate signed by SHA-1 et RSA

Depth: The number of certificates in the certification path starting from this authority, excluding the end certificate unlimited

Key identifier: ☒ Include key identifier (SubjectKeyId)

### Importing the Certification Authority Key

In this page, select the full pathname for the PKCS#12 file together with its password.

You can choose an exportable key, but this property may not be supported by a particular hardware security module.

You can enter the first serial number for certificates which will be generated by the certification authority. By default, numbering starts at 1 but it can be necessary to take into account the serial numbers for certificates already distributed by this certification authority with another PKI, insomuch as the serial numbers generation was also incremental.

If you use a hardware security module, you can choose not to set certain PKCS#11 attributes (see [Section 4.7.7, "Disabling PKCS#11 Attributes"](#)) when the key is imported.

The page showing the contents of the PKCS#12 file is then displayed. Confirm the import by clicking the Finish button. You are then taken directly to the database initialization report page (see [Section 5.3.7, "Initialization Report"](#)).

During this operation, the key certificate is also imported from the PKCS#12 file.



**File selection**

File name	<input type="text"/>	<input type="button" value="Browse..."/>
Password	<input type="password"/>	
Exportable key	<input type="checkbox"/> Mark key as exportable	
Certificates serial number	Starting to generate serial numbers from the number	<input type="text" value="1"/> (decimal base)

### Using a Key already Present in the Hardware Security Module

You can also re-use a key already present in the hardware security module as a certification authority. You provide the full pathname of the file containing the key certificate you are looking for in the security module.

**Authority's certificate**

Stormshield Data Authority Manager will search your hardware cryptographic module for a private key that corresponds to your certification authority's current certificate.

File name	<input type="text"/>	<input type="button" value="Parcourir..."/>
-----------	----------------------	---

The page showing the contents of the certificate and the attributes of the key found in the security module is then displayed.

You can enter the first serial number for certificates which will be generated by the certification authority. By default, numbering starts at 1 but it can be necessary to take into account the serial numbers for certificates already distributed by this certification authority with another PKI, insomuch as the serial numbers generation was also incremental.

**Certificate**

Please confirm you want to use the key that corresponds to the following certificate:

Certificate of CA HSM

This certificate is an intermediate authority certificate

- Subject: CA HSM
- Issued by: CA ROOT
- Serial No: 01B9
- Valid from avril 2015, 07 to avril 2025, 07
- Public Key
- Certificate footprints
- Signature
- Authority Key Identifier
- Key Identity
- Key Usage
- Issuing Basic Constraints
- CRL Distribution Points
- Certificate format version: 3

**Private key's attributes**

Algorithm	RSA 1024 bits
Identifiant	Stormshield Data Security C#0000
Label	Clé de CA HSM

**Setting**

Certificates serial number	Starting to generate serial numbers from the number	<input type="text" value="1"/> (decimal base)
----------------------------	---	---

From the page, you confirm the association by clicking the Finish button and you are then taken directly to the database initialization report page (see [Section 5.3.7, "Initialization Report"](#)).



### 5.3.7 Initialization Report

This page displays the database identifier and label with the report of the last operation carried out.

The screenshot shows the Stormshield Data Security Authority Manager web interface. The header includes the title 'Stormshield Data Security Authority Manager' and navigation links for 'CA ROOT', 'Main administrator', 'Close session', and 'Home'. The main content area is titled 'Initialize database' and displays the message: 'Database initialization complete. The certificate for the authority's key has been **successfully** generated and saved in the database.' A 'Home' link is visible at the bottom left of the content area.

### 5.3.8 Directory Structure Created during Initialization

When the database is initialized, the following folders are created under:

<sdam\_data\_install\_dir>\SBMData\<base\_id>

where <sdam\_data\_install\_dir> is the data folder (see [Section 4.4, "Directory Structure Created during Installation"](#)) and <base\_id> is the database identifier.

Folder	Contains:
\Certs	- certificates from another PKI to be imported in batches
\CertsPublished	- certificates generated by Stormshield Data Authority Manager when they are published "by file"
\Crl	- last CRL issued: <base_id>.crl
\CrlHistory	- CRL history in the form: <AAAAMMJJ – CrINbHexa>.crl
\Log	- manager log: <base id>.txt - database migration tool log: BaseUpgrade.txt
\MailTemplates	- definition files for emails issued
\MSITarget	- target for customizing the installation procedure
\Users	- user accounts
\UsersFiles	- list of files of Stormshield Data File and Shredder

## 5.4 Starting and Stopping a Database

To start and stop a database, use *SBMSTART.EXE* contained in the **Tools** folder of the Stormshield Data Authority Manager installation folder.

You can open a console directly on this folder from the **Start** menu by selecting **All Programs, Stormshield Data Authority Manager, then Open a shell console.**



**NOTE**

25 databases can be started simultaneously.

- To start a database:

```
SBMSTART /O [-b <identifier>] [-p <password>] [-s]
```

-b: database identifier entered when it was created (see section [Database Creation Wizard](#)). If this identifier is absent or incorrect, the list of databases that have not been started is displayed.

-p: start-up password for the database entered when it was initialized (see section [Entering the Startup Password](#)).

-s: silent mode: no messages are displayed.

- To stop a database:

```
SBMSTART /C [-b <identifier>] [-p <password>] [-s]
```

-b: database identifier entered when it was created (see section [Database Creation Wizard](#)). If this identifier is absent or incorrect, the list of databases that have been started is displayed.

-p: start-up password for the database entered when it was initialized (see section [Entering the Startup Password](#)).

-s: silent mode: no messages are displayed.

To display the status of the databases defined in the file *bases.ini*:

```
SBMSTART /L
```

- If the startup password contains non ASCII characters (accented characters for example), the tool *SBMSTART.EXE* cannot work. To get around this issue, you can run the base startup command in a PowerShell script. For more information, refer to the section [Starting a database with PowerShell](#).

## 5.5 Updating Stormshield Data Authority Manager

### 5.5.1 On the same machine

Stormshield Data Authority Manager is directly updated with the 10.1 version on the same machine, so the installation folder and the data folder are preserved.

1. Install Stormshield Data Authority Manager version 10.1 directly on top of previous versions. Stop the Security BOX Authority Manager service or the Stormshield Data Authority Manager service according to the version number, when asked during the installation.

If you choose an installation directory other than the previous version, you can activate the automatic configuration of the Web site when installing the new version.

If you choose the same installation directory:

- When installing the software for the first time, if you had chosen the automatic configuration of the Web server, you must activate the automatic configuration again.

**IMPORTANT**

All the customization done in IIS about the Stormshield Data Authority Manager web site will be lost.



- If you had performed the configuration manually, you must not activate the automatic configuration.

You must use the same data folder as for the previous release.

2. Start each database defined in the *bases.ini* file (see [Starting and Stopping a Database](#)).
3. Start the **Database update** tool on each base (see section [Running the database update tool](#)).

If the database is already up-to-date, only the populating feature is provided.

4. In IIS, rename the website by right-clicking the site name > **Rename** with Stormshield Data Authority Manager.

### 5.5.2 On a New Machine without Preserving the Tree Structure

The Stormshield Data Authority Manager version 10.1 software is installed on a new machine, without preserving the former database tree structures.

1. Install Stormshield Data Authority Manager version 10.1 on the new machine.
2. Copy the former versions database files *<base\_id>.sba* and the associated keystores files *<base\_id>.mng* into the folder *<sdam\_data\_install\_dir>/SBMData/Databases*.
3. Replace the new *bases.ini* file with the former *bases.ini* file.
4. Start each database defined in the *bases.ini* file (see [Starting and Stopping a Database](#)).
5. Run the Database update tool on each database (see section [Running the database update tool](#)).

#### NOTE

If the database is already up-to-date, only the populating feature is provided.

A structure tree is created for each database into the *<sdam\_data\_install\_dir>/SBMData* folder and the path names are updated in the general parameters.

### 5.5.3 On a New Machine and Copying the Tree Structure

The Stormshield Data Authority Manager version 10.1 software is installed on a new machine, and the former database tree structures are preserved.

1. Install Stormshield Data Authority Manager version 10.1 on the new machine and choose the automatic configuration of the Web site.
2. Copy the former versions database files *<base\_id>.sba* and the associated keystores files *<base\_id>.mng* into the folder *<sdam\_data\_install\_dir>/SBMData/Databases*.
3. Perform one of the following operations:
  - [step 4](#)
  - or [step 5](#).
4. If the data folder *<sdam\_data\_install\_dir>* is the same as the folder on the preceding machine:
  - For each base, copy the former database tree structure *<sdam\_data\_install\_dir>/SBMData/<base\_id>* on the new machine in the same folder *<sdam\_data\_install\_dir>/SBMData/<base\_id>*.
  - Replace the new *bases.ini* file with the former *bases.ini* file.
  - Start each database defined in the *bases.ini* file (see [Starting and Stopping a Database](#)).



- Run the Database update tool on each database (see section [Running the database update tool](#)).

If the database is already up-to-date, only the populating feature is provided.

#### IMPORTANT

The tool resets general parameters using the tree structure `<sdam_data_install_dir>/SBMData/<base_id>`. If you modified general parameters referring to the original tree structure, these changes are lost.

5. If the data folder `<sdam_data_install_dir>` is different from the folder on the preceding machine:
  - Copy the former database tree structure `<sdam_data_install_dir_former_version>/SBMData/<base_id>` on the new machine in the new folder `<sdam_data_install_dir>/SBMData/<base_id>`.
  - Replace the new *bases.ini* file with the former *bases.ini* file, and update the pathnames defined in the data BasePath and KSPath, using `<sdam_data_install_dir>`.
  - Start each database defined in the *bases.ini* file (see [Starting and Stopping a Database](#)).
  - Run the **Database update** tool on each database (see section [Running the database update tool](#)). The tool resets general parameters using the tree structure `<sdam_data_install_dir>/SBMData/<base_id>`.

If the database is already up-to-date, only the populating feature is provided.

### 5.5.4 Running the Database Update Tool

#### NOTE

When the database is up-to-date, the populating feature only is available.

1. Start the database former version.
2. Run the database update tool SbmUpBa.exe selecting All Programs, Stormshield Data Authority Manager, then Update a database from the Start menu.
3. On the first page:
  - a. Select the identifier for the Stormshield Data Authority Manager former version database to be updated from the identifiers of the databases started.
  - b. Enter the password for the main administrator of the database to be updated.
4. On the next page, confirm the database update.
5. On the last page, a detailed operation report is displayed, and you can edit the operations in a log file.

If the database is a Microsoft Access database, a compaction is carried out after the migration in order to reduce its size and improve the performances. The database must be restarted after this operation.





**i NOTE**

For a Microsoft Access database, if an error occurs when migrating a voluminous database (for example, a database containing more than 40000 certificates, or a database reaching at least 300Mb), you can try again to migrate the database by modifying a value in the registry:

1. From the Start Windows menu, select Execute, then enter regedit.
2. Go to the following key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Jet\4.0\Engines\Jet 4.0
3. Modify the MaxLocksPerFile value: save the former value (by default 9500 in decimal), and enter 250000 in decimal.

After you migrated the database, you must reposition the former value (by default 9500 in decimal).

Please remember this value will be used for all the connections on a database done by Jet, by all your server applications using Jet.

## 5.6 Populating a 10.1 database

### 5.6.1 Presentation

This function allows you to import the users of one 10.1 database into another 10.1 database. Among other things, it allows retrieving the content of a database whose root authority is outdated.

If you want to import a database previous to 10.1, we recommend that you first do an update of the database (see section [“Running the Database Update Tool”](#)).

It can import:

- standard users.

During importation, the “internal administrator” status (see section [Defining Administrators and Their Roles](#)) is not kept. If you want the imported user to be the addressed database administrator, you need to define him/her after you populated the database (see [Section 6.5.2, “Adding an Internal Administrator to the Database”](#)).

**i NOTE**

After you imported the addressed database users, it is relevant to import the certification authority certificate which certified the imported users keys (for example the source database certification authority) into the list of external certificates (see [Section 10.1.2, “Other External Certificates”](#)). This will allow you to distribute accounts with the certificates' trust chain from the destination database.

- templates.

During importation, if a template importation fails because a template with the same identifier is already present, the imported users deriving from this template will derive from the template present into the database.

- recovery accounts.
- security policies signatory.

This importation fails if the destination database already has one.



- certificate templates (see [Section 5.8.11, “Certificate Templates”](#)) and external certification authorities (see [Section 5.8.12, “External Certification Authorities”](#)) used by imported users.
- internal counters.

The “complete” importation in a Microsoft SQL Server 8.0 database of the Microsoft Access 8.0 database content is described in [Appendix C, Migrating from Microsoft Access to Microsoft SQL Server](#).

## 5.6.2 Use

To populate the database, run the SbmUpBa.exe database update tool from the Start menu, selecting All programs, Stormshield Data Authority Manager, then Update a database.

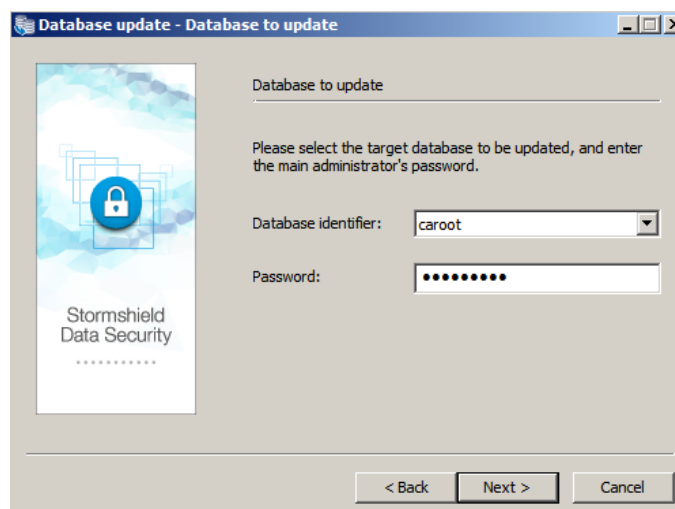
1. From the first page:

- Select the 10.1 database identifier to update among the started database identifiers.

The database to update must have been initialized (see [Section 5.3, “Initializing a Database”](#)).

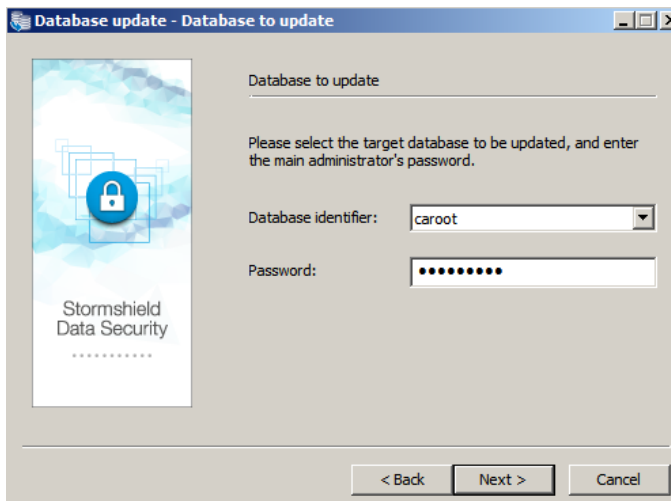
- Enter the main administrator password for the database to update.

If you cannot find the identifier of the database to update, check it has been started.



2. From the second page:

- Select Version 10.1 database.
- Select the 10.1 database from which you want to import the users. If you cannot find the identifier of the database you wish to use, check it has been started.
- Enter the main administrator password of the source database.

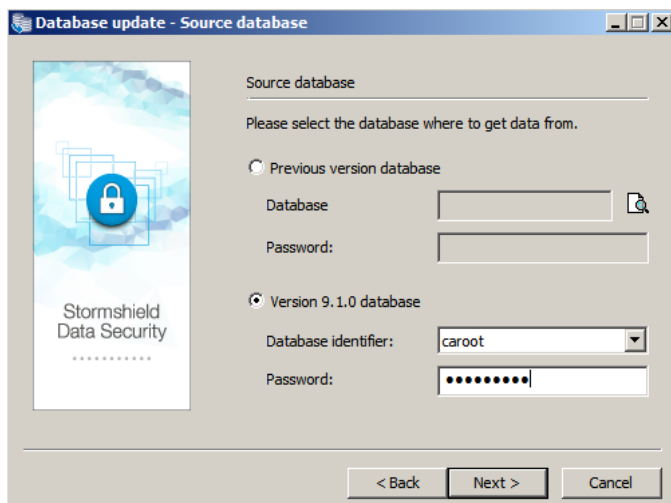


3. The following page allows you to choose which users and templates you want to import.

If you check the Import users box, the users sub-options become available. Choose to import:

- all the source database users. If some users derive from templates, they will also be imported.
- the users derived from a template. If this choice is selected, the template choice among all the source database templates becomes available. This template is also imported.

You can also choose to import all the templates.



4. The following page allows you to choose special users to import, that is to say:

- the recovery accounts.
- the security policy signatory. A database can contain only one security policy signatory: the database source signatory will not be imported if the database to update already contains one.

5. The following page is the last page before the update procedure. Please read again the collected information.

Click **Finish** to start the update.

This operation can take some time depending on the number of users to import.

The last page of the wizard displays the operations in progress and already carried out.



If you wish to cancel the procedure, all the operations already carried out are cancelled and the database is back to its initial state.

A log file is generated and provides more detailed information.

This log file is named BaseUpgrade.txt, and is created into the logs folder (see [the section called "Logs"](#)). It can be opened from the wizard using the Open log file button.

#### **i** NOTE

A warning message is displayed into the tree and the log if the lists files importation for a user or a template has not been carried out. Remember not to leave the destination database tree empty to avoid failure for impacted users distribution or the users deriving from the impacted templates.

## 5.7 Opening and Closing a Session on a Database

You must open a session on a database before working on it.

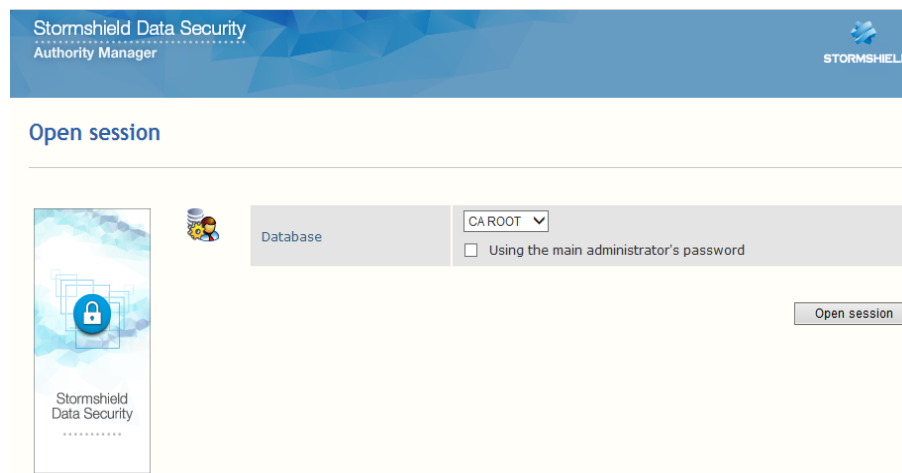
### 5.7.1 Opening a Session on a Database

To open a session on a database, enter the URL `<manager_root_url>/OpenSession` where `<manager_root_url>` is the root URL defined in [Section 4.5, "URL Access to Server"](#).

It shows the list of started databases (see [Section 5.4, "Starting and Stopping a Database"](#)).

Run your authentication for the selected database by clicking the **Open** button.

If opening by use of the main administrator password was authorized when the selected base was created (see [Section 5.2.1, "Database Creation Wizard"](#)), a check box giving the option of this authentication mode (see [Section 5.1.3, "Main Administrator and Other Administrators"](#)) is displayed.



This session is automatically closed by Stormshield Data Authority Manager after a period of inactivity lasting 15 minutes by default. This period can be changed in the *manager.ini* file (see [Section 4.7.4, "Session"](#)).

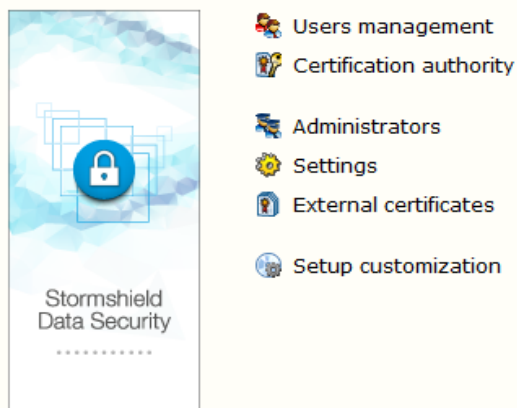
### 5.7.2 Homepage

The homepage is the Stormshield Data Authority Manager central page and it contains the following links:



- Users management (see section [Searching for Users](#)).
- Certification authority (see section [Certification authority operation](#)).
- Administrators management (see section [Administrators List Page](#)) for the database.
- Settings (see section [Settings Page](#)) for the database.
- External certificates for managing certificates external to the database (see section [Other External Certificates](#)).
- the Setup customization link to create a personalized installation procedure (see section [Customizing the Installation](#) ).

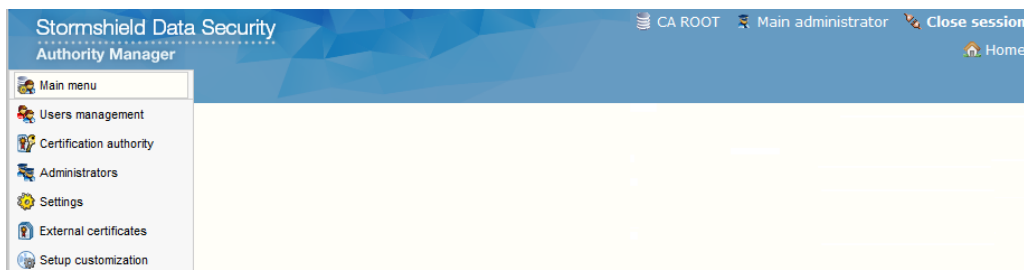
## Home



### 5.7.3 Closing a Session on a Database

The banner of each page contains:

- the database label
- the name of the authenticated administrator
- a link to close the session in the database
- a list of navigation links like “you are here”
- a drop-down menu containing the homepage links



Clicking the Close session link closes the session. The report page that is displayed contains the database label, the name of the authenticated administrator and contains a link back to the session opening page.

You will not be able to carry out any further operations on the database until you have been authenticated again.



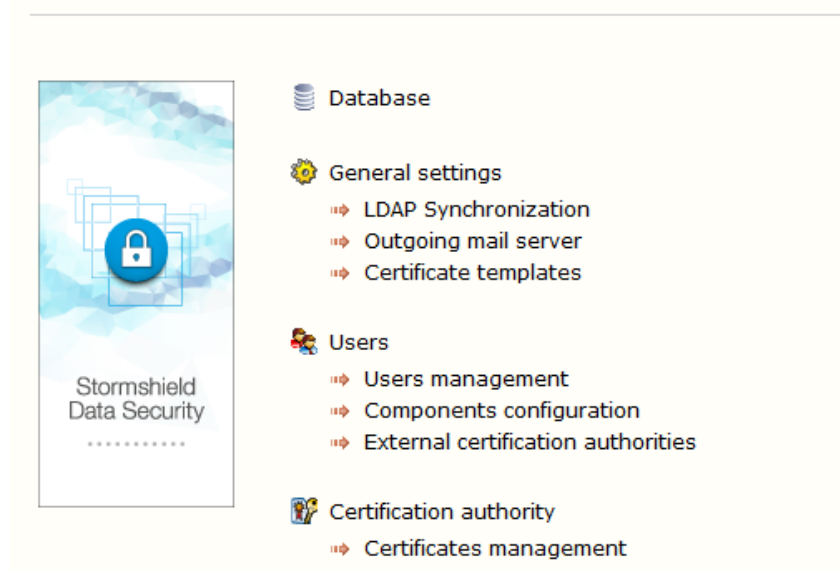
## 5.8 Entering the Operating Settings for the Database

### 5.8.1 Settings Page

To display or edit the settings for a database, open a session on the database and click the Settings link on the homepage (see [Section 5.7.2, “Homepage”](#)) or in the drop-down menu. This displays a menu which lets you:

- Access the page containing the data regarding the database (see [Section 5.8.2, “Database Page”](#), [Section 5.8.4, “Modifying the Start-up Password”](#) and [Section 5.8.5, “Modifying the Main Administrator Password”](#)).
- Display and modify:
  - Parameters defining the exchanges between Stormshield Data Authority Manager and an LDAP directory (see [Section 5.8.6, “LDAP Configuration”](#)).
  - Parameters defining the outgoing mail server for emails (see [Section 5.8.7, “Outgoing Mail Server”](#)).
  - Parameters defining certificate template (see [Section 5.8.11, “Certificate Templates”](#)).
- Display and modify:
  - User management parameters (see [Section 5.8.8, “User Management”](#)).
  - Component configuration parameters (see [Section 5.8.9, “Component Configuration Parameters”](#)).
  - External certification authorities (see [Section 5.8.12, “External Certification Authorities”](#)).
- Display and change certification authority parameters (see [Section 5.8.10, “Certificate Management Parameters”](#)).

### Settings



### 5.8.2 Database Page

To display the data specific to the database, click the Database link on the Settings page (see [Section 5.8.1, “Settings Page”](#)) or in the main drop-down menu.



### Database

Identifier	base
Created on	Tuesday, May 19, 2015 4:21:08 PM
Last open on	Tuesday, May 19, 2015 4:21:08 PM
Last startup password change on	Tuesday, May 19, 2015 4:21:08 PM
Protection algorithms	AES 256 bits

### Account unblocking

Identifier to use in order to activate the unblocking of a database user account	K74Q
Identifier to use in order to activate the unblocking of an account created by Security BOX Suite	LUQA

Both identifiers from this page allow to activate both remote unblocking account functions (see [Section 8.10, "Remote Account Unblocking"](#)). The identifier must be provided by the user before any unblocking account procedure to check the account to be unblocked is related to the opened session. They are indicated here to help you find the link between the distributed users and the database.

This need is specifically present for accounts created by Stormshield Data Security with a master from the database if you use several databases.

From the header on the top the page, a menu is displayed:

- from the Properties tab, you access the database properties (see [Section 5.8.3, "Database properties"](#)) ;
- from the Operations tab, you can:
  - Change the start-up password (see [Section 5.8.4, "Modifying the Start-up Password"](#)).
  - Change the password for the main administrator (see [Section 5.8.5, "Modifying the Main Administrator Password"](#)).

### 5.8.3 Database properties

This page can be accessed from the Properties drop-down menu in the Database page (see [Section 5.8.2, "Database Page"](#)) or from the main drop-down menu.

#### Database label

The database label defined during its creation can be modified.

Label

CA ROOT

#### Logs

Logging

Logging

☒ Activate Stormshield Data Authority Manager logging

Log files folder

C:\SBMData\ca-root\Log

Using the check box enables or disables the log of actions carried out on the database. If you enable the log, enter the full pathname of the folder that is to contain the log file. This file has the same name as the database with the .txt extension. As each action is carried out, a line is added to the log file. It provides:



- the date and time
- the machine name
- the Windows username
- the name of the database or user to which the action applies
- a description of the action carried out

This folder can also contain the database update log file, named BaseUpgrade.txt.

**NOTE**

Stormshield Data Authority Manager does not empty the log file.

### 5.8.4 Modifying the Start-up Password

This page lets you change the start-up password. It can be accessed by clicking the Modify start-up password link in the Operations drop-down menu (see [Section 5.8.2, "Database Page"](#)).

The start-up password is required when the database is started or stopped (see [Section 5.4, "Starting and Stopping a Database"](#)). It is defined when it is initialized (see [Section 5.3.2, "Entering the Start-up Password"](#)).

The screenshot shows a web interface titled "Password modification" with a sub-header "Password modification". Below the title is a small icon of a key. The form consists of three rows, each with a label and a text input field:

Former password	<input type="password"/>
New password	<input type="password"/>
Password confirmation	<input type="password"/>

### 5.8.5 Modifying the Main Administrator Password

This page lets you change the main administrator password. It can be accessed by clicking the Modify the main administrator password link in the Operations drop-down menu (see [Section 5.8.1, "Settings Page"](#)).

The main administrator password is required when a session is opened "using a password" (see [Section 5.7.1, "Opening a Session on a Database"](#) and [Section 5.1.3, "Main Administrator and Other Administrators"](#)).

The screenshot shows a web interface titled "Password modification" with a sub-header "Password modification". Below the title is a small icon of a key. The form consists of three rows, each with a label and a text input field:

Former password	<input type="password"/>
New password	<input type="password"/>
Password confirmation	<input type="password"/>

### 5.8.6 LDAP Configuration

The LDAP configuration page may be accessed from the Settings page (see [Section 5.8.1, "Settings Page"](#)) or from the Main drop-down menu.





## LDAP Server

Server name	<input type="text"/>
Port number	<input type="text" value="389"/>
LDAP version	<input type="text" value="2"/>
Protocol	<input type="checkbox"/> SSL
Encoding	<input checked="" type="radio"/> UTF-8 <input type="radio"/> ANSI
Duration of a connection attempt	<input type="text" value="30"/> seconds

These parameters define the LDAP server to which Stormshield Data Authority Manager has to connect during each LDAP operation.

You can choose to use SSL protocol and enter a maximum wait time during an attempt at connection. For more information, refer to Appendix C. LDAPS configuration, in the *Stormshield Data Security Administration guide*.

You must select the encoding used by the LDAP server: ANSI or UTF-8. Stormshield Data Authority Manager will use this encoding to transmit the requests to the server, and then to read the data sent back by this same server.

## Authentication

Authentication selection	<input type="radio"/> Authentication with a plaintext password	DN:	<input type="text"/>
		Password:	<input type="text"/>
	<input checked="" type="radio"/> Negotiated authentication	Domain or workgroup name:	<input type="text" value="mycompany.com"/>
		User name:	<input type="text" value="admin"/>
		Password:	<input type="text" value="P@ssw0rd"/>

You can connect to the LDAP server by:

- logging in and entering a DN and a password. If these fields are not entered, the connection is anonymous.
- performing a negotiated authentication: the authentication is performed with the most accurate method among those available on the server. You must enter the following identifiers: domain or workgroup (optional), user name and password. NTLM authentication is supported.

### NOTE

If the user name or the password is missing, the authentication is performed with the identifiers of the “network user” (see [Section A.3, “Assigning DCOM Rights for the Stormshield Data Authority Manager Service”](#)) under which the Web server is running.



## Finding an Entry

In this window, enter the data that will appear as default values in the search criteria when finding entries in the LDAP directory (see [Section 8.5.7, “Creating a User from an LDAP Directory”](#) and [Section 8.13, “Associating a User with an LDAP Entry”](#)):

- the database DN.
- the name of the class that will be used as search filter for entries associated with users (“person” standard class, or inherited).

You can also set a maximum wait time for a search query that uses the directory.

## Publication

When publishing user certificates on the LDAP server, the administrator can choose between the following options:

- publishing the current certificates of all the user's keys.
- publishing only the current certificate of the key that has the encryption role and the current certificate of the key that has the signature role.

## Publishing New Certificates

You can enter a resolution mask for the user LDAP DN that will be shown when a user is created and used when certificates are published.

It must be an LDAP DN which includes the following tags: <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>, <SecurityBoxUserId>.

When the mask is resolved, these tags will be replaced by the corresponding fields of the user identity.



## Attribute Names

Email address	mail
Common name	cn
Certificate in binary format	userCertificate;binary
Identifier	uid
Given name	givenName
Name	sn
Authority certificate in binary format	caCertificate;binary
CRL in binary format	certificateRevocationList;binary
Security policies update in binary format	sboxPolicyUpgrade;binary

Change the names of these LDAP attributes if they differ from the standard names shown.

The attribute used to update the security policy is specific to Stormshield Data Security. The LDAP directory must be set to support it. An example is provided in [Section E.2, “Configuring the LDAP Directory”](#).

The CRL attribute certificateRevocationList is standard: it is supported by the class cRLDistributionPoint (RFC 4523). The LDAP entry in which the CRL is published must be derived from this class. An example is provided in [Appendix G, Publishing and Downloading CRLs Using an LDAP Directory](#).

## 5.8.7 Outgoing Mail Server

The configuration page for the outgoing mail server (SMTP) may be accessed from the Settings page (see [Section 5.8.1, “Settings Page”](#)) or from the Main drop-down menu.

An outgoing mail server must be configured to:

- distribute update files [.usx] or installation files [.usi] by email (see [Section 8.9.4, “Sending by Email”](#))
- notify by email (see [the section called “Email Notifications”](#))

### SMTP Server

Name of local server	
Name of remote server	
Port number	25

Specify the name and, if required, the port number of the SMTP server which routes emails from Stormshield Data Authority Manager.

The name of the local server is entered by the remote server in the email's RFC822 header (Received: from <...> field); it must obviously contain neither spaces nor special characters.

## Connection Identifier and Sender Name

Username	
Password (non-hidden)	
Sender's email address	



If the SMTP server does not require any authentication, the user name and password fields must not be filled in.

They must be filled in if you connect to an authenticated SMTP server.

Stormshield Data Authority Manager supports LOGIN, PLAIN and CRAM-MD5 authentication mechanisms.

The sender's email address must be filled in whatever the SMTP server. This address must be in one of the following formats:

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

**i NOTE**

Certain SMTP servers only accept a connection if the email address is on an authorized email address list.

### 5.8.8 User Management

This page can be accessed from the Users management link on the Settings page (see [Section 5.8.1, "Settings Page"](#)) or from the Main drop-down menu.

#### Security Officer Password

Define a default security officer password policy which will be used each time an advanced account creation is processed (see [Section 8.5.1, "Advanced Creation"](#)):

- by entering a password which will be proposed each time an account is created.
- by choosing to propose a random password each time an account is created.
- by choosing not to have a security officer password.



Security officer password for the user accounts

☒ By default, use this password for all accounts:

0KwmjZMrpUTLVomP

☐ Suggest (and store) a different password for each account

☐ Disable security officer password for all accounts

**i NOTE**

You cannot use the remote account unblocking function (see [Section 8.10, "Remote Account Unblocking"](#)) for an account distributed with a security officer password longer than 16 characters. This limit corresponds to the random security officer passwords provided by Stormshield Data Authority Manager.

#### Identity

1. Define the mask used to build the subject used during generation and renewal of user certificates.

It must be a DN (Distinguished Name) which complies with standard RFC 2253, which means that the DN can contain the following attributes:

User identity mask



Abbreviated form	Tag
CN	Common Name
S	Surname
GN	Given name
I	Initials
GQ	Generation
DNQ	DN Qualifier
C	Country
L	Locality
ST	State
O	Organization
OU	Org Unit
T	Title
E	P9 Email
N	Name
SN	Serial Number
STREET	Street Address
D	Description
BC	Business Category
POC	Postal Code
TN	Telephone Number
UID	X500 User id
MB	DPAT RFC822 Mailbox
DC	DPAT Domain Component
DNSA	DNS Record

Stormshield Data Authority Manager allows you to insert the following tags in the mask:  
<CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>.

When the DN is resolved, these tags will be replaced by the fields corresponding to the users' identity. The result comprises the subject, which is present in the certificate.


2. Define the rule for building the user's common name.

Subject resolution mask	CN=<CommonName>,S=<SurName>,GN=<GivenName>,L=<Localit
Common name format	<input type="radio"/> Surname followed by given name <input checked="" type="radio"/> Given name followed by surname



### Account Distribution

1. Select the distribution folder for user accounts <user\_account\_dir>. By default, this is <sdam\_data\_install\_dir>\SBMData\<base\_id>\Users where <sdam\_data\_install\_dir> is the data folder and <base\_id> is the database identifier.
2. Select the number of attempts to enter the user and security officer passwords before the account is blocked.
3. Whether, when the card account is distributed, the account file (.usr file) created contains the public key and private key.
4. Whether the directory generated during the distribution contains only the user certificate and database authority certificates, or the certificates for all users of the database as well.

5. 

User account distribution folder	<input type="text" value="C:\SBMData\base\Users"/>	
Number of password entry attempts before locking	<input type="text" value="3"/>	for the user password
	<input type="text" value="3"/>	for the security officer password
Card account	<input type="checkbox"/> Make a copy of the private and public keys into the user account	
Address book	<input type="checkbox"/> Add to each user's address book the certificates of all users present in the database	

### Publication of Security Policy Updates

You can:

- enable LDAP publication of security policy updates. When this option is enabled, publication of updates in the LDAP directory is given as an option in the account distribution page (see [Appendix E, Publishing and Downloading Security Updates Using an LDAP Directory](#)).
- enable publication of security policy updates by file (see [Appendix F, Publishing and Downloading Security Updates using the Web Server](#)). When this option is enabled, publication by file is given as an option in the account distribution page (see [Section 8.9, "Distributing User Accounts"](#)). You have to enter the folder in which the update files are to be copied.

For more information concerning security policy update files, see [Section 8.9.2, "Security Policy Update File \(.usx\)"](#).

LDAP publication of updates (.usx)	<input checked="" type="checkbox"/> Activate LDAP publication of updates Caution, chose this option only if the users' LDAP entries belong to a class that accepts the update publication attribute, as set in the LDAP configuration.
File-based publication of updates (.usx)	<input checked="" type="checkbox"/> Activate file-based publication of updates Publication folder: <input type="text" value="C:\SBMData\base\Users"/>

### Publication of Installation Files

You can enable the publication of installation files (.usi). Once the option is enabled, the publication can be carried out from the accounts distribution page (see [Section 8.9, "Distributing User Accounts"](#)). You have to enter the folder in which the installation files are to be copied.

For more information about installation files, see [Section 8.9.1, "Installation File \(.usi\)"](#)



LDAP publication of updates (.usx)	<input checked="" type="checkbox"/> Activate LDAP publication of updates Caution, chose this option only if the users' LDAP entries belong to a class that accepts the update publication attribute, as set in the LDAP configuration.
File-based publication of updates (.usx)	<input checked="" type="checkbox"/> Activate file-based publication of updates Publication folder: <input type="text" value="C:\SBMDData\base\Users"/>

## Import, Export and Requests for Certificates

Enter the default folder which will contain certificates to be imported and exported certificates <certs\_dir>. By default, this is <sdam\_data\_install\_dir>\SBMDData\<base\_id>\Certs where <sdam\_data\_install\_dir> is the data folder and <base\_id> is the database identifier.

For certificate import, you can authorize the import of certificates whose validity start dates are prior to those of certificates already present in the database (see [the section called "Rules for Importing"](#)).

For certificate export, set the default choices:

- whether the parent-child relationship is to be added.
- the extension of the export file for multiple certificates.

Enter the format which will be:

- given as default value for the one-off export of a certificate (see [the section called "Exporting a Certificate"](#)).
- used for the export of certificates from the Users lists page (see [the section called "Exporting More than One Certificate"](#)).

**Certificate import and export**

User certificate import and export folder	<input type="text" value="C:\SBMDData\base\Certs"/>
Certificate import	<input type="checkbox"/> Authorize import of old certificates
Format for certificate export	<input checked="" type="radio"/> Base 64 format <input type="radio"/> Binary format
Trust chain export	<input type="checkbox"/> Add trust chain when exporting certificates
Extension for exporting several certificates	<input checked="" type="radio"/> p7b extension <input type="radio"/> p7c extension <input type="radio"/> sbc extension

## Email notification

This section allows you to activate and configure the email notification when a certificate expires (see [Section 10.2, "Email notification for a certificate expiry"](#)).

	<input checked="" type="checkbox"/> Send an information email before the certificates expiration
Information email	Number of days: <input type="text" value="30"/>
	Frequency: <input type="text" value="7"/> days
	Email address: <input type="text" value="administrateur@mycompany.com"/>
	Template: <input type="text" value="C:\SBMDData\caroot\MailTemplates\template_expiration_mail.sbp"/>



- The check box is used to enable the sending feature
- The first input field is to specify the period of anticipation before the expiry of a certificate: If the current date plus the specified time in the field, is after the expiry date of the certificate, it is then reported in the email notification

If [current date + number of days] > [certificate expiry date] => Report certificate

- The second field defines the frequency of searches for certificates in the database. This value should be less than the period of anticipation in order not to miss certificates whose expiry is imminent. The search for certificates, if successful, is followed by the sending of an email
- The third field is used to enter the details of the inbox notification message's recipient
- The last field to specify the location of the file used as a model for generating the email. It contains the formatting information for text mode and the html mode.

### 5.8.9 Component Configuration Parameters

The page for setting component configuration parameters can be accessed from the Settings page (see [Section 5.8.1, "Settings Page"](#)) or from the Main drop-down menu, by clicking in the Components configuration link.


The parameters specified in this page are not included directly in the distributed user accounts. They are used to help fill in the configuration pages for user components (see [Section 11.2, "Accessing Users' Configurations"](#)).

#### Stormshield Data Kernel: Downloading Security Policies

For each distribution point resolution mask specified, a button is added to the security policy download configuration page for users or templates. This button enables the distribution point mask to be added automatically to the list of distribution points.

The mask, once added to the list of distribution points, is resolved during user distribution.

Stormshield Data Kernel: Automatic update

	Resolution mask for LDAP distribution point	<input type="text"/>
	Resolution mask for HTTP distribution point	<input type="text"/>

An LDAP distribution point mask must be a valid LDAP URI which includes the <LdapHost>, <LdapPort>, <LdapDn> and <UserId> tags. When the mask is resolved, these tags will be replaced by the corresponding LDAP parameter (see [Section 5.8.6, "LDAP Configuration"](#)) and by the identifier of the distributed user. Example:

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

An HTTP distribution point mask must be a valid URI that includes the <UserId> tag. When the mask is resolved, the tag is replaced by the identifier of the distributed user. Example:

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

For more information, see [the section called "Configuring the Security Policies Download Component"](#).

### 5.8.10 Certificate Management Parameters

This page can be accessed from the Settings page (see [section Settings Page](#)) or from the Main drop-down menu.





## Certification Authority

You can specify the mask used to build the subject of the certification authority.

This mask will be used when the authority certificate is renewed if you choose to renew the subject (for more information, see section [Authority Certificate and Key Page](#)).

It must be a DN (Distinguished Name) which complies with standard RFC 2253, which means that the DN can contain the following attributes:

Certification Authority mask	
Abbreviated form	Tag
CN	Common Name
S	Surname
GN	Given name
I	Initials
GQ	Generation
DNQ	DN Qualifier
C	Country
L	Locality
ST	State
O	Organization
OU	Org Unit
T	Title
E	P9 Email
N	Name
SN	Serial Number
STREET	Street Address
D	Description
BC	Business Category
POC	Postal Code
TN	Telephone Number
UID	X500 User id
MB	DPAT RFC822 Mailbox
DC	DPAT Domain Component
DNSA	DNS Record



Stormshield Data Authority Manager allows you to insert the following tags in the mask:  
<CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>.

When the DN is resolved, these tags will be replaced by the corresponding fields of the certification authority identity. The result will comprise the subject in the certificate request.

The screenshot shows a window titled 'Certification authority'. Inside, there is a tab labeled 'Subject resolution mask'. The text area contains the string: `CN=<CommonName>,L=<Locality>,OU=<OrgUnit>,O=<Organization>`.

### Pre-entry of External Certificate Requests

To simplify filling out external certificate requests, you can specify values to be filled in by default for the Organization, Organization unit, City, State or province and Country fields of the identity for external certificate requests.

These values will be used in the next request pages (see the section [Filling out and Submitting a Certificate Request](#) and the section [Filling out and Submitting a Request for an Advanced Certificate](#)).

The screenshot shows a window titled 'External certificate requests pre-fill'. It contains a table with five rows, each with a label and a corresponding input field:

Organization	<input type="text"/>
Organization unit	<input type="text"/>
City	<input type="text"/>
State or province	<input type="text"/>
Country	<input type="text" value="France (FR)"/>

### Generated Certificates

1. Select: The default duration of a certificate.

This duration is only used when no certificate template is applied, i.e. when the user has requested an advanced and customized certificate.

2. The key size given by default to the CSPs (Cryptographic Service Providers).

When a CSP does not offer the key size selected, the nearest size supported by the CSP will be selected.

For more information on the mechanism of key generation by CSPs, see the section [Filling out and Submitting a Certificate Request](#).

3. The certificate signature algorithm.

We recommend you to use the "SHA-512 and RSA" algorithm. To avoid incompatibility with solutions which do not support SHA-512, you may choose "SHA-256 and RSA".

4. The location of the email address in standard certificates:

- Leave the email address in the identity only.
- Copy the identity email address into the Subject Alternative Name field of the certificate.
- Move the identity email address into the Subject Alternative Name field of the certificate.



If you choose to move the identity email address into the Subject Alternative Name field, in order to have the correct result:

- for the generation or the renewal of users certificates, do not position the email address in the resolution mask of the subject defined in the section [Identity](#) (E=<Email> present by default) ;
- during the validation of certificate request (see section [Making a Certificate Request](#)), do not keep the subject binary value issued from the PKCS#10 structure, if this value contains the email. You must use the proposed subject instead.

5. The mask used to build the LDAP DN for external certificates.

This mask will be used during validation of external certificate requests if you have configured an LDAP server (see section [LDAP Configuration](#)).

It must be valid LDAP search filter which includes the following tags: <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>.

When the DN is resolved, these tags will be replaced by the corresponding fields of the subject or the Subject Alternative Name field of the certificate generated. The result is the DN proposed for publishing the certificate.

If by default you want to carry out a search by criteria to find the LDAP publication entry, you can leave the DN resolution mask blank.

6. The mask used to build the LDAP entry search filter.

This mask will be used during validation of external certificate requests if you have configured an LDAP server (see section [LDAP Configuration](#)).

It must be valid LDAP search filter which includes the following tags: <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <Locality>, <State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>.

When the DN is resolved, these tags will be replaced by the corresponding fields of the subject or the Subject Alternative Name field of the certificate generated. The results constitute the filter proposed for looking for the publication LDAP entry.

7. Default action for certificates already present on the LDAP server:

- Keep them.
- Delete them.
- Replace certificates with the same uses and same issuer.

For more information, see section [Publishing a Certificate](#)

8. How the publication for each file is to be enabled and configured.

Activating publication for each file adds an option to all certificate publications.

This option consists of writing the certificate to a file located in a folder to be specified. The format of the file to be written (binary or "base 64") must also be specified.

The publication folder can be used for sharing, archiving or can be a document folder on a web server.



Default certificate validity duration	2 years
Default key size for CSPs	2048 bits
Algorithm	Certificate signed by SHA-1 et RSA
'Email' field	When generating a standard certificate (for which the SubjectAlternativeName extension was not filled at request time) <input type="radio"/> Leave the email address in the identity only <input checked="" type="radio"/> Copy the identity email address into the certificate's SubjectAltName field <input type="radio"/> Move the identity email address to the certificate's SubjectAltName field
Resolution mask of external certificates' LDAP DN	
Resolution mask of LDAP entry's search filter	(mail=<AltNameEmail>)
Certificates already published on the LDAP server	Default <input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input type="checkbox"/> Activate file-based certificates publication Publication folder: C:\SBMDat\cap12\CertsPublished File format: Binary

### Certificate Revocation Lists (CRLs)

For more information about publishing and downloading CRLs, refer to [Publishing and Downloading CRLs](#).

1. Select: The period the CRL is valid for in hours.

This will be used to calculate the "Next Update" date, which will be present in the CRL.

If you activate the CRL automatic generation service it is recommended to choose a CRL validity period equal to the generation frequency.

2. The LDAP DN used for publishing CRLs.

Entering a DN activates automatic publication of generated CRLs on the LDAP directory. Inversely, if the DN is blank, publication in this way is disabled.

3. The location where the current CRL is to be generated.

Enter here the full name, including pathname, of the file into which the current CRL is to be written.

Each time the CRL is generated, this file will be replaced by the new current CRL.

4. The CRL archive folder.

This folder is optional. If you enter it, each new CRL generated will be copied into this folder. Older CRLs are not overwritten as the serial number of the CRL is used in its filename.

5. Automatic generation of a CRL when it is revoked.

The user is given the option of generating a CRL when it is revoked. This option enables it to be selected by default.

6. Expired certificates to be included in the CRL.

In accordance with standard RFC 3280 chapter 5, a CRL lists non-expired certificates that have been revoked. Therefore, by default, a revoked certificate will not be included in CRLs later than its expiry date. This option allows expired revoked certificates also to be included in the CRL.

7. CRL distribution points.



CRL distribution points will be automatically included in the CrlDistributionPoint field for all generated certificates.

It is up to you to ensure these are consistent with the publication parameters for the CRLs and the organization of your server.

The supported protocols are http, https, ldap, ldaps and file. The syntactic check of the distribution point imposes that it starts with http://, https://, ldap://, ldaps:// or file://.

Example of valid distribution points using the protocol file:

- local pathname: file:///c:/folder/file.crl
- network pathname: file://server/sharing/folder/file.crl

#### NOTE

The address of the OCSP responder used during the check is the address defined in the certificate. You cannot add or edit this address in the revocation controller.

### Automatic CRL Generation Service

If you activate the automatic CRL generation service, Stormshield Data Authority Manager will automatically generate revocation lists at the frequency and time requested.

The frequency is entered in hours.

The generation time is used to initialize the generation service each time you start the database or when you update the certificate management parameters. Afterwards, the frequency is used to determine the next generation date.



## Email Notifications

Email notifications send information to the administrators regarding operations that have been carried out and inform users that their requests have been processed.

In Stormshield Data Authority Manager they are available as soon as an outgoing mail server (SMTP) has been configured (see section [Outgoing Mail Server](#)).

Certificate request deposit	<input type="checkbox"/> Send email notification on certificate request deposit Email address: <input type="text"/> Subject: <input type="text"/> Template : <input type="text" value="C:\SBMDData\cap12\MailTemplates\template_re"/>
Internal request validation	<input type="checkbox"/> Send email notification on validation of internal request Email address: <input type="text"/> Subject: <input type="text"/> Template : <input type="text" value="C:\SBMDData\cap12\MailTemplates\template_va"/> <input type="checkbox"/> Send a notification email to the requestor Subject: <input type="text"/> Template : <input type="text" value="C:\SBMDData\cap12\MailTemplates\template_va"/>
External request validation	<input type="checkbox"/> Send email notification on validation of external request Email address: <input type="text"/> Subject: <input type="text"/> Template : <input type="text" value="C:\SBMDData\cap12\MailTemplates\template_va"/> <input type="checkbox"/> Send a notification email to the requestor Subject: <input type="text"/> Template : <input type="text" value="C:\SBMDData\cap12\MailTemplates\template_va"/>

For each available notification, specify:

- the email subject,
- the complete path of the email template (.sbp file)

This parameter lets you use different email templates for each Stormshield Data Authority Manager database. You can customize notification emails by changing their template. If you customize a template, make sure to keep a valid MIME structure and only use the tags available in the original template. You can use the <BR> tag to insert a line break. It must be inserted in the entered text.

For notifications to administrators, specify the destination email address as well. This address must be in one of the following formats:

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

A use case is available in [Renewing Certificates](#).

### 5.8.11 Certificate Templates

This page can be accessed from the Settings page (see [Section 5.8.1, "Settings Page"](#)) or from the Main drop-down menu.

Certificate templates enable certificates to be easily generated for a given usage.



The templates may be fully customized and there is no limit on their number. By default, when Stormshield Data Authority Manager is installed, there are three of them:

- certificate for an encryption key (standard template)
- certificate for an signature key (standard template)
- authority certificate (advanced template)

These three default templates can be changed but not deleted as they may be used internally by Stormshield Data Authority Manager.

For each certificate template, select:

1. The name of the template.
2. The availability of the template in a standard certificate request.

The templates available in a standard request are also called standard templates. They will also be available when Stormshield Data Security user accounts are created (see [Section 8.4.1, "Operations Available"](#)).

3. Key usages. These will be written into the X.509 "Key Usage" extension of the certificate.
4. Extended key usages. These will be written into the X.509 "Extended Key Usage" extension of the certificate.
5. The duration for which the certificate is valid.
6. The certificate type (authority certificate or other).
7. The transmission depth of the certification capacity (in other words the number of authorized sub-authorities), whether this is an authority certificate.
8. The inclusion of the authority key identifier. This will be written into the X.509 "Authority Key Identifier" extension of the certificate.

You are advised to include this identifier in all non-root certificates as it enables the parent-child relationship between this certificate and its authority to be clearly established.

9. The inclusion of the subject key identifier. This will be written into the X.509 "Subject Key Identifier" extension of the certificate.

It is recommended to include this identifier in all authority certificates as it enables the parent-child relationship between this certificate and the certificates it signs (if these certificates have an "Authority Key Identifier") to be clearly established.

### 5.8.12 External Certification Authorities

A certificate request can be requested to an external certification authority for the key of the certification authority and also for each key of each user, even if the key has been certified by the internal certification authority (see [Section 7.3.2, "Making a Certificate Request"](#) and [Section 9.1, "Key and Certificate Page"](#)).

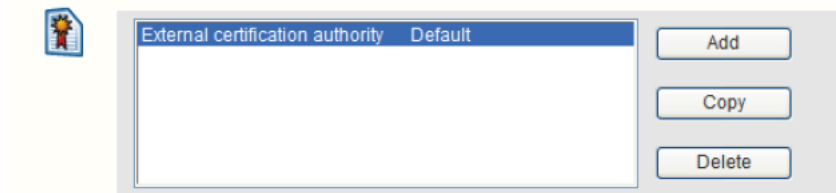
The External certification authority management page can be accessed from the Settings page (see [Section 5.8.1, "Settings Page"](#)) or from the Main drop-down menu. You can define a list of external certification authorities and enter the associated access parameters for each of them.

An external certification authority is associated to each key. You can modify this association in the Properties page of the key (see [Section 9.1, "Key and Certificate Page"](#)).

The certificate request page is pre-filled with the data from the external certification authority associated to the key (see [Section 10.3.2, "Creating a Request"](#)). Also, these data are used for every key when creating several requests in one operation (see [Section 10.3.3, "Creating Multiple Requests"](#)).



A default external certification authority is present and cannot be deleted. It is associated to every key that has been certified by the database internal certification authority. Thus the administrator can request a certificate to an external certification authority if necessary.



For each authority you can enter:

- A label used in Stormshield Data Authority Manager to identify the authority.
- The format of the certificate request (base 64 or binary).
- The folder containing the files created for the certificate requests, if this type of publication is used. By default, it is <sdam\_data\_install\_dir>\SBMData\<base\_id>\Certs where <sdam\_data\_install\_dir> is the data folder and <base\_id> is the database identifier.
- An email address and server URL which will be shown as default values when a certificate request in "base 64" format is created (see [Section 10.3.1, "Binary"/"base 64" Formats"](#)).

- The parameters of a remote Stormshield Data Authority Manager server:
- The root URL <manager root url> of the remote Stormshield Data Authority Manager server (see [Section 4.7, "Configuring the manager.ini File"](#)).
- The identifier of the database located on this server, which contains the certification authority to be used.
- The label of the certificate template, located in this database, which must be used to generate the certificate.
- A "timeout" network in milliseconds.

These parameters are for requests that are automatically submitted to a Stormshield Data Authority Manager remote certification server (see [Section 10.3.5, "Submitting a Request to a Remote Stormshield Data Authority Manager Server"](#)).





Remote Stormshield Data Authority Manager server

Server's URL	<input type="text"/>
Database identifier	<input type="text"/>
Certificate template name	<input type="text"/>
Network timeout (milliseconds)	<input type="text" value="5000"/>



## 6. Defining Administrators and Their Roles

This chapter describes how to define database administrators and their roles.

### 6.1 Introduction

A database can be managed by several physical administrators: each administrator may have different roles and must have a Stormshield Data Security account in order to be securely authenticated.

A physical administrator can be a user whose account is managed in the database: this is known as an "internal" administrator. Refer to [Section 6.5.2, "Adding an Internal Administrator to the Database"](#) to define a user as internal administrator.





A physical administrator can also have an account that is not managed in the database: this is known as an "external" administrator who is defined and identified using their certificate as explained in [Section 6.5.1, "Adding an External Administrator to the Database"](#).

#### NOTE

In this version of the product, revoking an external administrator is not checked.

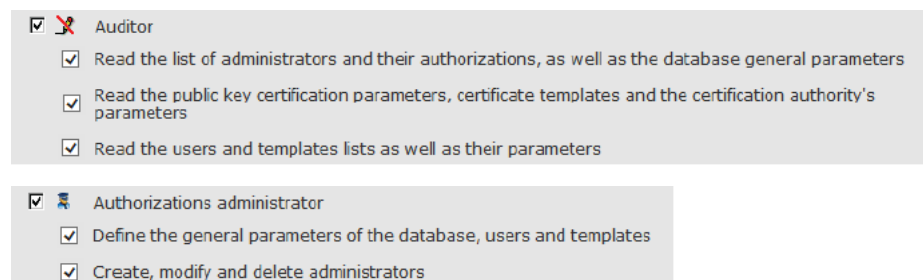
### 6.2 Authorizations


The four role profiles that can be assigned are as follows:

Profile	The administrator can mainly:
 Auditor	read all parameters read the list of users
 Authorization administrator	define administrators and their roles
 Certification agent	generate and revoke certificates
 User administrator	create, change and distribute users


The authorizations of each profile are detailed in the following screenshots.

The different authorization options for each profile are described on the interface. You can select one or many authorization options per profile. You can also select one or more profile per administrator.




☒  Auditor

- ☒ Read the list of administrators and their authorizations, as well as the database general parameters
- ☒ Read the public key certification parameters, certificate templates and the certification authority's parameters
- ☒ Read the users and templates lists as well as their parameters


☒  Authorizations administrator

- ☒ Define the general parameters of the database, users and templates
- ☒ Create, modify and delete administrators



<input checked="" type="checkbox"/>		Certification agent
<input checked="" type="checkbox"/>		Define the public key certification parameters and the certificate templates
<input checked="" type="checkbox"/>		Generate a database internal user's certificate
<input checked="" type="checkbox"/>		Revoke a database internal user's certificate
<input checked="" type="checkbox"/>		Generate the certificate for a user outside the database
<input checked="" type="checkbox"/>		Revoke the certificate for a user outside the database
<input checked="" type="checkbox"/>		Generate an advanced certificate
<input checked="" type="checkbox"/>		Revoke an advanced certificate

<input checked="" type="checkbox"/>		Users administrator
<input checked="" type="checkbox"/>		Create, modify and delete templates
<input checked="" type="checkbox"/>		Create, modify and delete recovery accounts
<input checked="" type="checkbox"/>		Create, modify and delete security policy signatories
<input checked="" type="checkbox"/>		Import, modify and delete an external recovery certificate
<input checked="" type="checkbox"/>		Import and delete an external address book certificate
<input checked="" type="checkbox"/>		Create users
<input checked="" type="checkbox"/>		Create users from a user template
<input checked="" type="checkbox"/>		Modify and delete users
<input checked="" type="checkbox"/>		Distribute accounts or users updates
<input checked="" type="checkbox"/>		Export users' keys
<input checked="" type="checkbox"/>		Read and modify the users' password and security officer password
<input checked="" type="checkbox"/>		Define and modify the users' password and security officer password
<input checked="" type="checkbox"/>		Unblock users accounts
<input checked="" type="checkbox"/>		Customize Stormshield Data Security Suite setup


### 6.3 Administrators List Page


To display the list of administrators, click the Administrators link in the homepage (see section [Homepage](#)).

From the Operations drop-down menu you can add an external administrator (see section [Adding an External Administrator to the Database](#)).

The page displays the list of administrators. For each administrator:

- The first column contains the name of the administrator (truncated in the display but visible in its entirety in the tooltip), together with an icon showing the type of the administrator:

 External administrator

 Internal administrator

- The following four columns summarize the administrator's authorizations. For each of the four authorization profiles (see section [Authorizations](#)), a checkbox indicates if the administrator has:



- ☒ All rights for the profile
- ☒ Certain rights for the profile
- ☐ None of the rights for the profile

By clicking the name of the administrator, you are taken to the Administrator page that displays all the administrator's properties.

Administrators list				
Administrators: 2 administrators				
Label				
▶ Beatrice ARMSTRONG		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Robert MILLER		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 6.4 Administrator Page

This page can be accessed from the Administrators list page (see section [Administrators List Page](#)) by clicking the name of the administrator.

It displays the administrator's properties:

- The name, which you can change.
- The type of the administrator (external or internal).
- All the authorizations split into four sections corresponding to the four authorization profiles. Each section may be displayed or hidden by clicking the name of the profile:
- Check or uncheck each authorization using the checkboxes opposite the authorizations.
- Check or uncheck all the authorizations for a profile using the checkboxes opposite the authorization profiles.

To register your changes, click the Create administrator button.

Properties										
	<table><tr><td>Label</td><td><input type="text" value="Jodie FISHER"/></td></tr><tr><td>Type</td><td>External administrator</td></tr></table>	Label	<input type="text" value="Jodie FISHER"/>	Type	External administrator					
Label	<input type="text" value="Jodie FISHER"/>									
Type	External administrator									
<table><tr><td rowspan="5">Authorizations</td><td><input checked="" type="checkbox"/> Auditor</td></tr><tr><td><input checked="" type="checkbox"/> Read the list of administrators and their authorizations, as well as the database general parameters</td></tr><tr><td><input checked="" type="checkbox"/> Read the public key certification parameters, certificate templates and the certification authority's parameters</td></tr><tr><td><input checked="" type="checkbox"/> Read the users and templates lists as well as their parameters</td></tr><tr><td><input checked="" type="checkbox"/> Authorizations administrator</td></tr><tr><td></td><td><input checked="" type="checkbox"/> Certification agent</td></tr><tr><td></td><td><input checked="" type="checkbox"/> Users administrator</td></tr></table>	Authorizations	<input checked="" type="checkbox"/> Auditor	<input checked="" type="checkbox"/> Read the list of administrators and their authorizations, as well as the database general parameters	<input checked="" type="checkbox"/> Read the public key certification parameters, certificate templates and the certification authority's parameters	<input checked="" type="checkbox"/> Read the users and templates lists as well as their parameters	<input checked="" type="checkbox"/> Authorizations administrator		<input checked="" type="checkbox"/> Certification agent		<input checked="" type="checkbox"/> Users administrator
Authorizations		<input checked="" type="checkbox"/> Auditor								
		<input checked="" type="checkbox"/> Read the list of administrators and their authorizations, as well as the database general parameters								
		<input checked="" type="checkbox"/> Read the public key certification parameters, certificate templates and the certification authority's parameters								
		<input checked="" type="checkbox"/> Read the users and templates lists as well as their parameters								
	<input checked="" type="checkbox"/> Authorizations administrator									
	<input checked="" type="checkbox"/> Certification agent									
	<input checked="" type="checkbox"/> Users administrator									

From the Administrator management drop-down menu you can delete the administrator.

If the administrator is external, from the Certificate drop-down menu you can:

- Display the contents of the signature key certificate for the administrator.
- Import a new signature key certificate for this administrator (see section [Importing a Signature Key Certificate](#)).



## 6.5 Adding an Administrator

### 6.5.1 Adding an External Administrator to the Database

#### Adding the Administrator

1. To add an external administrator, click the Add external administrator link in the Administrators list page (see section [Administrators List Page](#)).
2. In the page of administrator properties (see section [Administrator Page](#)):
  - a. Enter their name.
  - b. Define their authorizations.
  - c. Confirm the addition of the administrator by clicking the Create administrator button.
3. Then import the certificate for their signature key (see section [Importing a Signature Key Certificate](#)).

#### Importing a Signature Key Certificate

The first page lets you import the certificate either by pasting its value ("base 64" format) or by selecting a file.

The certificate must have an X.509 usage of "numeric signature" or "non repudiation".

The next page displays the contents of the certificate. In this page, confirm the import of the certificate by clicking the Import button.

### 6.5.2 Adding an Internal Administrator to the Database

A database user can be defined as the administrator of the database from their User page (see section [Users Page](#)) from the Properties tab, by clicking the Administrate database link.

In the page of administrator properties (see section [Administrator Page](#)):

1. Enter their name as database administrator.
2. Define their authorizations.
3. Confirm the addition of the administrator by clicking the Create administrator button.



## 7. Certification authority operation

This chapter explains how to manage certification authorities (CA) keys and certificate requests.

The certificate management includes the usual Public Key Infrastructure (PKI) functions via public access and via authenticated access.

### 7.1 Introduction

#### 7.1.1 Services Provided

Stormshield Data Authority Manager provides the following certificate management services:

- make a certificate request
- confirm/reject a request
- publish the issued certificates on an LDAP server
- revoke and publish the CRL
- display issued and revoked certificates
- send a notification email:
  - to an administrator when a user makes a certificate request
  - to the requesting user when the request is confirmed or rejected

#### 7.1.2 Public Access and Authenticated Access

Services intended for end-users are provided via "public" access (i.e. not requiring authentication).

These services are:

- make a certificate request
- display status of a request
- display issued and revoked certificates

Services intended for the certification agent require this agent be authenticated (known as "authenticated" access). These services are:

- manage certification authorities (CA) key
- confirm/reject a certificate request
- generate certificates
- publish the issued certificates on an LDAP server
- revoke certificates
- publish the CRL

All "public access" pages, as opposed to "authenticated access" pages, are compatible with Mozilla Firefox and Internet Explorer. All "authenticated access" pages are compatible with Internet Explorer only.



## 7.2 Homepage

### 7.2.1 Public Access Page

The public certification authority homepage can be accessed directly without authentication. Its direct access URL is of the form:

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

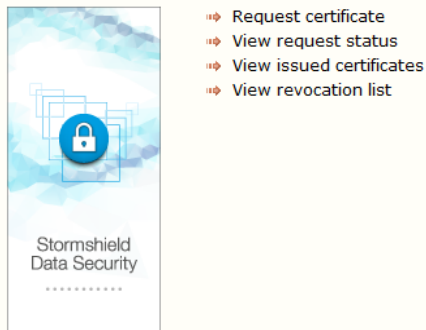
where <manager\_root\_url> is the root URL defined in [Section 4.5, "URL Access to Server"](#), and <base\_id> is the identifier of the database chosen when it was created.

It is recommended that this URL be communicated to end-users by means of an Intranet site link or by email.

From this page you can:

- request a certificate (see [Section 7.4, "Requesting a Certificate"](#)).
- display the status of a certificate request (see [Section 7.4.3, "Displaying the Status of a Certificate Request"](#)).
- display certificates issued (see [Section 7.6.1, "Finding a Certificate"](#)).
- display the revocation list (see [Section 7.7.1, "Displaying the Revocation List"](#)) when generated.

#### Certification authority



### 7.2.2 Authenticated Access Page

The certification authority homepage in authenticated access mode can be accessed from a Certification Authority link from the Stormshield Data Authority Manager homepage (see [Section 5.7.2, "Homepage"](#)).

From this page you can:

- display pending certificate requests (see [Section 7.5.1, "List of Pending Requests"](#))
- display certificates issued (see [Section 7.6.1, "Finding a Certificate"](#))
- display the revocation list (see [Section 7.7.1, "Displaying the Revocation List"](#)) when generated
- generate and distribute a new revocation list (see [Section 7.7.2, "Generating a Revocation List"](#))
- access the key management and certification authority certificate page (see [Section 7.3.1, "Authority Certificate and Key Page"](#))



If the certification authority does not yet have a certificate, only the key and certificate management (see [Section 7.3.1, "Authority Certificate and Key Page"](#)) page is available.

## Certification authority



- ⇒ Display pending requests
- ⇒ View issued certificates
- ⇒ View revocation list
- ⇒ Generate and distribute new revocation list
- ⇒ Key and certificate for the authority


## 7.3 Managing the Certification Authority Key


### 7.3.1 Authority Certificate and Key Page

The Authority certificate and key page can be accessed from the certification authority homepage (see [Section 7.2.2, "Authenticated Access Page"](#)) in authenticated access mode only. [Appendix H, Root Authority Certification](#) contains more information about the specific management of a root certification authority.

It shows, first of all, its usual name and the information concerning the certification authority key:

- encryption algorithm with its strength
- creation date of the key
- the security module in which this key is stored

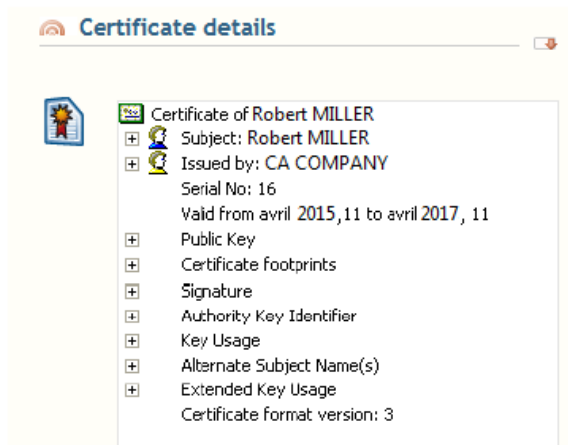
 **Key**

	Algorithm	RSA 2048 bits
	Created on	Tuesday, April 08, 2015 4:26:22 PM
	Security module	Internal

When the key for the authority is certified, the page shows the full contents of its certificate in the form of a tree.

When the key is not certified, the page shows the full identity of the authority.



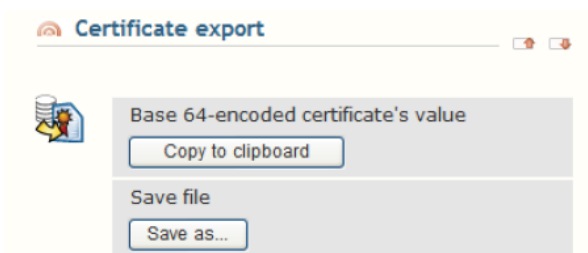


In the next section of the page, the information on a certificate request is displayed:

- date of the certification request in progress for this key, if any
- date of the last certificate import for this key, if any
- the name of the external certification authority associated to the key (see [Section 5.8.12, “External Certification Authorities”](#)).



When the key for the authority is certified, the certificate can be exported by copy-pasting its "base 64" value or by saving in a file. For more information, refer to the section [Exporting a Certificate](#).



In the banner on top of the page, a menu gives the following options. In the Properties tab, you can access the key properties. In this page, you can modify the external certification authority associated to the key properties.

- If the authority key is certified:
- in the Key management tab, you can export the key (see [Section 7.3.4, “Exporting the Key”](#))
- in the Certificate management tab, you can:
- request a certificate (see [Section 7.3.2, “Making a Certificate Request”](#))
- request a certificate and renew the subject (see [Section 7.3.2, “Making a Certificate Request”](#))

In this case, the subject of the PKCS#10 request is re-created from the identity of the authority.



**i NOTE**

This is not recommended if you have not set an Authority Key Identifier in all generated certificates each time or if the authority certificate does not have a Subject Key Identifier. In this case, the parent-child relationship between issued certificates and the authority is obtained by comparing the subject of the certificate issuer with the subject of the authority. This relationship is broken if the authority subject is renewed.

- importing a new certificate (see [Section 7.3.3, "Importing a New certificate "](#))
- If the authority key has not been certified yet:
- in the Certificate management tab, you can:
- make a request for a certificate (see [Section 7.4, "Requesting a Certificate "](#))
- import a new certificate (see [Section 7.3.3, "Importing a New certificate "](#))

### 7.3.2 Making a Certificate Request

The Certificate request page for a certification authority can be accessed from the Authority key and certificate page ([Section 7.3.1, "Authority Certificate and Key Page "](#)).

A request can be made either keeping the subject of the old certificate or renewing the subject depending on which link was used to access the page. For more information, refer to [Section 7.3.1, "Authority Certificate and Key Page "](#).

This page is identical to the certificate request page for a Stormshield Data Security user (see [Section 10.3.2, "Creating a Request"](#)).

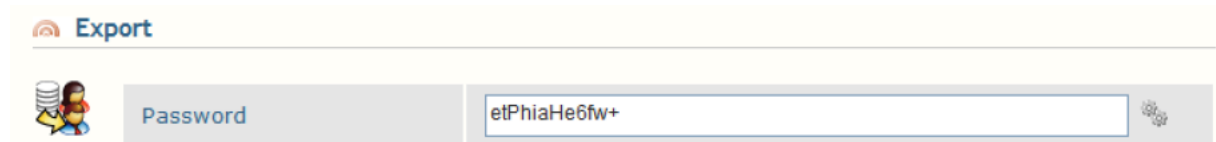
### 7.3.3 Importing a New certificate

The Certificate Import page for a certification authority can be accessed from the "Authority key and certificate" page (see [Section 7.3.1, "Authority Certificate and Key Page "](#)).


It is identical to the certificate import page for a Stormshield Data Security user (see section [Importing a Certificate](#)).

### 7.3.4 Exporting the Key

The Key Export page can be accessed from the Authority key and certificate page (see [Section 7.3.1, "Authority Certificate and Key Page "](#)).



You must enter the file protection password, and then click Exporting the key. The report is then displayed in a page offering you to save the created PKCS#12 file, and in which the key and associated certificate have been copied.

To ensure data confidentiality, it is recommended to enter a non-ordinary password. To help you choose the password, a random drawing is proposed by clicking the  icon.

## 7.4 Requesting a Certificate

A certificate request can only be made in public access mode.



The Certificate Request page, which can be accessed from the certification authority homepage (see [Section 7.2, "Homepage"](#)), lets you choose which type of certificate request you want to make.

A standard certificate request is available for the most usual cases: user encryption, signature or authentication certificate (see [Section 7.4.1, "Requesting a Standard Certificate"](#)).

An advanced certificate request is used to request a certificate for more specific uses, for example for an SSL/HTTPS server or a sub-authority (see [Section 7.4.2, "Requesting an Advanced Certificate"](#)).

### 7.4.1 Requesting a Standard Certificate

A standard certificate request is a simplified request for the most common uses (signature, encryption certificate, etc.).

A standard request comprises information about the requester and their key and gives the template of the requested certificate.

#### Filling out and Submitting a Certificate Request

In the Certificate request page (see [Section 7.4, "Requesting a Certificate"](#)), click the Fill out and submit a certificate request link.

The page that is displayed lets you generate a certificate request for a key provided by a security module present in your browser (CSP for Cryptographic Service Provider under Internet Explorer).

- Most security modules generate a private/public key pair, store the private key internally and provide the public key in the request.

The Microsoft CSP stores the private key in Internet Explorer's keystore. CSPs from smart card or token suppliers store the private key in the card or token respectively.

- The Stormshield Data Security CSP retrieves one of the keys present in the user account connected to Stormshield Data Security and generates a request for the public key.

The private key is never given to Stormshield Data Authority Manager. Only the certificate request containing the identity of the requester and the public key are sent to Stormshield Data Authority Manager.

#### **i** NOTE

The browser can request confirmation for executing the security module, depending on the browser security zone where the Stormshield Data Authority Manager server is running. You can avoid this request by adding the Stormshield Data Authority Manager server to the list of trusted sites of the browser.

The user's identity is entered on the first part of the page. This is written to the certificate request. When the request is being validated by a certification agent, it can be changed before being written into the subject of the generated certificate.

The email address is automatically copied and moved to the Subject Alternative Name field of the certificate in accordance with the general parameters for certificate management (see section [Generated Certificates](#)).

In order to simplify the procedure and avoid errors, you can configure Stormshield Data Authority Manager so that the Organization, Organization unit, City, State or province and Country fields are automatically filled in with default values. The default values are specified in



the general parameters for certificate management (see section [Pre-entry of External Certificate Requests](#)).

The 'Identity' form contains the following fields:

Name	
Given name	
Common name	
Organization	
Organization unit	
City	
State or province	
Country	France (FR)
Email address	

The second part of the page concerns the generation of keys by the CSP (Cryptographic Service Provider) or the security module. The key-pair is generated by the cryptographic service provider. You can choose:

- The CSP which will draw the key-pair and the request.
- The key usage (All uses, Exchange or Signature). This parameter is used by the CSP to draw the key. It is independent of the Stormshield Data Authority Manager certificate template specified afterwards.
- The size of the RSA key. The values available depend on the CSP and the use to which the key is to be put.
- To mark keys as exportable if in the future you want to be able to export the keys as PKCS#12 files.
- To enable reinforced protection for the private key.

For the Stormshield Data Security CSP, as the key is only retrieved rather than drawn, these options are not taken into account.

The 'Key' form contains the following fields:

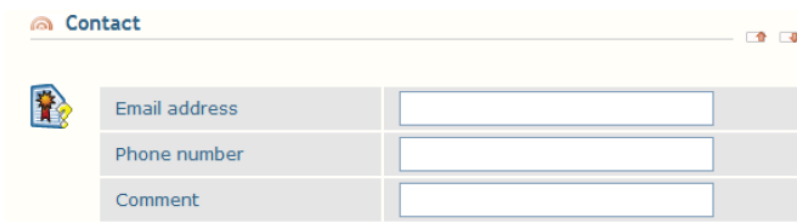
Cryptographic services provider	Microsoft Base Cryptographic Provider v1.0
Key usage	Any usage
RSA key size	1024
Advanced options	<input type="checkbox"/> Mark keys as exportable <input type="checkbox"/> Activate private key protection

The third section is used to select a certificate template from the standard certificate templates (see [Section 5.8.11, "Certificate Templates"](#)). This certificate template defines the properties of the certificate requested (validity date, uses, etc.). If you want to generate a special certificate, use the Advanced certificate request page (see section [Filling out and Submitting a Request for an Advanced Certificate](#)).

The 'Certificate' form contains the following fields:

Template	Encryption
----------	------------

The last section is used to specify information which enables the administrator to validate the request to contact the requester. This information is optional.



The screenshot shows a 'Contact' form with three input fields: 'Email address', 'Phone number', and 'Comment'. Each field has a corresponding label and a text input area.

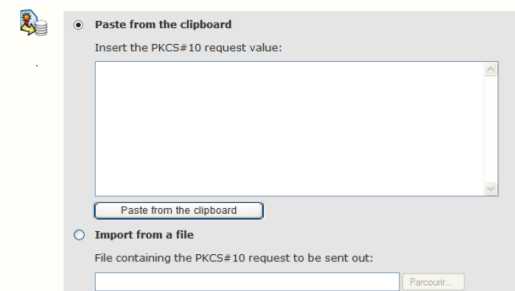
To validate your request, click Send request. Make a note of the request identifier: you use this to check the status of your request at any time (see [Section 7.4.3, "Displaying the Status of a Certificate Request"](#)).

### Submitting a Certificate Request from a PKCS#10 Structure

In the Certificate request page (see [Section 7.4, "Requesting a Certificate"](#)), click the Submit a request from a PKCS#10 structure link.

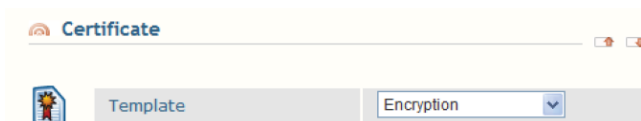
The page displayed lets you submit a certificate request for an already-existing key from a PKCS#10 structure coming from any product.

You can paste the value of the PKCS#10 structure encoded in "base 64" format or select a file.



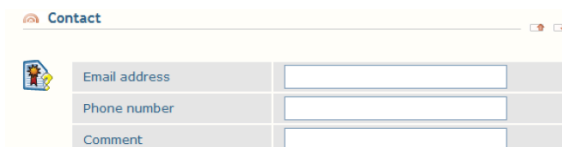
The screenshot shows a form for submitting a certificate request. It has two radio buttons: 'Paste from the clipboard' (selected) and 'Import from a file'. The 'Paste from the clipboard' option has a large text area for 'Insert the PKCS#10 request value:' and a 'Paste from the clipboard' button. The 'Import from a file' option has a label 'File containing the PKCS#10 request to be sent out:' and a 'Parcourir...' button.

The second section is used to select a certificate template from the standard certificate templates (see [Section 5.8.11, "Certificate Templates"](#)). This certificate template defines the properties of the certificate requested (validity date, uses, etc.). If you want to generate a special certificate, use the Advanced certificate request page (see [section Filling out and Submitting a Request for an Advanced Certificate](#)).



The screenshot shows a 'Certificate' form with a 'Template' dropdown menu and an 'Encryption' dropdown menu.

The last section is used to specify information to enable the administrator to validate the request to get in contact with the requester. This information is optional.



The screenshot shows a 'Contact' form with three input fields: 'Email address', 'Phone number', and 'Comment'. Each field has a corresponding label and a text input area.

To validate your request, click Send request.

Make a note of the request identifier: you use this to check the status of your request at any time (see [Section 7.4.3, "Displaying the Status of a Certificate Request"](#)).



## 7.4.2 Requesting an Advanced Certificate

A request for an "advanced" certificate lets you request a more specific certificate, for example an SSL certificate or a sub-authority certificate.

An advanced request comprises:

- information about the requester and their key
- if required, information stored in the Subject Alternative Name field of the certificate generated
- the template of the requested certificate or customized contents

### Filling out and Submitting a Request for an Advanced Certificate

In the Certificate request page (see [Section 7.4, "Requesting a Certificate"](#)), click the Advanced certificate link then the Fill out and submit an advanced certificate request link.

The page displayed is similar to the Standard certificate request page (see section [Filling out and Submitting a Certificate Request](#)). In addition, it has the following items:

You can now enter information stored in the Subject Alternative Name field of the certificate:

- an email address
- a domain name
- an IP address
- a principal name (UPN, Universal Principal Name, OID 1.3.6.1.4.1.311.20.2.3). Its value is encoded in UTF-8.

The email address for the identity will not be copied or moved into the Subject Alternative Name field, unlike in a standard certificate request. It is up to the requester to specify explicitly which information is the subject of the generated certificate and which information is the Subject Alternative Name.

The domain name and IP address are useful if you want to generate an SSL server certificate.

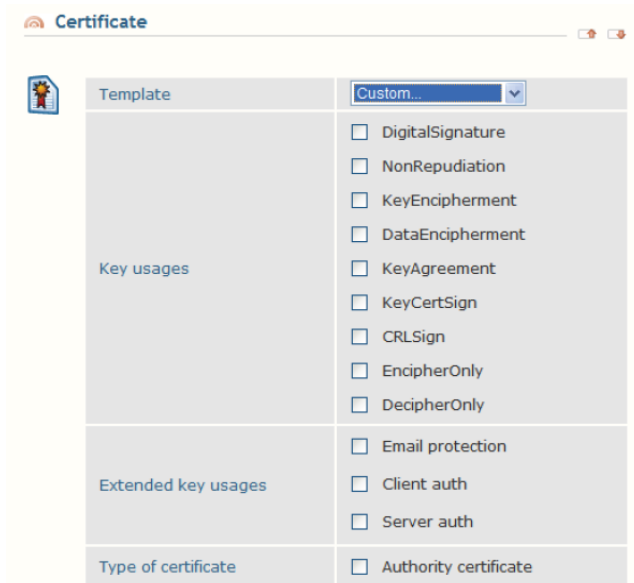
Alternative identity	
Email address	<input type="text"/>
Domain name	<input type="text"/>
IP address	<input type="text"/>
Universal principal name	<input type="text"/>

In the Certificate section, you can now select a certificate template from all the certificate templates configured in the Certificate templates page (see [Section 5.8.11, "Certificate Templates"](#)). This means the authority certificate template is available as are any specific templates you may have added.

The Custom option is also added to the list of certificate templates. This option shows additional options to enable you to request a certificate for which no existing template is suitable.

The additional options are:

- key usages
- extended key usages
- certificate type: whether it is an authority certificate or not



The screenshot shows a web form titled "Certificate". It has a "Template" dropdown menu set to "Custom...". Below this, there are two sections: "Key usages" and "Extended key usages". The "Key usages" section contains a list of checkboxes: DigitalSignature, NonRepudiation, KeyEncipherment, DataEncipherment, KeyAgreement, KeyCertSign, CRLSign, EncipherOnly, and DecipherOnly. The "Extended key usages" section contains checkboxes for Email protection, Client auth, and Server auth. At the bottom, there is a "Type of certificate" section with a checkbox for "Authority certificate".

To validate your request, click Send request.

Make a note of the request identifier: you will need this to check the status of your request (see [Section 7.4.3, "Displaying the Status of a Certificate Request"](#)).

### Submitting a Request for an Advanced Certificate from a PKCS#10 Structure

In the Certificate request page (see [Section 7.4, "Requesting a Certificate"](#)), click the Advanced certificate link then the Submit an advanced certificate request from a PKCS#10 structure link.

The page displayed is similar to the Standard certificate request from a PKCS#10 structure page (see [the section called "Submitting a Certificate Request from a PKCS#10 Structure"](#)).

In addition, you can now enter information stored in the Subject Alternative Name field of the certificate:

- an email address
- a domain name
- an IP address
- a principal name (UPN, Universal Principal Name, OID 1.3.6.1.4.1.311.20.2.3). Its value is encoded in UTF-8.

Note that the email address for the identity will not be copied or moved into the Subject Alternative Name field contrary to a standard certificate request. It is up to the requester to specify explicitly which information is the subject of the generated certificate and the Subject Alternative Name.

The domain name and IP address are useful if you want to generate an SSL server certificate.



The screenshot shows a web form titled "Alternative identity". It contains four input fields: "Email address", "Domain name", "IP address", and "Universal principal name". Each field has a corresponding label and a text input box.

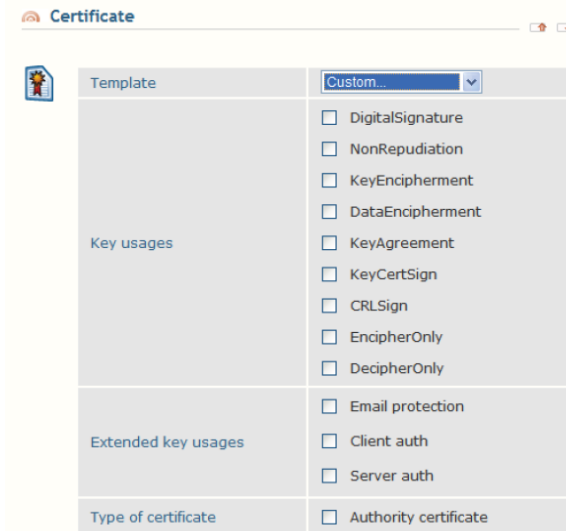
In the Certificate section, you can now select a certificate template from all the certificate templates configured in the Certificate templates page (see [Section 5.8.11, "Certificate Templates"](#)). This means the authority certificate template is available as are any specific templates you may have added.



The Custom option is also added to the list of certificate templates. This option shows additional options which allow you to request a certificate for which no existing template is suitable.

The additional options are:

- key usages
- extended key usages
- certificate type: whether it is an authority certificate or not



The screenshot shows a window titled "Certificate" with a "Template" dropdown menu set to "Custom...". Below the dropdown, there are three sections with checkboxes:

Section	Options
Key usages	<input type="checkbox"/> DigitalSignature <input type="checkbox"/> NonRepudiation <input type="checkbox"/> KeyEncipherment <input type="checkbox"/> DataEncipherment <input type="checkbox"/> KeyAgreement <input type="checkbox"/> KeyCertSign <input type="checkbox"/> CRLSign <input type="checkbox"/> EncipherOnly <input type="checkbox"/> DecipherOnly
Extended key usages	<input type="checkbox"/> Email protection <input type="checkbox"/> Client auth <input type="checkbox"/> Server auth
Type of certificate	<input type="checkbox"/> Authority certificate

To validate your request, click Send request.

Make a note of the request identifier: you use this to check the status of your request at any time (see [Section 7.4.3, "Displaying the Status of a Certificate Request"](#)).

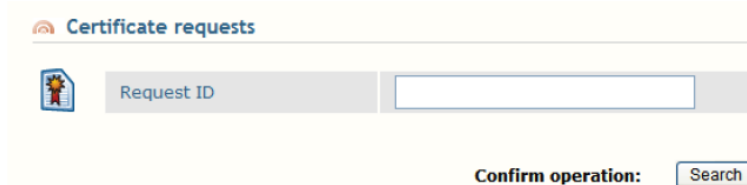
### 7.4.3 Displaying the Status of a Certificate Request

The Certificate request status page can be accessed from the certification authority homepage in public access mode only.

It asks you to enter a certificate request identifier.

Click Find. The following information displays one of the following statuses:

- a message showing that the request is pending
- the reject reason if the request has been rejected
- the certificate generated if the request has been validated (see [Section 7.6.3, "Displaying a Certificate"](#))



The screenshot shows a window titled "Certificate requests" with a "Request ID" input field and a "Search" button. Below the input field, there is a "Confirm operation:" label and a "Search" button.





## 7.5 Displaying and Processing Certificate Requests

### 7.5.1 List of Pending Requests

The List of pending requests page can be accessed from the certification authority homepage (see [Section 7.2.2, "Authenticated Access Page"](#)) in authenticated access mode only.

It displays all the certificate requests which have not yet been processed, i.e. not validated or rejected.

Ten requests are displayed per page. If more than 10 requests are awaiting processing, you can browse the various pages using the icons displayed under the list.



The list contains the following information for each certificate request:

- the first column contains the request identifier
- the second column contains:
  - the common name of the request
  - the full subject of the request
  - the date of the request
  - the certificate template requested
- the third column shows the request type:
  - request for standard certificate
  - request for advanced certificate

Clicking the request identifier or the requester's common name displays the request processing page (see [Section 7.5.2, "Processing a Certificate Request"](#)).

#### List of pending requests

Requests: requests 1 to 5 out of 5

Request Id	Summary	
▶ 23	<b>Robert MILLER</b> Subject: E=rmiller@mycompany.com,C=FR,OU=My Organisation Unit,O=My Company Date of request: Friday, April 11, 2015 Template : Signature	
▶ 22	<b>Robert MILLER</b> Subject: E=rmiller@mycompany.com,C=FR,OU=My Organisation Unit,O=My Company Date of request: Friday, April 11, 2015 Template : Encryption	
▶ 21	<b>Jodie FISHER</b> Subject: E=jfisher@mycompany.com,C=FR,OU=My Organisation Unit,O=My Company Date of request: Friday, April 11, 2015 Template : Signature	
▶ 20	<b>Jodie FISHER</b> Subject: E=jfisher@mycompany.com,C=FR,OU=My Organisation Unit,O=My Company Date of request: Friday, April 11, 2015 Template : Encryption	
▶ 19	<b>Alice SMITH</b> Subject: E=asmith@mycompany.com,C=FR,OU=My Organisation Unit,O=My Company Date of request: Friday, April 11, 2015 Template : Signature	



## 7.5.2 Processing a Certificate Request

The Certificate request validation page can be accessed from the List of pending requests page (see [Section 7.5.1, "List of Pending Requests"](#)) in authenticated access mode only.

It gives the choice of:

- changing the request if necessary then validating it, i.e. generating a certificate for a public key signed by the certification authority
- rejecting the request. If you want to reject the request, you do not need to enter all the options for the certificate to be generated. You can simply fill in the reject comment and click the Deny request button at the bottom of the page.

The first part of the page gives general information on the request to be processed:

- the request identifier
- its source which can be:
  - external, if the request comes from a certificate request page in public access mode or a remote certificate request sent by another Stormshield Data Authority Manager server
  - a Stormshield Data Security account managed in the database. This case arises only if an administrator who does not have certification rights creates a user. In this case a request is generated automatically and sent to the certification authority
- the type of certificate requested which can be:
  - advanced, if the request comes from an advanced certification request page in public access mode
  - standard for all other cases
- the subject of the certificate requested. This can be changed.

### NOTE

If the certification authority certificate is being renewed, do not change the subject, rather leave the binary value of the old subject unchanged so as not to risk breaking the parent-child relationship between this authority and the certificates that it has generated.

If you choose to move the identity email address in the Subject Alternative Name field (Email field parameter, [the section called "Generated Certificates"](#)), to obtain the correct functioning, you must not keep the binary value of the subject issued from the PKCS#10 structure, if this value contains the e-mail. You must use the subject proposed as a replacement.

The screenshot shows a web interface titled "Certificate request". It contains a table with the following data:

Request identifier	1
Origin	External
Type of certificate	Standard certificate
Subject	CN=John MAC CAIN,GN=MAC CAIN,S=John,C... <input type="checkbox"/> Do not keep PKCS#10 subject binary value: CN=John MAC CAIN,GN=MAC CAIN,S=John,C=FR,O=My Company,OU=My Organis

In the second section you can see and modify the information stored in the Subject Alternative Name field of the certificate:

- an email address
- a domain name
- an IP address
- a principal name (UPN, Universal Principal Name, OID 1.3.6.1.4.1.311.20.2.3). Its value is encoded in UTF-8.



Alternative identity	
Email address	jmaccaim@mycompany.com
Domain name	
IP address	
Universal principal name	

In the third section you can see and modify the certificate template selected when the request was made.

If no template is suitable for the certificate you want to generate, you can change each option manually. This could be used, for example, to generate a certificate with a shorter validity period for a particular user. For more information on the options available, see [Section 5.8.11, "Certificate Templates"](#). If you change an option manually, the certificate template becomes customized.

However, it is recommended to use certificate templates wherever possible and if necessary to create new ones (see [Section 5.8.11, "Certificate Templates"](#)).

Certificate	
Template	Signature
Key usages	<input checked="" type="checkbox"/> DigitalSignature <input checked="" type="checkbox"/> NonRepudiation <input type="checkbox"/> KeyEncipherment <input type="checkbox"/> DataEncipherment <input type="checkbox"/> KeyAgreement <input type="checkbox"/> KeyCertSign <input type="checkbox"/> CRLSign <input type="checkbox"/> EncipherOnly <input type="checkbox"/> DecipherOnly
Extended key usages	<input checked="" type="checkbox"/> Email protection <input type="checkbox"/> Client auth <input type="checkbox"/> Server auth
Validity period	2 years The certificate will be valid until Sunday, April 11, 2010.
Type of certificate	<input type="checkbox"/> Authority certificate
Depth	The number of certificates in the certification path starting from this authority, excluding the end certificate unlimited
Key identifiers	<input checked="" type="checkbox"/> Include the authority's key identifier (AuthorityKeyId) <input type="checkbox"/> Include the subject's key identifier (SubjectKeyId)

The fourth section shows the complete value of the public key to be certified together with its SHA-1 thumbprint.



Key		
Public key	30:82:01:0A 02:82:01:01 00:99:FE:DB 12:57:DF:D4 4D:23:89:9B 46:D0:BB:F3 CA:05:E3:3E C1:4D:56:49 74:E8:28:3C ED:5F:73:31 C7:DD:4B:8A 37:AC:8B:9D D8:ED:92:C2 C6:6F:32:35 77:54:25:F4 7D:19:0C:E8 C7:60:DD:10 3F:8F:F4:7B 04:A3:A4:38 63:09:90:81 C2:2E:E3:C9 DC:9B:1A:D8 7F:6A:C6:43 62:8E:65:9B 42:77:98:CE 6A:85:EE:6D 0C:AC:F0:6D 3D:8D:B0:59 0A:88:A2:18 FB:88:1F:26 F6:55:2C:F0 A0:B2:A9:0B 12:80:16:F7 41:AA:E7:E0 FB:94:FE:49 7B:32:D7:81 2D:7F:72:4F DF:06:BA:25 00:98:65:E8 6A:FC:F1:E8 AF:59:52:1A 55:7B:CD:4D BD:8E:B4:B7 5E:8C:FA:2A CC:DE:C1:3B D4:F1:3E:50 38:5A:64:E3 65:4C:44:57 5D:44:A3:3C A7:88:1C:4C 4E:65:48:53 91:A2:FC:B8 43:F4:91:9C 09:4D:D5:45 B9:A7:BE:D8 8F:95:C4:A6 AB:D4:02:42 B9:11:45:93 6D:19:53:C9 A1:C3:21:BE 22:B0:17:9C CE:3D:8D:12 A9:AC:30:00 70:F2:47:36 13:D8:D4:4B 38:D7:4B:F0 69:02:03:01 00:01	
Public key digest (SHA-1)	AB87/679C	AB:87:4E:F7:08:5A:14:3B:7C:3D 29:25:84:0F:20:BE:18:A8:67:9C

Depending on the general parameters, a fifth section gives you the option of publishing the certificate generated. If an LDAP server is configured [see [Section 5.8.6, "LDAP Configuration"](#)], the LDAP publication options are available. If publication by file is configured [see the section called ["Generated Certificates"](#)], this is given as an option. For more information, refer to the certificate publication section [see [Section 7.6.4, "Publishing a Certificate"](#)].

Publication	
LDAP publication	<input checked="" type="checkbox"/> Publish generated certificate <input type="radio"/> to the DN: <input type="text"/> <input checked="" type="radio"/> to the entry matching the criterion: <input type="text" value="(mail=jmaccain@mycompany.com)"/>
Certificates already published on the LDAP server	<input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates: <input checked="" type="checkbox"/> with the same X.509 usages <input checked="" type="checkbox"/> issued by this authority
File-based publication	<input checked="" type="checkbox"/> Publish certificate through a file

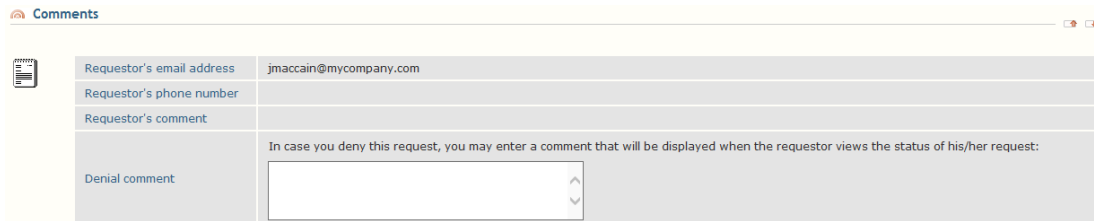
If an outgoing mail server (SMTP) is configured [see [Section 5.8.7, "Outgoing Mail Server"](#)] and you have enabled sending a notification email to the requester when the request is validated or rejected [see [Section 5.8.7, "Outgoing Mail Server"](#)], a section gives you the option of sending this notification email. The default email address is the email address of the contact entered when the certificate request was made [see [Section 7.4, "Requesting a Certificate"](#)].

Email notification	
Notification email	<input checked="" type="checkbox"/> Send a notification email to: <input type="text" value="jmaccain@mycompany.com"/>



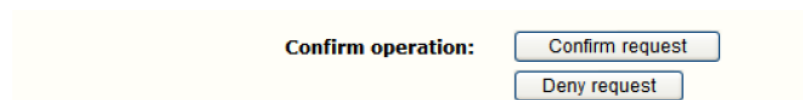
The last section shows information about the certificate requester. You can use this information to contact the requester before generating their certificate.

If you have chosen to reject the request, you can also use it to fill out a comment explaining the reason for refusal to the certificate requester.



The image shows a 'Comments' section with a header bar. Below it is a form with several fields: 'Requestor's email address' (containing 'jmaccaim@mycompany.com'), 'Requestor's phone number', 'Requestor's comment', and 'Denial comment'. The 'Denial comment' field has a text area with a placeholder message: 'In case you deny this request, you may enter a comment that will be displayed when the requestor views the status of his/her request:'.

Lastly, you choose whether to validate or reject the request by choosing one of the following buttons:



The image shows a 'Confirm operation:' label followed by two buttons: 'Confirm request' and 'Deny request'.

In either case, an email is sent to the requester. This email contains a link pointing to:

- the detail of the certificate generated if the request was validated
- the reason for rejection if the request was rejected

The type of certificate generated may differ from the one initially requested.

- a standard certificate in which only the validity period has been changed will give a standard certificate
- a standard request in which the certificate template has been changed for an advanced template, or has been replaced by custom parameters will give an advanced certificate
- any advanced request will give an advanced certificate even if this refers to a standard certificate template and does not contain a Subject Alternative Name.

## 7.6 Displaying and Processing Issued Certificates

### 7.6.1 Finding a Certificate

The Search for issued certificates page can be accessed from the certification authority homepage (see [Section 7.2.2, "Authenticated Access Page"](#)) in both public and authenticated access mode.

It shows various criteria which help you find one or more certificates from all the certificates issued by the certification authority.

If you do not select any search criterion, all certificates that have been issued will be returned. If you select one or more criteria, the list will be restricted to those certificates fulfilling these criteria.

The search criteria available are:

- serial number range. The minimum and maximum numbers in the series are entered in hexadecimal format (e.g. from 0a to ff);
- status (valid, expired, revoked, revoked or expired);
- uses;



- identity;
- origin.

Search criteria

☐ Search for certificates in a serial number range

Minimum serial number:

Maximum serial number:

☐ Search for certificates by status

Valid

☐ Search for certificates by usages

☐ DigitalSignature

☐ NonRepudiation

☐ KeyEncipherment

☐ DataEncipherment

☐ KeyAgreement

☐ KeyCertSign

☐ CRLSign

☐ EncipherOnly

☐ DecipherOnly

☐ Search for certificates by identity

Email:

Common name:

Organization:

Organization unit:

City:

Country:

☐ Search for certificates by origin

☐ External certificate

☒ Security BOX user's certificate

## 7.6.2 List of Certificates Issued

This list of certificates issued can only be obtained using a search for certificates issued in public or authenticated access mode (see [Section 7.6.1, "Finding a Certificate"](#)). If you want to display the full list of certificates generated you can run a search with no criteria specified.

Ten certificates are displayed per page. If more than 10 certificates are returned, you can browse the various pages using the icons displayed under the list.



The list contains the following information for each certificate:

- The first column contains the serial number of the certificate.
- The second column contains:
  - the common name of the certificate
  - the full subject of the certificate
  - the dates for which the certificate is valid
  - the uses of the certificate
- The third column shows the status of the certificate:
  - certificate valid
  - certificate revoked or expired

Clicking either the serial number of a certificate or the common name of its holder opens the certificate display page (see [Section 7.6.3, "Displaying a Certificate"](#)).



Certificates: certificates 1 to 8 out of 8

Serial no.	Summary	
▶ E	<b>Robert MILLER</b> Subject: CN=Robert MILLER,S=MILLER,GN=Robert,L=,OU=My Organisation Unit,O=My Company,C=FR,E=rml... Validity: from Thursday, February 05, 2015 to Sunday, February 05, 2017 Usages: KeyEncipherment, DataEncipherment	
▶ C	<b>Jodie FISHER</b> Subject: CN=Jodie FISHER,S=FISHER,GN=Jodie,L=,OU=My Organisation Unit,O=My Company,C=FR,E=jfishe... Validity: from Thursday, February 05, 2015 to Sunday, February 05, 2017 Usages: KeyEncipherment, DataEncipherment	
▶ B	<b>Alice SMITH</b> Subject: CN=Alice SMITH,S=SMITH,GN=Alice,L=,OU=My Organisation Unit,O=My Company,C=FR,E=asmith@m... Validity: from Thursday, February 05, 2015 to Sunday, February 05, 2017 Usages: KeyEncipherment, DataEncipherment	

### 7.6.3 Displaying a Certificate

The Certificate details page is available in both public and authenticated access modes.

In authenticated access mode, it can be accessed from the list of issued certificates (see [Section 7.6.2, "List of Certificates Issued"](#)).

In public access mode, this page can be accessed from the list of issued certificates (see [Section 7.6.2, "List of Certificates Issued"](#)), from the request status request when this request has been validated, and also directly using its URL:

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

where <manager\_root\_url> is the root URL as defined in [Section 4.5, "URL Access to Server"](#), <base\_id> is the identifier of the database chosen when it was created, and <serial\_number> is the serial number of the certificate in decimal.


The first section shows the complete contents of the certificate:

- as a table in public access mode
- in the form of a tree in authenticated access mode

If the certificate is revoked or expired, a warning is displayed in red above the details of the certificate.

The content of a complete certificate is detailed in ASN.1 in dans l'annexe E « Contenu d'un certificat émis par la PKI ».

Certificate details



Certificate of Robert MILLER

Subject: Robert MILLER

Issued by: CA COMPANY

Serial No: 16

Valid from avril 2015, 11 to avril 2017, 11

Public Key

Certificate footprints

Signature

Authority Key Identifier

Key Usage

Alternate Subject Name(s)

Extended Key Usage

Certificate format version: 3

The certificate can be exported by copy-pasting its "base 64" value or by saving in a file (see [the section called "Exporting a Certificate"](#)). Furthermore it can be:

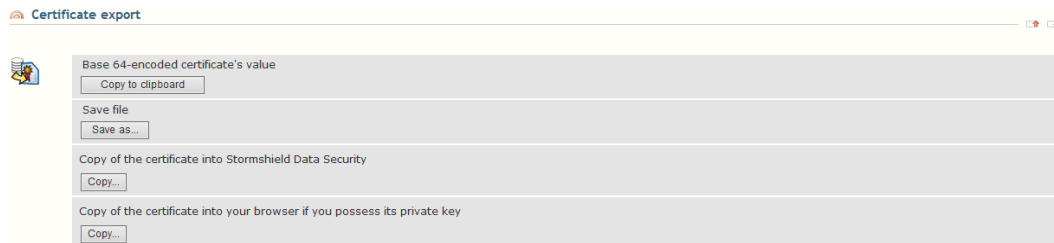


- Copied into Stormshield Data Security. This starts the Stormshield Data Security certificate import wizard. It is not available with browsers other than Internet Explorer.

**i NOTE**

An ActiveX component must be installed and executed on the client workstation when downloading the page, so that the page can propose this functionality. You must therefore:

- Add your Stormshield Data Authority Manager server to the list of "trusted sites" of the browser (Internet Explorer or Firefox) on the client workstation.
- Authorize execution of ActiveX components that are not marked as trusted (see [Section 4.6, "Configuring the Administrator Workstation"](#)).
- Copied into your browser. This sends the certificate to your browser, which associates it with the corresponding key in its keystore. The operation fails if the browser's keystore does not contain the corresponding key. It must therefore be carried out from the browser that drawn the key and made the request (see [the section called "Filling out and Submitting a Certificate Request"](#)).



In authenticated access mode, the page also lets you carry out various operations on the certificate displayed:

- Publish the certificate (see [Section 7.6.4, "Publishing a Certificate"](#)).
- Revoke the certificate (see [Section 7.6.5, "Revoking a Certificate"](#)).

## 7.6.4 Publishing a Certificate

You can publish a certificate as soon as it has been generated (see [Section 7.5.2, "Processing a Certificate Request"](#)).

You can also publish it later. To do this in authenticated access mode, open the certificate page (see [Section 7.6.3, "Displaying a Certificate"](#)). Depending on the general parameters, you can publish the certificate using a section at the bottom of the page.

If an LDAP server is configured in your general parameters (see [Section 5.8.6, "LDAP Configuration"](#)), the following options are available:

- Publish the generated certificate to a given DN.

The DN given by default is resolved from the DN mask specified in the general parameters and from the subject of the certificate to be published.

- Publish the generated certificate to the entry satisfying a given criterion.

A search in the LDAP directory using this criterion will be carried out and if it returns a unique result, the certificate will be published to the entry found.

The search criterion is resolved from the search criterion mask specified in the general parameters and from the subject of the certificate to be published.

If you want this option to be selected by default, do not specify a DN publication mask in the general parameters.





- Certificates already published on the LDAP server:

You can configure the operation to be carried out on any certificates already present on the LDAP server to the entry designated by the DN or found during the search:

- keep them
- delete them
- replace certificates having the same X.509 uses
- replace certificates issued by this authority

If this option is chosen, certificates not satisfying all the criteria will be kept, and those which do will be replaced by the certificate to be published.

If publication by file is enabled in your general parameters (see [the section called “Generated Certificates”](#)), a **Publish certificate through a file** option is available.

Publication	
LDAP publication	<input checked="" type="checkbox"/> Publish generated certificate <input type="radio"/> to the DN: <input type="text"/> <input checked="" type="radio"/> to the entry matching the criterion: <input type="text" value="(mail=jmaccain@mycompany.com)"/>
Certificates already published on the LDAP server	<input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates: <input checked="" type="checkbox"/> with the same X.509 usages <input checked="" type="checkbox"/> issued by this authority
File-based publication	<input checked="" type="checkbox"/> Publish certificate through a file

## 7.6.5 Revoking a Certificate

To revoke a certificate, open the certificate display page (see [Section 7.6.3, “Displaying a Certificate”](#)) in authenticated access mode. If the certificate has not already been revoked, you can revoke the certificate in a section at the bottom of the page.

Several revocation options are available:

- invalidity date

### NOTE

Unlike the revocation date, which is always used and is set to today's date, the invalidity date is optional. It is the date from which the certificate will become invalid or the date at which the key has become compromised. It will be shown in the InvalidityDate field for the entry in the CRL. There is no need to specify it if it is the same as the revocation date.

- the reason for the revocation.
- comments on the revocation. These comments will not be shown in the CRL. They are internal to Stormshield Data Authority Manager. However, they are shown in the certificate display page (see [Section 7.6.3, “Displaying a Certificate”](#)).
- the publication of a new revocation list.

It is recommended that a new revocation list be published immediately so that the revocation status of the certificate can take effect as soon as possible.



The CRL is generated and published in accordance with the options specified in the "General parameters for certificate management" (see [the section called "Certificate Revocation Lists \(CRLs\)"](#)).

Invalidity Date	<input type="checkbox"/> Indicate the Invalidity Date: [Month] [Day] [Year]
Revocation reason	Unspecified
Comment	<div></div>
Revocation list	<input checked="" type="checkbox"/> Publish a new CRL now

Confirm operation: Revoke certificate

It is also possible to revoke several certificates at a time. For more information, refer to the section [Revoking users](#).

## 7.7 Managing Certificate Revocation Lists (CRL)

Stormshield Data Authority Manager lets you revoke certificates (see [Section 7.6.5, "Revoking a Certificate"](#)) and manage revocation lists (see [Section 7.7.2, "Generating a Revocation List"](#) and [Section 7.7.3, "Generating Revocation Lists Automatically"](#)).

A certificate revocation list contains the list of all certificates revoked at a given date signed by the certification authority.

### 7.7.1 Displaying the Revocation List

The Revocation list page can be accessed from the certification authority homepage (see [Section 7.2.2, "Authenticated Access Page"](#)) by clicking the View revocation list link.

It is available in both public and authenticated access modes.

The first section provides some information concerning the current CRL:

- CRL issuer (this will be the subject of the base certification authority)
- date updated (ThisUpdate field in the CRL)
- date of next update (NextUpdate field in the CRL). The date depends on the validity period for CRLs which can be customized in the general certificate management parameters (see [the section called "Certificate Revocation Lists \(CRLs\)"](#)).
- CRL number (CrINumber field of the CRL)

Issuer	C=FR, O=My Company, CN=CA COMPANY
Update date	Friday, April 11, 2015 10:46:42 AM
Next update date	Saturday, April 12, 2015 10:46:42 AM
CRL number	5 (5)

Save CRL as...

The next section shows the list of revoked certificates in the current CRL. For each certificate:



- The first column contains the serial number of the certificate.
- The second column contains the date the certificate was revoked.
- The third column contains the reason the certificate was revoked, entered by the administrator who revoked it.

Clicking the serial number of the certificate displays the details for the certificate ([Section 7.6.3, “Displaying a Certificate”](#)).



Revoked certificates: 5 certificates

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

## 7.7.2 Generating a Revocation List

To create a revocation list, go to the Certification authority homepage accessed in authenticated access mode (see [Section 7.2.2, “Authenticated Access Page”](#)).

No list of options is given but the new CRL is immediately generated and published in accordance with the options specified in the general certificate management parameters (see [the section called “Certificate Revocation Lists \(CRLs\)”](#)).

When finished, a report is displayed followed by the new CRL. For more information on displaying the new CRL, see [Section 7.7.1, “Displaying the Revocation List”](#).

## 7.7.3 Generating Revocation Lists Automatically

Stormshield Data Authority Manager can automatically generate revocation lists at the frequency and time specified.

This operation is active only if the database is started.

The frequency of generation is defined in the Certificates management parameters page (see [the section called “Automatic CRL Generation Service”](#)).



## 8. User management

This chapter presents the different types of users and describes how to define, create and distribute user accounts.

### 8.1 The different Types of Users

Users are associated with a security account which contains their keys and operating parameters for the Stormshield Data Authority Manager suite. All users whose public key is certified by the same certification authority are grouped together in the same database. Users are segmented and shared depending on organizational considerations and company choices.

Users may be of the following types:

- the template user (see [Section 8.1.1, "Template "](#))
- the recovery account (see [Section 8.1.2, "Recovery Account "](#))
- security policy signatory (see [Section 8.1.3, "Security Policy Signatory "](#))
- the standard user, who can be created with a template (see [Section 8.1.4, "Standard User "](#))

#### 8.1.1 Template

A user template is different from the other users: it has no key and no certificate, but it has the necessary information to create the keys and certificates of users deriving from it. The template also contains the configurations of the Stormshield Data Security components. They can be released in a master.

A template is used to:

- Create users more quickly by using the parameters of the template (see [Section 8.5.2, "Creating a User from a Template "](#) to [Section 8.5.7, "Creating a User from an LDAP Directory "](#)).
- Centralize security officer password management (see [Section 8.8.2, "Changing Passwords "](#)).
- Centralize the definition of configurations of the Stormshield Data Security components (Security BOX Virtual Disk, Security BOX File, Security BOX Kernel, Security BOX Mail, Security BOX Shredder, Security BOX Sign, see section [Users Page](#)).

#### 8.1.2 Recovery Account

##### IMPORTANT

Creating a recovery account requires certain precautions to be taken on how this account is stored: this is critical for the security of the data encrypted with user accounts using this recovery mechanism. It must be provided with a password that is sufficiently secure and held in a secure location or, better, equipped with a smart card.

Creating recovery accounts in the user database depends on how the company confidentiality policy operates.

A recovery account is a normal user account used by Stormshield Data Security components. With such an account you can decrypt anything that has been encrypted with its certificate.



The certificate of the recovery key for a recovery account created in the database is included automatically in all user accounts created in this database. Thus everything encrypted by the users will be encrypted with the recovery certificate.

When creating a recovery account, its certificate is automatically added to the user accounts when the security policy is updated (.usx).

Deleting recovery accounts is not managed by this functionality. The certificates are not deleted from the user accounts.

When renewing a certificate of a recovery account, this functionality adds the new certificate in the user accounts and does not update the former certificate.

If you want to apply a compartmentalization policy (i.e. Stormshield Data Security accounts with different recovery keys) use several user databases.

### 8.1.3 Security Policy Signatory

#### ! IMPORTANT

Creating a security policy signatory requires certain precautions to be taken on how this account is stored: this is critical to the definition of your security policy.

A security policy signatory is used when a user account update is distributed. This is the certificate of the account, which authenticates Stormshield Data Authority Manager. It ensures the authenticity and validity of security policy update files.

Only one security policy signatory may be created per database.

When a user account is distributed, the distribution rules for the certificate of the security policy signatory are as follows:

- During a full distribution, if a signatory exists, their certificate is added to the user account.
- During an update distribution, as the presence of a signatory is mandatory, their certificate is added to the update file.

Thus, when the user uses the update file:

- If the certificate of the signatory is identical in the update file and in their Stormshield Data Security account, the component configurations are updated. The authentication carried out guarantees that the update for the configurations has been generated by Stormshield Data Authority Manager.
- In the opposite case, the user must grant their trust to the certificate from their update file to validate the operation. The signatory certificate is then imported into the user account.

It is therefore preferable that a security policy signatory be created before carrying out a full distribution.





The certificate of the security policy signatory can be seen in the configuration panel of Stormshield Data Security in the user's key ring under the Stormshield Data Authority Manager tab.

You can create a security policy signatory from a PKCS#12 file (see [Section 8.5.5, "Creating a User from a PKCS#12 File"](#)).

### 8.1.4 Standard User

The standard user has no special properties for a certification authority, template, recovery account or security policy signatory.



The user can have more than two keys. But only one key can have the encryption role  and only one key can have the signature role . The other keys are either keys with a signature usage , or decryption keys . The key usage (encryption and/or signature) depends on the X.509 usages of the certificate associated to the key. The key role (encryption key/decryption key, signature key/key with a signature usage) can be modified in the key Properties page (see [Section 9.2, "Key Properties Page"](#)).

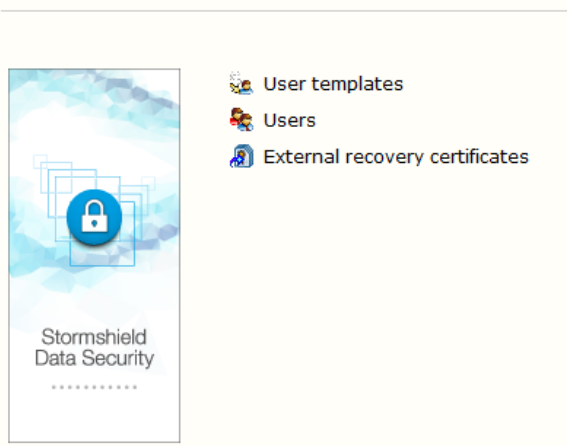
## 8.2 Users Management Page

The Users management page is the main page. It allows you to reach:

- User templates management (see [Section 8.3, "List of Templates Page"](#))
- Users list (see [Section 8.4, "Users List Page"](#))
- External recovery certificates management (see [Section 10.1.1, "External Recovery Certificates"](#))

You can reach this page from the homepage or from the Main menu.

### Users management



## 8.3 List of Templates Page

From the List of templates page you can manage templates in Stormshield Data Authority Manager. You can reach this page from Users management page and from the Main menu.

 **User templates:** 2 User templates 

Identifier	Description	
> MySignTemplate	Template 1 key Signature	
> MyUserTemplate	Template 2 keys Encryption Signature	

This page displays the list of templates present in the database, with the following information:

- the template identifier. If truncated in the display, it can be seen in full in the tooltip.
- the description that was entered during the template creation. If truncated in the display, it can be seen in full in the tooltip.
- an indicator showing the distribution of a master from this template

You can create a template from the Operations drop-down menu (see [Section 8.3.1, "Creating a User Template"](#)).

Click the template Identifier to open the template page (see [Section 8.3.2, "Template Page"](#)).



### 8.3.1 Creating a User Template

You can access the user Template creation page from the Operations drop-down menu of the List of templates page.

There are two types of data regarding templates:

- data on templates themselves
- data used when creating a user with the template

#### The data on templates:

- the identifier used by Stormshield Data Authority Manager to reference the template. This identifier is used as the name of the master file and must not contain the characters \ / : \* ? < > |
- an optional description
- a protection password for a master to be distributed from this template (a random selection of 12 characters is suggested by default)
- the DN of the LDAP entry used during publication in the LDAP directory of the update file

Template	
Identifier	MyUserTemplate
Description	Template 2 keys Encryption Signature
Master's password	1pJb146v94xr
DN of LDAP entry used for update file publication	ou=USX, ou=Users, dc=mycompany, dc=com

#### The data when creating a user:

The data needed when creating a user with this template are the following:

- an encryption algorithm (AES 256 bits by default)
- a thumbprint algorithm (SHA-512 by default)

Users accounts	
User accounts protection algorithms	Encryption: AES 256 bits With hashing: SHA-1

- the security officer password. This section is initialized in accordance with the configuration defined in the general parameters (see [the section called "Security Officer Password"](#)). You can also impose a randomly generated security officer password for each user created using the template.

Security officer password for user accounts	
Security officer password for user accounts	<p><input type="radio"/> Disable the security officer password</p> <p><input type="radio"/> Generate a different backup password for every user</p> <p><input checked="" type="radio"/> Use the following security officer password:</p> <p>t6ANUDIZmy46f8zJ</p> <p>General password</p> <p>This password will enable you to unlock this account if the user has lost his/her password.</p>

**NOTE**

You cannot use the remote account unblocking function (see [Section 8.10, "Remote Account Unblocking"](#)) for an account distributed with a security officer password longer than 16 characters. This limit corresponds to the random security officer passwords provided by Stormshield Data Authority Manager.

- the users' identity. This will be written into their certificate.

Users' identities

Organization	My Company
Organization unit	My Organization Unit
City	
State or province	
Country	France (FR)

- the data needed to create and certify keys. You can indicate the creation of only one key by selecting no certification mode for one of the two keys.

**Key 2**

Certification mode	Please select a certification mode...
--------------------	---------------------------------------

For each key, the data are the following:

- the encryption algorithm with its strength
- the certification mode: on top of the line that indicates the certification mode (which allows you not to create a key), the drop-down menu contains the list of certificate templates and the list of external CAs.

If you select a certificate template:

- If the database has a certified internal CA, the key is certified by this CA.
- If not, the key is self-certified, as indicated.

In both cases, the data from the certificate template are used.

- The validity period is filled with the information from the certificate template, and it can be modified.
- The Key role line indicates the role(s) of the future key. They are determined by the X.509 uses of the certificate template, and as such they cannot be modified.

**Key 1**

Certification mode	Internal CA - Encryption
Validity period	2 years Until Thursday, April 08, 2015
Key role	<input checked="" type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 1024 bits

If you select an external CA when creating a user, the key is drawn but not certified. You have to make a certification request for this key, and then import the certificate.

The selected external CA is associated to the key and its data will be used for the certification request.

To facilitate key management, you can indicate the expected role in the Key role line. Yet, in the end the role(s) of the key will be determined by the X.509 uses of the future certificate.





Key 1

Certification mode	External CA - External certification authority
Key role	<input type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 1024 bits

### 8.3.2 Template Page


To open the Template page, click a template identifier in the List of templates page.

The Template page contains the following:

- the data that are specific to the template: identifier, description, DN for the LDAP entry, creation date, last modification date, and master distribution date, if any
- the data to be used when creating a user from the template: identity, key list, encryption algorithm for the account

The key list indicates: the selected certification mode, the validity period of the future certificate (if a certificate template was selected), the key role and the encryption algorithm with its strength.

 User's keys and certificates: 2 keys

Certification	Certificate validity period	Role	Key algorithm
Internal CA - Encryption	from Tuesday, April 08, 2008 to Thursday, April 08, 2015		RSA 2048 bits
Internal CA - Signature	from Tuesday, April 08, 2008 to Thursday, April 08, 2015		RSA 2048 bits

In the banner on top of the page, a menu gives the following options:

- In the Properties tab, you can access the Properties page that is identical to the Creation page. In this page, you can modify everything except the template identifier. If the template has two keys, you can delete one key by selecting no certification mode for one of the two keys.
- In the Template management tab, you can:
  - Distribute a master in one of the following ways:
    - with password configuration or with card configuration in order to use it with Stormshield Data Security (.usr file) (see [Section 8.3.4, "Distributing a Master"](#))
    - with all configurations in order to export a template to another database (.msr file)
  - Distribute a security policy update file (.usx) in one of the following ways: with password configuration or with card configuration (see [Section 8.3.6, "Distributing a Security Policy Update File \(.usx\)"](#)).
  - Duplicate a template (see [Section 8.3.7, "Creating a Template by Duplicating an Existing Template"](#)).
  - Deleting a template. It is possible only if the template is not referenced by a user, or by the Stormshield Data Security installation customization.
- In the Components tab, you can:
  - Configure the following components:
    - Stormshield Data Disk
    - Stormshield Data File
    - Stormshield Data Kernel



- Stormshield Data Mail
- Stormshield Data Shredder
- Stormshield Data Sign
- Import the component configurations from a master (.msr file).
- In the Operations tab, you can call the user creation page from a template (see [Section 8.5.2, “Creating a User from a Template”](#)).

### 8.3.3 Template Properties Page

The Template properties page can be accessed from the Template page (see [Section 8.3.2, “Template Page”](#)) in the Properties tab.

It is identical to the Creating page (see [Section 8.3.1, “Creating a User Template”](#)).

From this page, you can modify all the fields except the template identifier. If the template has two keys, you can delete a key by selecting no certification mode for the keys.

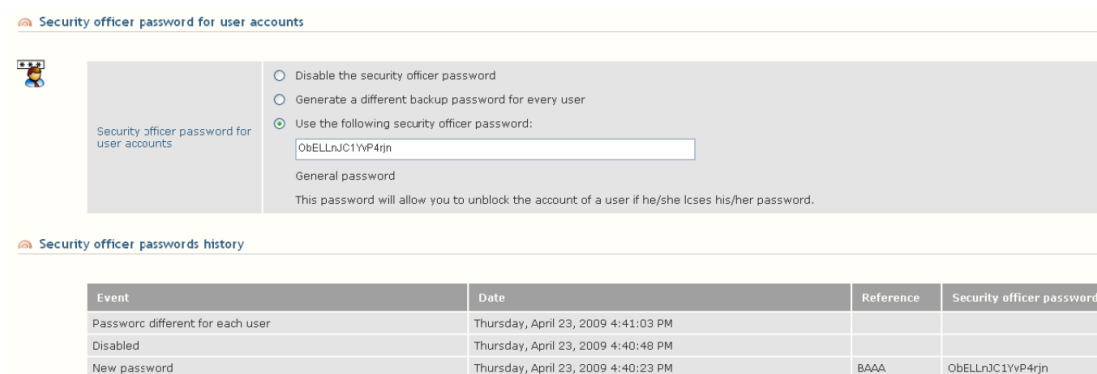
The section dealing with the SO password page is divided into two parts:

- A Security officer password for user accounts part to disable, generate a Security Officer password different for each user or use a defined password.

#### NOTE

You cannot use the remote account unblocking function (see [Section 8.10, “Remote Account Unblocking”](#)) for an account distributed with a security officer password longer than 16 characters. This limit corresponds to the random security officer passwords provided by Stormshield Data Authority Manager.

- A Security officer password history containing the Security Officer passwords already defined for this template. This list displays the events from the latest to the oldest.



Event	Date	Reference	Security officer password
Password different for each user	Thursday, April 23, 2009 4:41:03 PM		
Disabled	Thursday, April 23, 2009 4:40:48 PM		
New password	Thursday, April 23, 2009 4:40:23 PM	BAAA	ObELLnJC1YvP4rjn

The administrator must click Apply changes if a new Security Officer password has been entered or if it is disabled.

The latest entered password is automatically displayed on the Template properties page into Use the following security officer password.

### 8.3.4 Distributing a Master

This operation is available from the Template management tab in the menu of the Template tab.



This operation creates a master in the <user\_account\_dir>/<template\_id> folder, in which <user\_account\_dir> is the distribution folder defined in the general parameters, and <template\_id> is the template identifier.

If some list files are associated to the configurations of Stormshield Data File and Stormshield Data Shredder components, they are also copied in the <user\_account\_dir>/<template\_id> folder.

In case of distribution with password configuration or card configuration (see section [Configuring Stormshield Data Kernel](#)), the master is a .usr file.

During the creation of the master file, if the <LdapDn> or <UserId> tags are used in the distribution points present in the configuration of the Security policies download component, they are replaced by the template data (see section [Configuring the Security Policies Download Component](#)).

In case of distribution with all configurations, the master is a .msr file. This feature, associated with the Importing component configurations from a master (.msr file) function, enables templates to be exchanged between databases.

### 8.3.5 Importing Component Configurations from a Master (.msr file)

This operation is available from the Components tab in the menu of the Template page.

This operation allows you to import component configurations from a master (.msr file), and also the list files, if any, associated to the Stormshield Data File and Stormshield Data Shredder components.

A master (.msr file) is obtained by exporting a template (see [Section 8.3.4, "Distributing a Master"](#)). You can use these features to exchange templates between databases.

#### IMPORTANT

During this operation, the components of the applications are replaced by the configurations from the file, so they are definitively lost.

To import configurations:

1. Select a master (.msr file).
2. Enter its password.
3. Select any list files associated with the components.
4. Click Import.



The screenshot shows two sections of the Stormshield interface. The first section, titled "File selection", contains two rows: "Master (\*.msr)" and "Password", each with a text input field and a "Browse..." button. The second section, titled "Selection of list files associated with components", contains five rows, each with a label, a text input field, a "Browse..." button, and a red "X" icon. The labels are: "File: encryption list (\*.enc)", "File: decryption list (\*.dec)", "File: protection list (\*.efp)", "Shredder: cleanup list (\*.cln)", and "Shredder: protection list (\*.cfp)".

### 8.3.6 Distributing a Security Policy Update File (.usx)

#### Distribution

This operation is available from the Template management tab in the menu of the Template tab.

This operation creates a security policy update file (.usx, see [Section 8.9.2, "Security Policy Update File \(.usx\)"](#)) in the <user\_account\_dir>/<template\_id> folder, in which <user\_account\_dir> is the distribution folder defined in the general parameters, and <template\_id> is the template identifier.

To distribute update files, a security policy signatory account must have been created beforehand (see [Section 8.1.3, "Security Policy Signatory"](#) and [Section 8.7, "Creating a Security Policies Signatory"](#)).

#### Use

This update is based on a template and can be applied to all users. It contains either a password configuration or a card configuration (see [Section 8.9.3, "Configuring Stormshield Data Kernel"](#)).

During the creation of the master file, if the <LdapDn> or <UserId> tags are used in the distribution points present in the configuration of the Security policies download component, they are replaced by the template data (see [the section called "Configuring the Security Policies Download Component"](#)).

#### Publication

To make the updates available for automatic downloading, Stormshield Data Authority Manager allows them to be published:

- in the LDAP directory (see [Appendix E, Publishing and Downloading Security Updates Using an LDAP Directory](#)). The update file is published to the DN for the LDAP entry created specification for this process (see [Section 8.3.1, "Creating a User Template"](#)) in the sboxPolicyUpgrade;binary attribute defined in the LDAP parameters (see [the section called "Attribute Names"](#)).

#### NOTE

Check that the LDAP entry belongs to a class that accepts this attribute. If necessary, you can create a new class that accepts this attribute and have the entry derived from this class.



- by file. The update file is copied into the configured folder (see [the section called “Import, Export and Requests for Certificates”](#)).

### 8.3.7 Creating a Template by Duplicating an Existing Template

This operation is available from the Template management tab in the menu of the Template page.

This enables a template to be created from an existing template. This feature lets you, for example, quickly create largely similar templates within the same database.

You only have to enter:

- the identifier used by Stormshield Data Authority Manager to reference the template. This identifier is used as the name of the master file and must not contain the characters \ / : \* ? < > |
- an optional description
- a protection password for a master to be distributed from this template (a random selection of 12 characters is suggested by default)

Once validated, the template is created and you can access a report page that contains a link to the template, and which allows you to perform the duplication operation again.

## 8.4 Users List Page

The Users list page is the main user management page in Stormshield Data Authority Manager.

### 8.4.1 Operations Available

In the banner on top of the page, a menu contains the following options:

#### Creating special users:

- recovery accounts (see [Creating a Recovery Account](#)).
- security policy signatories (see [Creating a Security Policies Signatory](#)).

#### Creating standard users:

- advanced creation (see [Advanced Creation](#)).
- creating from a template (see [Creating a User from a Template](#)).
- creating from a list contained in a file (see [Creating a Large Number of Users from a File](#)).
- creating from a smart card (see [Creating a User from a Smart Card](#)).
- creating from a PKCS#12 file (see [Creating a User from a PKCS#12 File](#)).
- creating from a user file (see [Creating a User from a user File](#)).

#### User management

Actions to be carried out for users selected from the two lists on the page:

- renewing keys.
- certification (see [Renewing More than One Certificate](#)).
- distribution (see [Distributing More than One Account](#)).
- deletion (see [Deleting More than One User](#)).
- revocation (see [Revoking users](#)).



You can access the remote account unblocking from this menu (see [Remote Account Unblocking](#)).

### Certificate management

Actions to be carried out for users selected from the two lists on the page:

- creation of certificate requests (see [Creating Multiple Requests](#)).
- cancellation of certificate requests (see [Cancelling Requests](#)).
- certificate import (see [Importing More than One Certificate](#)).
- certificate export (see [Exporting More than One Certificate](#)).

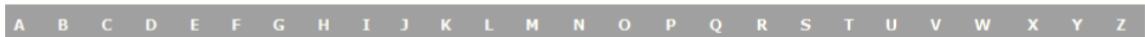
### LDAP management

- LDAP server synchronization operations (see [Synchronizing with an LDAP Directory](#)).

## 8.4.2 Searching for users

The users list contains the result of the query performed in the database.

A query can be quickly performed by clicking one of the letters of the banner: all the users whose common name starts by this letter are then displayed.



You can display all the users by clicking the icon

The search criteria can be displayed or hidden by clicking the **Search criteria** link.

The icon allows you to re-initialize all the search criteria.

The search criteria are organized in five topics. They are detailed below:

1. The identifiers pre-selection filter based on a .csv file: select a .csv file in the ANSI format, which contains users identifiers in the first column. The separator character used in the .csv file can be a comma, semi-colon, space character or vertical bar.  
If you leave the search page, the name of the .csv file is not saved. You need to select the file again.
2. The user identity: common name, email address, identifier, description, organization, organization unit, city, state and country. For each field (except country) you can enter a string with the joker character '\*' at the beginning and/or at the end of the word to replace several characters.
3. One of the following account properties:
  - "Needing distribution": Stormshield Data Authority Manager considers that the account is to be distributed. This case happens:
    - when it has not been published yet,
    - when the password or security officer password for the user has been changed,
    - when a new certificate has been imported for the user,
    - when the configuration of a component has been changed for this user or their template,
    - when a recovery account has been created or deleted,
    - when a new certificate has been imported for a recovery account,
    - when the properties of a recovery account have been changed,
    - when an external certificate has been added or deleted.



- “From template”: the configuration of the components of the account derives from the selected template. You can also select the users that do not derive from any template.
  - “Associated to a card”: the account has been created from a card, or it has been created first, and then associated to a card.
  - “With a non-certified key”: at least one of the user's keys is not certified.
4. The property of the current certificate of at least one of the keys:
    - expiry date,
    - certificate request currently in progress or not,
    - self-certified.
  5. The user type: standard or special (recovery, security policy signatory).

The search criteria can be added.

You can run the search by clicking the **Search** button. Then, the page is reloaded and the users list is updated.

The result display is performed by batch, which means that a limited number of users are displayed in the page. This number of users is defined in the **Display** section of the search criteria. Navigation buttons allow you to move from one page to another.



The users are displayed in alphabetical order. In the list, the line for each user is structured as follows:

1. The first column contains the user's common name. If truncated in the display, it can be seen in full in the tooltip. If the user is a special user, an icon is displayed in this column:
  - recovery account,
  - security policy signatory.
2. The second column contains the user email. If truncated in the display, it can be seen in full in the tooltip.
3. The check box in the third column is used to select the user to which an action is to be applied.

The total number of users present in the database is displayed in the section heading.

The number of users that meet the search criteria is displayed in the header of the first column. The first column also contains the batch of users displayed in this page.

Users 1 - 50 of 191 found

The number of users selected with the check box in the third column is displayed in the heading of the second column. You can select all the users found by the query by clicking the icon , and deselect them by clicking the icon .

The last icon indicates whether all the users of the page are selected (, only certain users are selected (, or no user is selected (). Clicking these icons selects or deselects all users of the page.

191 selected users





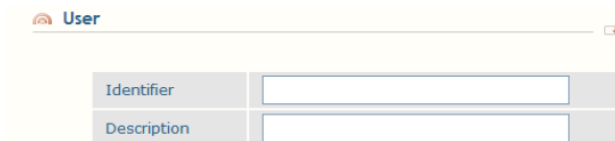
## 8.5 Creating Users

The creation operations described in this section can be accessed from the main Users lists page (see [Section Users List Page](#)).

### 8.5.1 Advanced Creation

The Advanced creation option is available in the Creating standard users tab of the Users list page.

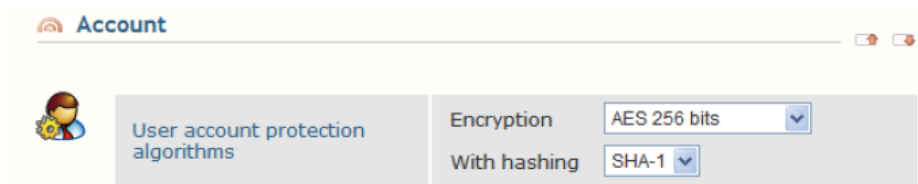
1. In the User section of the Creation page enter:
  - a. The user account Identifier. This identifier is used as the name of the account file and the address book file and must not contain the characters \ / : \* ? < > |. It is limited to 32 characters.
  - b. A Description.



The screenshot shows the 'User' section of the creation page. It has a title bar with a red icon and the word 'User'. Below the title bar, there are two input fields: 'Identifier' and 'Description'.

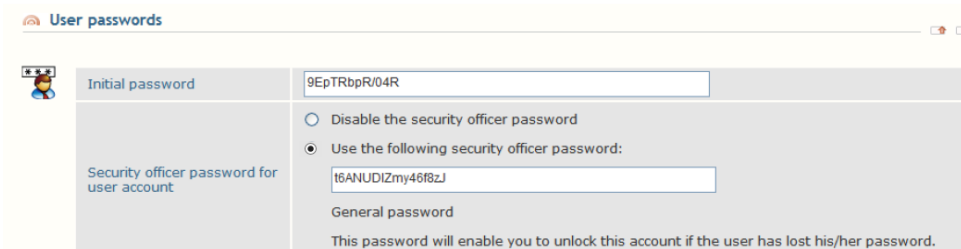
2. In the Account section enter:
  - a. An encryption algorithm (AES 256 bits by default).
  - b. A thumbprint algorithm (SHA-512 by default).

These are used to protect the account.



The screenshot shows the 'Account' section of the creation page. It has a title bar with a red icon and the word 'Account'. Below the title bar, there is a user icon and a section titled 'User account protection algorithms'. To the right of this section, there are two dropdown menus: 'Encryption' set to 'AES 256 bits' and 'With hashing' set to 'SHA-1'.

3. In the User passwords section, enter:
  - a. The account password (a random selection of 12 characters is suggested by default).
  - b. The security officer password. This section is initialized in accordance with the configuration defined in the general parameters (see the section [Security Officer Password](#)).



The screenshot shows the 'User passwords' section of the creation page. It has a title bar with a red icon and the words 'User passwords'. Below the title bar, there is a user icon and a section titled 'Initial password' with a text input field containing '9EpTRbpR/04R'. Below this, there are two radio buttons: 'Disable the security officer password' (unselected) and 'Use the following security officer password:' (selected). Below the selected radio button, there is a text input field containing 't6ANUDIZmy46f8zJ'. Below this, there is a section titled 'General password' with a text input field and a note: 'This password will enable you to unlock this account if the user has lost his/her password.'

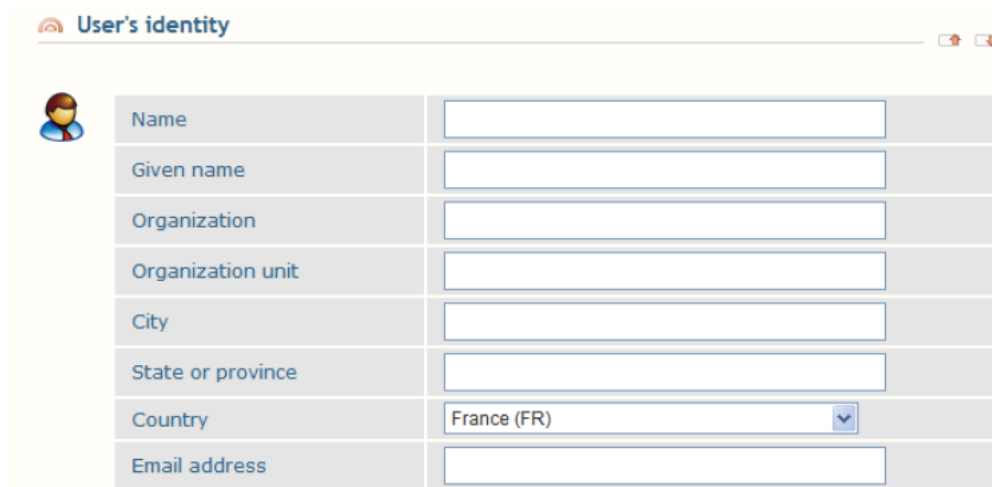
#### **i** NOTE

You cannot use the remote account unblocking function (see section [Remote Account Unblocking](#)) for an account distributed with a security officer password longer than 16 characters. This limit corresponds to the random security officer passwords provided by Stormshield Data Authority Manager.





4. Then enter the user's identity. This will be written into their certificate.

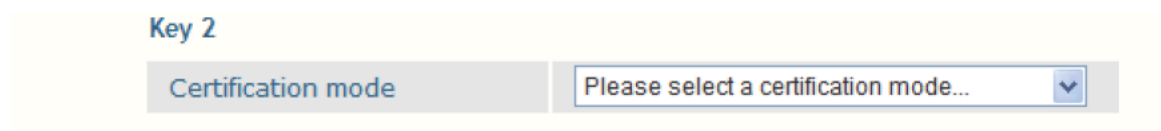


The 'User's identity' form contains the following fields:

Field	Value
Name	
Given name	
Organization	
Organization unit	
City	
State or province	
Country	France (FR)
Email address	

5. The following section allows you to define the number and role of keys, and the necessary information to their certification.

You can indicate the creation of only one key by selecting no certification mode for one of the two keys.



The 'Key 2' form shows a 'Certification mode' dropdown menu with the value 'Please select a certification mode...'.

For each key the information includes:

- encryption algorithm with its strength
- the certification mode: on top of the line that indicates the certification mode (which allows you not to create a key), the drop-down menu contains the list of certificate templates and the list of external CAs.

If you select a certificate template:

- If the database has a certified internal CA, the key is certified by this CA.
- If not, the key is self-certified, as indicated.

In both cases, the data from the certificate template are used.

- The validity period is filled with the information from the certificate template, and it can be modified.
- The Key role line indicates the role(s) of the future key. They are determined by the X.509 uses of the certificate template, and as such they cannot be modified.



The 'Key 1' form shows the following configuration:


Field	Value
Certification mode	Internal CA - Encryption
Validity period	2 years Until Thursday, April 08, 2015
Key role	<input checked="" type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 1024 bits

If you select an external CA, the key is drawn but not certified. You have to make a certification request for this key, and then import the certificate.



The selected external CA is associated to the key and its data will be used for the certification request.

To facilitate key management, you can indicate the expected role in the Key role line. Nevertheless, in the end the role(s) of the key will be determined by the X.509 uses of the future certificate.

 <b>Key 1</b>	
Certification mode	External CA - External certification authority
Key role	<input type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 1024 bits


6. Check the subject included in the certificate. This subject is obtained automatically by resolving the mask specified in the general parameters (see section [Identity](#)) and by using the user identity. You can change it manually, but it must remain in compliance with standard RFC 2253.

When the account has two keys, the subject is identical in both certificates so it only has to be specified once.


The keys are drawn automatically by the Stormshield Data Crypto software security module.

7. In the Publication section:

- a. Enter the LDAP DN resolution mask including the following tags: <CommonName>, <SurName>, <GivenName>, <Organization>, <OrgUnit>, <City>, <State>, <Country>, <Email>, <AltNameEmail>, <AltNameDNS>, <AltNameIP>, <SecurityBoxUserId>. When the DN is resolved, these tags will be replaced by the fields corresponding to the user's identity.
- b. Choose the publication mode for the certificates (see section [Publishing a Certificate](#)).

 <b>Publication</b>	
LDAP entry's DN	<input type="text"/>
LDAP publication	<input type="checkbox"/> Publish generated certificate in the LDAP directory
Certificates already published on the LDAP server	<input type="radio"/> Keep <input type="radio"/> Delete <input type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input checked="" type="checkbox"/> Publish certificate through a file

You can have a standard user inherit the security policies of a template (see section [Template](#)). This choice can be changed after the account is created (see section [Choosing a Template](#)). The list contains the templates present in the database.

 <b>User account configuration</b>	
<input type="checkbox"/> Use as template	MyUserTemplate

## 8.5.2 Creating a User from a Template

This operation is available from the Users creation tab in the menu of the Users list page, by clicking the From a template link (see section [Operations Available](#)).

1. Enter the identifier, description, last name, first name and email address.
2. Choose the publication mode for the certificate(s) (see section [Publishing a Certificate](#)).
3. Select a template from those in the database.



The account password is made up of 16 characters selected at random. You can display and change this password once the user has been created.

Other information is extracted automatically from the template:

- the encryption algorithm for the account
- the thumbprint algorithm
- the other general information making up the user's identity
- the number of keys, their strengths and the certification mode

The user also inherits the security officer password (see the section [Security Officer Password](#)) and security policies from the template (see the sections [Users Page](#) and [Choosing a Template](#)).

The screenshot shows the 'User' creation form. It has three main sections: 'User', 'User identity', and 'User account configuration'. The 'User' section contains 'Identifier' and 'Description' text boxes. The 'User identity' section includes a user icon and 'Name', 'Given name', and 'Email address' text boxes. The 'User account configuration' section has a 'Use as template' checkbox and a dropdown menu currently set to 'MyUserTemplate'.

### 8.5.3 Creating a Large Number of Users from a File

This operation is available from the User creation tab in the menu of the Users list page, by clicking the From a file link (see [Section 8.4.1, "Operations Available"](#)).

This enables a large number of users to be created automatically from a file.

It is only available if the database has at least one template.

The file is a text file in CSV format (extension .csv). Each line of the file corresponds to a user to be created. It is made up of 6 fields (the last name, first name, identifier, email address, password and description) separated by ";". The last three fields are optional:

```
LastName1;FirstName1;LastName1_FirstName1;FirstName1@arkoon.fr;secret_code_1;description1
LastName2;FirstName2;LastName2_FirstName2;FirstName2@arkoon.fr;secret_code_2
LastName3;FirstName3;LastName3_FirstName3;FirstName3@arkoon.fr;;description3
LastName4;FirstName4;LastName4_FirstName4;;;description4
LastName5;FirstName5;LastName5_FirstName5;;secret_code_5
LastName6;FirstName6;LastName6_FirstName6;FirstName6@arkoon.fr
LastName7;FirstName7;LastName7_FirstName7
```

If the password is not entered or is blank, a random 16-character password is generated.

The mechanics of creating the user is the same as when it is created from a template (see [Section 8.5.2, "Creating a User from a Template"](#)).



1. Select the .csv file to process.
2. Select a template from those in the database.

### Create users from file

**Import file**

File name

**Publication**

LDAP publication	<input type="checkbox"/> Publish generated certificate in the LDAP directory
Certificates already published on the LDAP server	<input type="radio"/> Keep
	<input type="radio"/> Delete
	<input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input checked="" type="checkbox"/> Publish certificate through a file

**User profile configuration**

Use as template

After each user has been created, Stormshield Data Authority Manager outputs a report and requests confirmation for the next one.

### Confirm user account creation

Do you confirm the user creation for **Benedict LANE** ?

You can avoid these confirmation requests by clicking the All button.

### Creation in progress

User processed	Benedict LANE
	Creation successfull
User creation in progress	Beatrice ARMSTRONG
Number of users processed	1 / 4

When all the lines of the .csv file have been processed, Stormshield Data Authority Manager displays a report page:



### Report: users accounts creation

#### Parameters



Import file

D:\Test\CSV&gt;List.csv

#### Results



Report

Creation complete

Number of users

4 users created

#### 4 users created

Common name	Identifier
▶ Beatrice ARMSTRONG	barmstrong
▶ Benedict LANE	blane
▶ Bob GREEN	bgreen
▶ Brian HOOKER	bhooker

This page displays the list of users that have been created, and also the list of users whose creation has failed, if any. To save the time needed to display the page, the two lists are limited to 100 users. The complete lists can be downloaded by clicking the icon

### 8.5.4 Creating a User from a Smart Card

This operation is available from the Users creation tab in the menu of the Users list page, by clicking the **From a smart card** link (see [Section 8.4.1, "Operations Available"](#)). This creates a user from a physical card or token that already contains the keys and certificates.

It is only available if the database has at least one template.

1. Connect to the smart card so that Stormshield Data Authority Manager can read its contents and displays all the keys found on the card.

#### Connection



PIN code

Please insert a card in the reader, enter the PIN code, and click on [Connect]. Do not remove the card from the reader before processing is over.

\*\*\*\*\*

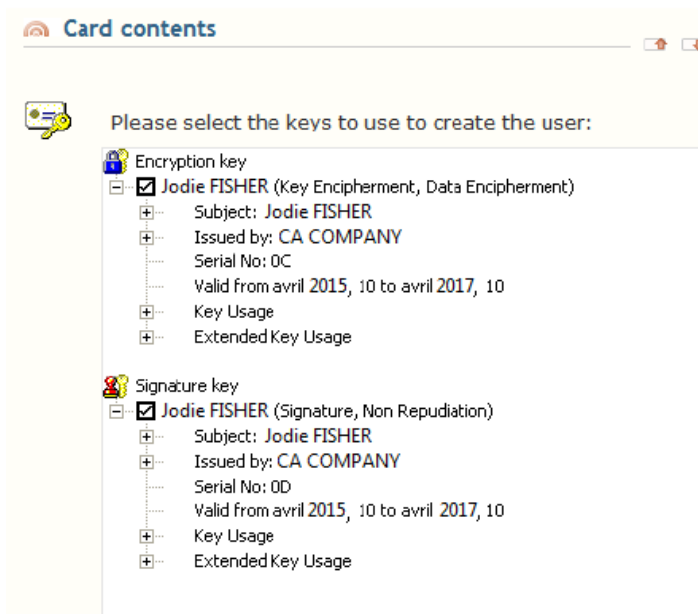
Connect

Report

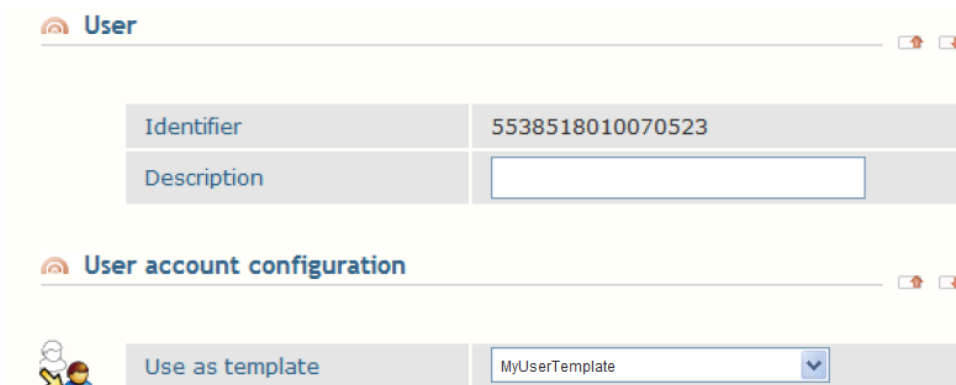
Reading OK

The keys are sorted by role: encryption, signature, and personal for those that have both roles. The key roles are determined from the X.509 uses of the associated certificate.

2. Select the keys to be used to create the account.



3. The user account identifier is the number of the card. Enter the description of the account and select a template from the ones in the database.



To create the account, the information extracted from the template is:

- the encryption algorithm for the account
- the thumbprint algorithm
- the security officer password. As defined in the template, either the password is disabled, or it is randomly-generated, or the password defined in the template page is used.

The user also inherits the security officer password (see [the section called “Security Officer Password”](#)) and component configurations from the template (see [Section 8.8, “Users Page”](#) and [Section 8.8.5, “Choosing a Template”](#)).

Stormshield Data Authority Manager extracts the user's identity and the public keys from the certificates present on the card. It copies the certificates but not the private keys into the database.

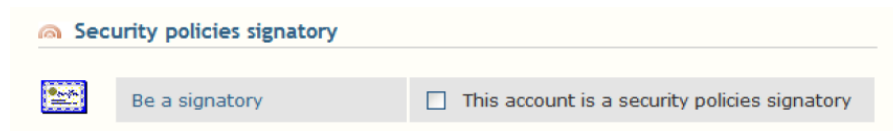
### 8.5.5 Creating a User from a PKCS#12 File

This operation is available from the User creation tab in the menu of the **Users list** page, by clicking the **From a PKCS#12 file** link (see [section Operations Available](#)). This is used to create a user from a key exchange file (PKCS#12 format). The key(s) present in the file together with the associated certificates are assigned to the user created.

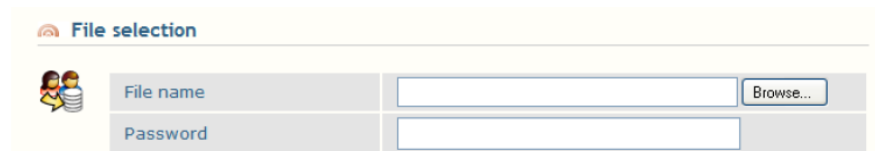


It is only available if the database has at least one template.

If the database does not contain any security policy signatory, a checkbox that allows you to create one is displayed on the page User creation from a PKCS#12 file.



Enter the password for the PKCS#12 file to access its contents.

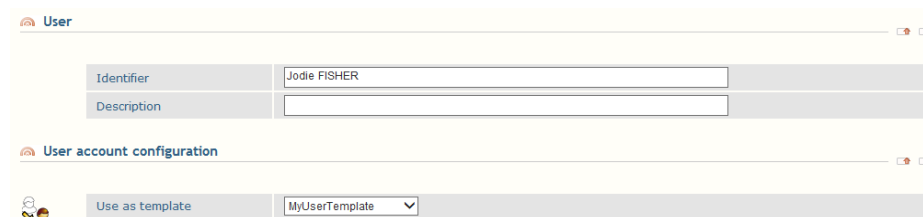


After the password has been verified, the contents of the file are displayed:

- the key list: the keys are sorted by role: encryption, signature, and personal for those that have both roles. The key role is determined from the X.509 uses of the associated certificate.



- the user identity.



To create the user:

1. Select the keys to be used to create the account.
2. Enter an identifier and a description.
3. Select a template from those in the database.

To create the account, the information extracted from the template is:

- the encryption algorithm for the account
- the thumbprint algorithm



- the security officer password. As defined in the template, either the password is disabled, or it is randomly-generated, or the password defined in the template page is used.

The user also inherits the security password (see the section [Security Officer Password](#)) and component configurations from the template (see sections [Users Page](#) and [Choosing a Template](#)).

The account password is made up of 16 characters selected at random. You can display and change this password once the user has been created.

The user identity is obtained from the subject included in certificates. If the email is not indicated in the subject, it will be searched in **Subject Alternative Name**.

In the **Users list** page, the link giving access to the user is the common name. If no common name is present in the certificate subject, it is created by concatenating the first and last names, if they exist. So if the certificate does not contain a common name, first name or last name, no operation can be carried out on the user without a name due to the lack of a link. It can, however, be deleted.

### 8.5.6 Creating a User from a user File

This operation is available from the Users creation tab in the menu of the Users list page, by clicking the From a user file link (see [Section 8.4.1, "Operations Available"](#)). This creates a user from a user .usr file keeping:

- the keys.
- the associated certificates (current and old).
- the component configurations.
- A user file associated with a smart card is not accepted.
- For the Stormshield Data Sign, Revocation controller and Automatic update components, only the configurations carried out using Stormshield Data Authority Manager are kept.
- The file must not be in use (the user must not be connected).

To display the contents of the file:

1. Select a user file.
2. Enter its password.
3. Select any list files associated with the components.

**File selection**

User file (\*.usr)  Browse...

Password

**Selection of list files associated with components**

File: encryption list (*.enc)	<input type="text"/>	Browse...
File: decryption list (*.dec)	<input type="text"/>	Browse...
File: protection list (*.efp)	<input type="text"/>	Browse...
Shredder: cleanup list (*.cln)	<input type="text"/>	Browse...
Shredder: protection list (*.cfp)	<input type="text"/>	Browse...

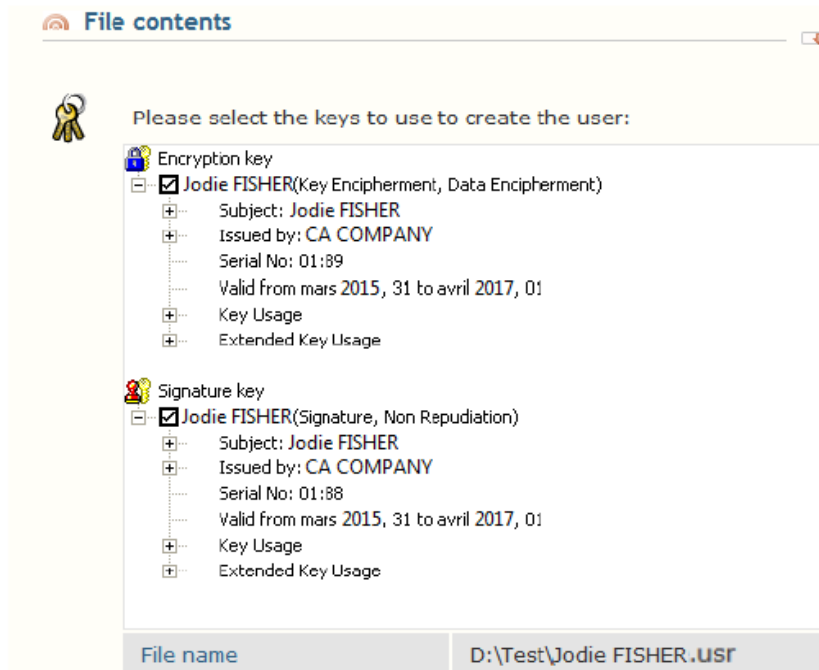
Confirm operation:

After the password has been checked, a page displays the key list. The keys are sorted by role: encryption, signature, and personal for those that have both roles. The key role is determined





from the X.509 uses of the associated certificate. They are displayed for your information. They cannot be selected.



To create the user:

1. Enter an identifier and a description.
2. Choose the security officer password.

#### **i** NOTE

You cannot use the remote account unblocking function (see [Section 8.10, "Remote Account Unblocking"](#)) for an account distributed with a security officer password longer than 16 characters. This limit corresponds to the random security officer passwords provided by Stormshield Data Authority Manager.

### 8.5.7 Creating a User from an LDAP Directory

This operation is carried out from the main LDAP directory synchronization page ([Section 8.12, "Synchronizing with an LDAP Directory"](#)).

It is only available if the database has at least one template.

1. Start the operation by looking for LDAP entries "To associate or use to create users".

Stormshield Data Authority Manager searches for entries in the LDAP directory (see [Section 5.8.6, "LDAP Configuration"](#)) that meet the search criteria entered.

#### **i** NOTE

If the search result indicates that no entry has been found, it may mean that the authentication failed. Please check the authentication data entered in the LDAP configuration parameters.



Search base	OU=Users, DC=My Company, DC=com
Filter	(Objectclass=person)
Depth	Searching: <input checked="" type="radio"/> entire tree under the base <input type="radio"/> one level under the base <input type="radio"/> base only

- Stormshield Data Authority Manager gives the option of creating a user from each entry that cannot be associated with a database user (see [Section 8.13, "Associating a User with an LDAP Entry"](#)).

**Confirm user creation**

Results of the analysis of the users present in the database

311 entries returned by the LDAP directory	3 entries already associated 0 entry to associate 308 useable to create users
--	---

Do you wish to create a user from the following LDAP entry?

DN: CN=Bob Johnson, OU=Users, DC=My Company, DC=com

**User**

Identifier	Bob Johnson
Description	

- To create the user:

The fields are filled in automatically by Stormshield Data Authority Manager according to the attributes found in the LDAP directory in compliance with the attribute names entered in the LDAP parameters (see [Section 5.8.6, "LDAP Configuration"](#)). If needed, you can modify the identifier, description, last name, first name, common name and email address.

**User identity**

Name	Bob
Given name	JOHNSON
Common name	Bob JOHNSON
Email address	bjohnson@mycompany.com

**Publication**

LDAP publication

☐ Publish generated certificate in the LDAP directory

Certificates already published on the LDAP server

☐ Keep  
☐ Delete  
☒ Replace certificates that have the same usages and the same issuer

**User account configuration**

Use as template: MyUserTemplate

- Choose the publication mode for the certificates (see [Section 7.6.4, "Publishing a Certificate"](#)).
- Select a template from those in the database.

The rules for creating the user are the same as when it is created from a template (see [Section 8.5.2, "Creating a User from a Template"](#)).

Each user is automatically associated with the LDAP entry processed. After the process, Stormshield Data Authority Manager displays a report and requests you confirm for the next step (association or creation).

You can avoid these requests by activating the automatic entry process with the All button. During automatic process, Stormshield Data Authority Manager first tries to associate the entry with a database user and then, if it is not possible, it creates a user from this entry. This creation fails if the identifier or the name are not present.



Once all entries have been processed, a report page is displayed.

**Results**

7 analyzed LDAP entries

- 0 entry already associated
- 2 recently associated entries
- 3 users created
- 2 entries not associated

**2 recently associated entries**

User	LDAP entry
Maurice Alais	CN=Maurice Alais,OU=Users,DC=My Company,DC=com
Kenneth Arrow	CN=Kenneth Arrow,OU=Users,DC=My Company,DC=com

**3 users created**

Common name	Identifier	LDAP entry
Michel Aglietta	MAglietta	CN=Michel Aglietta,OU=Users,DC=My Company,DC=com
Robert Aumann	RAumann	CN=Robert Aumann,OU=Users,DC=My Company,DC=com
Daniel Bernouilli	DBernouilli	CN=Daniel Bernouilli,OU=Users,DC=My Company,DC=com

**2 entries not associated**

LDAP entry	Summary
CN=Georges A. Akerlof,OU=Users,DC=My Company,DC=com	Processing canceled
CN=Benry Ben,OU=Users,DC=My Company,DC=com	Processing canceled

This page displays the list of associated entries, the list of created users, and the list of entries for which neither association nor creation were possible. To reduce the page display time, these lists are limited to 100 lines. The complete lists can be downloaded by clicking

## 8.6 Creating a Recovery Account

This operation is available from the Special users tab in the menu of the Users list page, by clicking the Recovery account link (see [Section 8.4.1, "Operations Available"](#)).

A recovery account only has one key, and its key certificate must have the X.509 uses for encryption.

The initial sections of the creation page are described in [Section 8.5.1, "Advanced Creation"](#).

Configure the recovery parameters as follows:

**Usage of recovery certificate**

This certificate will be register as a recovery certificate in all users accounts in this database.

Attributes	
	<input checked="" type="checkbox"/> Visible to every user to whom it is applied
	<input type="checkbox"/> Modifiable by all the users to whom it is applied
Stormshield Data Security components on which it is applied	<input checked="" type="checkbox"/> All Stormshield Data Security components
	<input type="checkbox"/> Security BOX SmartFILE
	<input type="checkbox"/> Stormshield Data Virtual Disk
	<input type="checkbox"/> Stormshield Data File
	<input type="checkbox"/> Stormshield Data Mail
	<input type="checkbox"/> Stormshield Data Safe
	<input type="checkbox"/> Stormshield Data Team

These choices can be changed after the account is created (see [Section 8.8.3, "Changing the Properties of a Recovery Account"](#)).

### ! IMPORTANT

Creating a recovery account requires certain precautions to be taken on how this account is stored: this is critical to the security of the data encrypted with user accounts using this recovery mechanism. It must be provided with a password that is sufficiently secure and held in a secure location.



## 8.7 Creating a Security Policies Signatory

This operation is available from the Special users tab in the menu of the Users list page, by clicking the Policies signatory link (see [Section 8.4.1, "Operations Available"](#)).

A signatory has only one key with signature key usage.

It is also possible to create the policies signatory from a PKCS#12 file (refer to [Section 8.5.5, "Creating a User from a PKCS#12 File"](#)).

### ! IMPORTANT

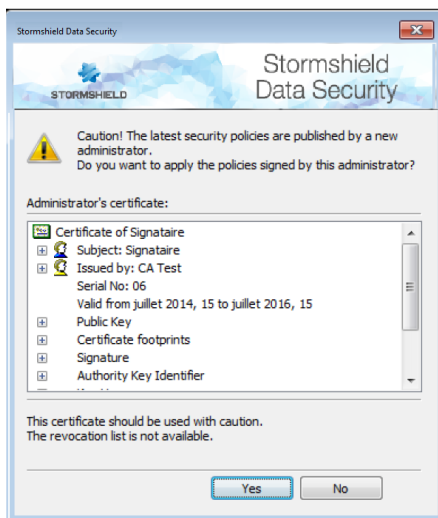
Creating a security policy signatory requires certain precautions to be taken on how this account is stored: this is critical to the definition of your security policy. It must be provided with a password that is sufficiently secure.

### 8.7.1 Renewing a Security Policies Signatory

To renew the security policies signatory, the signatory's signature key must first be renewed.

To do so, on the signatory user page, click the serial number of the signature certificate and then click the link Renew the certificate in the Certificate Management menu.

When the policies signatory is renewed, it is necessary to distribute again the update files for the users involved. Next time they will connect to their account, they will be required to trust the certificate coming from the update file by clicking Yes in the following window:



If the user clicks No, the update will not be applied and will be proposed again at the next connection.

### 8.7.2 Re-creating a Security Policies Signatory

Instead of renewing the security policies signatory, it is also possible to create the signatory again. To do so, on the signatory user page, click the link Delete in the User Management menu to delete the account.

To create again the signatory account, refer to [Section 8.7, "Creating a Security Policies Signatory"](#).

When the policies signatory is re-created or renewed, it is necessary to distribute again the update files for the users involved (refer to the previous section).



## 8.8 Users Page

This page can be accessed from the Users lists page (see [Section 8.4, “Users List Page”](#)) by clicking the user's common name.

It displays information on the user's identity:

Identifier	Robert MILLER
Template	MyCompanyTemplate

Name	MILLER
Given name	Robert
Common name	Robert MILLER
Organization	My Company
Organization unit	My Organisation Unit
Country	FR
Email address	rmiller@mycompany.com

For a special user, the User properties line illustrates the user type with one of the following icons:



recovery account.



security policy signatory.

The line User template displays if a user derives from a template. It contains the template identifier as a link to access its page (see [Section 8.3.2, “Template Page”](#)).

Then, the page displays the user's key list:

- the key role (see [Section 8.1.4, “Standard User”](#)).
- the serial number of the certificate associated to the key. Clicking the serial number of the certificate displays the key properties.
- the validity period.

Role	Certificate serial number	Certificate validity period
	0188	from Monday, March 31, 2008 to Thursday, April 01, 2010
	01AD	from Thursday, April 03, 2008 to Saturday, April 03, 2010
	0F	from Thursday, April 10, 2008 to Saturday, April 10, 2010
	10	from Thursday, April 10, 2008 to Saturday, April 10, 2010

The page displays the user DN LDAP, if any.

DN of associated LDAP entry
CN=Robert MILLER,OU=Users,DC=My Company,DC=com

At the bottom, it displays details of the user's account:

User account protection algorithms	AES 256 bits / SHA-1
Created on	Thursday, April 10, 2008 11:27:57 AM
Last modification on	Thursday, April 10, 2008 11:27:57 AM
Last distribution on	The user account has not yet been distributed

A menu is available in the banner on top of the page. The content of the menu depends on the type of user (card account, recovery account).

- In the Properties tab:



- Change the user's password and security officer password (see [Section 8.8.2, "Changing Passwords"](#)).
- Change the user's identity (see [Section 8.8.1, "Changing the Identity"](#)).
- Choose or modify the template (see [Section 8.8.5, "Choosing a Template"](#)).
- Change the properties of a recovery account (see [Section 8.8.3, "Changing the Properties of a Recovery Account"](#)).
- Remove a user's association with an LDAP entry (see [Section 8.8.4, "Removing a User's Association with an LDAP Entry"](#)).
- In the User management tab, you can:
  - Distribute the user's account (see [Section 8.9.5, "Distributing an Account"](#)).
  - Unblock the user's account (see [Section 8.10, "Remote Account Unblocking"](#)).
  - Associate the account with a smart card (see [Section 8.8.6, "Associating a Smart Card or Token"](#)).
- Define the user as the database administrator.
- Delete the user (see [Section 8.11, "Deleting Users"](#)).
- In the Keys and certificates tab, you can:
  - Export user keys to a PKCS#12 file (see [Section 9.4, "Exporting Keys in a PKCS#12 File"](#)).
  - Renew a key.

The Components tab appears if the user derives from a template. You can:

- Configure components or access the user template page (see section [Configuring Stormshield Data Authority Manager Components](#)).

## 8.8.1 Changing the Identity

This page lets you change the user's identity. It can be accessed from the User page (see [Section 8.8, "Users Page"](#)) from the Properties tab by clicking the Identity link.

All the fields that make up the user's identity as well as the description and DN in the LDAP entry associated with them can be changed.

The DN for the LDAP entry can be entered directly or supplied by the component by resolving the mask defined in the LDAP parameters (see [the section called "Publishing New Certificates"](#)).

The screenshot shows the 'Identity' and 'Publication' configuration sections of the Stormshield interface. The 'Identity' section contains a form with the following fields: Name (MILLER), Given name (Robert), Organization (My Company), Organization unit (My Organization Unit), City, State or province, Country (France (FR)), and Email address (rmiller@mycompany.com). The 'Publication' section contains a field for the DN of LDAP entry (CN=Robert MILLER,OU=Users,DC=My Company,DC=com) and a checkbox labeled 'Suggest a DN by resolving the mask defined in the general settings'.

Identity	
Name	MILLER
Given name	Robert
Organization	My Company
Organization unit	My Organization Unit
City	
State or province	
Country	France (FR)
Email address	rmiller@mycompany.com

Publication	
DN of LDAP entry	CN=Robert MILLER,OU=Users,DC=My Company,DC=com
	<input type="checkbox"/> Suggest a DN by resolving the mask defined in the general settings



## 8.8.2 Changing Passwords

This page lets you change the user's password and security officer password. It can be accessed from the User page (see [Section 8.8, "Users Page"](#)) from the Properties tab by clicking the Password link.

### Security Officer password management

- If the user does not derive from a template:

The security officer password management is carried out at user level.

If you choose to use a security officer password while it is disabled, Stormshield Data Authority Manager operates according to the configuration defined by the general parameters (see [the section called "Security Officer Password"](#)):

- If the By default, use this password for all accounts option is selected, the general security officer password is shown.
- If one of the other two options is selected, Stormshield Data Authority Manager proposes a special randomly-generated password.

Passwords

Initial password: dSI3ED9OVsCJ

Security officer password for the user's account:

- ☐ Disable the security officer password for this account
- ☒ Use the following security officer password: t6ANUDIZmy46f8zJ

General password

This password will enable you to unlock this account if the user has lost his/her password.

- If the user derives from a template:

The security officer password management is carried out at template level:

- either it is disabled at template level
- either a value is imposed at template level
- or the security officer password existence is imposed at template level but its value can be modified within this page.

In any case, the Security officer passwords history section displays the distributed passwords lists with their distribution date, from the latest to the oldest.

#### **i** NOTE

You cannot use the remote account unblocking function (see [Section 8.10, "Remote Account Unblocking"](#)) for an account distributed with a security officer password longer than 16 characters. This limit corresponds to the random security officer passwords provided by Stormshield Data Authority Manager.

## 8.8.3 Changing the Properties of a Recovery Account

This page lets you change the properties of a recovery account after it has been created. It can be accessed from the User page (see [Section 8.8, "Users Page"](#)) from the Properties tab by clicking the Recovery link.



Attributes	
	<input checked="" type="checkbox"/> Visible to every user to whom it is applied
	<input type="checkbox"/> Modifiable by all the users to whom it is applied
Stormshield Data Security components on which it is applied	<input checked="" type="checkbox"/> All Stormshield Data Security components
	<input type="checkbox"/> Security BOX SmartFILE
	<input type="checkbox"/> Stormshield Data Virtual Disk
	<input type="checkbox"/> Stormshield Data File
	<input type="checkbox"/> Stormshield Data Mail
	<input type="checkbox"/> Stormshield Data Safe
	<input type="checkbox"/> Stormshield Data Team

### 8.8.4 Removing a User's Association with an LDAP Entry

This operation removes the association between the user and the LDAP entry (see [Section 8.5.7, "Creating a User from an LDAP Directory"](#) and [Section 8.13, "Associating a User with an LDAP Entry"](#)). It can be accessed from the User page (see [Section 8.8, "Users Page"](#)) from the Properties tab by clicking the Delete LDAP association link.

The last publication date for user certificates in the LDAP directory is also deleted.

### 8.8.5 Choosing a Template

This page can be accessed from the Properties tab.

The choices suggested in the page depend on the user.

If the user derives from a template, by clicking the Change template link, you can make it derive from another template.

If the user does not derive from a template, but:

- if their component configurations are inherited from a template, by clicking the Change template link you can do one of the following:
- Inherit from another template in the database.
- No longer inherit from a template. You can then choose to assign to a user the configurations of a template that you select from the database. Otherwise, the user will have the default Stormshield Data Security configurations.

☒ the components configuration is derived from the following template:

M2CS2ko (Template 2 keys 2...) ▼

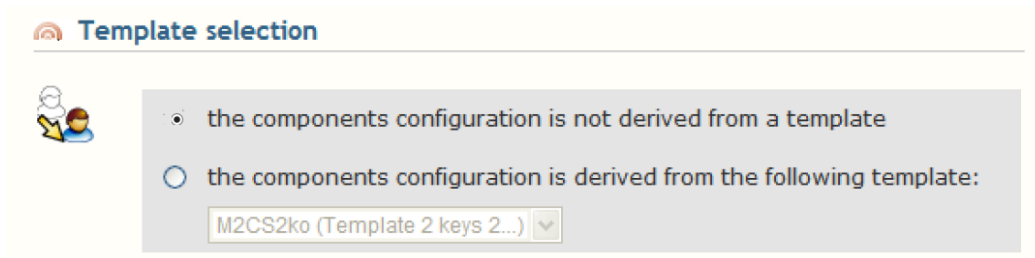
☐ the components configuration is no longer derived from a template

☐ Copy the components configuration from the following template:

M2CS2ko (Template 2 keys 2...) ▼

- if the component configurations are not inherited from a template, by clicking the Choose a template link you can choose to inherit from a template in the database.





**Template selection**

☒ the components configuration is not derived from a template

☐ the components configuration is derived from the following template:

M2CS2ko (Template 2 keys 2...) ▼

For more information on how to configure components, refer to section [Configuring Stormshield Data Authority Manager Components](#).

### 8.8.6 Associating a Smart Card or Token

A user can be associated with a physical smart card or token from the User page (see [Section 8.8, “Users Page”](#)) from the User management tab by clicking the Associate a smart card with a user link.

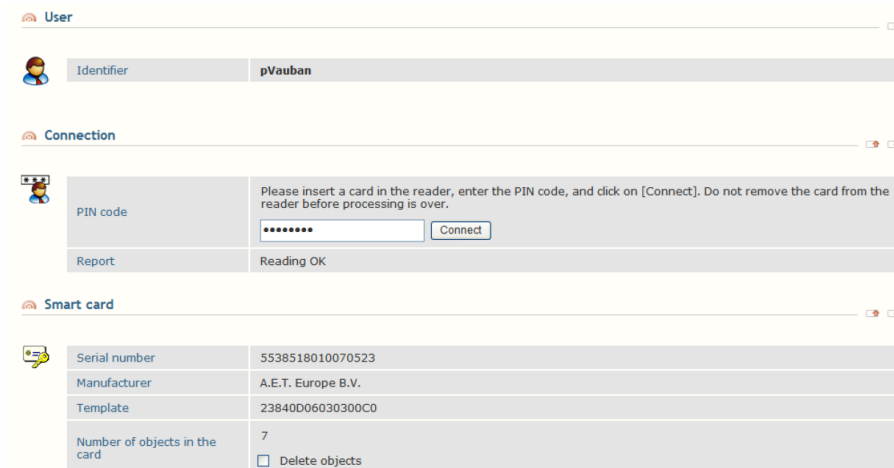
All their keys must be certified.

Connect to the card so that Stormshield Data Authority Manager can read its contents. If the connection succeeds, Stormshield Data Authority Manager displays the general information concerning the card and gives you the option of confirming the association.

During association, Stormshield Data Authority Manager writes the user's private keys, certificates and public keys to the card. If a failure occurs when the public keys are written, the association is still made. A special message is displayed in the report page.

By default, objects present on the card are kept. To delete them, check the **Delete objects** box.

During the association, the card number becomes the new user account identifier and the card's confidential code becomes the account's secret code.



**User**

Identifier: pVauban

**Connection**

PIN code: [Input field with masked characters] [Connect]

Report: Reading OK

**Smart card**

Serial number	5538518010070523
Manufacturer	A.E.T. Europe B.V.
Template	23840D06030300C0
Number of objects in the card	7

☐ Delete objects

### 8.9 Distributing User Accounts

User account and update files are distributed in the <user\_account\_dir>/<user\_id> folder, in which <user\_account\_dir> is the distribution folder defined in the general parameters, and <user\_id> is the user's identifier.

The update files can furthermore be published in the LDAP directory or by file if these features have been configured (see section [Account Distribution](#)).



The distribution modes are as follows:

- Full distribution, which creates an account file `[.usr]`, the address book `[.usd]` and moves any list files defined in the Stormshield Data File and Stormshield Data component configurations into the user's folder (see section [Users Page](#)).

The files from a full distribution can be encapsulated in an installation file `[.usi]`, see section [Installation File \(.usi\)](#). If the publication file is not activated in the general parameters, a checkbox proposing the option is displayed;

- An update file is generated `[.usx]`, see section [Security Policy Update File \(.usx\)](#). If the publication in an LDAP directory has been activated in the general parameters, a checkbox proposing the option is displayed. This is the same thing for the publication in a file.

Stormshield Data Authority Manager lets you send the update or installation files automatically by email (see section [Sending by Email](#)):

- the update or the installation files.
- a download link for the published update or the installation files.

### 8.9.1 Installation File `[.usi]`

#### Definition

A `.usi` installation file is a script that installs a user account. The user therefore does not need to manually copy the files belonging to their account.

After Stormshield Data Security has been installed on the user's workstation, they can double-click the `.usi` file. The installation procedure then copies all the files in the user's account, which then becomes operational.

#### Publication

To make the installation files available by download, Stormshield Data Authority Manager enables to publish them in this folder. This folder is defined in the general parameters (see [the section called "Publication of Installation Files"](#)). It can be a folder from your Web server. The file will then be accessible by HTTP download.



It is possible to publish the file with an unidentifiable name. This name is generated at random and is not saved. Consequently, this option is used when sending a download link by email (see [Section 8.9.4, "Sending by Email"](#)).

This feature enables to distribute the installation file to users by using a download link and prevent an attacker from using the link to download other identified users installation files.

## 8.9.2 Security Policy Update File (.usx)

### Overview

An update file allows you to change the Stormshield Data Security security policies in the user account (add or remove restrictions for example), while keeping the configuration customized by the user.

When a .usx file is activated, the current user configuration is merged with the new configuration rules contained in the file.

To take into account a setting modification during a merge (which means, as a consequence, that the user's customization will be lost), the following condition must be fulfilled in the configuration: the user must not be allowed to modify the setting in question. Otherwise, the user's customization is kept.

The update file also allows you:

- to import automatically the external certificates (see section [About External Certificates](#)) present in Stormshield Data Authority Manager to the user's account.
- to import the current certificate of each key in the user key ring. This functionality must be selected in the distribution page.

#### **i** NOTE

This operation cannot update the list files associated with the components. Consequently, the changes in the lists from Stormshield Data File for encryption, decryption and protection, and also the cleanup lists and protection lists from Stormshield Data Shredder will not be taken into account. It does not allow either to modify a [.ini] configuration file, to delete certificates or to update the identifiers and passwords of an account.

### Use

There are two ways of activating an update file:

- The user double-clicks the .usx file.
- The file of updates is automatically downloaded to the user's connection (from Stormshield Data Security) (see section [Publication](#)).

An internal counter in the file allows Stormshield Data Security to identify and apply only the most recent policies.

This counter is not taken into account if the user double-clicks on the .usx file to install it manually.

To distribute update files, a security policy signatory account must have been created beforehand (see sections [Security Policy Signatory](#) and [Creating a Security Policies Signatory](#)).

The security policy update is used after an initial configuration, a full account distribution and an installation of this configuration on the user's workstation.



## Publication

To make the updates available for automatic downloading, Stormshield Data Authority Manager allows them to be published:

- in the LDAP directory (see [Appendix E, Publishing and Downloading Security Updates Using an LDAP Directory](#)). The update file is published to the user's DN in the `sboxPolicyUpgrade;binary` attribute defined in the LDAP parameters (see section [Attribute Names](#)).

### **i** NOTE

Check that the users' LDAP entries belong to a class that accepts this attribute. If necessary, you can create a new `sboxPerson` class that accepts this attribute and have the entries for your users derived from this class (see [Publication of Security Policy Updates](#)).

- by file. The update file is copied into the configured folder (see section [Import, Export and Requests for Certificates](#)).

## 8.9.3 Configuring Stormshield Data Kernel

### Configuring security policies download

During the distribution of a user account or an update file, whether the components configurations derive from a template or not, if the `<LdapDn>` or `<UserId>` tags are used in the distribution points included in the Security policies download component, they are replaced by the data of the distributed user (see [the section called "Configuring the Security Policies Download Component"](#)).

### Secret Code and Connection Configuration

The Stormshield Data Kernel component has two "Secret code and connection" configurations (see [the section called "Configuring the User Account"](#)): one for a password account, and another for a smart card account.

There are two versions of both configurations depending on the version of Stormshield Data Security installed on the user's workstation: older or more recent than the version 5.

When the user account is distributed, Stormshield Data Authority Manager writes into the account file only the two versions of the configuration of the mode concerned: password or smart card.

### Key ring Configuration

Stormshield Data Kernel has two "key ring" configurations: one for a "single key pair" and one for a "double key pair" (see [the section called "Configuring the User Account"](#)). When a user account is distributed, Stormshield Data Authority Manager always writes the configuration corresponding to the number of user keys to the account file.

## 8.9.4 Sending by Email

If an outgoing mail server (SMTP) is configured (see [Section 5.8.7, "Outgoing Mail Server"](#)), it is possible to distribute by email:

- a `.usi` installation file which installs a user account
- a `.usx` update file which configures the Stormshield Data Security components on the user workstation



- a download link for the published .usi installation file;
- a download link for the published .usx installation file;

The email is sent to the user's electronic address during the distribution. The .sbp template file, the subject and the contents of the email may be configured:

Transmission by email

☐ Send the file by email

☒ Sending an email containing a download link

Template file (\*.sbp):  
C:\SBMDData\cacompany\MailTemplates\template\_user\_account\_mail\_link.sbp

Subject:  
Installing your Stormshield Data Security account

Text:  
Please find below a link to download the Stormshield Data Security account installation file.

URL associated to the link attached to the email and onto which the filename is concatenated.  
http://server.mycompany.com

The modifications of these data are kept in order to be proposed for the next sending by email. A message is displayed in the distribution report if the email could not be sent (incorrect address for example).

For an email with a download link, it is necessary to enter the URL on which Stormshield Data Authority Manager will concatenate automatically the published file name.

### 8.9.5 Distributing an Account

This is carried out from the User page (see [Section 8.8, "Users Page"](#)) from the User management tab by clicking the Distribute account link.

It only applies to the current user.

### 8.9.6 Distributing More than One Account

Several users may be distributed in one operation from the main Users list page (see [Section 8.4, "Users List Page"](#)) from the User management tab.

1. Select the users to whom you want to distribute accounts by checking the box on the line for each user. Then you carry out the distribution by clicking the Distribute users link.

After each user has been distributed, Stormshield Data Authority Manager outputs a report and requests confirmation for the next one:

#### Confirm user account distribution

User processed	Beatrice ARMSTRONG
	Distribution successfully issued

Do you confirm the user distribution for Benedict LANE?

Yes All No Cancel

2. You can avoid these confirmation requests by clicking the All button:

#### Distribution in progress

User processed	Benedict LANE
	Distribution successfull
User distribution in progress	Bob GREEN
Number of users processed	2 / 4

Progress bar: 10 blue squares, 2 are filled.



3. When all the users have been processed, Stormshield Data Authority Manager displays a report page:

Users distribution report

Results

Report	Distribution not complete: check reports
Number of users	3 users distributed 1 user not distributed

3 users distributed

Common name	Identifier
> Benedict LANE	blane
> Bob GREEN	bgreen
> Bob HOOKER	bhooker

1 user not distributed

Common name	Identifier	Summary
> Beatrice ARMSTRONG	barmstrong	Distribution canceled

This page displays the list of users that have been distributed, and also the list of users whose distribution has failed, if any. To save the time needed to display the page, the two lists are limited to 100 users. The complete lists can be downloaded by clicking the icon

## 8.10 Remote Account Unblocking

This function allows the administrator to remotely unblock a user account without anyone else able to reproduce the procedure. To be unblocked, the account must have been generated by Stormshield Data Authority Manager or created from a template also created by Stormshield Data Authority Manager.

Accessing remote account unblocking requires the Unblock users accounts permission from the Users' administrator role. See [Section 6.2, "Authorizations"](#).

### NOTE

This function is only available if the Security Officer password length does not exceed 16 characters.

To reduce entry errors, all the data to provide are encoded in Base32 into this part of the product. This means you can only encounter the following characters: ABCDEFGHIJKLMNOPQRSTUVWXYZ234567.

### 8.10.1 Managing S0 Passwords

The Security Officer passwords history for a template or a user must be kept to avoid desynchronization between the blocked keystore S0 password and the latest S0 password entered by the administrator if he/she has not distributed the keystore.

Each S0 password is identified with a reference which is provided by the user when requesting the administrator to unblock the account.

For each template, the administrator can choose between attributing the same S0 password to all the users from a template or defining an S0 password different for each user deriving from a template.

### 8.10.2 Distributing an Account

When distributing an account:



If the user does not derive from a template and if he/she does not disable his/her Security Officer password, or if he/she derives from a template for which the Generate an SO password different for each user option has been selected, if a new SO password has been defined, this password is put into the user passwords history.

If the user derives from a template imposing the SO password, the SO password is put into the user passwords history.

If the user derives from a template disabling the user password or if the user does not derive from a template and disable the SO password, the distribution with a disabled SO password is put into the user passwords history.

### 8.10.3 Unblocking an Account Generated by Stormshield Data Authority Manager

The Unblock an account function can be accessed from:

- the Users list page in the Users Management, Unblock menu, by clicking Database user account (see [Section 8.4, "Users List Page"](#)).
- the User page in the User Management menu, by clicking Unblock the account (see [Section 8.8, "Users Page"](#)).

If the function was called from the Users list page:

1. Enter the identifier provided by the user, then click Activate to check the identifier and access the SO password reference field (see [Section 5.8.2, "Database Page"](#)).
2. Enter the SO password reference provided by the user.

Activation

Unblocking the user account is only available for users created on and distributed from the database.  
Enter the identifier provided by the user:

5PRA

Entry for the security officer password reference

Security officer password reference

3. Click Search for users.

Stormshield Data Authority Manager searches for the SO password identified by the provided reference and then displays the list of users distributed with this password.

The list display is limited to 100 users. The complete list can be downloaded clicking

4. Enter the characters provided by the user:

Entry

Enter the characters provided by the user:

K4HAN - JOPCU - 235IF - 7

MENBF - GBSTE - CLHFN -

ESVK7 - BJH76 -  -



Once all the characters of the line are provided, the entry control is carried out and the icon indicates the result.

5. Click Encrypt the S0 password.

Stormshield Data Authority Manager displays a new page containing the data to provide to the user in order to unblock the account.

#### If the function was called from the User page:

1. Enter the identifier provided by the user and then click Activate to check the identifier and access the S0 password reference entry field.
2. Enter the S0 password reference provided by the user.
3. Click Check.

Stormshield Data Authority Manager checks the user has been distributed with this S0 password and then displays a new entry page.

4. Enter the characters provided by the user.

Once all the characters of the line have been entered, the entry control is carried out and the icon indicates the result.

5. Click Encrypt the security officer password

Stormshield Data Authority Manager displays a new page with the data to provide to the user in order to unblock the account.

### 8.10.4 Unblocking an Account Generated by Stormshield Data Security

The unblocking function can be accessed from the Users list page in the Users management, Unblock menu clicking An account created by Stormshield Data Security.

To do so:

1. Enter an identifier provided by the user and click Activate to check the identifier and access the S0 password reference entry field (see [Section 5.8.2, "Database Page"](#)).
2. Enter the characters provided by the user.

Enter the characters provided by the user:					
OIZMF2	-	2DK3SC	-	A	✓
75CNSN	-	UPIMSS	-	V	✓
XFQE22	-	ES2QOS	-	B	✓
EQK3IU	-	2MBTYV	-	M	✓
IKVUNG	-	J6GX5R	-	S	✓
DM07ZI	-	ILWGNP	-	E	✓
KR2VXU	-	G3STQ6	-	L	✓
PUXQV6	-	NHSSLC	-		✗
6PTRYO	-		-		✗
BZ5NGN	-	V4	-	H	✓

Paste from the clipboard

Once all the characters from the line have been entered, the entry control is carried out and the icon indicates the result.

3. Click Find the security officer password.

Stormshield Data Authority Manager displays a new page with the data to provide to the user in order to unblock the account.

## 8.11 Deleting Users

A user can be deleted from the database.





**NOTE**

This operation does not delete the files generated during account distribution or any published certificate.

### 8.11.1 Deleting a User

This is carried out from the User page (see [Section 8.8, "Users Page"](#)) from the User management tab by clicking the Delete link.

It only applies to the current user.

### 8.11.2 Deleting More than One User

Several users may be deleted in one operation from the main Users lists page (see [Section 8.4, "Users List Page"](#)) from the User management tab.

1. Select the users you want to delete by checking the box on the line for each user.
2. Click the Users accounts deleting link.
3. After each user has been deleted, Stormshield Data Authority Manager outputs a report and requests confirmation for the next one:

The screenshot shows a confirmation dialog box. At the top, it says "User processed" and "Beatrice ARMSTRONG" with "Deleting successfully issued". Below this, it asks "Do you confirm the user deleting for Benedict LANE?". At the bottom right, there are four buttons: "Yes", "All", "No", and "Cancel".

4. You can avoid these confirmation requests by clicking the All button:

The screenshot shows a "Deleting in progress" status. It lists "User processed" for "Bob GREEN" with "Deleting successfull" and "User deleting in progress" for "Brian HOOKER". At the bottom, it shows "Number of users processed" as "3 / 4" with a progress bar.

5. When all the users have been processed, Stormshield Data Authority Manager displays a report page:

The screenshot shows the "Users deleting report" page. It has a "Results" section with a "Report" table showing "Deleting complete" and "Number of users" as "4 users deleted". Below this, it says "4 users deleted". At the bottom, there is a table with two columns: "Common name" and "Identifier". The table lists four users: Beatrice ARMSTRONG (barmstrong), Benedict LANE (blane), Bob GREEN (bgreen), and Brian HOOKER (bhooker).

This page displays the list of users that have been deleted, and also the list of users whose deletion has failed, if any. To save the time needed to display the page, the two lists are limited to 100 users. The complete lists can be downloaded by clicking

## 8.12 Revoking users

Users' certificates may be revoked.

You can either revoke a single certificate or several certificates at the same time.



It is recommended that you publish a new revocation list once a certificate has been revoked so that the certificate's revocation status can be applied as soon as possible.

CRLs are generated and published according to the options specified in the "Certificate management parameters" (see the [Certificate revocation lists \(CRLs\)](#) section).

### 8.12.1 Revoking a single user

A user may be revoked from his certificate's display page or from the main **List of users** page.

To revoke a user from his certificate's display page, refer to the section on [Revoking a Certificate](#).

To revoke a single user from the main **List of users** page ([Homepage](#) section):

1. Select the user that you wish to revoke.
2. Open the **User management** menu and click on **Revoke users**. You will see several revocation options:
  - Invalidity date,

#### NOTE

Unlike the revocation date, which will always be included and will be the current date, the invalidity date is optional. It is the date from which the certificate will be invalid or the date on which the key was compromised, and will be included in the **InvalidityDate** field in the CRL entry. There is no need to specify whether it is the same as the revocation date.

- Comments regarding the revocation. These comments will not appear in the CRL; they are used only in Stormshield Data Authority Manager. However, they will appear in the certificate's display page ([Certificate display](#) section);
  - Publication of a new revocation list.
3. Click on **Revoke users**. A report page appears.

### 8.12.2 Revoking several users

To revoke several users at the same time from the main **List of users** page ([Homepage](#) section):

1. Select the users that you wish to revoke.
2. Open the **User management** menu and click on **Revoke users**. You will see several revocation options:
  - Invalidity date,

#### NOTE

Unlike the revocation date, which will always be included and will be the current date, the invalidity date is optional. It is the date from which the certificate will be invalid or the date on which the key was compromised, and will be included in the **InvalidityDate** field in the CRL entry. There is no need to specify whether it is the same as the revocation date.

- Comments regarding the revocation. These comments will not appear in the CRL; they are used only in Stormshield Data Authority Manager. However, they will appear in the certificate's display page ([Certificate display](#) section);
  - Publication of a new revocation list.
3. Click on **Revoke users**.



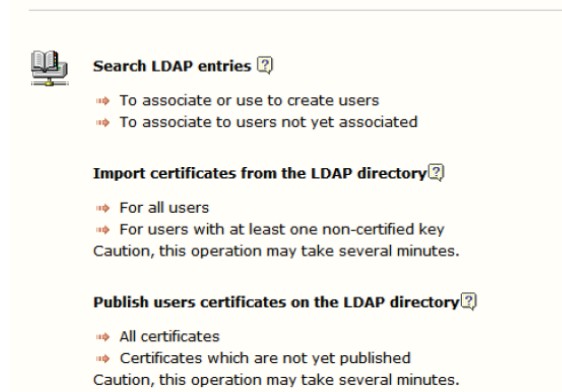
4. After every revocation, Stormshield Data Authority Manager will provide a report and request confirmation for the next revocation.
5. Once all users have been processed, Stormshield Data Authority Manager will display a report page.

## 8.13 Synchronizing with an LDAP Directory

The main LDAP directory synchronization page can be accessed from the Other tab in the menu of the Users lists page by clicking the LDAP Synchronization link (see [Section 8.4.1, "Operations Available"](#)).

The LDAP server to which Stormshield Data Authority Manager connects is defined in the general parameters (see [the section called "LDAP Server"](#)).

### Synchronization with the LDAP directory



This page has a menu with options to:

- associate LDAP entries with database users (see [Section 8.13, "Associating a User with an LDAP Entry"](#))
- create users from LDAP entries (see [Section 8.5.7, "Creating a User from an LDAP Directory"](#))
- import certificates for users associated with LDAP entries from the directory (see [the section called "Importing Certificates from an LDAP Directory"](#))
- publish certificates for users associated with LDAP entries in the directory (see [Section 10.7, "Publishing Certificates in an LDAP Directory"](#))

## 8.14 Associating a User with an LDAP Entry

Stormshield Data Authority Manager gives the option of associating an LDAP entry with a database user when they have the same email address and/or common name and/or identifier and/or first and last names. The email address and the common name are mandatory.

There are two ways of finding entries in the directory to be associated with database users:

- Click the To associate or use to create user link. Stormshield Data Authority Manager then looks for a user in the database, which can be associated with each entry read from the directory. If it fails, it gives you the option of creating a user from this entry (see [Section 8.5.7, "Creating a User from an LDAP Directory"](#)).
- Click the To associate to users not yet associated link. Stormshield Data Authority Manager then carries out a search in the directory for an entry that could be associated with a user for all database users who have not yet been associated with an entry.



In both cases, Stormshield Data Authority Manager searches for entries in the LDAP directory (see [Section 5.8.6, “LDAP Configuration”](#)), which meet the search criteria entered:

Search criteria

Search base	OU=Users, DC=My Company, DC=com
Filter	(Objectclass=person)
Depth	Searching: <input checked="" type="radio"/> entire tree under the base <input type="radio"/> one level under the base <input type="radio"/> base only

For each possible association, Stormshield Data Authority Manager displays a confirmation page:

Confirm entry association

Analysis results for users present in the database

Report 3 users to associate

LDAP entry to associate

DN	CN=Alice SMITH,OU=Users, DC=My Company, DC=com
mail	asmith@mycompany.com
cn	Alice SMITH
sn	SMITH
givenName	Alice

User to associate

Common name	Alice SMITH
Identifier	Alice SMITH
Email address	asmith@mycompany.com

Confirm association? Yes All No Cancel

You can avoid these requests by activating the automatic renewing with the All button.

When all the possible associations have been proposed, a report page is displayed.

Results

3 users to associate 2 recently associated users 1 user not associated

2 newly associated users

User	LDAP entry
> Alice SMITH	CN=Alice SMITH,OU=Users, DC=My Company, DC=com
> Robert MILLER	CN=Robert MILLER,OU=Users, DC=My Company, DC=com

1 user not associated

User	Summary
> Jodie FISHER	User association canceled

This page displays the list of associated users and the list of users for whom the association has failed. To limit the page display time, these two lists are limited to 100 users. The complete lists can be downloaded by clicking



## 9. Managing User Keys

This chapter describes how to manage user keys.

### 9.1 Key and Certificate Page

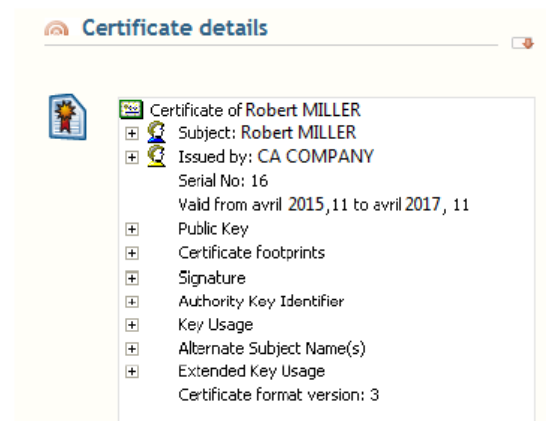
This page can be accessed from the User page (see [Section 8.8, “Users Page”](#)) by clicking the serial number of the key certificate.

The first section shows:

- the encryption algorithm with its strength
- the key role (see [Section 8.1.4, “Standard User”](#))



The second section displays the full contents of the certificate in the form of a tree.

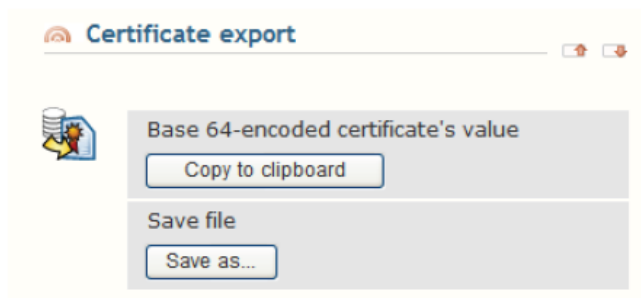


In the next section, the information on a certificate request (if any) are displayed:

- the date of any certificate request in progress for this key
- the name of the external CA associated to the key (see [Section 5.8.12, “External Certification Authorities”](#))



In the last section, you can export the certificate by copy-pasting its "base 64" value or by saving in a file (see [the section called “Exporting a Certificate”](#)).



In the banner on top of the page, a menu gives the following options:

- In the Properties tab, you can access the key properties.
- In the Key management tab, you can delete the key.

### ! IMPORTANT

If you delete an encryption key, you will not be able to decrypt the data encrypted by this key. This option is not available if the user is associated to a card.

- In the Certificate management tab, you can:
- Renew the certificate for the key (see [Section 10.4.1, "Renewing one Certificate"](#)).
- Make a certificate request for the key (see [Section 10.3.2, "Creating a Request"](#)).
- Import a certificate for the key (see [Section 10.5.1, "Importing Internal Certificates"](#)).
- If the key has been certified by the database internal certification authority, you can access the certificate page and revoke the certificate.

## 9.2 Key Properties Page

The Key properties page can be accessed from the Template page, in the Properties tab.

You can change:

- The key role:

Among all the user keys, only one key can own the encryption role and only one key can have the signature role, knowing that one unique key can have both roles.

- A encryption key can be attributed an encryption role or a decryption role. When you attribute an encryption role to a key, if another key already has the encryption role, then it automatically loses the encryption role and becomes a decryption key.

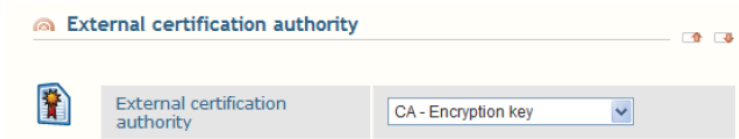


- A signature key can be attributed a signature role, otherwise it is merely a key with the signature usage. When you attribute a signature role to a key, if another key already has the signature role, then it automatically loses it.





- The name of the external certification authority associated to the key (see [Section 5.8.12, “External Certification Authorities ”](#)).



## 9.3 Renewing Keys

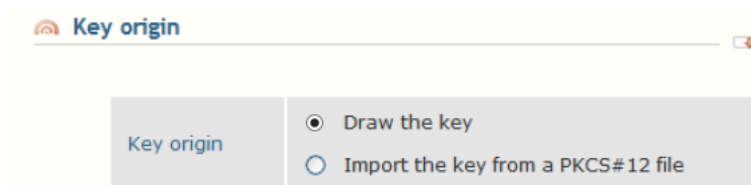
### 9.3.1 Renewing a key

You can renew a key from the User page (see [Section 8.8, “Users Page ”](#)) from the Keys and certificates tab by clicking the Renew a key link.

This operation consists in adding a key to a user. This new key automatically obtains the role(s) given by its certificate. These roles are determined by the certificate X.509 usages. The keys that previously owned these roles mechanically become decryption keys or merely keys with a signature usage.

In the first part of the page, you have to select the origin of the new key:

- either draw the key (see [the section called “Drawing the Key ”](#)).
- or import the key from a PKCS#12 file (see [the section called “Importing the Key from a PKCS#12 File ”](#)).



### Drawing the Key

To draw the key, proceed as follows:

1. Select the encryption algorithm with its strength.
2. Select the certification mode: on top of the line that indicates the certification mode, the drop-down menu contains the list of certificate templates and the list of external CAs.
  - If you select a certificate template:
  - If the database has a certified internal CA, the key is certified by this CA.
  - If not, the key is self-certified, as indicated.

In both cases, the data from the certificate template are used.

The validity period is filled with the information from the certificate template, and it can be modified.

The Key role line indicates the role(s) of the future key. They are determined by the X.509 uses of the certificate template, and as such they cannot be modified.

- If you select an external CA, the key is drawn but not certified. You have to make a certification request for this key, and then import the certificate.

The selected external CA is associated to the key and its data will be used for the certification request.



To facilitate key management, you can indicate the expected role in the Key role line. Nevertheless, in the end the role(s) of the key will be determined by the X.509 uses of the future key.

Certification	External CA - CA - Encryption key
Key role	<input type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 1024 bits

- Depending on the general parameters, a section gives you the option of publishing the certificate generated.

If an LDAP server is configured (see [Section 5.8.6, "LDAP Configuration"](#)), you can choose to publish the certificate in the LDAP directory.

Configure the operation to be carried out if there are any certificates already present on the LDAP server at the entry designated by the DN:

- Keep them.
  - Delete them.
  - Replace certificates with the same X.509 uses and issued by this authority.
- If publication by file is configured (see [the section called "Generated Certificates"](#)), this is given as an option. For more information, refer to the certificate publication section (see [Section 7.6.4, "Publishing a Certificate"](#)).

LDAP publication	<input checked="" type="checkbox"/> Publish generated certificate in the LDAP directory
Certificates already published on the LDAP server	<input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input checked="" type="checkbox"/> Publish certificate through a file

## Importing the Key from a PKCS#12 File

To import the key from a PKCS#12 file, proceed as follows:

- Select the PKCS#12 file.
- Enter its password.

File name	<input type="text"/> Browse...
Password	<input type="text"/>

After the password verification, the list of the keys contained in the file are displayed.

The keys are sorted by role: encryption, signature, and personal for those that have both roles. The key roles are determined from the X.509 uses of the associated certificate.

- Select the key that you want to add and validate. Only one key must be selected.

## User Associated to a Smart Card

For a user associated to a smart card, the two procedures described above have to be completed with a further step: writing the key (either drawn or imported from a PKCS#12 file) into the smart card. You have to reconnect to the smart card and validate.

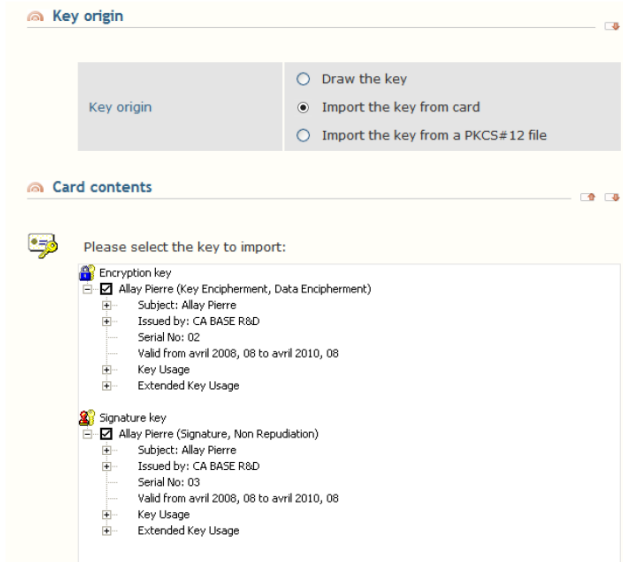
Otherwise, you can import the key from the smart card:





1. Connect to the smart card.
2. Select the import of the key from the smart card. Then the list of keys is displayed.

The keys are sorted by role: encryption, signature, and personal for those that have both roles. The key roles are determined from the X.509 uses of the associated certificate.



3. Select the key that you want to add and validate. Only one key must be selected.

### 9.3.2 Renewing several keys

Renewing several keys in one operation can be carried out from the Users list main page ( see [Section 8.4, “Users List Page ”](#) ).

#### **i** NOTE

When renewing several keys in one operation, it is only possible to draw keys.

To renew a key for each user:

1. Select the users for whom you want to renew a key. This selection is carried out by checking the box available for each user concerned by the process.
2. Run the renewing process by clicking the Renew a key link from the Users management menu.
3. Select the certification mode from the following page: in addition to the line indicating you must select a certification mode, the scroll down menu contains the certificate templates list and the external certification authorities certificate list.
  - If you select a certificate template:
  - if the database has a certified internal certification authority, the key is certified by this certification authority.
  - otherwise, the key is self-certified and this information is provided.

In both cases, the template certificate data are used.

You can modify the validity date (already provided with the certificate template).

The Key role line indicates the role(s) for the future key. They are determined from the X.509 usages of the certificate template and cannot be modified.



- If you select an external certification authority, the key is drawn but not certified. You must request for a key certificate and then import it.

The selected external certification authority is associated with the key and its data will be used during the certificate request.

To facilitate the key management, you must indicate the desired role for the key into the Key role line. After a while, the X.509 uses for the future certificate will give the key role(s).

### Key renewal

**Key origin**

Key origin	Draw the key
------------	--------------

**Key and certificate**

Certification	Internal CA - Encryption
Validity period	2 years Until Thursday, May 19, 2011
Key role	<input checked="" type="checkbox"/> Encryption <input type="checkbox"/> Signature
Key algorithm	RSA 1024 bits

4. Depending on the general parameters, a section offers you the possibility to publish the generated certificate(s).

If an LDAP server is configured (see [Section 5.8.6, "LDAP Configuration"](#)), you can choose to publish the certificate into the LDAP directory. The publication will always be carried out towards the user's DN for whom the certificate is being renewed. Configure the operation to be carried out on any certificates already present onto the LDAP server at the entry indicated by the DN:

- keep them.
- delete them.
- replace certificates with the same X.509 uses and issued by this authority.

If publication by file is configured (see [the section called "Generated Certificates"](#)), it will be proposed. For more information, refer to [Section 7.6.4, "Publishing a Certificate"](#).

**Publication**

LDAP entry's DN	
LDAP publication	<input type="checkbox"/> Publish generated certificate in the LDAP directory
Certificates already published on the LDAP server	<input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input checked="" type="checkbox"/> Publish certificate through a file

5. Run the process by clicking Renew.

After each renewing, Stormshield Data Authority Manager displays a report and requests for a confirmation for next renewing:

**Confirm user account keys modification**

User processed	Beatrice ARMSTRONG
Keys modification successfully issued	

Do you confirm the user keys modification for **Benedict LANE**?

Yes All No Cancel

You can avoid these requests by activating the automatic renewing with the All button:

**Keys modification in progress**

User processed	Benedict LANE
Keys modification successful	
User keys modification in progress	Bob GREEN
Number of users processed	2 / 4



Once all the keys have been renewed, Stormshield Data Authority Manager displays a report page:

#### Users keys modification report

**Results**

Report	Keys modification not complete: check reports	
Number of users	3 users modified	1 user not modified

**3 users modified**

Common name	Identifier
» Benedict LANE	blane
» Bob GREEN	bgreen
» Bob HOOKER	bhooker

**1 user not modified**

Common name	Identifier	Summary
» Beatrice ARMSTRONG	barmstrong	Keys modification canceled

This page displays the list of users for whom a key has been renewed and possibly the list of users for whom renewing has failed. To limit the display time, these two lists are limited to 100 users. The complete lists can be downloaded by clicking

## 9.4 Exporting Keys in a PKCS#12 File

This is carried out from the User page (see [Section 8.8, "Users Page"](#)) from the Keys and certificates tab, by clicking the Export keys link:

**Keys certified**

Certificate serial number	Certificate validity period	Role	<input checked="" type="checkbox"/>
» OC	from Thursday, April 10, 2008 to Saturday, April 10, 2010		<input checked="" type="checkbox"/>
» OD	from Thursday, April 10, 2008 to Saturday, April 10, 2010		<input checked="" type="checkbox"/>

**Export**

Password

1. The list of the user's keys is displayed. Select the keys to be exported by checking the checkbox present on every line next to the key you want to export. The icon indicates whether all keys are selected (☒ icon) or if only certain keys are selected (☒ icon), or no key is selected (☐ icon). Clicking these icons selects or deselects all keys.
2. Enter the password.  
To guarantee the confidentiality of the data, it is recommended that you enter a strong and difficult password.  
For help in entering the password, a random choice can be made by clicking the icon.
3. Click Export keys.
4. A report page is displayed. You are proposed to save the created PKCS#12 file, in which the associated keys and certificates have been copied.



## 10. Managing Certificates

This chapter describes the different types of internal and external certificates, and how to import and export them.

### 10.1 About External Certificates

Stormshield Data Authority Manager can manage certificates that it has not generated, that is external certificates.

There are two types of external certificates:

- external recovery certificates (see section [External Recovery Certificates](#)) which are incorporated into the user accounts for recovery.
- other external certificates (see section [Other External Certificates](#)) which can be certification authority certificates:
- added to users' address books (.usd), and users' update files (.usx).
- used to build the parent-child relationships of certificates generated by the internal certification authority.

#### 10.1.1 External Recovery Certificates

To manage external recovery certificates, go to the Users Management page (see [Section 8.4.2, "Searching for Users"](#)) and also the Users list page (see [Section 8.4, "Users List Page"](#)).

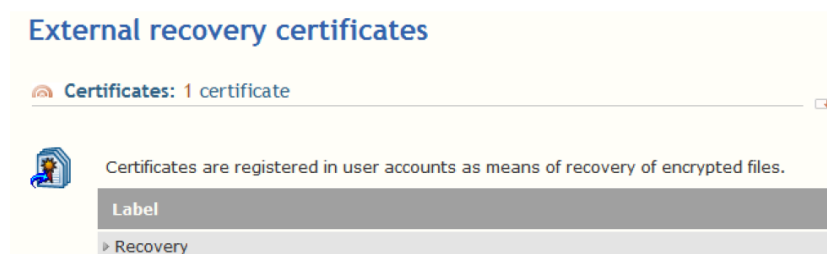
During distribution, these certificates are written to the user account for the recovery of encrypted data.

When importing an external recovery certificate, it is automatically added to the user accounts when the security policy is updated (.usx).

#### NOTE

Deleting external recovery certificates is not managed by this functionality. The certificates are not deleted from the user accounts.

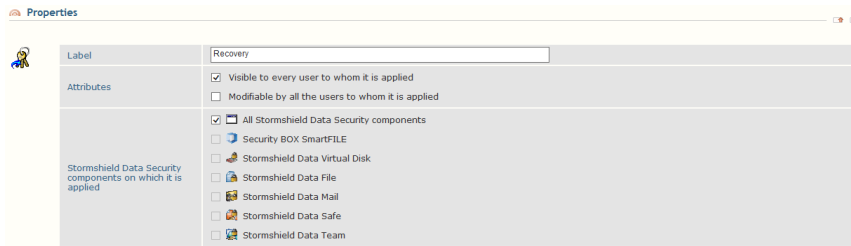
The page of external recovery certificates shows the list of recovery certificates already imported into the database. You can import a new certificate from the Operations drop-down menu (see [Section 10.5.2, "Importing External Certificates"](#)).



The certificates are identified by a label. Clicking this label displays a page showing the properties of the certificate.

From this page you can:

- detail the contents of the certificate
- change the label of the certificate and its recovery properties
- delete the certificate



### 10.1.2 Other External Certificates

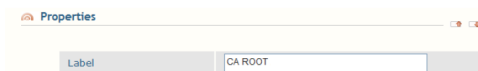
External certificates to be added to the address books, update files (.usx), and making up the parent-child relationship chain are managed from the homepage.

These certificates are added to the address books of all users when they are distributed. The authority certificates are present in the Authorities tab of the address book. The other certificates are present in the Certificates tab.

They are copied in the user's update file .usx in order to be imported in the user's address book.

These certificates are also used to build the parent-child relationship chain for certificates generated by the internal certification authority. When a certificate generated by the internal certification authority is exported (see [Section 10.6.1, "Exporting Internal Certificates"](#)), Stormshield Data Authority Manager reads the certificate for the authority and browses through these external certificates to build the most complete parent-child relationship chain possible. So if you want to export certificates with their parent-child relationships (.p7b, .p7c), import all the certificates in the parent-child chain into the external certificates.

The page of external certificates shows the list of certificates already imported into the database and a link used to import a new certificate (see [Section 10.5.2, "Importing External Certificates"](#)).



The certificates are identified by a label. Clicking this label displays a page showing the properties of the certificate.

From this page you can:

- detail the contents of the certificate
- change the label of the certificate
- delete the certificate

## 10.2 Email notification for a certificate expiry

You can be notified by email when user certificates are about to expire.

The email provides information related to users impacted such as the id, the first name and last name and the email address. It provides also information related to certificates such as the serial number, the expiry date and the cryptographic use (signature or encryption). To activate and set up this functionality, refer to [the section called "Email notification"](#).

- To activate this functionality, you need to set up first the connection information to the SMTP server (refer to [the section called "SMTP Server"](#));
- Only the users current certificates are listed in the notification email. Old certificates and revoked certificates are not mentioned;



- Notification emails are sent with the frequency set up in the related field, even if certificates are expired;
- The list can include certificates corresponding to renewed keys;
- Stormshield Data Authority Manager does not send any email if no certificate is about to expire.

### 10.3 Creating PKCS#10 Certificate Requests

Stormshield Data Authority Manager gives you the option of generating certificate requests in PKCS#10 format for user keys.

The date the certificate request currently in progress was created is shown in the Key and certificate page (see [Section 9.1, "Key and Certificate Page"](#)).

#### 10.3.1 "Binary"/"base 64" Formats

The choice of format is made in the parameters of the external CA associated to the key (see [Section 5.8.12, "External Certification Authorities"](#)).

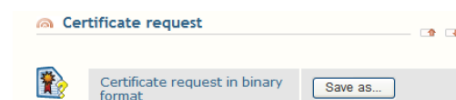
A certificate request in "base 64" format can be edited. It can be copy-pasted, sent by email or entered in an HTML form.

#### 10.3.2 Creating a Request

This operation creates a certificate request for a user key. It is carried out from the Key and certificate page (see [Section 9.1, "Key and Certificate Page"](#)) in the Certificate management tab by clicking the Certificate request link.

When the page is displayed, the request has been generated. You choose the distribution mode for this request.

If the certificate request is in "binary" format, the request may only be recorded in a PKCS#10 file.



If the certificate request is in "base 64" format, you can:

- Copy the request into the clipboard.
- Record the request in a PKCS#10 file.



## 10. MANAGING CERTIFICATES

- Send the request by email. The email address is filled in by default using the address entered in the parameters of the external CA associated to the key (see [Section 5.8.12, “External Certification Authorities”](#)). The email subject is filled in automatically to include the key usage and user name. You have to paste the certificate request, which has been automatically placed on the clipboard, into the body of the message.
- Contact a certification server. The URL is filled in by default using the URL entered in the parameters of the external CA associated to the key. The certificate request is automatically placed on the clipboard.

You must confirm the operation so that Stormshield Data Authority Manager memorizes that a certificate request has been performed and saves the date.

Request processed

You could also choose to submit the request to a remote Stormshield Data Authority Manager server (see [Section 10.3.5, “Submitting a Request to a Remote Stormshield Data Authority Manager Server”](#)). No need to parametrize anything in this page. The request is sent to the remote Stormshield Data Authority Manager server defined in the parameters of the external CA associated to the key. The date is automatically saved.

Confirm operation:

The report page displays the identifier of the certificate request sent back from the remote certification server.

### 10.3.3 Creating Multiple Requests

Several certificate requests may be created in one operation from the main Users lists page (see [Operations Available](#)) in the Certificate management tab.

Multiple creations let you:



- Create PKCS#10 requests recorded in PKCS#10 files. Each request is created in a specific PKCS#10 file. The format of the requests ("Binary" or "base 64") and the destination folder are those defined in the parameters of the external CA associated to the key (see [Section 5.8.12, "External Certification Authorities"](#)).

The name of the file is the user's identifier concatenated with the key role ([Encryption], or [Signature] or [Encryption, Signature]) and a counter that guarantees that the file is unique.

- Create PKCS#10 requests and submit them to a remote Stormshield Data Authority Manager server. The request is sent to the remote Stormshield Data Authority Manager server defined in the parameters of the external CA associated to the key.

For each selected user, the operation is only applied to the key with the encryption role, and/or the key with the signature role.

To create the requests:

1. Select the users for whom you want to create a certificate request. The selections are made by checking the box on the line for each user.
2. Run the creation by clicking the Create request link.
3. In the next page, select the keys for whom you want to create certificate requests. The selection is made with the external CA.
4. Specify if the requests have to be submitted to a remote Stormshield Data Authority Manager server (see [Section 10.3.5, "Submitting a Request to a Remote Stormshield Data Authority Manager Server"](#)) instead of being recorded in the files.

**Certificate requests**

Select the keys for which you wish to make certificate requests:

Keys selection

☐ All keys

☒ Keys with the following certificate authority:

External certification authority

Distribution mode

☒ Create certificate request files

☐ Submit certificate requests to remote Stormshield Data Authority Manager certification server(s)

Confirm operation:

5. After each user has been created, Stormshield Data Authority Manager outputs a report and requests confirmation for the next one:

**Confirm certificate request**

Request processed	Certificate request for encryption key of user Beatrice ARMSTRONG
	Certificate request successfully issued

Do you confirm the certificate request for the signature key of user Benedict LANE?

You can avoid these confirmation requests by clicking the All button.

**Certificate request in progress**

Request processed	Certificate request for signature key of user Bob GREEN
	Request successfull
Request in progress	Certificate request for encryption key of user Bob GREEN

Number of processed requests: 5 / 8

- 6.

When all the requests have been processed, Stormshield Data Authority Manager displays a report page.





## Certificate requests report

Results		
	Report	All requests completed
	Number of requests	8 requests processed
8 requests processed		
User	Roles	File name
» Beatrice ARMSTRONG		barmstrong [Signature].1.p10
» Beatrice ARMSTRONG		barmstrong [Encryption].2.p10
» Benedict LANE		blane [Signature].1.p10
» Benedict LANE		blane [Encryption].3.p10
» Bob GREEN		bgreen [Signature].1.p10
» Bob GREEN		bgreen [Encryption].3.p10
» Brian HOOKER		bhooker [Signature].1.p10
» Brian HOOKER		bhooker [Encryption].3.p10

This page displays the list of keys for which a request has been performed, and also the list of keys the request of which has failed, if any. For each of them, the common name of the user is displayed, and the key role, and the name of the file, or the identifier of the request.

To save the time needed to display the page, the two lists are limited to 100 keys. The complete lists can be downloaded by clicking the icon .

### 10.3.4 Having a Request Signed by a Physical Smart Card

A certificate request is signed by the private key. For a user created from a physical smart card, the private key is only present on the card. The request must therefore be signed by the card.

This can only be carried out from the Key and certificate page (see [Section 9.1, “Key and Certificate Page”](#)) in the Certificate management tab, by clicking the Issue certificate request link.

Stormshield Data Authority Manager requests the card be inserted to create the certificate request: insert the smart card (or token), enter the password and run the request created.

Creation of certificate request using smart card	
	Please insert a card in the reader, enter the PIN code then click on the [Create request] button and not withdraw the card from the reader before the certificate request is complete.
PIN code	<input type="password"/> <input type="button" value="Create request"/>
	DO NOT REMOVE THE CARD. Caution, this operation may take several minutes.
Report	Creation completed

After, Stormshield Data Authority Manager gives the option of using different distribution modes for the request according to its format. These are described in [Section 10.3.2, “Creating a Request”](#).

### 10.3.5 Submitting a Request to a Remote Stormshield Data Authority Manager Server

A certificate request can be automatically submitted to a remote Stormshield Data Authority Manager server. This can be carried out from a single creation request (see [Section 10.3.2, “Creating a Request”](#)) or a multiple creation request (see [Section 10.3.3, “Creating Multiple Requests”](#)).

The request is sent to the remote Stormshield Data Authority Manager server defined the parameters of the external CA associated to the key: URL of the distant server, database identifier, certificate template label.

Doing this:

- Sends the request to the remote server via an HTTP or HTTPS query.
- Adds the request to the list of requests awaiting the certification authority for the database specified on the remote server.



- Displays the request identifier returned by the remote server in the report page. You use this to display the status of the request on the public request status page on the remote server (see [Section 7.4.3, "Displaying the Status of a Certificate Request"](#)) and retrieve the generated certificate once the request has been validated.

Note that an HTTP proxy (see [Section 4.7.2, "Hardware Security Module "](#)) may have to be configured to enable communication.

### 10.3.6 Cancelling Requests

A certificate request can be cancelled. This is carried out internally to Stormshield Data Authority Manager. Cancellation is used to change the status of the request in the database:

- The key has no certificate request in progress.
- The request date is deleted (see [Section 9.1, "Key and Certificate Page "](#)).

Canceling a certificate request can only be carried out from the main Users lists page in the Certificate management tab by clicking the Cancel requests link.

The procedure is similar to creating multiple requests, which was described in [Section 10.3.3, "Creating Multiple Requests "](#).

## 10.4 Renewing Certificates

A use case is available in [Appendix D, Renewing Certificates](#).

### 10.4.1 Renewing one Certificate

The renewal page for a user certificate can be accessed from the Key and certificate page (see [Section 9.1, "Key and Certificate Page "](#)) by clicking the Certificate renewal for key link.

1. In the first section you can configure the certificate to be generated:
  - a. Choose the certificate template to be used from the standard certificate templates (see [Section 5.8.11, "Certificate Templates "](#)).
  - If the database has an internal certified CA, the key is certified by this CA.
  - If not, the key is self-certified, as indicated.

In both cases, the data from the certificate template are used.

- b. The Key role line indicates the role(s) of the future key. They are determined by the X.509 uses of the certificate template, and as such they cannot be modified.
- c. Choose the duration for which the generated certificate is to be valid. The default duration is that of the certificate template selected.

2. If you want to generate a customized certificate in the event that no certificate template is suitable, you must perform the following operations:



- a. Create a request (see [Section 10.3.2, "Creating a Request"](#)).
  - b. Connect using the public access to the certification authority (see [Section 7.2.1, "Public Access Page"](#)).
  - c. Make the request (see [Section 7.4, "Requesting a Certificate"](#)).
  - d. Have it validated by an administrator (see [Section 7.5.2, "Processing a Certificate Request"](#)). The certificate can be customized in more detail during validation.
3. Depending on the general parameters, a second section gives you the option of publishing the certificate that has been generated.
- If an LDAP server is configured (see [Section 5.8.6, "LDAP Configuration"](#)), you can choose to publish the certificate in the LDAP directory. Publication will always take place to the DN of the user for whom the certificate is being renewed.

Configure the operation to be carried out if there are any certificates already present on the LDAP server at the entry designated by the DN:

- keep them.
- delete them.
- replace certificates with the same X.509 uses and issued by this authority.
- If publication by file is configured (see [the section called "Generated Certificates"](#)), this is given as an option. For more information, refer to the certificate publication section (see [Section 7.6.4, "Publishing a Certificate"](#)).

Configuration	Status
LDAP publication	<input checked="" type="checkbox"/> Publish generated certificate in the LDAP directory
Certificates already published on the LDAP server	<input type="radio"/> Keep <input type="radio"/> Delete <input checked="" type="radio"/> Replace certificates that have the same usages and the same issuer
File-based publication	<input checked="" type="checkbox"/> Publish certificate through a file

4. Once the various options have been configured, renew the certificate by clicking the Certify key button.

## 10.4.2 Renewing More than One Certificate

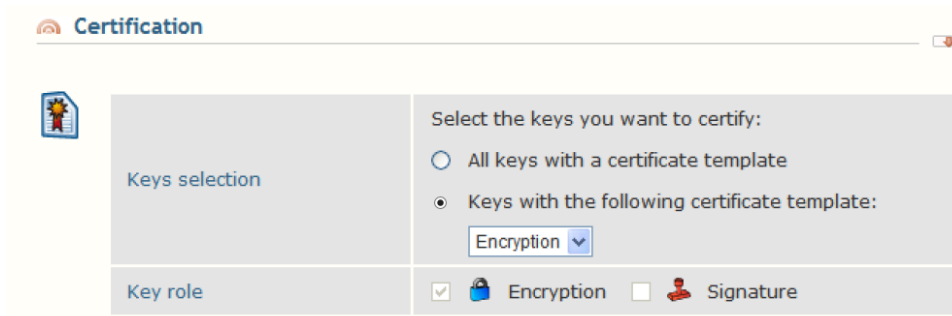
Several certificates may be renewed in one operation from the main Users list page (see [Section 8.4, "Users List Page"](#)).

1. Select the users for whom you want to certify or recertify one or both keys. The selections are made by checking the box on the line for each user concerned.
2. Run the renewal operation by clicking the Certify users link.

For each selected user, the operation applies only to the key with the encryption role and/or to the key with the signature role.

3. Then select the keys to be certified.

The selection has to be performed taking into account the certificate template associated to the key. Consequently, you cannot certify keys that have been created with an external CA (unlike the certificate renewal operation described in the preceding chapter).



The Certification dialog box has a title bar with a red icon and the word "Certification". It contains two main sections: "Keys selection" and "Key role". The "Keys selection" section has a sub-section "Select the keys you want to certify:" with two radio buttons: "All keys with a certificate template" and "Keys with the following certificate template:". The "Keys with the following certificate template:" option is selected, and a dropdown menu shows "Encryption". The "Key role" section has two checkboxes: "Encryption" (checked) and "Signature" (unchecked).

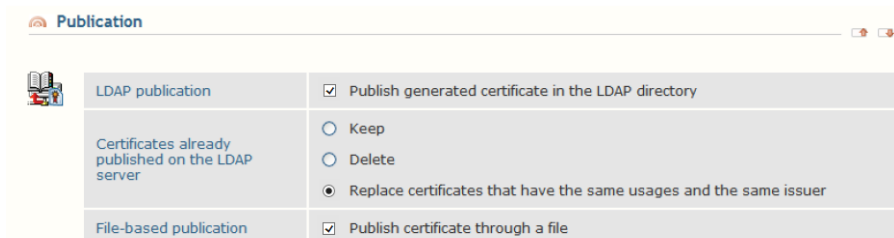
If the database has a certified internal CA, the key is certified by this CA. If not, the key is self-certified, as indicated.

- Depending on the general parameters, a section gives you the option of publishing the certificate(s) generated.

If an LDAP server is configured (see [Section 5.8.6, "LDAP Configuration"](#)), you can choose to publish the certificate in the LDAP directory. Publication will always take place to the DN of the user for whom the certificate(s) is (are) being renewed. Configure the operation to be carried out if there are any certificates already present on the LDAP server at the entry designated by the DN:

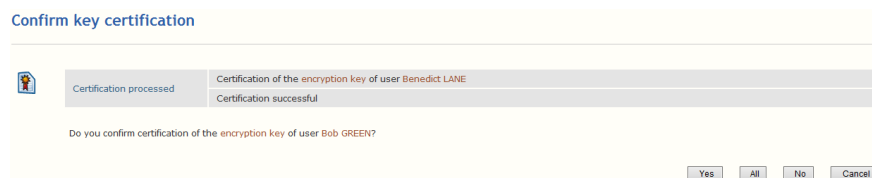
- keep them
- delete them
- replace certificates with the same X.509 uses and issued by this authority

If publication by file is configured (see [the section called "Generated Certificates"](#)), this is given as an option. For more information, refer to the certificate publication section (see [Section 7.6.4, "Publishing a Certificate"](#)).



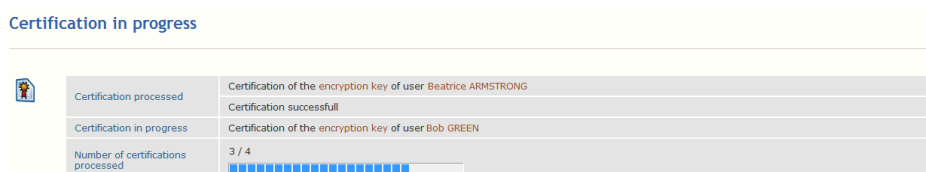
The Publication dialog box has a title bar with a red icon and the word "Publication". It contains two main sections: "LDAP publication" and "File-based publication". The "LDAP publication" section has a checkbox "Publish generated certificate in the LDAP directory" (checked) and a sub-section "Certificates already published on the LDAP server" with three radio buttons: "Keep", "Delete", and "Replace certificates that have the same usages and the same issuer" (selected). The "File-based publication" section has a checkbox "Publish certificate through a file" (checked).

- Stormshield Data Authority Manager then gives you the option of certifying each key. After each certification, a report is displayed and you are asked to confirm the next certification:



The Confirm key certification dialog box has a title bar with a red icon and the word "Confirm key certification". It contains a table with two rows: "Certification processed" and "Certification successful". The "Certification processed" row shows "Certification of the encryption key of user Benedict LANE". The "Certification successful" row shows "Certification successful". Below the table, there is a question: "Do you confirm certification of the encryption key of user Bob GREEN?". At the bottom, there are four buttons: "Yes", "All", "No", and "Cancel".

You can avoid these confirmation requests by clicking the All button:



The Certification in progress dialog box has a title bar with a red icon and the word "Certification in progress". It contains a table with two rows: "Certification in progress" and "Number of certifications processed". The "Certification in progress" row shows "Certification of the encryption key of user Bob GREEN". The "Number of certifications processed" row shows "3 / 4" and a progress bar with 3 out of 4 bars filled.

- When all the keys have been certified, Stormshield Data Authority Manager displays a report page:



#### Key certification report

Results	
Report	All certifications are complete
Number of certifications	4 certifications complete
4 certifications processed	
User	Key certificate roles
Beatrice ARMSTRONG	
Benedict LANE	
Bob GREEN	
Brian HOOKER	

This page displays the list of certified keys, and also the list of keys the certification of which has failed, if any. For each of them, the common name of the user is displayed, and the key role.

To save the time needed to display the page, the two lists are limited to 100 keys. The complete lists can be downloaded by clicking the icon

## 10.5 Importing Certificates

### 10.5.1 Importing Internal Certificates

If the user key has been certified by an external certification authority, for example in order to renew a certificate, the new certificate must be imported.

Stormshield Data Authority Manager keeps a history of old certificates. When the account is distributed, the user's old certificates are inserted so that old data can be decrypted correctly.

For the new certificate to be imported, you will either be given a value in "base 64" format, or a file (with extension .cer for a certificate on its own or extension .p7b or .p7c for a certificate with its parent-child relationship).

#### Attributing Key Roles

During the attribution operation, the key keeps the role(s) it already has, insofar as its new certificate has not lost the corresponding X509 usages.

The rules for importing (see the section [Rules for Importing](#)) allow the import of a certificate that has more X509 usages than the preceding certificate. In this case, the key does not obtain the supplementary role(s) given by the new X509 usages of its new certificate.

The key roles can be modified in the Key properties page (see section [Key Properties Page](#)).

#### Rules for Importing

When you import a certificate, consistency checks must be carried out.

For a certificate to be considered as valid, it must contain at least:

- an object
- an issuer
- a serial number
- validity dates
- X509 uses
- signature and hash mechanisms

Whatever the certificate's usage, the import is rejected in the following cases:



- The public key does not correspond to the current user.
- The certificate has expired, i.e. the validity end date of the certificate has been passed.
- The certificate is too old, i.e. its validity start date is prior to that of the certificate currently in the database. You can remove this rule in the general parameters (see the section [Import, Export and Requests for Certificates](#)).
- The certificate is identical to one already present on the database.
- The format of the certificate is incorrect.
- The certificate does not contain at least one use in common with the previous certificate.
- It lacks an encryption X509 use (KeyEncipherment and/or DataEncipherment) for the certificate associated with the encryption key (or personal key if the account has only one key).
- It lacks a signature X509 use (DigitalSignature and/or NonRepudiation) for the certificate associated with the signature key (or personal key if the account has only one key).

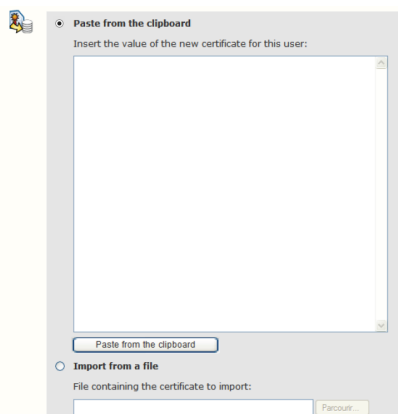
When importing a certificate for a security policy signatory, the certificate must have at least the NonRepudiation X509 use or the DigitalSignature X509 use.

If an authority certificate is being imported, the import is rejected if the certificate does not have the KeyCertSign X.509 attribute.

Importing a certificate which does not have BasicConstraints is possible if it has the X.509 KeyCertSign attribute.

### Importing a Certificate

From the Key and certificate page (see section [Key and Certificate Page](#)), you can import a new certificate for the key by clicking the Import new certificate link in the Certificate management tab.



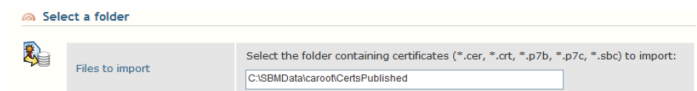
You can paste the value of the certificate ("base 64" format), or select a file.

If the new certificate obeys the consistency rules (see the section [Rules for Importing](#)), its contents are displayed and after a final validation it is imported into the database.

### Importing More than One Certificate

Multiple imports let you process all the users in a database in one operation.

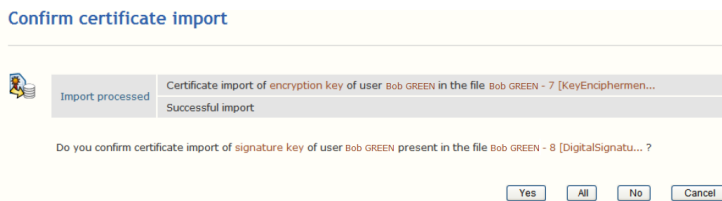
You select a folder; Stormshield Data Authority Manager gives the option of using the default folder <certs\_dir> specified in the general parameters (see the section [Import, Export and Requests for Certificates](#)). All the files in this folder that may contain certificates (i.e. those with extensions cer, .crt, .p7b and .p7c) are analyzed.



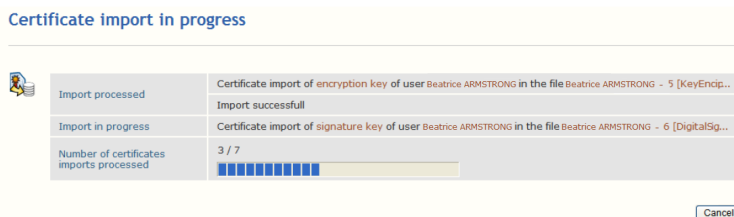
An association test with a database user is carried out for each certificate.

The certificate must obey the consistency rules (see the section [Rules for Importing](#)) and the following rule: if more than one certificate is valid for a given user, the most recent certificate is selected. A certificate is considered more recent than another if its validity start date is later. The date can also be prior to the validity start date of the database certificate if the import of old certificates is allowed (see the section [Import, Export and Requests for Certificates](#)).

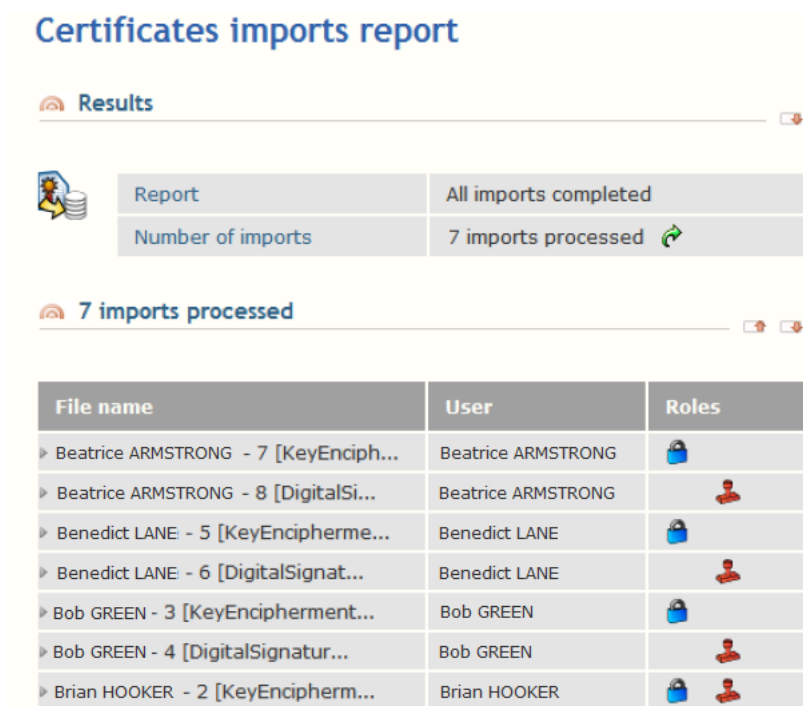
Stormshield Data Authority Manager gives the option of importing every certificate that obeys these rules. For each import, a report page is displayed and confirmation requested for importing the next certificate:



You can avoid these confirmation requests by clicking the All button:



When all the files have been processed, Stormshield Data Authority Manager displays a report page:



This page displays the list of keys for which a certificate has been imported, and also the list of keys the import of which has failed, if any. For each of them, the name of the file containing the



imported certificate is displayed, and the common name of the user that owns the key, and the key role. To save the time needed to display the page, the two lists are limited to 100 keys. The complete lists can be downloaded by clicking the icon

## Importing Certificates from an LDAP Directory

If a user is associated with an LDAP entry (see section [Associating a User with an LDAP Entry](#)), you can import a certificate from the LDAP directory.

### ! IMPORTANT

The certificate must be in binary format.

Define the name of the attribute to be read in the LDAP parameters (see the section [Publishing New Certificates](#)).

Run the import from the main LDAP directory synchronization page (see section [Synchronizing with an LDAP Directory](#)) by clicking either:

- For all users link: for each user associated with an LDAP entry, Stormshield Data Authority Manager looks for the attribute corresponding to the certificate (see the section [Attribute Names](#)). If it finds it, it reads the value of the certificate then runs the import mechanism described in the section [Rules for Importing](#). If the user has more than one key, Stormshield Data Authority Manager tries to import the certificate for each of the keys.
- For self certified users link: for each user associated with an entry for whom at least one of the certificates has not been issued by a certification authority, Stormshield Data Authority Manager looks for the attribute corresponding to the certificate (see the section [Attribute Names](#)). If it finds it, it reads the value of the certificate then runs the import mechanism described in the section [Rules for Importing](#).

The layout and sequence of the pages is the same in both cases.

After each import, Stormshield Data Authority Manager outputs a report and requests confirmation for the next.

**Import confirmation**

Analysis results for users present in the database

Analysis	4 users to import
----------	-------------------

User

	Common name	Michel Aglietta
	Identifier	MAglietta
	DN	CN=Michel Aglietta,OU=Users,DC=My Company,DC=com

Are you sure you want to import the key certificates for this user?

You can avoid these confirmation requests by clicking the All button:





When all the users have been processed, Stormshield Data

### Import confirmation

#### Report of previous operation

User certificates Beatrice ARMSTRONG were imported.

User

Common name	Robert Aumann
Identifier	RAumann
DN	CN=Robert Aumann,OU=Users,DC=My Company,DC=com
Number of users processed	3 / 4

Cancel

Authority Manager displays a report page:

Import report

Results

4 users to import 3 users successfully imported 1 user failed

3 users successfully imported

User	DN
» Michel Aglietta	CN=Michel Aglietta,OU=Users,DC=My Company,DC=com
» Beatrice ARMSTRONG	CN=Beatrice ARMSTRONG,OU=Users,DC=My Company,DC=com
» Robert Aumann	CN=Robert Aumann,OU=Users,DC=My Company,DC=com

1 user failed

User	DN	Report
» Daniel Bernoulli	CN=Daniel Bernoulli,OU=Users,DC=...	Encryption key : identical ... Encryption key : identical certificate - Signature key : identical certificate

This page displays the list of users for whom at least one certificate has been imported, and possibly the list of users for whom the importation has failed. To limit the page time display, these two lists are limited to 100 users. The complete lists can be downloaded by clicking [📄](#).

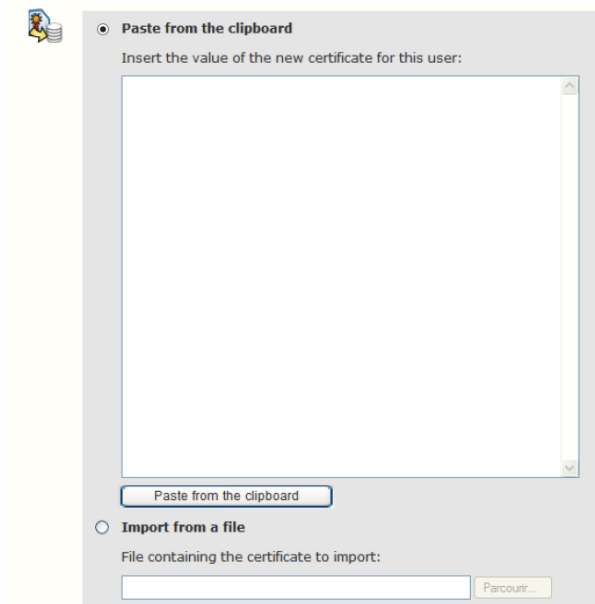
## 10.5.2 Importing External Certificates

The Import new certificate link is present in the external certificate pages (see [Section 10.1.1, "External Recovery Certificates"](#) and [Section 10.1.2, "Other External Certificates"](#)). Clicking this link displays a page that lets you import a new external certificate into the database:

- either by copy-pasting its base 64 coded value
- or by selecting a file containing a single certificate (.cer or .crt files)

When you confirm the import, a page is displayed which details the contents of the certificate and enables you to enter the properties to be associated with the certificate when it is imported into the database:

- a label to identify the certificate
- the recovery parameters for a recovery certificate



## 10.6 Exporting Certificates

### 10.6.1 Exporting Internal Certificates

Stormshield Data Authority Manager can export a certification authority key certificate (see [Section 7.3.1, "Authority Certificate and Key Page"](#)) and user key certificates (see [Section 9.1, "Key and Certificate Page"](#) and [Section 8.4.2, "Searching for Users"](#)).

Export files have the following extensions:

- .cer: a single certificate in binary format
- .crt: a single certificate in base 64 format
- p7b or p7c (Stormshield Data Security Certificates): multiple certificates in binary format

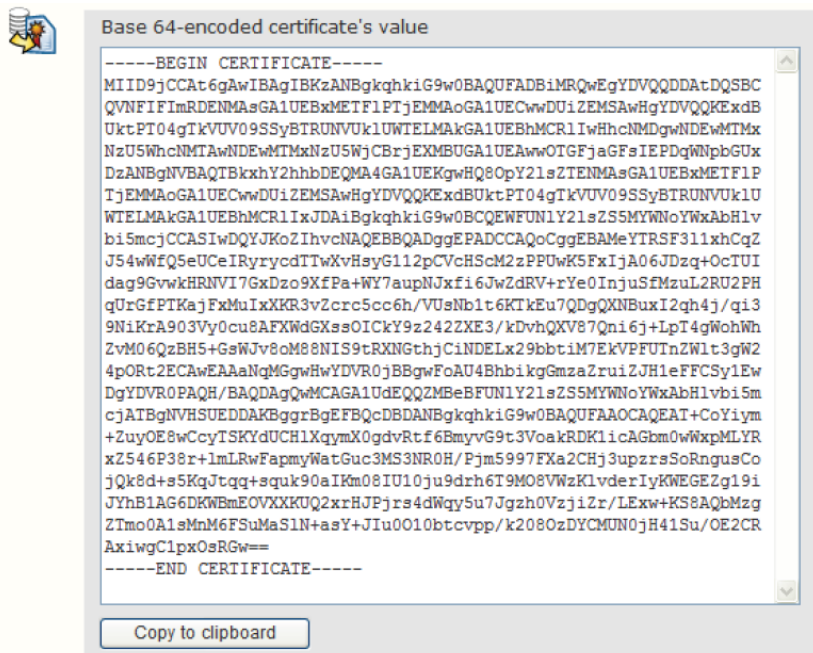
#### Exporting a Certificate

A single export is carried out from the Export certificate section of the following pages:

- Key and certificate for the authority (see [Section 7.3.1, "Authority Certificate and Key Page"](#)) for a certification authority key certificate
- Key and certificate (see [Section 9.1, "Key and Certificate Page"](#)) for a user key certificate

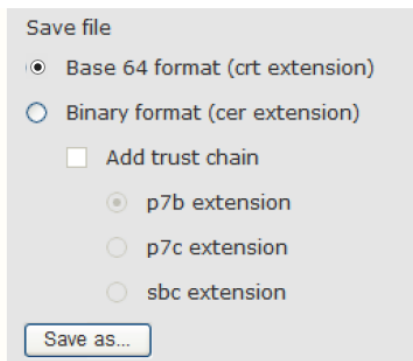
You can display or hide the contents of the sections by clicking the Base 64-encoded certificate's value or Save file links.

The Base 64- encoded certificate's value shows the certificate's "base 64" value which you can copy.



The Save file link saves the value of the certificate in a file. Specify the format, whether the parent-child relationship is to be added and the extension. The configuration defined in the general parameters (see [the section called “Import, Export and Requests for Certificates”](#)) is used by default.

The Add trust chain checkbox is disabled if no parent-child relationship is found for the key in the database.



The name of the file is the user's identifier concatenated with the key role ([Encryption], or [Signature] or [Encryption, Signature]).

## Exporting More than One Certificate


Several certificates may be exported in one operation from the main Users lists page (see [Section 8.4.1, “Operations Available”](#)):

1. Select the users to whom you want to export certificates. The selections are made by checking the box on the line for each user.
2. Run certificate export by clicking the Export certificates link in the Certificate management tab.
3. In the next page, select the keys whose certificates you want to export.
4. Define the contents of the files to be generated. Several combinations are possible:



- one file for each certificate (default choice), with or without parent-child relationship
  - one file for each user, with or without certificate parent-child relationship
  - one file containing all the certificates of all users with or without their parent-child relationship
5. Choose whether or not to delete existing files.
  6. Select the prefix used to name generated files: identifier, common name or email address. The prefix is used only if one file is created for each certificate with or without parent-child relationship and if the key usages exactly match the [KeyEncipherment,DataEncipherment], [DigitalSignature,NonRepudiation] or [DigitalSignature] usages.

**Certificates export**



Certificates selection

Select the certificates you want to export:

- ☒ Certificates associated with encryption keys
- ☒ Certificates associated with signature keys

Contents of generated files

☐ Include all user's certificates in the same file  
☐ Include all users' certificates in the same file  
☐ Add trust chain  
☐ Overwrite existing files

Name of generated files

Prefix Identifier

**Confirm operation:** Export certificates

To guarantee that the file is unique:

- In the case where a file is created for each certificate (first case in step 4 above), the name of the file is the selected prefix concatenated with the key usages defined in step 6 or concatenated with the key role ([Encryption], or [Signature] or [Encryption, Signature]) if usages are different.
- In one of the two other cases in step 4, the name of the file is the user's identifier concatenated with the key role and the certificate serial number.









When all the files have been generated, Stormshield Data Authority Manager displays a report page.

**Certificates export report**

**Results**

Report	All exports complete
Number of exports	8 exports processed

**8 exports processed**

User	Roles	File name
» Beatrice ARMSTRONG		barmstrong [KeyEncipherment,DataEncipherment].crt
» Beatrice ARMSTRONG		barmstrong [DigitalSignature,NonRepudiation].crt
» Benedict LANE		blane [KeyEncipherment,DataEncipherment].crt
» Benedict LANE		blane [DigitalSignature,NonRepudiation].crt
» Bob GREEN		bgreen [KeyEncipherment,DataEncipherment].crt
» Bob GREEN		bgreen [DigitalSignature,NonRepudiation].crt
» Brian HOOKER		bhooker [KeyEncipherment,DataEncipherment].crt
» Brian HOOKER		bhooker [DigitalSignature,NonRepudiation].crt

This page displays the list of keys for which a certificate has been exported, and also the list of keys the export of which has failed, if any.

For each of them, the common name of the user that owns the key is displayed, and the key role, and the name of the created file.



To save the time needed to display the page, the two lists are limited to 100 keys. The complete lists can be downloaded by clicking the icon

## 10.7 Publishing Certificates in an LDAP Directory

If a user is associated with an LDAP entry (see [Section 8.13, “Associating a User with an LDAP Entry”](#)), you can publish their certificate in the LDAP directory.

1. Define the name of the attribute to be written in the LDAP parameters (see [the section called “Publishing New Certificates”](#)).

The date of last publication for the certificates is displayed in the User page (see [Section 8.8, “Users Page”](#)).

2. Run publication from the main LDAP directory synchronization page (see [Section 8.12, “Synchronizing with an LDAP Directory”](#)) by clicking either:
  - The All certificates link: for each certificate for a user associated with a particular entry, Stormshield Data Authority Manager writes an attribute containing the certificate value into that entry.
  - The Certificates which are not yet published link: for each certificate for a user associated with a particular entry whose certificates have not yet been published, Stormshield Data Authority Manager writes an attribute containing the certificate value into that entry.

The layout and sequence of the pages is the same in both cases.

3. After each publication, Stormshield Data Authority Manager outputs a report and requests confirmation for the next.

**Confirm publication**

Analysis results for users present in the database

	Analysis	3 users to publish
--	----------	--------------------

User to publish

	Common name	Robert Aumann
	Identifier	RAumann
	DN	CN=Robert Aumann,OU=Users,DC=My Company,DC=com

Do you confirm the user certificates publication ?

4. You can avoid these confirmation requests by clicking the All button:

**Confirm publication**

Report of previous operation

User certificates Bob GREEN were published.

User to publish

	Common name	Michel Aglietta
	Identifier	MAglietta
	DN	CN=Michel Aglietta,OU=Users,DC=My Company,DC=com
	Number of users processed	2 / 5

When all the users have been processed, Stormshield Data Authority Manager displays a report page:



**Publication report**

**Results**

3 users to publish    3 users published

**3 users published**

User	DN
» Michel Aglietta	CN=Michel Aglietta,OU=Users,DC=My Company,DC=com
» Robert Aumann	CN=Robert Aumann,OU=Users,DC=My Company,DC=com
» Bob GREEN	CN=Bob GREEN,OU=Users,DC=My Company,DC=com

This page displays the list of users for whom at least one certificate has been published, and possibly the list of users for whom the publishing has failed. To limit the page time display, these two lists are limited to 100 users. The complete lists can be downloaded by clicking .



# 11. Configuring Stormshield Data Authority Manager Components

This chapter describes how to configure Stormshield Data Security components when using Stormshield Data Authority Manager.

## 11.1 Description

Stormshield Data Authority Manager enables users to configure each component in Stormshield Data Security. You can:

- Configure each component as if from the Stormshield Data Security configuration panel (checkboxes, drop-down lists, lists, etc.).
- Configure parameters which restrict the operation of the components.
- Impose this configuration on the user by limiting their choices or prohibiting access to controls, buttons, etc.

The default configurations given by Stormshield Data Authority Manager are the same as those given by default by the Stormshield Data Security components. They contain no user restrictions.

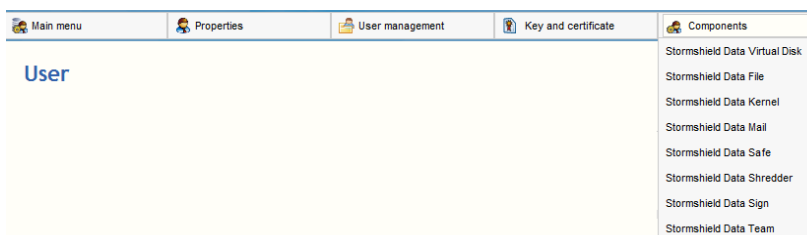
Changes made to configurations only take effect when the user account is distributed.

You can change component configurations after a distribution using an update file (see [Section 8.9.2, "Security Policy Update File \(.usx\) "](#)).

## 11.2 Accessing Users' Configurations

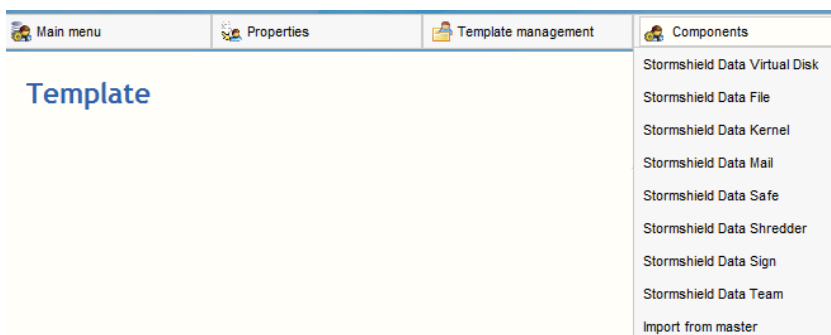
You access users' component configurations from the User page (see section [Users Page](#)). The user's configuration is either:

- individual (personalized configuration)



Each link displays the main page for configuring a component (see section [Configuring a Component](#)).

- or inherited from a template (see section [Template](#)):





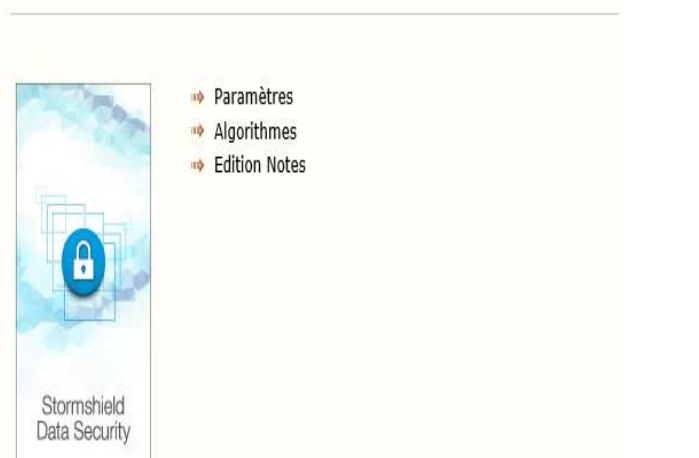
The template identifier, which the user inherits, is displayed as a link in the Template line of the User section. Clicking this link displays the Template page for the template and thus gives access to the component configurations.

To change the template, refer to section [Choosing a Template](#).

### 11.3 Configuring a Component

Stormshield Data Authority Manager displays a main page for each component that contains a menu.

#### Stormshield Data Mail - Configurateur

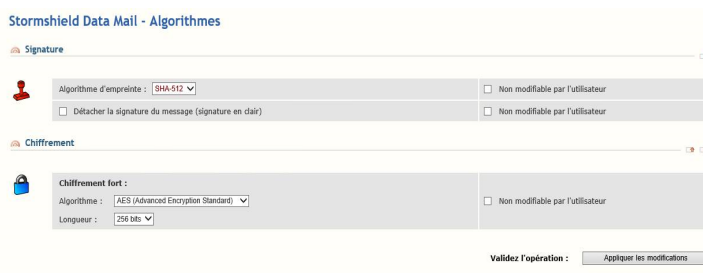


For Stormshield Data Virtual Disk, Stormshield Data File, Stormshield Data Mail, Stormshield Data Shredder and Stormshield Data Sign components, the first link, called Stormshield Data Security Settings, is used to configure the general settings which restrict how the component operates. These settings cannot be accessed from the Stormshield Data Security configuration panel.

The other links correspond to a tab in the component configuration window, which can be accessed from the Stormshield Data Security configuration panel.

Thus each page corresponding to a tab contains:

- A left-hand column giving the same configurable parameters as those shown in the Stormshield Data Security configuration window. For explanations on these parameters, you must refer to the manual for the component.
- A right-hand column containing the user's restrictions (see [Section 11.4, "Imposing a Configuration on a User"](#)). The text in this column is in black.







## 11.4 Imposing a Configuration on a User

The component parameter configuration pages contain a right-hand column that allows you to restrict user access to tabs, buttons, drop-down menus and controls (checkboxes, etc.).

### 11.4.1 Description of Main Restrictions



Each restriction applies to the control(s) situated opposite in the left-hand column:


<input type="checkbox"/> Cannot be modified by the user	The control will be visible in the configuration window but will be grayed out, which means not accessible, so non-modifiable.
<input type="checkbox"/> Not visible	The button or menu choice will be grayed out, so not accessible to the user.
<input type="checkbox"/> Element not visible	The element selected in the list will not be shown in the list given to the user.
<input type="checkbox"/> The user is not allowed to add items	The component will not give the user the option of adding an element to the list.
<input type="checkbox"/> The user is not allowed to modify the selected item	The user will not be able to change the properties of this element of the list.
<input type="checkbox"/> Not visible	The tab will not be shown in the configuration window.

### 11.4.2 Limiting the List of Proposed Algorithms

For Stormshield Data Virtual Disk, Stormshield Data File and Stormshield Data Mail components, you can hide algorithms so they are not given as options to the user.

Each algorithm is defined by its name and its strength. It is represented by a ball associating a row and a column:

- A green checkbox  indicates the algorithm will be accessible.
- A red cross  indicates the algorithm will not be accessible.

Clicking the checkbox changes the status of the algorithm. You can change a complete row or column using the  button.

The default algorithm given to the user must be accessible, so associated with a green ball.



Algorithms that may be selected by the user:

		40 bits	64 bits	128 bits	192 bits	256 bits
		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AES	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Triple DES	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RC5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RC4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RC2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Standard DES	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			

## 11.5 Advanced configuration

### 11.5.1 Stormshield Data Kernel Parameters

#### Configuring the Security Policies Download Component

The distribution points entered in the component's configuration can contain the following tags:

- an LDAP point must be a valid URI LDAP, in which you can include the `<LdapHost>`, `<LdapPort>`, `<LdapDn>`, `<UserId>` tags;
- an HTTP distribution point must be a valid URI, in which you can include the `<UserId>` tag.

Examples of URI:

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

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

During the distribution, the tags are replaced by:

- the corresponding LDAP parameter (see section [LDAP Configuration](#));
- LDAP DN of the user or the distributed template;
- the user or distributed template identifier.

These replacements are carried out according to the following rules:

#### 1. For a template:

- during the distribution of a `.usr` master file (that is to say with a password mode connection configuration or a card mode connection configuration, section [Distributing a Master](#)), and during the distribution of a `.usx` update file (see section [Distributing a Security Policy Update File \(.usx\)](#)), the tags are replaced with the data of the distributed template;
- during the distribution of a `.msr` master file (that is to say with all the configurations, see section [Distributing a Master](#)), the tags are not replaced, for the distribution points to be kept during their importation in the new template (see section [Importing Component Configurations from a Master \(.msr file\)](#)).



2. For a user, whether the configurations of the components derive from a template or not, the tags are always replaced by the data of the distributed user (see section [Distributing User Accounts](#)).

Resolution masks for distribution points can be entered in the general parameters in order to be automatically proposed in the component configuration page (see section [Component Configuration Parameters](#)).

### Configuring the User Account

Four "Secret code and connection" configurations are available:

- two for "password" mode, one for version 5 and below and one for version 6 and above of Stormshield Data Security;
- two for "card" mode, one for version 5 and below and one for version 6 and above of Stormshield Data Security.

A standard user cannot have two connection modes or a variable number of keys. There is therefore no point in filling out pages that do not correspond to their profile. For the connection mode used, fill in the page corresponding to the Stormshield Data Security version installed on the user's workstation.

A template can be applied to users requiring these different profiles. You therefore need to enter all these configurations for a given template.

Configuration distribution is described in the section [Distributing User Accounts](#).

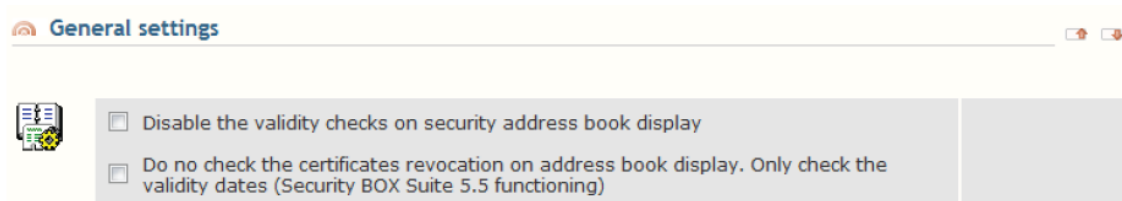
### Creating the Secret Code

The syntax you define in the Personal code syntax section on the Connection and personal code page comes into effect when a password is changed.

### Configuring the directory

In the Address book page, section General settings, you can operate the following settings:

- Do not operate validity checks while opening the security address book. By default, the checks are activated.
- Do not control the certificates revocation while displaying the address book in order to speed up the address book. This means that only the validity dates are controlled (Security BOX Suite 5.5 functioning). By default, the dates and revocation are controlled.



### Configuring the automatic update of the address book

In the **Address book** page, section **Automatic update of the address book**, the following parameters can be configured:

Activation and execution:

- Activate the address book automatic update (disabled by default) by indicating how frequently processes will be run (in hours).



- Launch the address book update treatment on Stormshield Data Security users connection. Stormshield Data Security Updates are not launched by default when users connect.
- Allow manual execution of update operations (prohibited by default). This parameter is applied only if the **Update the address book** feature is enabled.

Automatic replacement of certificates:

- Activate the local address book update with more recent certificates in an LDAP directory (disabled by default).

This parameter is applied only if the **Update the address book** and **Automatic replacement** features are enabled. The replacement works only when the certificate is valid.

- Indicate whether valid, expired and/or revoked certificates will be replaced.
- Indicate whether you wish to import missing certificates. This configuration is used only when an e-mail is sent via Outlook.
- You can filter the certificate-issuing authorities to which automatic replacement applies, by replacing the **All** keyword (by default) with the list of CommonNames of authorities that issued the certificates in question (separated by semicolons).

When manually searching for a user to send an e-mail via Outlook, the address book will only be updated if the authority is known; the filter will be ignored. Stormshield Data Authority Manager

**i NOTE**

The automatic update of the local address book relies only on the e-mail address included in the user certificates to match the LDAP directory.

Automatic deletion of expired certificates:

- Activate the automatic deletion of expired certificates (disabled by default). This parameter is applied only if the **Update the address book** feature is enabled.
- You can filter the certificate-issuing authorities involved when certificates are automatically removed on their expiry date, by replacing the **All** keyword (by default) with the list of CommonNames of authorities that issued the certificates in question (separated by semicolons).

This parameter is only taken into account if the **Update the address book** and **Automatic deletion** features are activated.

Automatic deletion of revoked certificates:

- Activate the automatic deletion of revoked certificates (disabled by default). This parameter is applied only if the **Update the address book** feature is enabled.
- You can filter the certificate-issuing authorities involved when certificates are automatically removed when they are revoked, by replacing the **All** keyword (by default) with the list of CommonNames of authorities that issued the certificates in question (separated by semicolons).

This parameter is only taken into account if the **Update the address book** and **Automatic deletion** on revocation features are activated.



## 11.5.2 Stormshield Data Team Parameters

### Restriction parameter

In the Security rules page, in the List of folders to secure panel, the Restriction parameter allows you to define the way the rule is displayed in the list of rules of the Security rules tab of the Stormshield Data Team component, in the user's properties.

### Update a co-worker key in the known Team rules after a key renewal (requires the LDAP synchronization to be activated) parameter

In the Parameters page, in the General parameters panel, the Update a co-worker key in the known Team rules after a key renewal (requires the LDAP synchronization to be activated) parameter allows to automatically update keys in the Team rules. The synchronization of the trusted address book with an LDAP directory must be activated (refer to [Section 8.12, "Synchronizing with an LDAP Directory"](#)).

If this option is activated, the Team rules are automatically updated after the synchronization of the trusted address book. A new icon displays in the notification zone to indicate the start of the processing. Double-click the icon to display the update progress window.

The processing includes two steps:

1. The rules of which the user is the owner are updated with the new certificates taken from the address book. The icon in the notification zone indicates the end of this step. The progress window lists all the rules impacted by this update.
2. The new security policy is applied on all updated rules. This step must be performed manually by the user.

Open the progress window by double-clicking the icon in the notification zone and then click Apply. This action triggers the update of the security of the folders whose rule has been modified and the transciphering of the folder files (according to the policy defined about transciphering in the user account).

### Stormshield Data Security behaviour according to file dates when performing encryption/decryption operations parameter

In the Parameters page, in the General parameters panel, the Stormshield Data Security behaviour according to file dates when performing encryption/decryption operations parameter gives three actions possible on the files creation, modification and last access dates which can be selected together. If no option is selected, dates remain unchanged when encryption/decryption operations are performed.

During files synchronization for a mobile device, Windows uses the files modification date to find out if the files need to be synchronized. By default, Stormshield Data Team keeps the files modification date when their security has changed (first encryption, adding a new user, decryption). In this case, file previously synchronized are not synchronized in their new state. This parameter allows to guarantee the files synchronization for a mobile device.

### Access parameters to encrypted file if the certificate is revoked

In the Parameters page, in the General parameters panel, the following options combinations allow to configure two modes of access to encrypted files if the certificate of the encryption key is revoked:

- Default mode:



☐ If the CRL cannot be downloaded and the certificate is in the local cache, use the state of the local certificate.

Opening an encrypted file not allowed if encryption key is revoked:

- ☒ The user can access the encrypted files even if the certificate of the encryption key is revoked
- ☐ The user cannot access the encrypted files if the certificate of the encryption key is revoked
- ☐ The user cannot access encrypted files if it is not possible to assert he/she has not been revoked (for example if the trust chain is not complete or if the CRL is expired or unavailable)

This mode enables the user to access the encrypted files even if the certificate of the encryption key is revoked.

- Secured mode:

☒ If the CRL cannot be downloaded and the certificate is in the local cache, use the state of the local certificate.

Opening an encrypted file not allowed if encryption key is revoked:

- ☐ The user can access the encrypted files even if the certificate of the encryption key is revoked
- ☐ The user cannot access the encrypted files if the certificate of the encryption key is revoked
- ☒ The user cannot access encrypted files if it is not possible to assert he/she has not been revoked (for example if the trust chain is not complete or if the CRL is expired or unavailable)

This mode enables the user to access the encrypted files if the CRL is available online (forced download) and if the certificate of the encryption key is not revoked.

#### **i** NOTE

This verification can take some time, in particular when network time-outs are at stake if the CRL cannot be downloaded (for example if the host server cannot be accessed) or if the CRL becomes voluminous.

### Automatic update of the Team rules

If you want Team rules to be automatically updated, the address book automatic update must be enabled (by LDAP synchronization). To do so:

1. In the template Kernel settings, select the following options:

**Automatically updating the address book**

**Activation and execution:**

- ☒ Activate the address book automatic update
- Treatment activation frequency:  hours
- ☒ Launch the address book update treatment on Security BOX users connection
- ☒ Allow manual execution of update operations

**Automatic replacement from an LDAP directory:**

- ☒ Activate the local address book replacement with more recent certificates found in an LDAP directory
- ☒ Execute the treatment on **valid** certificates
- ☒ Execute the treatment on **expired** certificates
- ☒ Execute the treatment on **revoked** certificates

2. In the template Team settings, enable the rules automatic update:

Stormshield Data Security Authority Manager

CA COMPANY Main administrator Close session

Home > Users management > Users > Recovery > Stormshield Data Team > Settings

Main menu

☐ When deleting one or several co-workers of a rule, do not transcipher the files.

☒ Update a co-worker key in the known Team rules after a key renewal.  
Note: this option requires the directory automatic update to be enabled (via LDAP synchronization).



### 11.5.3 Stormshield Data File settings

#### Building file lists

You must build the exclusion list [.efp], decryption list [.dec] and encryption list [.enc] using Stormshield Data File, then select them in the corresponding pages.

#### Choice of file format

By default, files encrypted by SDS are in SBOX format. If you want to change the file format (SDSX), select it in the **Encryption/decryption** section of the **Stormshield Data File settings** page.

#### Prohibition to encrypt (or decrypt) files

In the **Encryption/decryption** section of the **Stormshield Data File Settings** page, you can prohibit the encryption or decryption of any file and/or any folder.

#### Encrypting/decrypting network files

In the **Network files** section of the **Advanced** page, you can allow the user to encrypt or decrypt the files which are on the network.

Network files	
<input checked="" type="checkbox"/> Allow network files encryption	<input type="checkbox"/> Cannot be modified by the user
<input type="checkbox"/> Allow network files decryption	<input type="checkbox"/> Cannot be modified by the user

### 11.5.4 Stormshield Data Shredder Parameters

#### Building File Lists

You must build the list of files to protect [.cfp] and the list of files to delete [.cln] using Stormshield Data Shredder, then select them in the corresponding pages.

#### Prohibition to Shred

In the Encryption/decryption section of the Stormshield Data Shredder Settings page, you can prohibit the shredding of any file and/or any folder.

### 11.5.5 Stormshield Data Mail Outlook Edition settings

Users can send their encryption certificates to their coworkers by sending them a signed e-mail. Recipients can then import the encryption certificate into their trusted address books to update it.

This update procedure only applies if the recipient was able to verify the signature of the e-mail received.

To prevent the user from making changes to this configuration, select the checkbox **Cannot be modified by the user**.

#### Manual update

There are three options:





- **None:** the user will not be prompted to update the trusted address book.
- **Only for a trusted authority:** the user will only be prompted to import the issuer's certificate if it was issued by an authority with a certificate already in the recipient's address book.
- **For all authorities:** the user will be prompted to import the issuer's certificate even if it was issued by an authority with a certificate that does not appears in the recipient's address book.  
For this option, the import of user certificates and authority certificates must be allowed in **Stormshield Data Kernel > Address book > General settings**.

User intervention is required in this mode. When users receive a signed e-mail with encryption certificates that are not in the trusted address book, they must import the certificates by clicking on the link given at the bottom of the e-mail.

#### Automatic update

There are two options:

- **None:** the address book will not be updated.
- **Only for a trusted authority:** the issuer's encryption certificate will be imported only if it was issued by an authority with a certificate already in the recipient's trusted address book.

No user intervention is required in this mode.

### 11.5.6 Configuring e-mail templates

To change the appearance of e-mails sent from Stormshield Data Authority Manager, you can modify the e-mail template files created in the \MailTemplates folder when Stormshield Data Authority Manager was installed.

The following files can be modified in any text editor:

- template\_expiration\_mail
- template\_request
- template\_user\_account
- template\_user\_account\_mail\_link
- template\_validation\_external\_admin
- template\_validation\_external\_user
- template\_validation\_internal\_admin
- template\_validation\_internal\_user

Change the HTML code between the <HTML> and </HTML> tags to adapt the appearance of e-mails.

All the variables in these files included between the flags #D and #F must not be deleted or modified.





## 12. Customizing the Installation

This chapter describes how to customize Stormshield Data Security installation in two different ways:

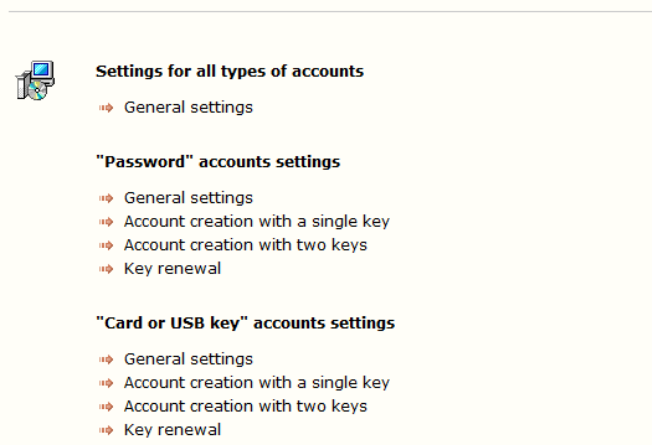
- You can modify the configuration held in the files *sbox.ini* and *cardchoice.ini*, which are specific to the workstation on which Stormshield Data Security is installed. Thus the customization applies to all users who connect to Stormshield Data Security on this workstation.
- Or you can modify the Stormshield Data Security installation procedure, to create a new Stormshield Data Security 10.0.X.msi installation file.

From Stormshield Data Authority Manager, you can customize the installation file of the same version or of a previous version still supported of Stormshield Data Security. The contrary is not possible.

### 12.1 Description

The Stormshield Data Security installation may be customized from the homepage or from the Main menu by clicking the Set up customization link.

#### Customize Stormshield Data Security Suite setup



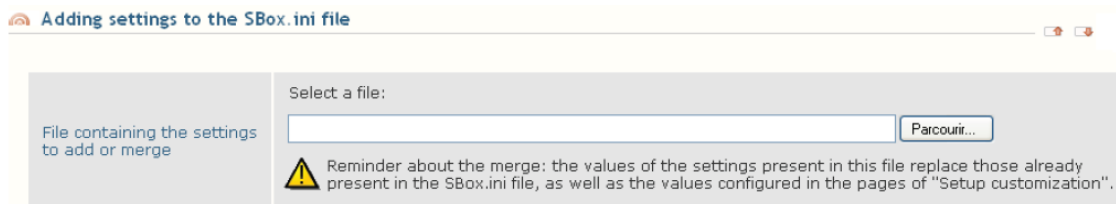
Customizing allows you to:

- Configure part of the Stormshield Data Security operation on the user workstation (connection, account creation, key renewal, see [Configuring Stormshield Data Security Operation](#)).
- Configure the Stormshield Data Security installation procedure (see [Configuring the Stormshield Data Security Installation Procedure](#)).

It modifies:

- The *SDS\_Suite\_10.0.xxx.msi* file which contains the installation procedure.
- The *sbox.ini* and *cardchoice.ini* files which configure Stormshield Data Security.

It is also possible to add or merge other parameters that are not managed by the customization pages of the installation. To do so, go to General settings > Adding settings to the Sbox.ini files:



The added settings are only taken into account during the generation of the customized .msi file.

## 12.2 Configuring Stormshield Data Security Operation

There are two ways of configuring Stormshield Data Security which complement each other:

- Component configuration, which is carried out from the User page (see [Section 11.1, "Description"](#)). This configuration is specific to the user account (default configuration, restrictions). These Stormshield Data Security component configurations are stored in the account file [.usr] of the user account during distribution.
- The configuration described in this chapter. This configuration is held in files *sbox.ini* and *cardchoice.ini* specific to the workstation on which Stormshield Data Security is installed. Thus it applies to all users who connect to Stormshield Data Security on this workstation.

So two users who connect to Stormshield Data Security on the same workstation have a personal configuration from their user account and a common configuration provided by the *sbox.ini* and *cardchoice.ini* files.

Customizing the installation allows you to configure:

- elements relating to user connections
- creation rules for accounts with one or two keys
- key renewal rules
- various other user-independent parameters

The changes made are only applied after a new installation procedure is generated (see [Configuring the Stormshield Data Security Installation Procedure](#)).

The following sections only describe the parameters that require additional information regarding the content of HTML pages. Configuring the parameters in the *sbox.ini* file is described in detail in the *Administration Guide*.

### 12.2.1 Using a master to create an account

You can define a master for each following creating account creation:

- Password account with 1 key
- Password account with 2 keys
- Card account with 1 key
- Car account with 2 keys

A master is composed of

1. A template, selected from those in the database.

#### NOTE

Using a template to create an account implies that the password for the template has to be



entered. The process of creating an account tries to open the template with a blank password and if this blank password is refused, a screen is displayed asking the user for the right password. This means that one password attempt is used up systematically. Using a template with a blank password avoids the need to enter a password.

During the product installation, the *sbox.ini* file is automatically updated: the MasterPath parameter is filled in the section corresponding to the impacted account creation.

When a master is defined, any user created inherits the following information from the template:

- Stormshield Data Security component configurations
  - visible recovery keys
  - lists for Stormshield Data File and Stormshield Data Shredder
2. A file containing certificates to be added to the directory of accounts created (PKCS#7 format).

During the product installation, the *sbox.ini* file is automatically updated: the DirectoryModel and DirModelsfolder parameters are filled in the section corresponding to the impacted account creation.

During the user creation, the directory is automatically filled with the certificates contained in this file.

## 12.2.2 Parameters for Password Accounts

### Configuring the Entry of a Password

The rules to be applied to passwords defined on this page apply when an account is created. They are distinct from those defined in the Stormshield Data Kernel configuration (see [the section called "Creating the Secret Code"](#)), which apply when a password is changed.

They do not apply to the security officer password.

When the Do not display the security officer password entry window option is checked (Miscellaneous section), a security officer password is generated at random. Since it is not disclosed, it cannot be used to unlock the user account.

## 12.2.3 Parameters for Smart Card or USB Token Accounts

### Defining the Type of Smart Card or USB Token Used

The smart card extension or USB token to be used is defined in the general parameters for smart card or USB token accounts.

You can:

- Select an *.ini* file which contains the configuration for one or more smart card extensions (this might be the Stormshield Data Security *cardchoice.ini* present on your workstation). Then select the smart card extension you want to use from the drop-down list.



When the installation procedure is generated, the content of the *.ini* file is merged with the content of the *cardchoice.ini* file located in the *SDS Suite 9.1.xxx.msi* file used (see section [Configuring the Stormshield Data Security Installation Procedure](#)).

- Choose to use a smart card extension that is not present in the *.ini* file selected. It can be defined and configured on the page. It will be written into the *cardchoice.ini* file when the installation procedure is generated.

## Defining the automatic creation of a card account

You can define the automatic creation from **Setup customization > "Card or USB token" accounts parameters > General settings**.

It is activated when the **Allow automatic account creation** checkbox is selected and one of the four options above is selected.

### Stormshield Data Security Suite: "card or USB key" accounts

Activating the automatic creation of a card account automatically checks some parameters on the other pages of the setup customization:

- **Creation authorization and Reduced usages** on the page **"Card or USB token" Account creation with a single key** ;
- **Creation authorization** on the page **"Card or USB token" Account creation with two keys**.

These parameters cannot be modified as long as the automatic creation of a card account is activated.



### Sorting out authorities for card account automatic creation

If the account automatic creation is enabled, it is possible to sort out certificates according to the certification authority name which provided the certificates.

According to the account type (single-key, key pair), the related fields are available to enter the name of the certification authority(ies).

Certificates delivered by other authorities than the ones specified on this page will not be used for card/token account creation.



### Filter smart card readers

If several smart card readers are connected to a workstation, a filter can be configured to allow communication with only a specific smart card reader without displaying other readers.

Select the checkbox **If several readers are connected to the workstation, apply only the next reader** and indicate a description and vendor for the reader.

Special characters "\*" and "?" can be used with the filter to obtain more results.

## 12.3 Configuring the Stormshield Data Security Installation Procedure

Configure the Stormshield Data Security installation procedure in the Generating setup procedure page. This page can be accessed from the Operations menu by clicking the Generate setup procedure link.

Create a procedure that contains:

- a license number to avoid the user having to enter it
- the list of components to be selected by default when the installation procedure runs
- an installation folder, if you want to install Stormshield Data Security in a folder other than the default one

Enter

- a complete name for *SDS Suite 10.0.xxx.msi* source file which can be accessed by the server hosting Stormshield Data Authority Manager. This complete name must be written "as the server will interpret it". It can contain spaces in the file name but not in the path and must not exceed 256 characters. For example:

**C:\SBMData\<base\_id>\SDS\_Suite\_10.0.xxx.msi**

- an existing target folder situated on this server (do not select a folder which is shared on your network). It must be written "as the server will interpret it". For example:

**C:\SBMData\<base\_id>\MSITarget**

The generation process creates a new *SDS\_Suite\_10.0.xxx.msi* file in the target folder.



## Appendix A. Deployment methodology

This appendix identifies the procedure for installing Stormshield Data Authority Manager, and it lists the most commonly used features in the best order for performing them.

This appendix is designed to help you quickly become familiar with this user guide.

It is not exhaustive and does not go into details about the features. It references the relevant sections where the administrator can find all of the information necessary to make architectural decisions.

### A.1. Server

On the server, perform the following operations:

1. Install Stormshield Data Authority Manager (see [Section 4.2, "Installing and Configuring Web IIS Server"](#)) or update Stormshield Data Authority Manager version 6 (see [Section 5.5, "Updating versions of Security BOX higher to 6.x"](#)).
2. Configure the server (see [Section A.1, "Configuring an IIS Web Server"](#)).
3. Update the WebServer section of the Manager.ini file (see [Section 4.7.1, "Web Server"](#)).
4. Set the network user rights (see [Section A.2.2, "Assigning the NTFS Rights Required for the Network User"](#)) for:
  - The *bases.ini* file
  - The *manager.exe* file
  - The *c:\sbmdata* folder
  - The *c:\Windows\Temp* folder
5. Set the DCOM rights (see [Section A.3, "Assigning DCOM Rights for the Stormshield Data Authority Manager Service"](#)).
6. Create the database (see [Section 5.2, "Creating a Database"](#)) or start up (see [Section 5.4, "Starting and Stopping a Database"](#)) and update (see [Section 5.5.4, "Running the Database Update Tool"](#)) a previous version of the database.

### A.2. Client

On the client workstation, use the Internet Explorer browser to perform the following operations:

1. Add the server to the list of trusted sites and lighten the restrictions concerning ActiveX for trusted sites (see [Section 4.6, "Configuring the Administrator Workstation"](#)).
2. Go to Stormshield Data Authority Manager (see [Section 4.5, "URL Access to Server"](#)).

In Stormshield Data Authority Manager:

1. Initialize the database (see [Section 5.3, "Initializing a Database"](#)).
2. Create the database administrators (see section [Defining Administrators and Their Roles](#)).
3. Create the external certification authorities (see [Section 5.8.12, "External Certification Authorities"](#)).
4. Create the certificate templates (see [Section 5.8.11, "Certificate Templates"](#)).
5. Have the database certification authority certified (see [Section 7.3, "Managing the Certification Authority Key"](#)): request a certificate (see [Section 7.3.2, "Making a Certificate Request"](#)) and import the certificate (see [Section 7.3.3, "Importing a New certificate"](#)).



6. Import the certificates related to the database certification authority into the external certificates (see [Section 10.1.2, "Other External Certificates"](#)).
7. Configure the synchronization with the LDAP server (see [Section 5.8.6, "LDAP Configuration"](#)).
8. In the general user settings, enable:
  - the publication of security updates (see [the section called "Publication of Security Policy Updates"](#), [Appendix E, Publishing and Downloading Security Updates Using an LDAP Directory](#)).
  - the publication of installation files (see [the section called "Publication of Installation Files"](#)).
9. In the general settings, assign the certification authority (see [the section called "Certificate Revocation Lists \(CRLs\)"](#), [Appendix G, Publishing and Downloading CRLs Using an LDAP Directory](#)):
  - the CRL distribution point in which CRLs generated by the certification authority will be published. This distribution point will be included in all of the certificates generated by the certification authority.
  - the publication DN to run the CRL publication feature.
  - the publication by file of generated certificates (see [the section called "Generated Certificates"](#)).
10. Configure the SMTP server (see [Section 5.8.7, "Outgoing Mail Server"](#)).
11. Create the templates (see [Section 8.1.1, "Template"](#) and [Section 8.3.1, "Creating a User Template"](#)).
12. For each template, configure the components with the distribution points for security updates (see [Appendix E, Publishing and Downloading Security Updates Using an LDAP Directory](#)).
13. Create the security policy signatory account (see [Section 8.1.3, "Security Policy Signatory"](#) and [Section 8.7, "Creating a Security Policies Signatory"](#)).
14. Set up the recovery:
  - Create the recovery account(s) (see [Section 8.1.2, "Recovery Account"](#) and [Section 8.6, "Creating a Recovery Account"](#)).
  - And/or import the external recovery certificate(s) (see [Section 10.1.1, "External Recovery Certificates"](#)).
15. Create the users from the templates: from a file (see [Section 8.5.3, "Creating a Large Number of Users from a File"](#)), from an LDAP directory (see [Section 8.5.7, "Creating a User from an LDAP Directory"](#)), etc.
16. Publish a CRL (see [Section 7.7.2, "Generating a Revocation List"](#)).
17. Distribute the users by creating installation files and sending by email either the files or the download links to the published files (see [Section 8.9, "Distributing User Accounts"](#)).





## Appendix B. Configuring Windows Server

To configure the server:

1. Configure the Web server.
2. Enable Stormshield Data Authority Manager to access the network (this step only impacts you if Stormshield Data Authority Manager is to access the files stored on a network resource).
3. Assign DCOM rights to the network user for Stormshield Data Authority Manager service.

### B.1. Configuring an IIS Web Server

#### B.1.1. Declaring CGI

1. Click **Start > Control panel > Administrative Tools**, then open the **Internet Information Services (IIS) Manager**.
2. In the tree, select the server name.
3. On the home page, double-click **ISAPI and CGI Restrictions**.
4. Click **Add** at the top right of the page.
5. Select the `<sdam_install_dir>\Bin\Manager.exe` file and place it between " " if it contains spaces.
6. Enter Stormshield Data Authority Manager as a description.
7. Check **Allow extension path to execute** and then validate.

#### B.1.2. Adding Website

1. Right-click **Sites**, then **Add web site**.
2. In the wizard, enter a site name (for example Stormshield Data Authority Manager).
3. Select the Stormshield Data Authority Manager installation folder `<sdam_install_dir>`.
4. Enter a new `<port>` value for the port.

#### NOTE

You must control the configuration of the firewall present on the server. It is possibly required to add an incoming traffic rule dedicated to the control of connections to the specific local TCP port `<port>`.

To configure assigned ports (for example the secured port 443 for https protocol), refer to [Section J.1, "Activating HTTPS protocol on Stormshield Data Authority Manager"](#).

#### B.1.3. Defining authorizations for Web site

1. In the tree, go to the Stormshield Data Authority Manager site.
2. Double-click **Handler Mappings**.
3. Click the link **Edit Feature Permissions....**
4. Uncheck all boxes and validate.



5. Select the **ActiveX** folder, right-click **Handler Mappings**.
6. In the right column, click the link **Edit Feature Permissions....**
7. Select **Read** and validate.
8. Enter the **Htdocs** folder and double-click **Handler Mappings**.
9. In the right column, click the link **Edit Feature Permissions....**
10. Select **Read** and validate.
11. Select the **Bin** folder, right-click **Handler Mappings**.
12. In the right column, click the link **Edit Feature Permissions....**
13. Select **Read, Script** and **Execute**, then validate.
14. Restart the Web site.

#### B.1.4. Configuring *manager.ini* file

Configure your *manager.ini* (see section [Web Server](#)) file so that the web page links are compatible with the IIS configuration. For the configuration example given above, the values to enter in the [WebServer] section are:

```
ManagerRootUrl = http://<hostname>/bin/manager.exe  
ManagerDocUrl = /
```

Where <hostname> is the name of the machine hosting the server or <IP address>:<port>.

### B.2. Giving Stormshield Data Authority Manager Access to the Network

This section only applies if you need to access files stored on a networked resource.

If this is the case:

1. Choose or create an NT user for this purpose with access rights to the network resources. This user is referred to as the network user.

If you use a IIS server, the network user is the Internet Guest Account (IUSR\_<machine\_name> for IIS6 and IUSR for IIS 7.0) that hosts the web server.

If necessary, to create the network user, in the Windows **Start** menu, select **Administrative Tools, Computer Management, Local Users, Users**, then right-click and select **New User**.

2. Configure your web server to use the network user (see [Configuring IIS Web Server](#) for IIS).
3. Give the network user sufficient NTFS rights on the folders used by Stormshield Data Authority Manager (see section [Assigning the NTFS Rights Required for the Network User](#)).
4. Give the network user the DCOM right to invoke the Stormshield Data Authority Manager service (see section [Assigning DCOM Rights for the Stormshield Data Authority Manager Service](#)).

**i NOTE**

Use UNC (Universal Naming Convention) syntax when describing network resources in Stormshield Data Authority Manager: `\\machine\folder\file` is a valid path, but `Z:\folder\file` is not.

**i NOTE**

If you are using SGBD Microsoft Access, the database created must not be a network resource.

### B.2.1. Configuring IIS Web Server

Configure an IIS Web server as follows:

1. From the **Internet Information Services (IIS) Manager**, browse to the **Bin** folder from Stormshield Data Authority Manager Web site.
2. Double-click **Authentication**.
3. Select **Anonymous Authentication** from the list.
4. From the right column, click **Edit...**
5. Select **Specific user**, click **Set...**, then enter **IUSR** without password. These are the values by default.
6. Validate twice clicking **OK**.

### B.2.2. Assigning the NTFS Rights Required for the Network User

The network user must have:

- execution rights to the file: `<sdam_install_dir>\Bin\Manager.exe`
- change rights on the file: `<sdam_install_dir>\bases.ini`
- change rights on the Stormshield Data Authority Manager default directory: `<sdam_data_install_dir>\SBMData` and its subdirectories
- change rights on the temporary directory for the machine, by default `C:\WINDOWS\TEMP`

**i NOTE**

The network user must also be allowed to modify the temporary folder from Stormshield Data Authority Manager. By default, it is the folder defined by the TempPath parameter in the [Path] section of the *manager.ini* configuration file (see section [Temporary Files Folder](#)). The installation gives the `<sdam_data_install_dir>\SBMData\tmp` value. If you decide to modify this value to work on another folder, give the modification right on the used folder.

To do so:

1. In the Windows **Start** menu, select **Run**, then enter explorer.
2. Go to the `<sdam_install_dir>` folder.
3. Right-click the *bases.ini* file, select **Properties**, and then the *Security* tab.
4. Click **[Modify]** then **Add**, enter the name of the network user, and validate.
5. Give the modification right to the network user, and then validate.
6. Go to the `<sdam_install_dir>\Bin` folder.
7. Right-click the *Manager.exe* folder, select **Properties**, and then the *Security* tab.
8. Click **[Modify]** then **Add**, enter the name of the network user, and validate.



9. Give only read and execute rights to the network user, and then validate.
10. Go to the <sdam\_data\_install\_dir> folder.
11. Right-click the **SBMData** folder, select **Properties**, and then the *Security* tab.
12. Click **Add**, enter the network user name, and validate.
13. Allow the modification right to the network user, and validate.
  - Click **Advanced** and select the *Permissions* tab.
  - Click Edit permissions....
  - Click Replace all existing inheritable permissions [ ... ] and validate.
14. Go to the **C:\WINDOWS** folder.
15. Right-click the **Temp** folder, select **Properties**, and then the *Security* tab.
16. Click **[Modify]** then **Add**, enter the name of the network user, and validate.
17. Give the modification right to the network user, and then validate.

### B.3. Assigning DCOM Rights for the Stormshield Data Authority Manager Service

The Stormshield Data Authority Manager service is implemented in the form of COM components. It must be able to be invoked by the Windows user under which the Web server is running.

You must explicitly grant the right to invoke Stormshield Data Authority Manager to this user in the following situations:

- The product accesses network resources. You have defined a "network user" for the account under which the Web server is running (see section [Giving Stormshield Data Authority Manager Access to the Network](#)).
- You are using an IIS server. The Web server runs under the Internet Guest Account, which is IUSR~ <machine\_name>.

To do so:

1. From the Windows **Start** menu, select **Run**, then enter **dcomcnfg**.
2. From the tree structure, choose **Component Services, Computers, My Computer, DCOM Config**.
3. Right-click **Stormshield Data Authority Manager Service**, then select **Properties**.
4. From the *Security* tab, select **Customize** in the **Launch and Activation Permissions** zone, then click **Edit....**
5. Click **Add** and enter the network user and validate.
6. Select **Local Launch, Remote Launch, Local Activation** and **Remote Activation** in the **Authorize** section.
7. Validate twice with **OK**.



## Appendix C. Migrating from Microsoft Access to Microsoft SQL Server

Using Microsoft tools, it is possible to import the content of a Microsoft Access database into a Microsoft SQL Server database.

### C.1. Presentation

This appendix describes the importation of a Microsoft Access database into a Microsoft SQL Server database with the use of the SQL Server Import and Export Wizard tool included in Microsoft SQL Server 2005 product.

If the `<base_id_source>.sba` source Microsoft Access database is a database previous to version 10.1, it must be updated beforehand (see [Section 5.5.4, "Running the Database Update Tool "](#)). If it is a previous version, its content can be imported into the destination database with Stormshield Data Authority Manager tool (see [Section 5.5.4, "Running the Database Update Tool "](#)).

The following Microsoft SQL Server components have been installed:

- Database Services
- Analysis Services
- Integration Services
- Client components

The authentication mode is: identifier sa, password `<Authentication_logon_password>`.

### C.2. Procedure

#### C.2.1. Creating the SQL Server Destination Database

1. Open **SQL Server Management Studio**.
2. In the server tree, right-click the **Databases** folder, then select **New Database ...**.
3. In **Database name**, enter the `<base_name>` database name, then validate with **OK**. The database is created.
4. Right-click the created database and select **New Query**. In the right part of the window, copy-paste the content of the `create_database_sqlServer_for_import.sql` file included in the folder.
5. From the toolbar, select **Execute**. The database is populated.

#### C.2.2. Importing the Access Source Database Data

1. Still in SQL Server Management Studio, from the trees databases, right-click the newly created `<base_name>` database, select **Tasks**, then **Import Data ...**. The **SQL Server Import and Export Wizard** wizard is launched.
2. From **Data source**, select **Microsoft Access**.
3. From **File name**, select the `<base_id_source>.sba` Access source database to import, leave **User name** and **Password** empty, then validate.



4. Select the SQL Server authentication mode, enter `sa` in the **User name** and the `<Authentication_logon_password>` password in **Password**, check the selected database in **Database** is `<base_name>`, then validate.
5. Validate the following page and leave the **Copy data from one or more tables or views** selection.
6. Select all the tables by clicking the checkbox next to **Source** and uncheck the line of the COUNTERS table if any, then validate.
7. Validate the following page and leave the **Execute immediately** selection.
8. Launch the execution.
9. Once the treatment is finished, you can close the **SQL Server Import and Export Wizard**, then **SQL Server Management Studio**.

### C.2.3. Declaring the SQL Server database in Stormshield Data Authority Manager

#### On the same machine

If the previous version of Stormshield Data Authority Manager was updated with version 10.1 on the same machine, the installation and data folders were kept.

1. Edit the `bases.ini` file present in Stormshield Data Authority Manager `<sdam_install_dir>` installation folder.
2. From the `<base_id_source>` database section, replace the value of `ConnectionString` data by the following connection chain:

```
Provider=SQLOLEDB;Data Source=<server name>;DataBase=<databasename>;
User Id=<user ID>;Password=<password>
```

where

<code>&lt;servername&gt;</code>	is the server name (visible in <b>Control Panel, System, Computer Name</b> tab) ;
<code>&lt;database name&gt;</code>	is the <code>&lt;base_name&gt;</code> SQL Server database name ;
<code>&lt;user ID&gt;</code>	is the <code>sa</code> connection identifier ;
<code>&lt;password&gt;</code>	is the <code>&lt;Authentication_logon_password&gt;</code> connection password.

3. Save the file.

The database can be restarted.

#### On a new machine

If Stormshield Data Authority Manager version 10.1 was installed on a new machine:

1. Click **Start, All Programs, Stormshield Data Authority Manager**, then **Create a new database**.
2. From the wizard, enter the source database `<base_id_source>` identifier to create the link with the `<base_id_source>.mng` keystore file. You can enter a label different from the source database label but you will then need to modify the label modified in the database in order to match them. (see [the section called "Database label"](#)).
3. In the following page, enter the Microsoft SQL Server database type.
4. Enter the server name (visible in **Control Panel, System, Computer Name** tab), the `<base_name>` SQL Server database name, the `sa` identifier name and the `<Authentication_logon_password>` connection password by unselecting the password request.



5. Test the connection. If the connection is launched, execute the last pages of the wizard to end the database declaration.
6. Copy the `<base_id_source>.mng` keystore file in the `<sdam_data_install_dir>/SBMData/Databases` folder previously associated to the Access source database and now associated to the new SQL server database.
7. Creating the tree:
  - If you do not want to keep the former database tree, create in the `<sdam_data_install_dir>/SBMData` folder, the tree described in [Section 5.3.8, "Directory Structure Created during Initialization"](#) by using `<base_id_source>` as the database identifier. It is highly recommended to duplicate an existing tree, by emptying all the folders except the `MailTemplates` folder.
  - If you want to keep the former database tree, copy this tree in the `<sdam_data_install_dir>/SBMData/<base_id_source>` folder.

The database can be restarted.

The database can be restarted but an update of the paths included in the general parameters may be necessary to take into account the new location of the `<sdam_data_install_dir>` data folder (refer to the general settings defined in [Section 5.8.3, "Database properties"](#), [Section 5.8.8, "User Management"](#), [Section 5.8.10, "Certificate Management Parameters"](#) and [Section 5.8.12, "External Certification Authorities"](#)).



## Appendix D. Renewing Certificates

This appendix describes the use of Stormshield Data Authority Manager features to renew a user certificate, with a “card” account or a “password” account. It describes the steps from the generation of the new certificate to the importation in the user account.

### D.1. Activating Email Notification

The email notification to the requester during the validation of an internal request must be activated in the certificates management parameters (see [the section called “Email Notifications”](#)).

### D.2. Renewing the Certificate

In Stormshield Data Authority Manager, you can renew a user certificate:

- with one certificate from the **Key and certificate** page of the user (see [Section 10.4.1, “Renewing one Certificate”](#));
- with several certificates from the **Users list** (see [Section 10.4.2, “Renewing More than One Certificate”](#)).

The new certificate is generated by the database certification authority. A notification email is sent to the address included in the certificate subject.

### D.3. Importing the new Certificate in the User Account

The user receives a notification email that contains a link requesting him/her to access the public page of the PKI introducing the generated certificate.

This page displays several backup features of the certificate, notably its copy in Stormshield Data Security if it is displayed with Internet Explorer (see [Section 7.6.3, “Displaying a Certificate”](#)).

If using this function, the user launches the importation wizard for the Stormshield Data Security certificate that imports the certificate in the account. It is also imported in the card if it is a “card” account.





## Appendix E. Publishing and Downloading Security Updates Using an LDAP Directory

Stormshield Data Authority Manager allows security policy updates to be published in an LDAP directory. It also allows the “Automatic Update” component to be configured so that Stormshield Data Security downloads the published updates.

### E.1. Publishing Updates

Whether it is for a user ([Section 8.7, “Creating a Security Policies Signatory”](#)) or for a template ([Section 8.3.7, “Creating a Template by Duplicating an Existing Template”](#)), an update can be published in the LDAP directory when the update is released if:

- an LDAP server is configured ([Section 5.8.6, “LDAP Configuration”](#)).
- the option is checked in the general settings ([the section called “Publication of Security Policy Updates”](#)).

The LDAP entry DN `<LDAP_entry_DN>`, in which the update is published, represents:

- for a user: the entry DN associated with the user ([the section called “LDAP Server”](#), [Section 5.8.9, “Component Configuration Parameters”](#), [Section 8.13, “Associating a User with an LDAP Entry”](#)).
- for a template: the DN that was specifically input for this operation ([Section 8.3.1, “Creating a User Template”](#)).

### E.2. Configuring the LDAP Directory

The LDAP must support the `<security_policies_upgrade_attribute>` attribute, which is specific to Stormshield Data Security products. In Stormshield Data Authority Manager, it is defined in the LDAP server settings (see [the section called “Attribute Names”](#)). Its default value is `sboxPolicyUpgrade;binary`.

The LDAP entry in which the update is published must derive from a class supporting the `<security_policies_upgrade_attribute>` attribute. Ideally, a new `sboxPerson` class would be created, which derives from `inetOrgPerson` and supports the `<security_policies_upgrade_attribute>` attribute. Example of the `sboxperson.schema` file:

```
# This file can be used to support Security BOX
# security policies upgrade.
#
# Requires files: core.schema, cosine.schema, inetorgperson.schema,

# sboxPolicyUpgrade
# Must be transferred using ;binary
attributetype ( 1.2.250.1.63.1.6.1.2.3
NAME 'sboxPolicyUpgrade'
DESC 'Security BOX security policies upgrade'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )

# sboxPerson
Objectclass ( 1.2.250.1.63.1.6.1.1
NAME 'sboxPerson'
DESC 'Security BOX User'
SUP inetOrgPerson
STRUCTURAL
```



```
MAY ( sbboxPolicyUpgrade )  
)
```

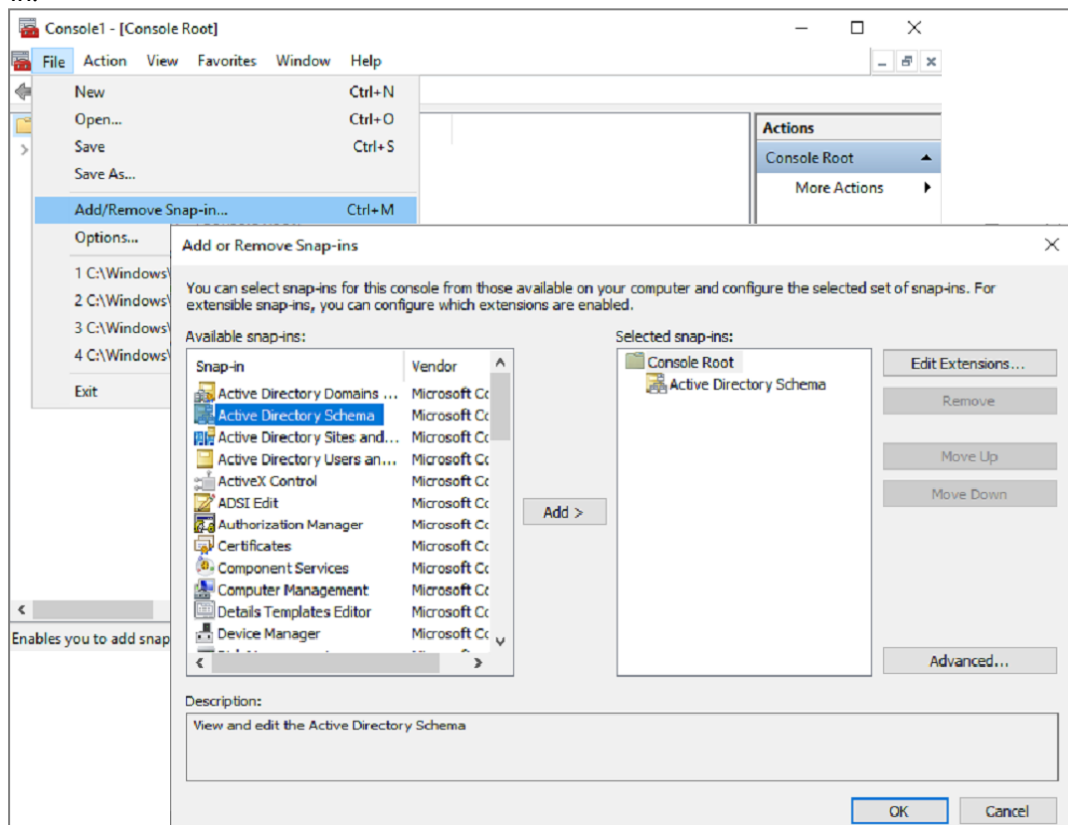
The LDAP entry must derive from this class.

In an existing directory, if it is not possible to make the existing entry derive from a new class; it is always possible to update an existing class.

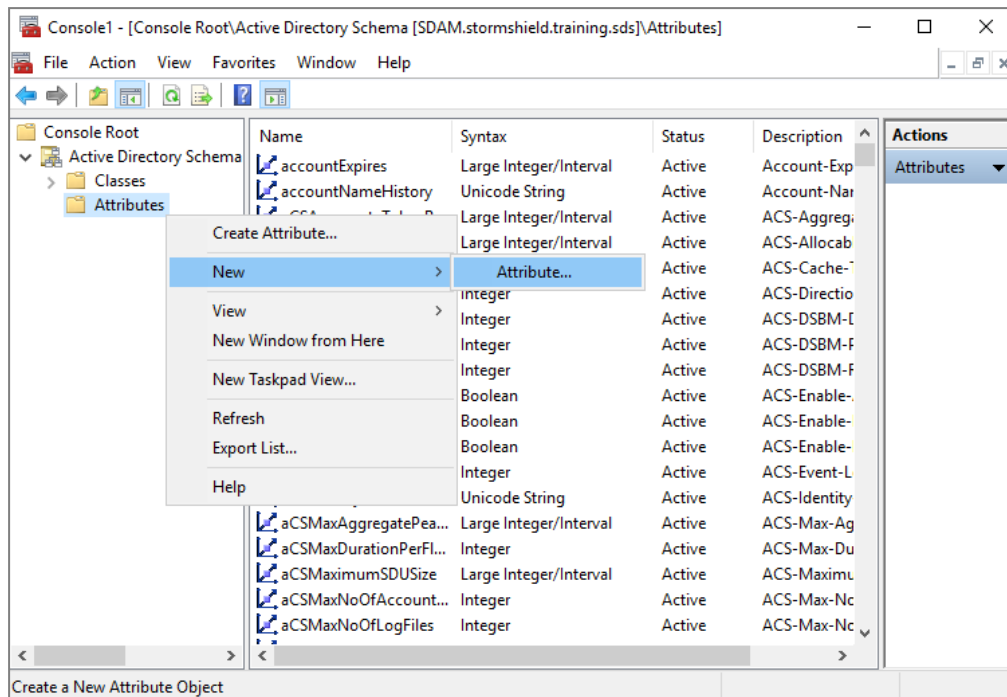
In compliance with the RFC 2252 standard, if the syntax defined in the schema ends with .8 (Certificate type syntax), “;binary” must appear at the end of the attribute name in its definition in Stormshield Data Authority Manager and in the distribution point. If the syntax ends with .5 (Binary type syntax), “;binary” must not be present.

#### Example of adding `sbboxPolicyUpgrade` attribute to `inetOrgPerson` class on Active Directory

1. On the Active Directory, execute MMC.exe in order to add the **Active Directory Schema** snap-in.



2. In the **Active Directory Schema** folder, add a new attribute.



3. Fill in the fields and click **OK**.

### ! IMPORTANT

Creating an attribute is definitive, you cannot delete an attribute. Make sure you fill in the fields properly.

Create a New Attribute Object

Identification

Common Name:

LDAP Display Name:

Unique X500 Object ID:

Description:

Syntax and Range

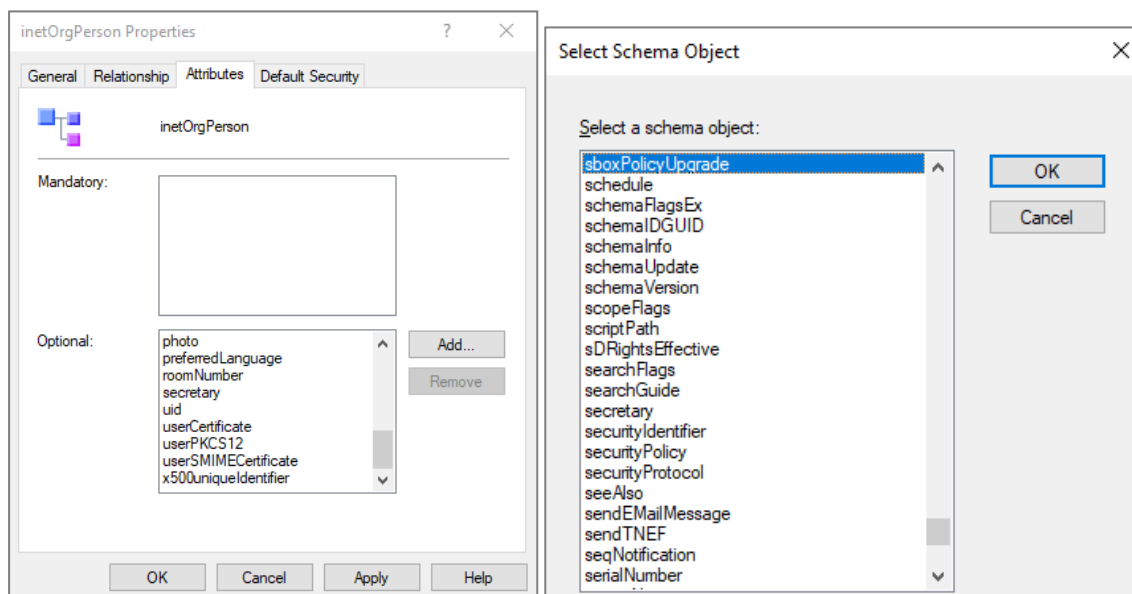
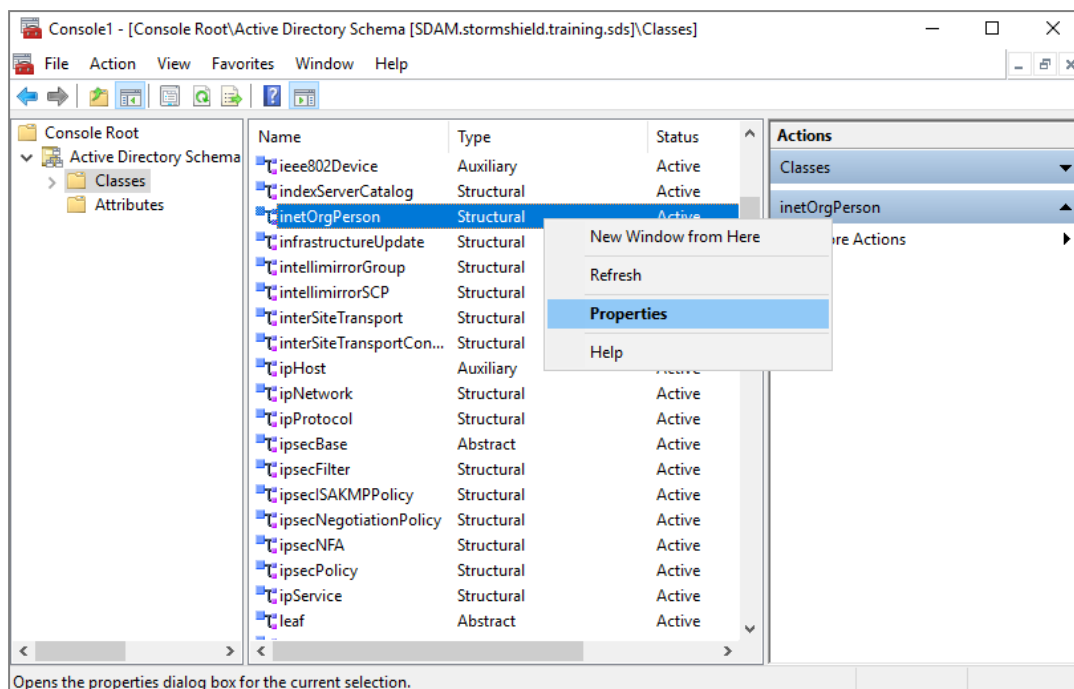
Syntax:

Minimum:

Maximum:

☐ Multi-Valued

4. Add the newly created attribute to the `inetOrgPerson` class.



### E.3. Downloading Updates

The **Automatic Update** component must be configured to automatically download available security policy updates when logging in.

In Stormshield Data Authority Manager, the configuration page for this component is available from the configuration page for the Kernel component by clicking the **Downloading Security Policies** link.

You must add the following distribution point:

```
ldap://<LDAP_server_name>:<LDAP_port>/<LDAP_entry_DN>?<security_policies_upgrade_attribute>
```

Where:



<LDAP_server_name>	is the LDAP server name (see <a href="#">the section called “LDAP Server”</a> ).
<LDAP_port>	is the port (see <a href="#">the section called “LDAP Server”</a> ).
<LDAP_entry_DN>	is the LDAP entry DN (defined above).
<security_policies_upgrade_attribute>	is the name of the attribute published to (defined above).



## Appendix F. Publishing and Downloading Security Updates using the Web Server

Stormshield Data Authority Manager enables to publish security policies updates in a folder. It also enables to configure the “Automatic update component” so that Stormshield Data Security downloads the published updates.

### F.1. Publishing Updates

For a user (see [Section 8.9, “Distributing User Accounts ”](#)) or a template, the publication of an update by a file can be carried out when you distribute it, if the option is activated in the general parameters (see [the section called “Publication of Security Policy Updates ”](#)).

The `<USX_publication_dir>` folder in which the updates files are copied, is defined in the general parameters.

### F.2. Configuring the IIS Web Server

A file server has to be configured in order to allow the download of files published in the `<USX_publication_dir>` folder.

1. From **Internet Information Services (IIS) Manager**, unroll the server tree and then the **Sites** one.
2. Right-click the web site created for Stormshield Data Authority Manager; then select **Add Virtual Directory...**
3. In the wizard, enter an alias `<USX_publication_alias>`, preferably without a space; then select the physical access path to the `<USX_publication_dir>` folder. Validate by clicking **OK**.
4. Go to the newly created virtual directory, then double-click **Handler Mappings**.
5. From the right column, click the **Edit Feature Permissions...** link.
6. Select **Read**, then validate.
7. Double-click **MIME Types**.
8. From the right column, click the **Add...** link, then enter `"usx"` in **File name extension** and `"application/octet-stream"` in **MIME Type**. Validate by clicking **OK**.

### F.3. Downloading Updates

The **Automatic update** component must be configured for automatic download when connecting for security policies updates. In Stormshield Data Authority Manager, the component configuration page is available from the Kernel component configuration page, by clicking the **Download security policies** link.

The following distribution point must be added:

```
http://<hostname>/<USX_publication_alias>/<UserId>.usx
```

where



<code>&lt;hostname&gt;</code>	is either the name of the machine hosting the server, or <code>&lt;IPaddress&gt;:&lt;port&gt;</code> by using the access port to the Web site created for Stormshield Data Authority Manager.
<code>&lt;USX_publication_alias&gt;</code>	is the virtual directory alias (defined above).
<code>&lt;UserId&gt;</code>	is the user identifier.



## Appendix G. Publishing and Downloading CRLs

Stormshield Data Authority Manager allows CRLs to be published in an LDAP directory and/or on a Web server. We recommend you to set up distribution points on both types of server.

It also allows the Revocation Controller component to be configured so that Stormshield Data Security downloads the published CRLs.

The two following steps are required to define the CRLs distribution points:

1. Configuring the LDAP directory and the IIS Web server,
2. Specify the distribution points in Stormshield Data Authority Manager.

### ! IMPORTANT

We recommend you to generate users certificates after you defined the CRLs distribution points.

## G.1. Configuring the LDAP directory and the IIS Web server

### G.1.1. LDAP directory

The CRL attribute `certificateRevocationList` is standard: it is supported by the `cRLDistributionPoint` class (RFC 4523).

```
( 2.5.4.39 NAME 'certificateRevocationList'
  DESC 'X.509 certificate revocation list'
  EQUALITY certificateListExactMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

( 2.5.6.19 NAME 'cRLDistributionPoint'
  DESC 'X.509 CRL distribution point'
  SUP top STRUCTURAL
  MUST cn
  MAY ( certificateRevocationList $
    authorityRevocationList $ deltaRevocationList ) )
```

The LDAP entry in which the CRL is published must therefore derive from this class.

As indicated in the standard, `;binary` must appear at the end of the attribute name in its definition in Stormshield Data Authority Manager and in the distribution point.

### Active Directory

Add first the object `organizationalUnit` in the Active Directory schema in order to store the CRL in an organizational unit (the procedure to add the Active Directory schema software component is provided in the appendix [Publishing and Downloading Security Updates Using an LDAP Directory](#)):

1. In the Active Directory schema, expand the classes,
2. Right-click the `cRLDistributionPoint` class and open the menu **Properties**,
3. Display the tab **Relationship**,
4. Click on **Add Superior**,
5. Add `organizationalUnit` and confirm,
6. Close the Active Directory schema.

Add then the object `cRLDistributionPoint` in the Active Directory organizational unit:





1. In **Start, Administrative Tools**, select **ADSI Edit**,
2. Expand the directory tree structure,
3. In the organizational unit selected to store the CRL, right click and select **New > Object**,
4. Select **cRLDistribution Point**,
5. Enter a name and confirm.

### G.1.2. IIS Web server

A file server has to be configured in order to allow the download of CRLs automatically published in the <CRL\_publication\_dir> folder of the Stormshield Data Authority Manager server.

1. From **Internet Information Services (IIS) Manager**, unroll the server tree and then the **Sites** one.
2. Right-click on the Web site created for Stormshield Data Authority Manager; then select **Add Virtual Directory....**
3. In the wizard, enter an alias <CRL\_publication\_alias>, preferably without a space; then select the physical access path to the <CRL\_publication\_dir> folder.
4. Validate by clicking on **OK**.
5. Go to the newly created virtual directory, then double-click on **Handler Mappings**.
6. From the right column, click on the **Edit Feature Permissions...** link.
7. Select **Read**.
8. Uncheck **Script**, then validate.

## G.2. Configuring in Stormshield Data Authority Manager

For more information about the revocation lists settings, refer to the section [Certificate Revocation Lists \(CRLs\)](#).

### G.2.1. Publishing CRLs

In the LDAP directory case, to allow Stormshield Data Authority Manager to automatically publish CRLs on the directory:

1. In Stormshield Data Authority Manager, click on **Settings** on the home page,
2. Click on **Certificate management**,
3. In the field **CRLs publication DN LDAP** in **Revocation lists (CRLs)**, enter the distribution point DN you have just created during the previous step. As long as this parameter is set and the LDAP directory is properly configured, any CRL generated by Stormshield Data Authority Manager is automatically published in the LDAP entry corresponding to the DN specified here. For more information, refer to [LDAP Configuration](#).

In the IIS Web server case, the download page has already been set during last step.

### G.2.2. Downloading CRLs

#### Automatic inclusion of CRLs in certificates

When automatically downloading a CRL, the “Directory” component in Stormshield Data Security is used to check the validity of user key certificates for each certificate in the string of related



certificates to be validated. The result of this validity check and these possible CRL downloads is displayed in the Revocation Controller component.

For this to be possible, each certificate must contain a CRL distribution point that can verify its validity.

Therefore, in Stormshield Data Authority Manager, for each database, each certificate generated by the database certification authority must contain the distribution point where the certification authority publishes its CRLs.

- Add your distribution points in the parameter **CRL Distribution Points**. Once it is set, they are automatically included in the **CrlDistributionPoint** field for generated certificates.

For a publication in an LDAP directory, the distribution point is:

```
ldap://<LDAP_server_name>:<LDAP_port>/<LDAP_entry_DN>?certificateRevocationList;binary
```

Where:

<LDAP_server_name>	is the LDAP server name (see section <a href="#">LDAP server</a> );
<LDAP_port>	is the port (see section <a href="#">LDAP server</a> );
<LDAP_entry_DN>	is the LDAP entry DN (defined above).

## Configuring the Revocation Controller Component

Since the user certificates do not have CRL distribution points, the **Revocation Controller** component can be configured to automatically download any available CRLs at the first use, after connecting.

1. In Stormshield Data Authority Manager, click on **Users management** on the home page,
2. Click on **User templates** > Name of the template,
3. In the **Components** menu in the upper ribbon, click **Stormshield Data kernel**,
4. Click on the **Revocation controller** link.

It is recommended that you define all of the related authorities in the sender list, defining at least one CRL distribution point for each. There is a button for adding the database authority to the list. For a publication in an LDAP directory, the distribution point is defined above.



## Appendix H. Root Authority Certification

The root authority certification is certified by itself. Its certificate is “auto-certified” and its management may thus require some additional information.

### H.1. Renewing the Certificate

The root certification authority self-certifies. Indeed, its certificate is “self-certified”, and its management requires additional information.

The renewal of the root authority certificate is rarely carried out; there is therefore no dedicated feature in Stormshield Data Authority Manager.

You can renew a certificate the following way:

- generate a certificate request for the certification authority key (no subject renewal) (see [Section 7.3.2, “Making a Certificate Request ”](#));
- make a certificate request to this certification authority (see [Section 7.4.2, “Requesting an Advanced Certificate ”](#));
- validate the certificate request (see [Section 7.5.2, “Processing a Certificate Request ”](#)) and export the obtained certificate value (see [Section 7.6.3, “Displaying a Certificate ”](#));
- import this new certificate for the certification authority key. (see [Section 7.3.3, “Importing a New certificate ”](#)).

### H.2. Renewing the Certificate after Modifying its Identity

It is possible to modify the root certification authority identity, that is to say updating the subject of its certificate.

#### **i** NOTE

This operation can be dangerous if you do not systematically position a `AuthorityKeyIdentifier` in the generated certificates, or if the authority certificate does not own a `SubjectKeyIdentifier`. In this case, the parent-child relationship between the issued certificates and the authority is obtained by comparing the subject of certificates issuer and the authority subject. This relationship is broken if the authority subject is modified, and it will be necessary to:

- renew the “sons”certificates”. Only one level is required, that is to say, most of the time, the sub-authorities certificates certified by the root authority;
- issue the new parent-child relationship chain for certificates issued by the complete “certification tree” (from sub-authorities to final users).

To renew the certificate with an identity modification:

- generate a certificate request for the certification authority key (no subject renewal) (see [Section 7.3.2, “Making a Certificate Request ”](#));
- make a certificate request to this certification authority (see [Section 7.4.2, “Requesting an Advanced Certificate ”](#));
- from the request validation page (see [Section 7.5.2, “Processing a Certificate Request ”](#)), modify the subject by entering the new identity in the DN;



- validate the certificate request (see [Section 7.6.3, "Displaying a Certificate"](#));
- import this new certificate for the certification authority key. (see [Section 7.3.3, "Importing a New certificate"](#)).

From this step, the certificate subject contains the new identity and the certificate issuer contains the former identity. It is not considered as self-certified and cannot be used as it is.

You need to certify it again:

- generate a certificate request for the certification authority key (no subject renewal);
- make a certificate request to this certification authority;
- validate the certificate request but do not modify the subject, and export the obtained certificate value;
- import this new certificate for the certification authority key.

The new certificate is considered as self-certified, both the subject and issuer own the new identity.

### H.3. Revoking the Certificate

The root certification authority certificate is displayed in the list of certificates issued by the authority (see [Section 7.6, "Displaying and Processing Issued Certificates"](#)).

It is possible to revoke it from the certificate page (see [Section 7.6.5, "Revoking a Certificate"](#)). It will appear in the next issued revocation list (CRL) (see [Section 7.7, "Managing Certificate Revocation Lists \(CRL\)"](#)).

#### WARNING

Revoking the root certification authority certificate disables all the parent-child relationships chains from this authority.



## Appendix I. Content of a Certificate issued by the PKI

This appendix displays the content of a certificate issued by Stormshield Data Authority Manager. All attributes and extensions proposed by the PKI are included.

```
SEQUENCE :
  SEQUENCE :
    CONTEXT SPECIFIC (0) :
      INTEGER : 2
    INTEGER : 5
    SEQUENCE :
      OBJECT IDENTIFIER : sha1withRSAEncryption [1.2.840.113549.1.1.5]
      NULL : ''
    SEQUENCE :
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : commonName [2.5.4.3]
          PRINTABLE STRING :
            'CA ROOT'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : localityName [2.5.4.7]
          PRINTABLE STRING :
            'LYON'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
          PRINTABLE STRING :
            'SI'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : organizationName [2.5.4.10]
          PRINTABLE STRING :
            'ARKOON'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : countryName [2.5.4.6]
          PRINTABLE STRING :
            'FR'
    SEQUENCE :
      UTC TIME : '091119162058Z'
      UTC TIME : '111119162058Z'
    SEQUENCE :
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : commonName [2.5.4.3]
          PRINTABLE STRING :
            'Foureaux Pierre'
      SET :
        SEQUENCE :
          OBJECT IDENTIFIER : surname [2.5.4.4]
          PRINTABLE STRING :
            'Foureaux'
```



```
SET :
  SEQUENCE :
    OBJECT IDENTIFIER : givenName [2.5.4.42]
    PRINTABLE STRING :
      'Pierre'
SET :
  SEQUENCE :
    OBJECT IDENTIFIER : localityName [2.5.4.7]
    PRINTABLE STRING :
      'LYON'
SET :
  SEQUENCE :
    OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
    UTF8 STRING :
      'R&D'
SET :
  SEQUENCE :
    OBJECT IDENTIFIER : organizationName [2.5.4.10]
    PRINTABLE STRING :
      'ARKOON'
SET :
  SEQUENCE :
    OBJECT IDENTIFIER : countryName [2.5.4.6]
    PRINTABLE STRING :
      'FR'
SET :
  SEQUENCE :
    OBJECT IDENTIFIER : emailAddress [1.2.840.113549.1.9.1]
    IA5 STRING :
      'pfoureaux@arkoon.net'
SEQUENCE :
  SEQUENCE :
    OBJECT IDENTIFIER : rsaEncryption [1.2.840.113549.1.1.1]
    NULL : ''
  BIT STRING UnusedBits:0 :
    SEQUENCE :
      INTEGER :
        00B36AE27B97D69E490A438AB355666233A9ADFE94
        D28389C0B5F468BD5DAC2FBD5A9EC18730C52C320B
        6B41136A552045922338C6F6C580234A0572ABCA10
        28B14D39CF05E81A49892155BF65FAF7898BF7B313
        A0FEEB1A3E58C23F6C06383A5E610951B6D62D1478
        E4FAD37D57767B74F28869F32CD1CCF176810E88C6
        1E04E7
      INTEGER : 65537
CONTEXT SPECIFIC (3) :
  SEQUENCE :
    SEQUENCE :
      OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
      OCTET STRING :
        SEQUENCE :
          CONTEXT SPECIFIC (0) :
            C2B7D055F0CC0B2545D813CE26A7011967AD
            13C6
SEQUENCE :
  OBJECT IDENTIFIER : subjectKeyIdentifier [2.5.29.14]
  OCTET STRING :
    OCTET STRING :
      ECD1033DA6AE8411303B6A78826AE0F9E8CDF73
      7
SEQUENCE :
  OBJECT IDENTIFIER : keyUsage [2.5.29.15]
  BOOLEAN : 'y'
  OCTET STRING :
    BIT STRING UnusedBits:7 :
      FF80
```



```

SEQUENCE :
  OBJECT IDENTIFIER : subjectAltName [2.5.29.17]
  OCTET STRING :
    SEQUENCE :
      CONTEXT SPECIFIC (1) :
        'test@'
      CONTEXT SPECIFIC (2) :
        'pFoureurx'
      CONTEXT SPECIFIC (7) :
        0A0A0A0A
      CONTEXT SPECIFIC (0) :
        OBJECT IDENTIFIER : szOID_NT_PRINCIPAL_NAME [1.3.6.1.4.1.311.20.2.3]
        CONTEXT SPECIFIC (0) :
          UTF8 STRING :
            'ID44712'
SEQUENCE :
  OBJECT IDENTIFIER : basicConstraints [2.5.29.19]
  BOOLEAN : 'y'
  OCTET STRING :
    SEQUENCE :
      BOOLEAN : 'y'
      INTEGER : 6
SEQUENCE :
  OBJECT IDENTIFIER : extKeyUsage [2.5.29.37]
  OCTET STRING :
    SEQUENCE :
      OBJECT IDENTIFIER : emailProtection [1.3.6.1.5.5.7.3.4]
      OBJECT IDENTIFIER : clientAuth [1.3.6.1.5.5.7.3.2]
      OBJECT IDENTIFIER : serverAuth [1.3.6.1.5.5.7.3.1]
SEQUENCE :
  OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
  OCTET STRING : ''
  SEQUENCE :
    SEQUENCE : ''
    CONTEXT SPECIFIC (0) :
      CONTEXT SPECIFIC (0) :
        CONTEXT SPECIFIC (6) :
          'ldap://srv2k3.lyon2k3.labs:'
          '389/cn=CRL,dc=test,dc=Arkoo'
          'n?certificateRevocationList'
          ';binary'
    SEQUENCE :
      CONTEXT SPECIFIC (0) :
        CONTEXT SPECIFIC (0) :
          CONTEXT SPECIFIC (6) :
            'file:server/sharing/folder/'
            'file.crl'
SEQUENCE :
  OBJECT IDENTIFIER : sha1withRSAEncryption [1.2.840.113549.1.1.5]
  NULL : ''
BIT STRING UnusedBits:0 :
2CDA469A61040735433422DA2DAE860877BE0959FD18FF3B648DBF
947777393110C765D1FC0D82CA7E6DC9BB0A50EAC3A02C8810663D
06DC9A752A72285CAD662DCC48CA50D7EFD583AC24FA05BAADE9A
A990A2F2347955AF9DBE98E02BE87744321B707253C2AC38CA43BC
1E5953E1D09455D0BCBCFB1946E95223FCF78DAF2E7096ABFEB1F7
2DF8791469A458AF0F3C7A433E92A6FD1523C28B3F7310FD396031
14FEE8616FA2432354586D5FC228C6DAD29C7DE45B4B3F71B9C411
576A4E8CFD3352FA26B9724A4B3F4DCBD273E90101279B709F1EC7
0F58D009B22D6F635FA3618029C3CB922637FD4CFE37ABCCA689CE
F2C53B8D8A24BCC462CC27991B

```



## Appendix J. Starting a database with PowerShell

The *SBMSTART.EXE* tool located in the **Tools** folder of the Stormshield Data Authority Manager installation folder allows starting and stopping a database. In some cases, you will need to use a PowerShell script to run the *SBMSTART.EXE* command. For example, it will be the case if the database password contains non ASCII characters.

1. Create a file with the extension *.ps1* which contains the following command:

```
& "C:\Program Files\Arkoon\Security BOX Authority  
Manager\Tools\SBMSTART.exe" "/O" "-b" "<base_id>" "-p"  
"<password>"
```

- The "&" character at the beginning indicates to PowerShell that the character string following the "&" is a command to run.
  - Each parameter is enclosed in double quotes in order to avoid a misinterpretation of the PowerShell parameters.
2. Before the first execution of the script, enter the following command in PowerShell: `Set-ExecutionPolicy Unrestricted`. It allows the script to be run on the machine by all users. This authorization can be restricted to the current user only by adding the argument `-Scope CurrentUser` to the command.
  3. To run the script, you have two options:
    - Right-click the file and select **Run with PowerShell**.
    - Open PowerShell and indicate the path to the script (for example: `"C:\Users\foobar\Desktop\sbmstart.ps1"`) or drag and drop the file, and then press Enter.

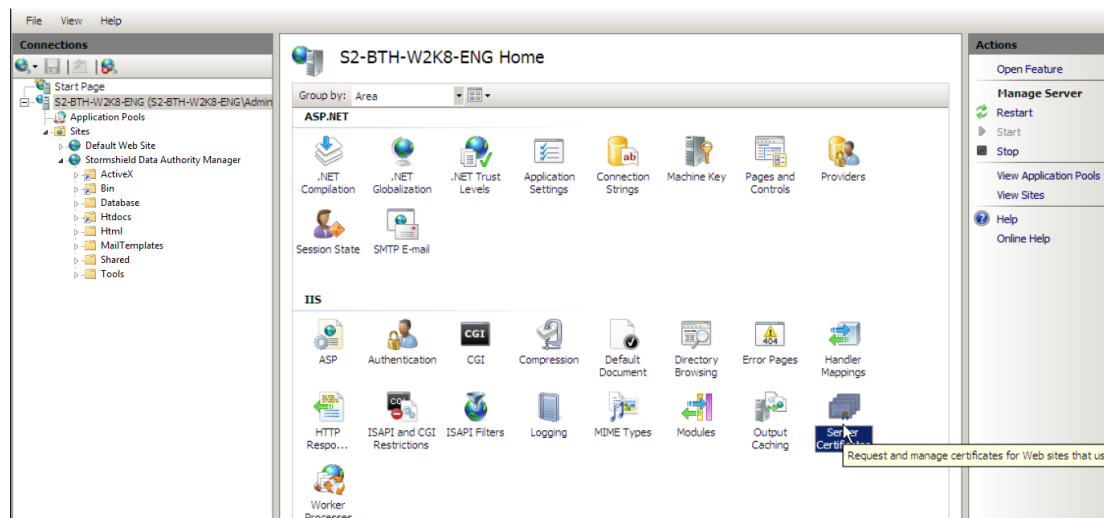




## Appendix K. Activating HTTPS protocol on Stormshield Data Authority Manager

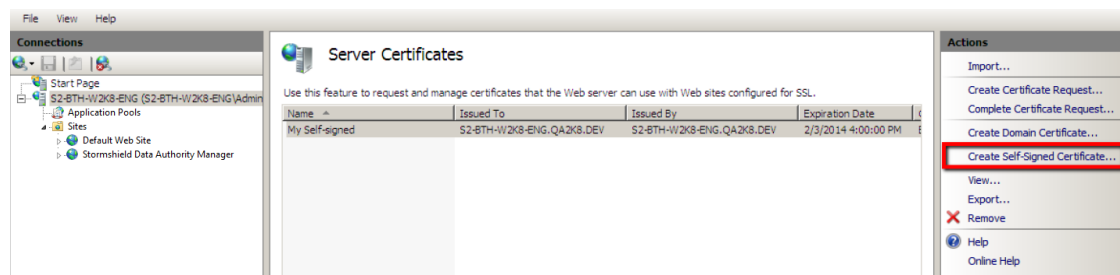
To activate the HTTPS protocol on Stormshield Data Authority Manager, follow the procedure below:

1. Click **Start > Control panel > Administration tool** and open the **Internet Information Services (IIS) Manager**.
2. You need to define a certificate to use. Click **Server Certificates** on the home page.

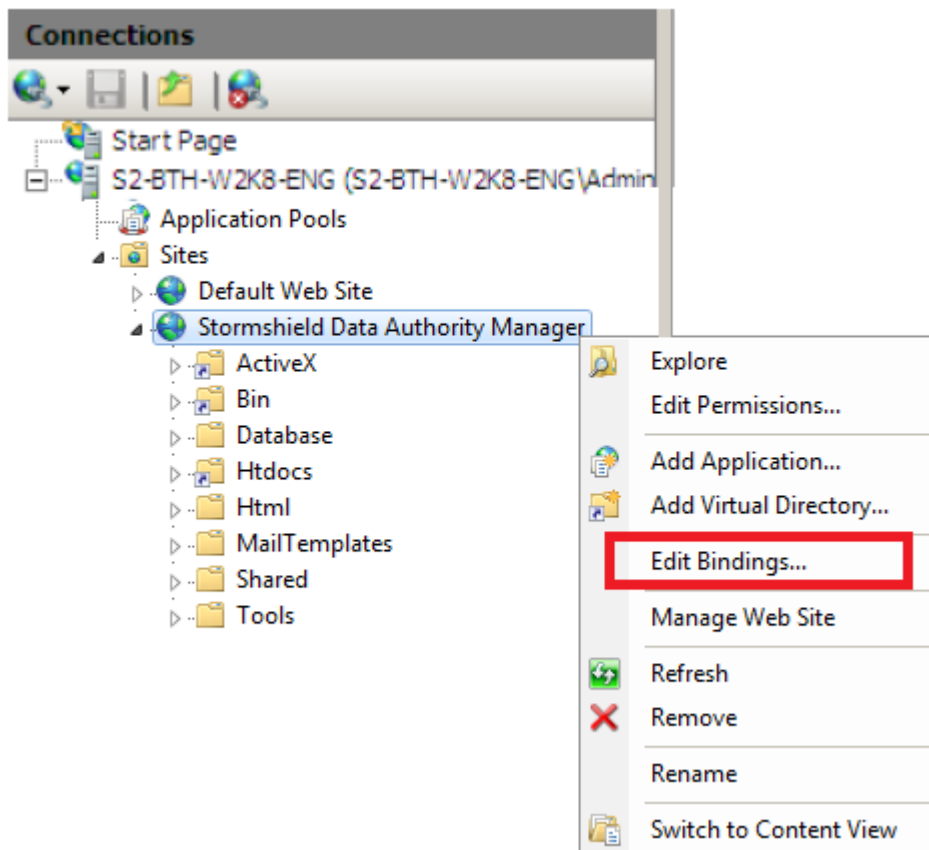


3. In order to create a certificate, click the **Create Self-Signed Certificate** link on the right panel. This option is useful if you do not want to generate a certificate with an external PKI and import it with its trust chain in IIS. When created, the certificate displays in the **Server Certificates** list.

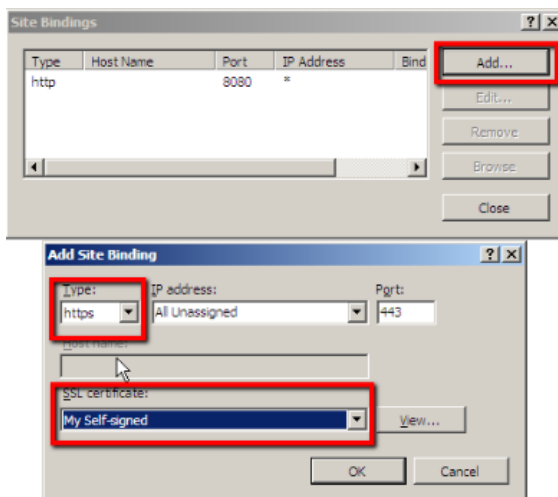
If you want to generate the certificate with an external PKI, you must create an SSL certificate model which uses will be Key encryption (maybe Data encryption as well) and Server authentication.



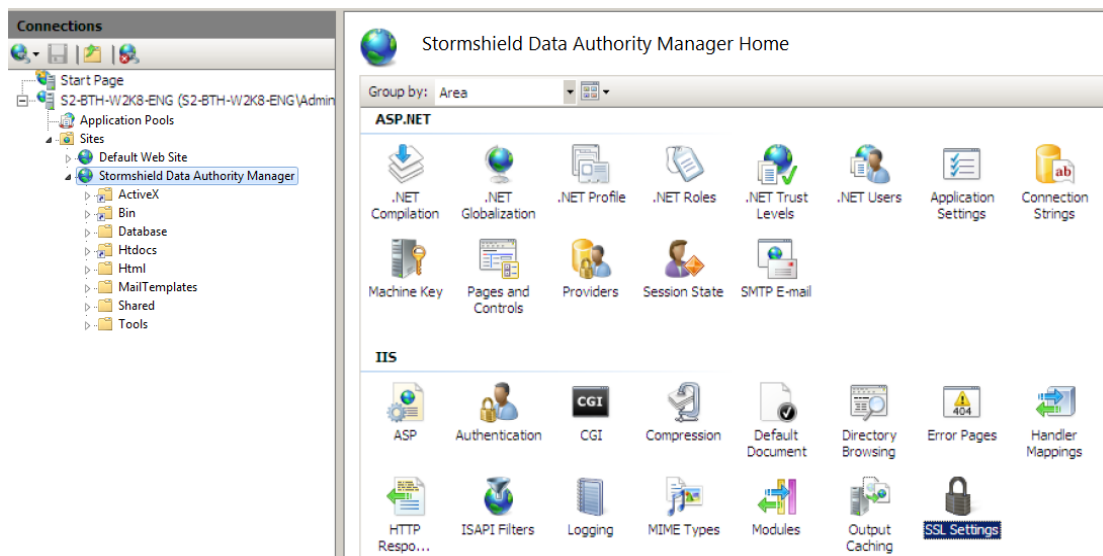
4. Then, you need to indicate that it must be possible to reach the Stormshield Data Authority Manager website with the HTTPS protocol. To do so, right-click the website in the tree view on the left and select **Edit Bindings**.



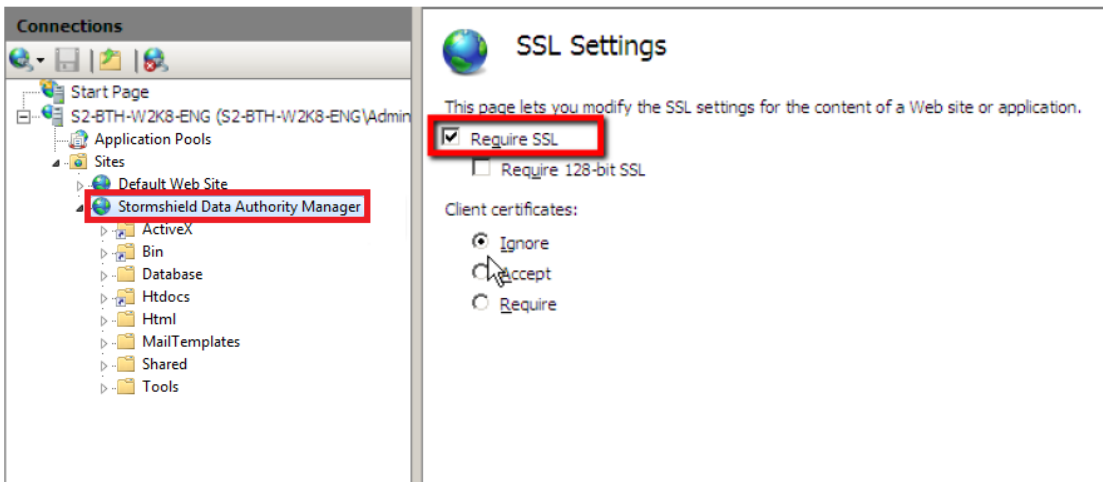
5. In the **Site Bindings** window, click **Add**. In the next window, select **https** in the **Type** field and choose the certificate previously generated in the SSL certificate field. Click **OK**.



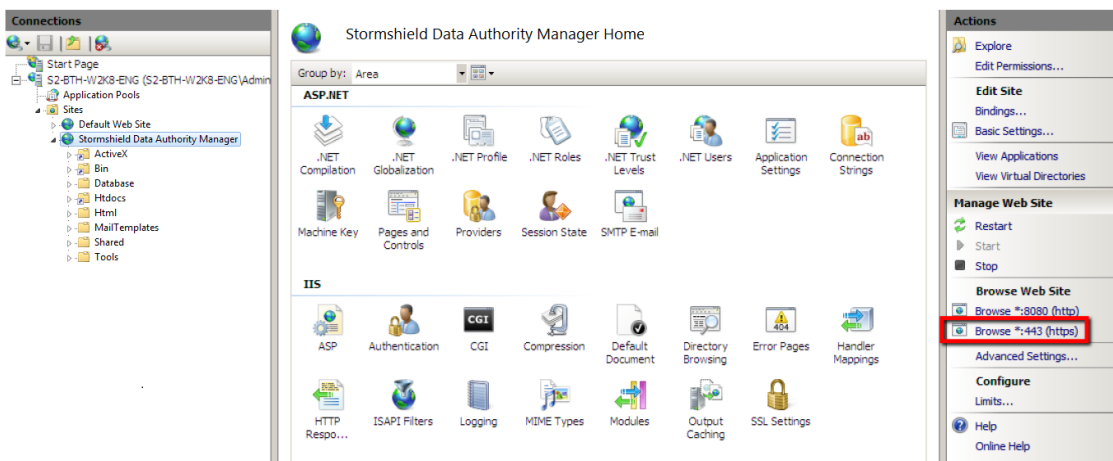
6. When coming back to the home page, select **SSL Settings**. The Stormshield Data Authority Manager website must be selected in the tree view on the left.



7. Check the **Require SSL** option.

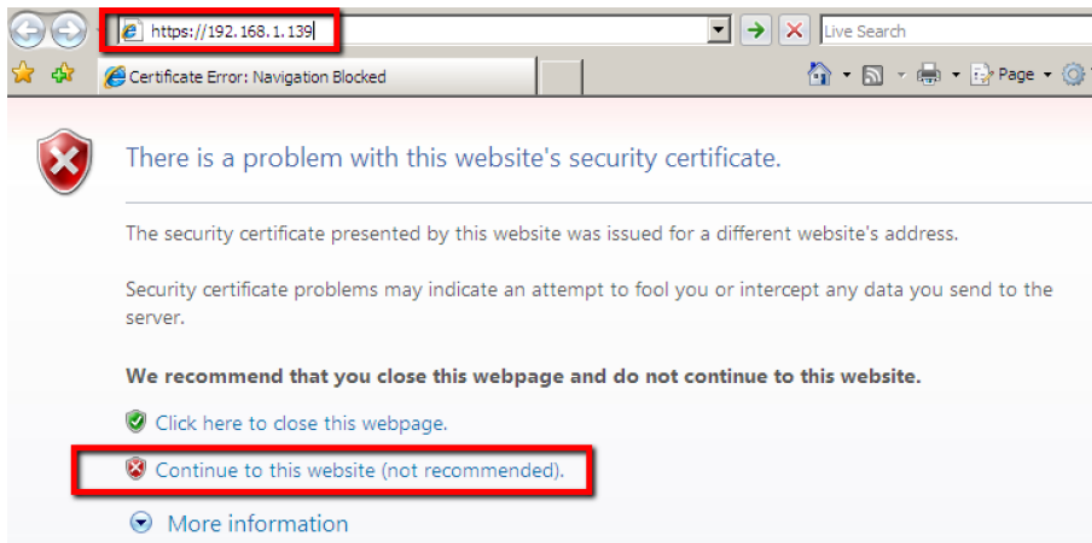


8. To check the procedure works, click **Browse \*:443 (https)** on the **Actions** panel on the right.



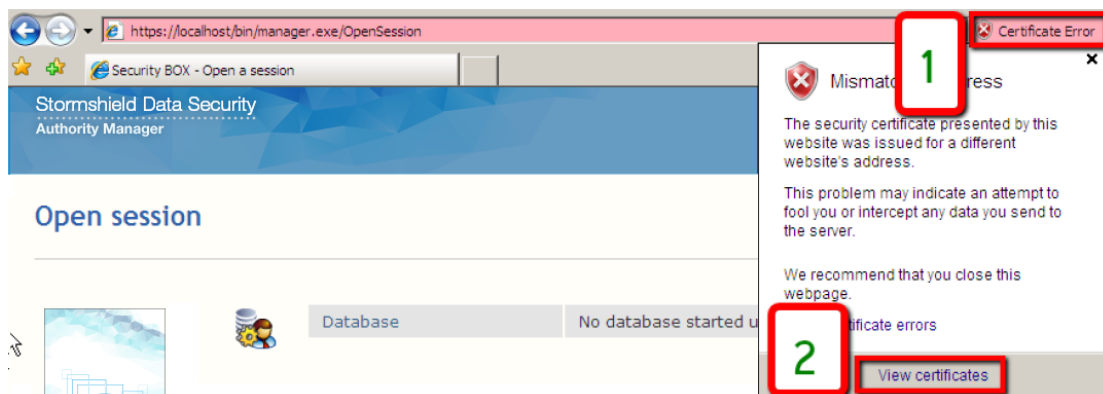
9. Internet Explorer opens. Be careful, the https address in the address bar is incomplete. You need to add **/bin/manager.exe/Opensession**.

Because the new certificate is not in the Internet Explorer certificate store, the warning below displays :

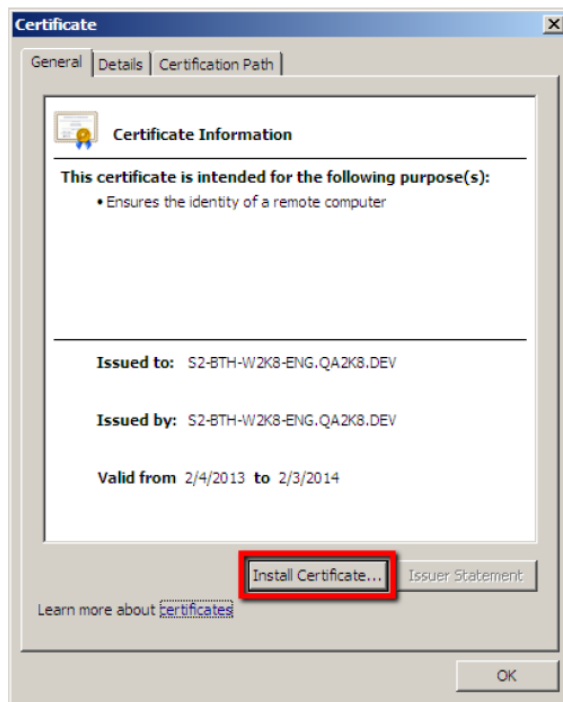


Click **Continue** to this website (not recommended).

10. To prevent this warning from displaying again, import the certificate previously or click **Certificate Error** and then **View certificates**.



11. Install the certificate.





## Appendix L. Database Backup/Restoration

Follow the procedures below to backup and restore your databases.

### L.1. Backup

1. Stop all databases and the sbasrv service (with the command `net stop sbasrv`).
2. Save the file `<sdam_install_dir>\SBMData`.
3. Save the folder `<sdam_data_install_dir>\SBMData`.

### L.2. Restoring

1. Stop all databases and the sbasrv service (with the command `net stop sbasrv`).
2. Restore the file `bases.ini` in the folder `<sdam_install_dir>`.
3. Restore the folder `<sdam_data_install_dir>\SBMData`.
4. Start the sbasrv service (with the command `net start sbasrv`) and all databases.

If the path `<sdam_data_install_dir>` is not the same than the path specified for the backup, it will be necessary to update the paths specified in the file `<sdam_install_dir>\bases.ini` (BasePath and KSPath data). Also, it will be necessary to check the configuration of Stormshield Data Authority Manager because the path `<sdam_data_install_dir>` may be specified in the settings (for example in the page **Settings>User Management**). We recommend thus keeping the same path for the folder `<sdam_data_install_dir>` when restoring.



**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.*