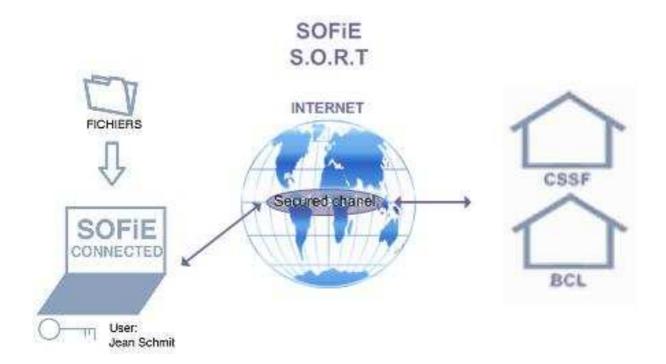
USER Manual SOFIE S.O.R.T

This document contains all information related to the SOFiE S.O.R.T. Cetrel Securities proposes SOFiE S.O.R.T to its customers to execute Secured Online Reporting Transfert towards the **C**ommission de **S**urveillance du **S**ecteur **F**inancier and the **B**anque **C**entrale du Luxembourg.

The user manual addresses the needs of IT specialists for the installation and configuration of the network, as well as those of final users for the SOFiE S.O.R.T functions.



The reproduction of this document is prohibited without the written authorization of Cetrel Securities.

Cetrel Securities.
10 Parc d'Activité Syrdall
L-2956 Munsbach

Phone: 00352 3 55 66 - 349

Table of contents

USE	R Manual SOFiE S.O.R.T	1
Table	e of contents	2
Conte	tacts	4
Intro	oduction	5
1.	Basic Functions of the SOFiE S.O.R.T tool	5
2.	SOFiE S.O.R.T concept	6
3.	Installation	7
4.	Components	7
5.	Technical Requirements	8
Wind	dows installation	10
1.	Upload the installashield	10
2.	Other Platform Installation	13
SOFi	iE Crypt or Transport Configuration	14
1.	Starting SOFiE client	14
2.	Login	14
3.	User not defined	15
4.	Generate your LuxTrust certificate request for the first time	16
5.	Certify your certificate from LuxTrust	23
6.	To fill in your order form	29
7.	To retrieve my certificate	31
8.	To do with the certificates	32
9.	Load SOFiE.config	33
Main	n menu	35
1.	Introduction	35
2.	Processing of files	36
3.	Tools	37
4.	Help	37
CSSI	F encryption with your SOFiE Crypt client	38
1.	Start the CSSF encryption process	38
2.	Follow the CSSF encrpytion process	39
CSSI	F Decryption with your SOFiE Crypt client	41
1.	Start the CSSF decryption process	41
Sond	ling to CSSE and RCL with your SOFIE Transport client	43

1.	Start the sending process	43
2.	Follow the sending process	44
Recei	ve from CSSF and BCL with your SOFiE Transport client	46
1.	Start the receive process	46
Routi	ng between your SOFiE Crypt client and your SOFiE Transport client	49
Certif	ficate expiration	50
1.	Certificate has reached limit date and renewal was not requested	50
2.	Certificate expired	50
Chan	ge password	51
Optio	ns	52
1.	Options - Gui Settings	52
2.	Options - Log Settings	53
3.	Options - Users Settings	54
4.	Options - Batch Settings	55
5.	Options - HTTP Settings	56
Input	file import	57
Canc	el Certificate Request	58
User	Configuration File Input	59
Impo	rt Certificates	60
Use	the import function and select the file containing the certificate	60
Logs.		61
1.	Technical Log	61
2.	Audit Log	62
3.	The log files	62
Abou	<i>t</i>	64
Batch	n mode	65
1.	Batch execution using the config file	65
2.	Manual batch execution	66
3.	Tracking the batch processing using the return code	67
4.	Tracking the batch processing using the Audit Log	67
Usefu	ıl information	69
1.	Packages	70
2.	Standalone/Connected mode	70
3.	Change the mode	71
4.	Verify Certificates	72

Contacts

User Help Desk

Please contact the User Help Desk for any information you need. Either for the installation or the use of SOFiE S.O.R.T

phone: (+352) 3 55 66 -424

e-mail: <u>helpdesk@cetrel-securities.lu</u>

Cetrel Securities

Please contact Cetrel Securities for any information related to your SOFiE S.O.R.T contract.

phone: (+352) 3 55 66 - 349

e-mail: reporting@cetrel-securities.lu

Introduction

SOFiE S.O.R.T is a tool proposed by Cetrel Securities and processed by Cetrel S.C. to transfer reportings in a secured way towards the CSSF (Commission de Surveillance du Secteur Financier) and the BCL (Banque Centrale du Luxembourg). SOFiE S.O.R.T is fully compliant with circulars 08/334 and 08/344 from the CSSF and certified by the CSSF and the BCL.

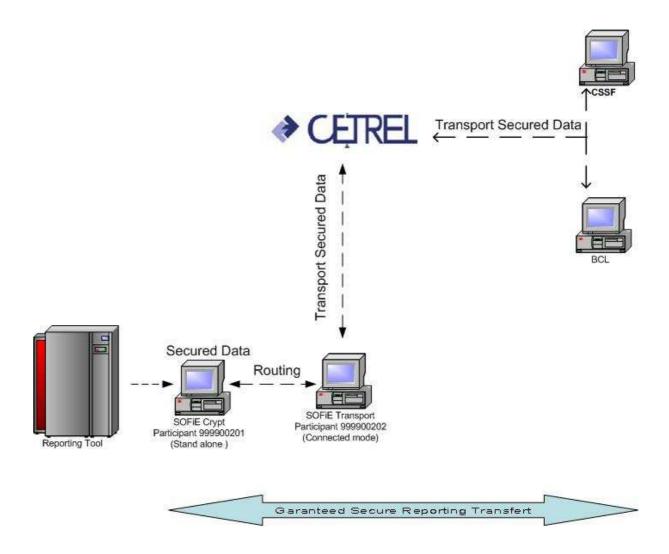
For data security, the SOFiE S.O.R.T solution relies on LuxTrust Certification Authority.

Find on www.cetrel-securities.lu or call our HelpDesk or Cetrel Securities to get all detailed information to adhere to this Cetrel Securities service.

1. Basic Functions of the SOFiE S.O.R.T tool

- 1) SOFiE S.O.R.T implements the security principles, authentication, non-repudiation, confidentiality and integrity defined by the CSSF and BCL and uses 2 distinct SOFiE clients:
 - SOFiE Crypt
 - SOFiE Transport
- 2) SOFiE S.O.R.T uses Certificates (X.509) established by the LuxTrust Certification Authority
- 3) The SOFiE Crypt mechanisms are fully compliant with the CSSF encryption specifications.
- 4) The SOFiE Transport mechanisms to send/receive files are based on HTTP/S protocols. This renders SOFiE Transport independent from complex network security requirements.
- 5) To encrypt the reporting files following the CSSF's specification, you should use the SOFiE Crypt client.
- 6) To send encrypted reporting files you must use SOFiE Transport client.
- 7) SOFIE Crypt offers a functionality to recognize and verify structured files before the securitization of the content. This functionality avoids the transmission of incorrectly structured files.
- 8) SOFiE Transport is capable to distinguish the context of an exchange. In "Production" context the exchange of real operational information is processed. The "Test" context is used to exchange data for test purpose.
- 9) For the exchange of data, SOFiE Transport participants subscribe to packages. This allows a participant to exchange data only according to rules established for the package (ex. TAF, COREP,FINREP). The rules for every package are documented and available on www.cetrel.lu.
- 10) A package may include additional functionalities. For the TAF report, Cetrel developed a package which is commercialized by Cetrel Securities that permits users to type in data. Data are formatted into a file, according to the requirements of the CCSF. When data capture is completed, they are securely sent to the CSSF.
- 11) All detailed information on the service is available by www.cetrel.lu.

2. SOFIE S.O.R.T concept



The concept of SOFiE S.O.R.T is very simple and compliant with the CSSF requirements:

- The participant 999900201 encrypts/decrypts the reporting file or feedback file with the SOFiE Crypt client. The format file generated is a PKCS#7 file.
- 2. The participant 999900202 sends/receives with the SOFiE Transport client the encrypted reporting/feedback to/from the CSSF and BCL.

Some particular applications of SOFiE S.O.R.T are documented further on in this documentation (Useful information).

3. Installation

The installation and configuration process has been simplified and automated at its most. You can get your version of SOFiE by downloading it from our Website.

For upgrading your SOFiE version, we use the JNLP [TM] technology via the Webstart [TM] tool. It allows you to get an update of your SOFiE program every time you start the program. The SOFiE modules are electronically signed, protecting you from the delivery of a non-Cetrel version.

To respect the CSSF technical requirements, you must install 2 SOFiE instances: one for the client "SOFiE Crypt" in a safety network and one for the client "SOFiE Transport" in a DMZ.

4. Components

JRE [TM]	SOFiE uses the Java Runtime Environment. It is the standard JRE as delivered by SUN [TM]. The JRE is automatically installed.
Webstart[TM]	Webstart[TM] is a tool delivered by SUN[TM]. It implements the JNLProtocol, to synchronize a program between a client station and the version existing on a webserver. CETREL uses this technique to synchronize the SOFiE program with its customers. Webstart verifies the electronic signature of a module. Using this technique, you are always sure that the installed module is coming from CETREL. The certificate is installed automatically during first installation. Additionally, Webstart uses the sandbox mechanism of JAVA. This functionality allows customers to be sure that the SOFiE program has only access to authorised resources of your computer. If you are familiar with this concept, you can yourself change the rights.
SOFIE	The SOFiE program consists of a number of signed JAR's. The functionalities of the program can be used either by the GUI or via batch mode.

5. Technical Requirements

5.1 Platforms

Refer to www.cetrel.lu to get all the information concerning the supporter platforms and the technical requirements for the SOFiE tool.

5.2 Communication

The file exchanges with CETREL are done via an Internet Connection. Any type of communication can be used: leased line, modem,

Before installing SOFiE client please make sure you have admin rights and if you pass by a "firewall" or even a "proxy" URL and the ports must be open:

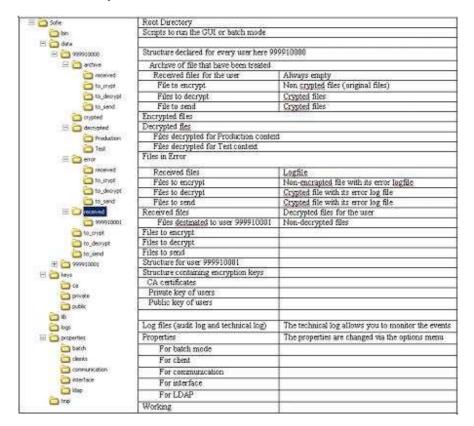
Port	Using	Possibility of using a web proxy
80	SOFiE client:	Yes, but without authentication
	An update of the application in batch mode	
	or JavaWebStart	
443	SOFiE at SSL	Yes, but without authentication
389	LDAP	LDAP needs a direct TCP connection
		/ NAT

URLs are accessed as follows:

- To allow the transmission of data, you need to open the following URL and TCP/IP sockets.
 http://www.cetrel.lu/jws/sofie/index.html
 https://www.cetrel.lu/cgi-bin/prot/chgpass
- To be able to have the automatic update of new SOFiE versions, allow the URL https://www.cetrel.lu/secure/prot/sofie/jsp/servlet/SofieMain
- To have access to the LDAP, authorize use of the LDAP protocol with port 389 LDAP: // ca.cetrel.lu

5.3 Directory Structure

To integrate SOFiE client in your automated process, it is important to know the usage of the directory structure, installed and used by SOFiE.

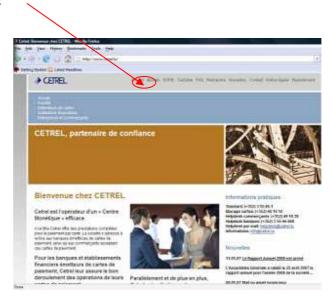


Directory	Recommended actions
999900****	backup the structure regularly
Archive	clean the structure regularly
Error	backup (for tracing) and clean regularly
Received	all files received for the user are decrypted and can be used for further treatment
received/999900207	all files received are transmitted to user 999900207 and are not (cannot be) decrypted
to_crypt	basic directory scanned every time you execute the encryption process
to_decrypt	basic directory scanned every time you execute the decryption process
to_send	basic directory scanned every time you execute the sending process
Keys	backup regularly
Logs	contains the log files. You can use the files to monitor SOFiE It is recommended to make a regular backup and clean the directory.
Properties\batch	backup regularly
Properties\clients	backup regularly

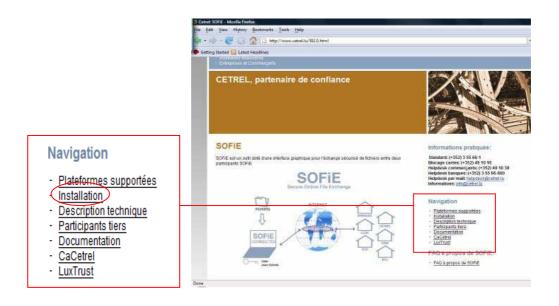
Windows installation

1. Upload the installashield

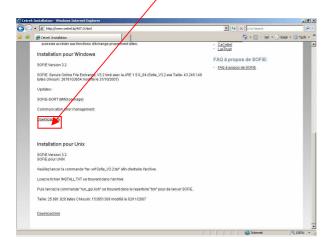
Go on www.cetrel.lu and click on SOFiE



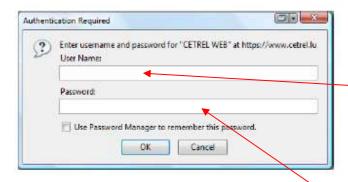
Go on Navigation and click on Installation



Click on **Download** Link for Windows



The system ask your User Id* and password*



*These information has been transmitted by courier.

Having entered your data, you have 2 opportunities for download.



1. First opportunity, click on RUN (adviced)



Start of installation



At the end of download, the application displays the following message

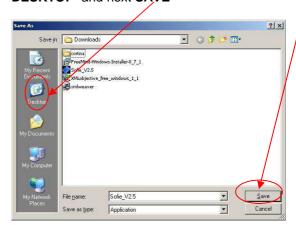


Click on RUN to continue

2. First opportunity, click on SAVE



Please save the installshield on your desktop for that click **DESKTOP** and next **SAVE**



Start of download



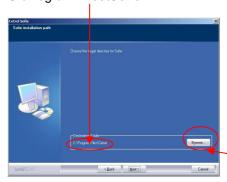
After the download, you must launch the installshield



Sofie_V3.2.exe which is in your desktop to start the installation.

The installation will start and the application asks you the SOFiE installation folder. By default, the folder is ;

C:\Program Files\Cetrel



If you want install SOFiE client on another folder, click on BROWSE and indicate the path.

At the end of installation, you have an icone on your desktop.



2. Other Platform Installation

- 1. Use your User-Id and Password to download from www.cetrel.lu your TAR file or get your CD from CETREL.
- 2. Copy the TAR file to its destination, and execute the UNTAR utility with the instruction:

uncompress sofie.verxyz.tar.Z

tar -xvf sofie.verxyz.tar

- 3. The following components have been installed:
 - the latest JRE [TM] supported by SOFiE (refer to www.cetrel.lu for the actual version)
 - the SOFiE program
- 4. Start SOFiE using the run_gui.ksh script.

SOFIE Crypt or Transport Configuration

1. Starting SOFiE client

Use the icon

on your desktop to start your SOFiE Crypt or Transport client.

By default, SOFiE client is installed under folder C:\CETREL\sofie.

If you want install SOFiE client on a network, you change the letter C by the letter of your driver example: f:\......



SOFiE client is started through Java Webstart [TM]. Every time you start SOFiE, it will try to synchronize your SOFiE version with the reference at Cetrel.

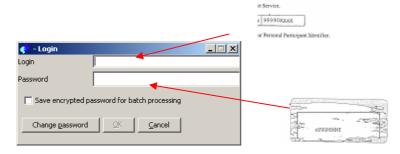
When a new version is downloaded, the starting of SOFiE client will last somewhat longer (depending on your telecommunication infrastructure).

Notice: The synchronization happens only if you have access to the required <u>URL</u>.

2. Login

The login allows you to access the functions of SOFiE S.O.R.T.

Fill in Your User Id and Your Password



Remember that the first time you log to SOFiE, you have to type in the password contained in your envelope.

During the configuration wizard, you will have to change your password. SOFiE requests that your password will have at least 8 characters, one upper case letter, one lower case letter and a digit.

After 3 erroneous attempts, the Login terminates automatically. You can nevertheless restart SOFiE and try to log in again.

!!!! Important !!!!

If you forget/loose your password once you have created your profile, you can no longer use SOFiE.

You must contact CETREL to get a new participant ID.

SOFiE saves the status of your user and during the login, according to the status, different functions may only be available

3. User not defined

As your User Id is yet not declared on your computer, you are requested to confirm the creation of the user.



Confirm the creation of a new user and you will continue with the configuration wizard

Do not confirm the creation of a new user and get the information

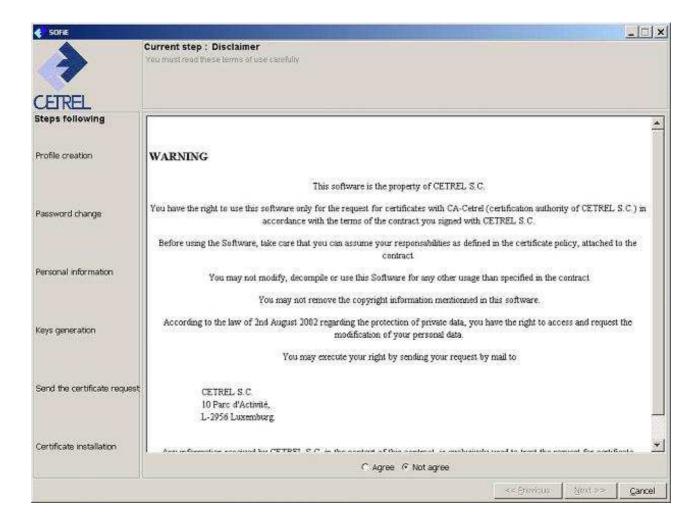


After confirming with you return to the login screen.

4. Generate your LuxTrust certificate request for the first time

The configuration wizard leads you through all the configuration steps you have to execute before having access to the SOFiE S.O.R.T functions (Crypt or Transport). If for any reason you stop during the process, the next time you login, the wizard will automatically guide you to the last configuration step performed. You continue with the procedure.

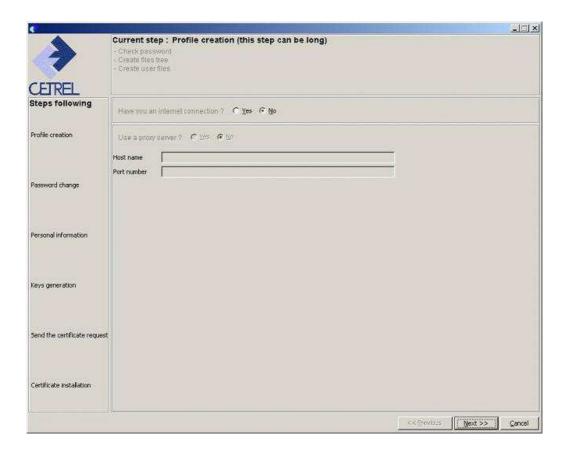
The Disclaimer informs about the responsibilities when using SOFiE client



Agree and go further with ______ to

1. The profile creation

- confirm your internet connection
- when yes, confirm your proxy and give the Host name and the port number of your proxy server (ask
 your network administrator for these informations)

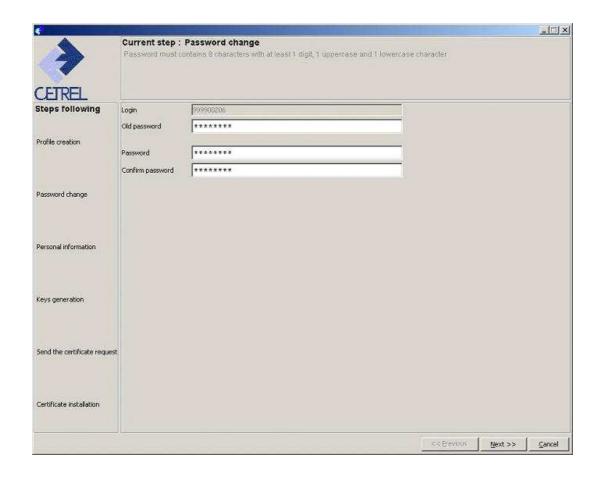


- confirm whether you are connected to the internet
- If you have an Internet connection, you are asked to complete:
 - whether you have a proxy server
 - and give the Host name and the port number of your proxy server (ask your network administrator for these informations)

go further with _____ to

3. You are requested to change the password

Repeat your old password and fill in your new password (respect the rules for declaring a password).

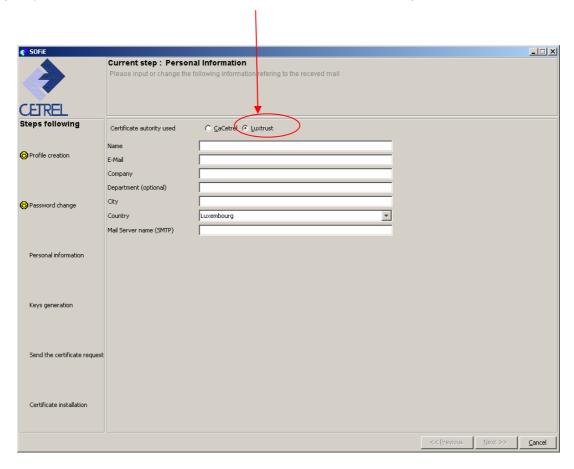


Repeat your old password, and introduce your new password (respect the rules for declaring a password).

Notice: Your password for accessing the protected Internet site of CETREL has also been changed

and continue with ____to

4. Fill in your personal information and check LuxTrust as Certification Authority



After selecting LuxTrust, the following message displays



After confirming with , you can fill in the information.

Notice: This information will be used for your certificate request, and the LuxTrust can refuse your certificate request if information is wrong and different of your order form.

Name: your name

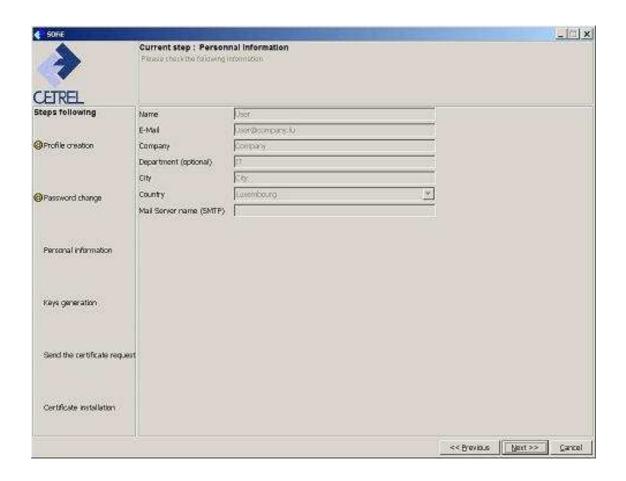
E-mail: your e-mail address (the certificate will be sent to this address)

Company: company name
Department: your department
City: your city
Country: your country

Mail server: name of your mail-server (consult your network/system administrator)

continue with to

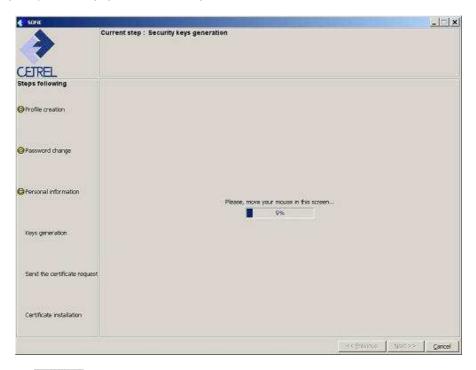
5. Confirm your personal information



continue with to

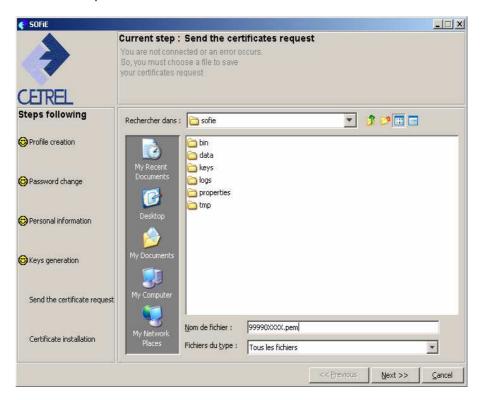
6. Generate your private/public key

To generate your private key, you must move your mousse until 100%.

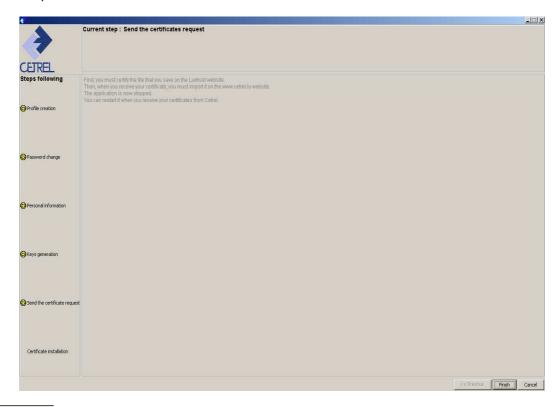


continue with to

7. Save the Certificate request



You must save the Certificate request. The Certificate request is a file which contains all information about your public key. The name file is your user id with extension pem. Example: 999900000.pem

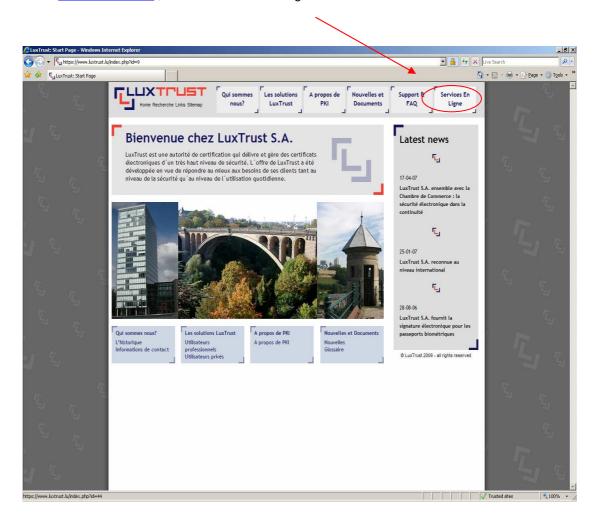


Click to Finish

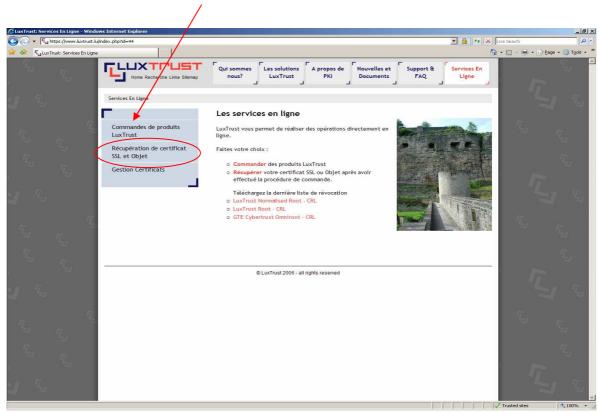
- 8. The first phase of your configuration process has been executed and SOFiE is stopped.
- Send your Certificate request to LuxTrust and retrieval your certificate certified by LuxTrust. Following the instruction defined on: https://www.luxtrust.lu/fileadmin/user-upload/downloads/SSL_quide_online.pdf.

5. Certify your certificate from LuxTrust

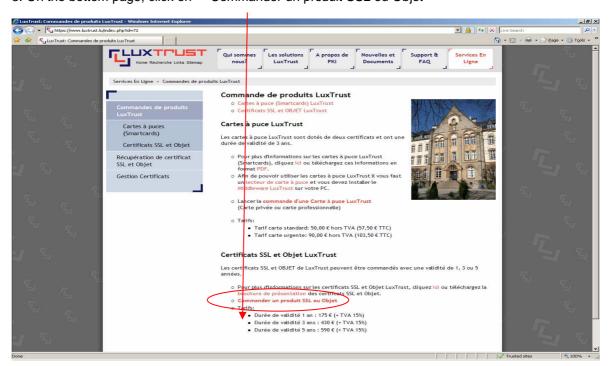
1. On www.LuxTrust.lu, click on « Service en ligne »



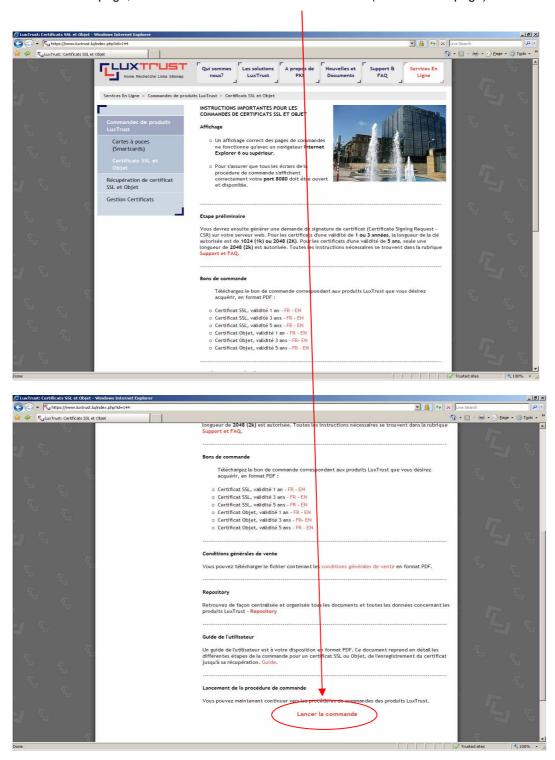
2. Select « Commande de produits LuxTrust »



3. On the bottom page, click on « Commander un produit SSL ou Objet »

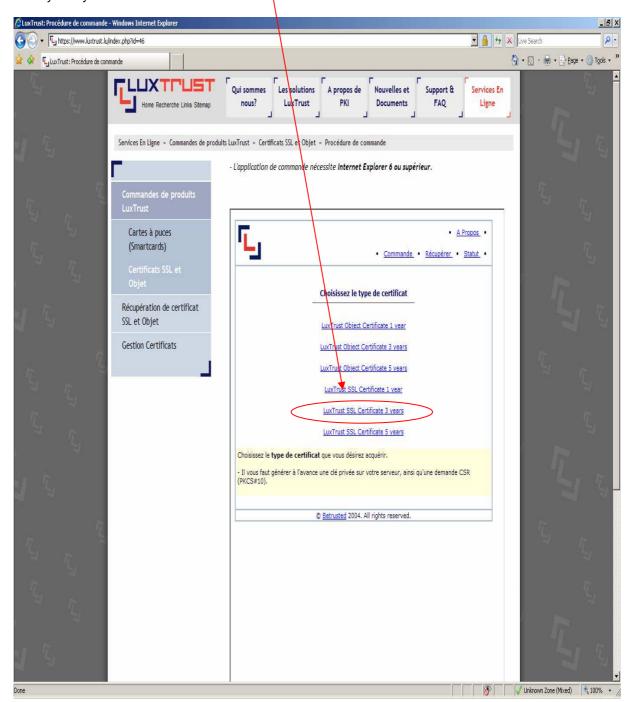


4. On the next page, we must select « Lancer la commande » (in the bottom page)

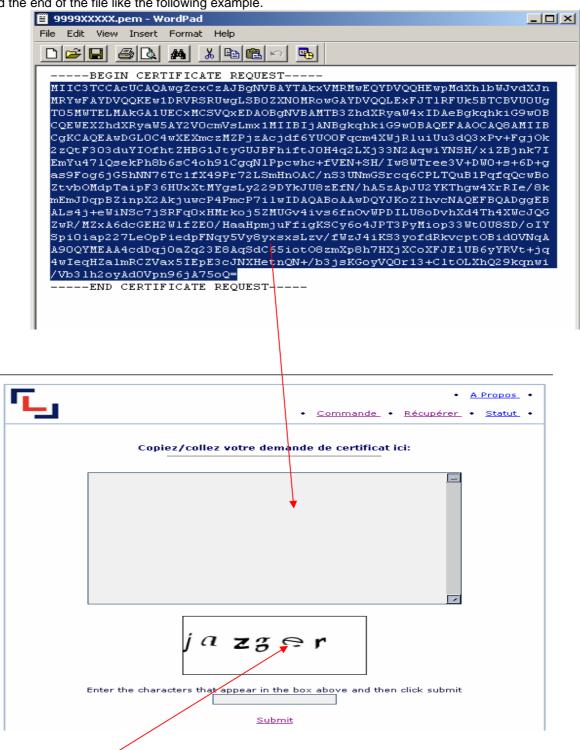


5. You **must** choose a LuxTrust SSL Certificate 3 years.

For maintenance reasons and to keep a standard, SOFiE supports only the certificate with a validity of 3 years.



6. In this page, you must copy the content of your 9999XXXXX . pem which you have saved before without the begin and the end of the file like the following example.

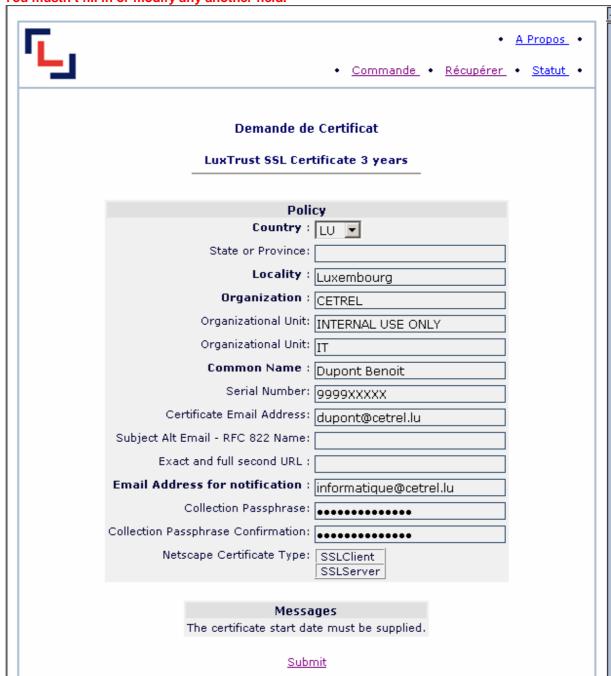


7. And fill in the characters appeared in the box above and submit the request

8. In the next screen, you must just fill in the 3 following fields to retrieve your certificate after LuxTrust certification :

- Email Address for notification
- Collection Passphrase:
- Collection Passphrase Confirmation

You mustn't fill in or modify any another field.



9. Click on Submit

The screen displays the transaction number



After these steps, we must send your order form to LuxTrust. With your contract copy and your passwords, you have received a special SOFiE LuxTrust order form that you must complete and send to LuxTrust.

6. To fill in your order form

In your order form, there are 4 parts:

- First part for your SOFiE Transport Certificate
- Second part for your SOFiE Crypt Certificate
- Third part One for the payment
- Fourth part for the signature

To complete the first and second part, you must indicate the same information in your order form than in your certificates requests. Example

Policy	
Country : LU 🔻	1
State or Province:	
Locality : Luxembourg	2
Organization : CETREL	3
Organizational Unit: INTERNAL USE ONLY	4
Organizational Unit: IT	5
Common Name : Dupont Benoit	6
Serial Number: 9999XXXXX	7
Certificate Email Address: dupont@cetrel.lu	8
Subject Alt Email - RFC 822 Name:	
Exact and full second URL :	
Email Address for notification : informatique@cetrel.lu	
Collection Passphrase:	
Collection Passphrase Confirmation:	

Part 1: Order information for your SOFiE Transport certificate

Information appearing in the certificate

IMPORTANT: You need to send your CSR (PKCS#10) request to LuxTrust via the Internet site http://orders.luxtrust.lu. The indications in this part of the order form have to correspond **exactly** to the information in your CSR. It is possible that certain fields will not be available in your CSR generation tool! **The fields are mandatory!** Please also refer to the certification policy and the certificate profiles under http://repository.luxtrust.lu

	Technicate promos and integrate postery radia doctra		
7	ld SOFiE Transport :	9999XXXXX (Serial number in the CSR)	
6	Common name :	Dupont Benoit (Person name included in the CSR)	
3	Company name:	CETREL (Company name or other equivalent official denominal	ition)
2	Company address (city):	Luxembourg	
1	Country:	LU (ISO Code (LU, DE, FR,) of the country where the company's legal headquarter is located)	
8	E-mail address:	dupont@cetrel.lu	
5	OrganizationalUnit1 (optionnel) :	: пј	
4	OrganizationalUnit2 :	INTERNAL USE ONLY	continued p.2 \Rightarrow

To complete the fourth part, you must indicate your transaction number



7. To retrieve my certificate

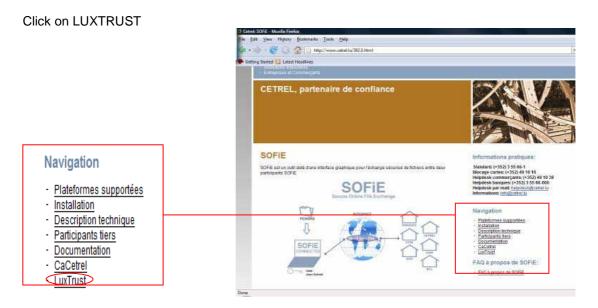
You will receive a email from Luxtrust to inform that your certificate has been validated. To retrieve your certificate, you must go to Luxtrut website www.luxtrust.lu under heading « Services en ligne » -> « Récupération de certificat ».



You can save the certificate either Der format or Pem format.

8. To do with the certificates

Upload your certificates Crypt and Transport on www.cetrel.lu under SOFiE heading to continue the SOFiE installation.



To upload your certificate, you must enter your user Id and your password.



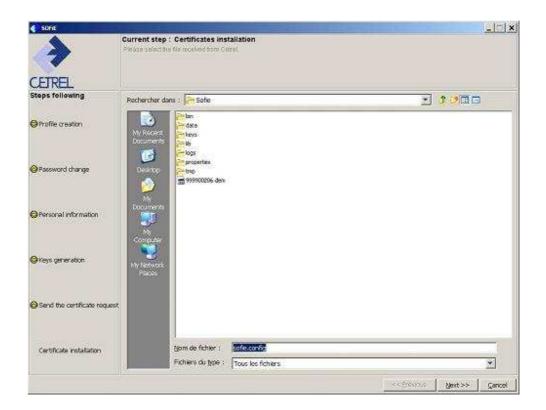
To upload your certificates, click on browse to select your certificate and after clicking on upload

You must sent your Crypt certificate to CSSF following rules indicated in circulaire 08/334

9. Load SOFiE.config

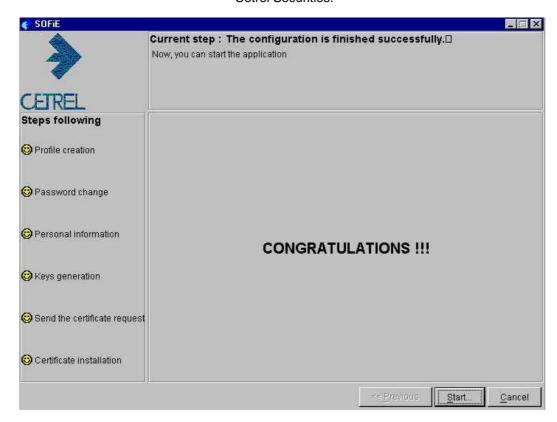
CETREL will send you by email the "SOFIE.CONFIG" file, containing your new certificate and your profile.

After starting the application, you are requested to load the "SOFIE.CONFIG" file, you received from CETREL



Select the file and continue with

When your SOFiE.Config is installed, the configuration wizard will finish with this screen



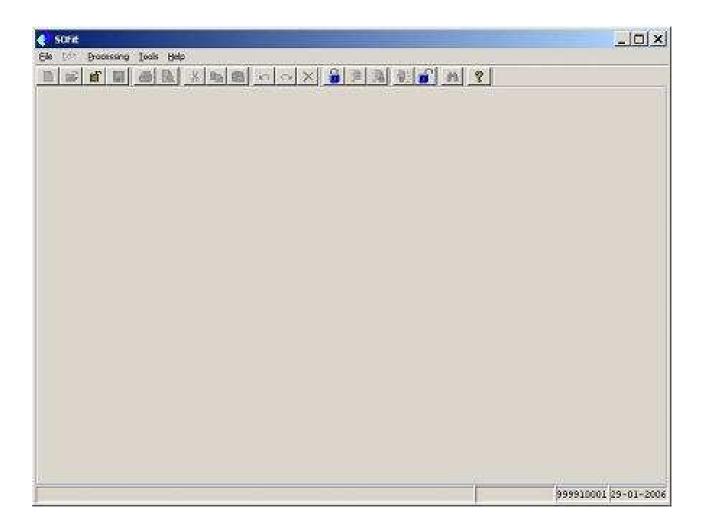
SOFiE is started automatically and your SOFiE Crypt or Transport client is setup

Main menu

1. Introduction

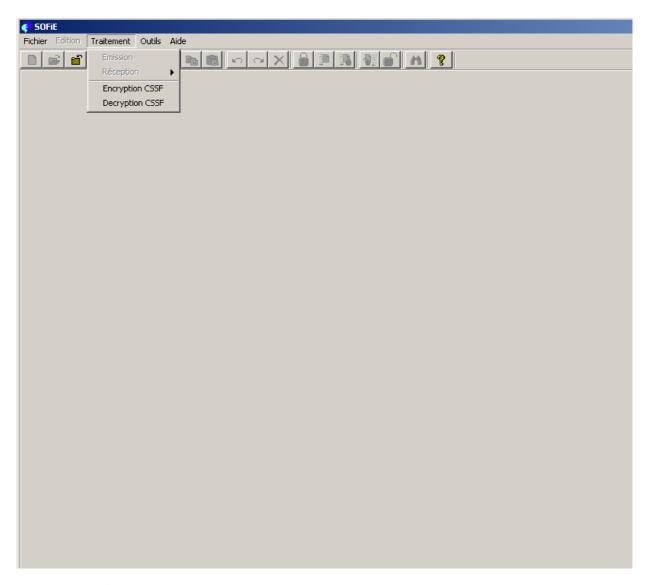
You can access to the functions using the menus or using the different shortcuts for your client SOFiE Crypt and SOFiE Transport.

Access to functions depends whether you have an Internet connection, and that the certificate has not expired.



The main menu of SOFiE client gives access to the different functions of SOFiE S.O.R.T

2. Processing of files



For your user SOFiE Transport, the following functionalities are active :

The <u>Emission</u> functionality allows you to send encrypted files to CSSF and BCL
The <u>Receipt</u> functionality allows you to receive encrypted feedback files from CSSF and BCL

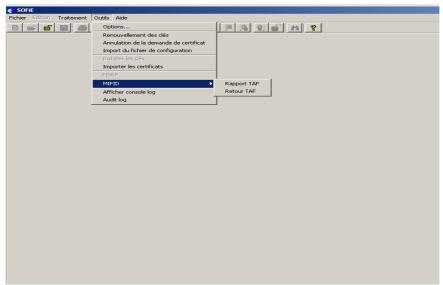
For your user SOFiE Crypt, the following functionalities are active :

The <u>CSSF Encryption</u> functionality allows you to encrypt your reporting following the CSSF specification

The CSSF Decryption functionality allows you to decrypt the feedback files from CSSF and BCL

3. Tools

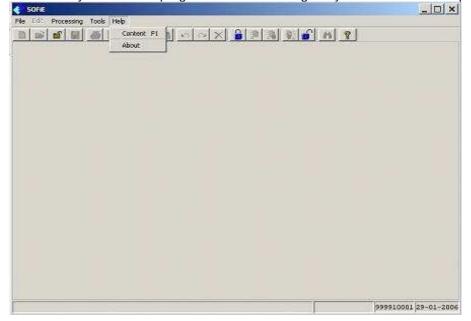
The Tools menu gives access to



- the different Settings to customize SOFiE according to your needs
- the functionality to execute the key renewal and to load a new configuration file
- the functionality to consult the different logs (log console , audit log)
- the access to the TAF GUI

4. Help

The Help menu informs you about the programme version and gives you access to the Help

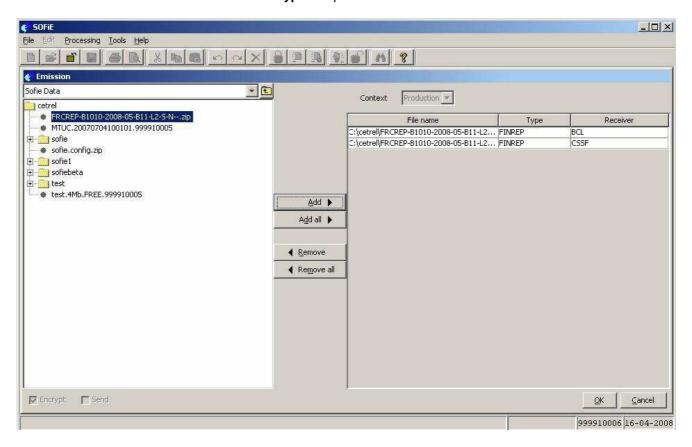


CSSF encryption with your SOFiE Crypt client

The CSSF Encryption functionality allows you to encrypt your reporting following the CSSF specification

1. Start the CSSF encryption process

1. Choose on the toolbar the CSSF Encryption option



Establish the list of files you want SOFiE to treat

Select the directory where your files are located and use the directory to your list

or

Select the specific file and use the button to add the file to your list.

You can also use the normal Windows options for selecting directories and files (Shift + select, Ctrl + select,)

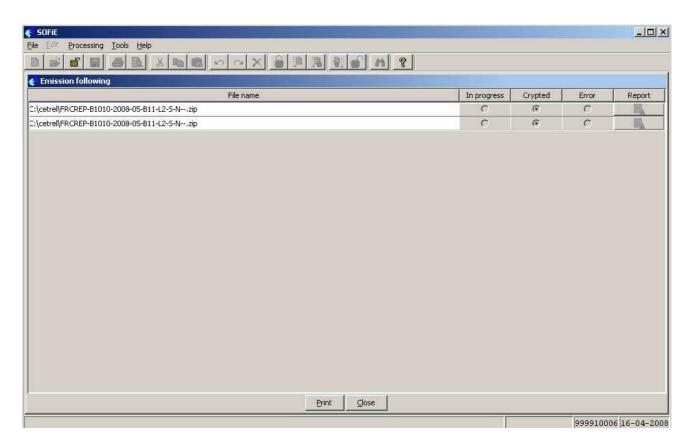
When adding the file(s) to your list, SOFiE executes automatically the <u>automatic recognition for file contents</u> based to the naming or the content of the file

Refer to the documentation of file format and naming conventions for the files supported by the different packages. The documents are awailable on www.cetrel.lu or can be requested at Cetrel.

2. Confirm with to start the encryption to the CSSF/BCL format

2. Follow the CSSF encryytion process

1. After starting the emission process, SOFiE Crypt client attaches the Follow-up screen.



2. The complete list of all the selected files is attached.

According to the automatic processing of SOFiE, the status of the files is attached.

In progress : The file is about to be treated by SOFiE

• Crypted : The file is crypted to the CSSF/BCL or decrypted

Error : The file, that for any reason could not be treated correctly
 Report : Have direct access to the informations, that allow you to

find out why the processing of your file did not work

3. Congratualation, your file is encrypted in CSSF/BCL Format or decrypted in clear.

The naming of the file becomes:

The name in entrance with the extension

.CSSFSEC.CSSF if the file is destined to CSSF

or

- . CSSFSEC.CSSF if the file is destined to BCL

For example :

To_crypt:

FRCREP-B1010-2008-04-B11-L2-S-N--.zip

Crypted:

FRCREP-B1010-2008-04-B11-L2-S-N--.zip.CSSFSEC.CSSF

And

FRCREP-B1010-2008-04-B11-L2-S-N--.zip.CSSFSEC.BCL

4. When the encryytion of all the files completes, you can print out a report containing the information of the files that have been processed.

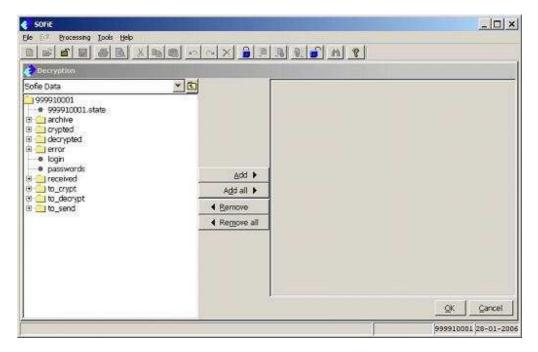
!!!! Print out the report immediately, you will not have the opportunity to request the reprint of the report!!!

CSSF Decryption with your SOFiE Crypt client

The CSSF Decryption functionality allows you to decrypt the feedback files from CSSF and BCL

1. Start the CSSF decryption process

1. Choose the CSSF Decryption function



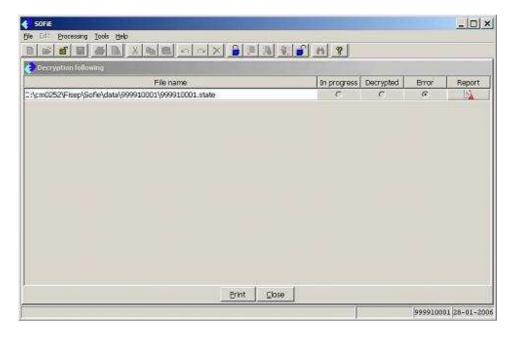
1. Establish the list of files you want SOFiE to treat

Select the directory where your files are located and use the files contained in the directory to your list or

Select the specific file and use the button to add the file to your list.

You can also use the normal Windows options for selecting directories and files (Shift + select, Ctrl + select,)

3. Confirm with **OK** to start the decryption process



Process: The file is about to be treated

• Decrypted : The file has been decrypted

Error : The file has not been treated correctly

• Report : Have direct access to the informations, that allow you to find out why the processing of your file did not work

2. When the processing of all the files completes, you can print out a report containing the information of the files that have been processed.

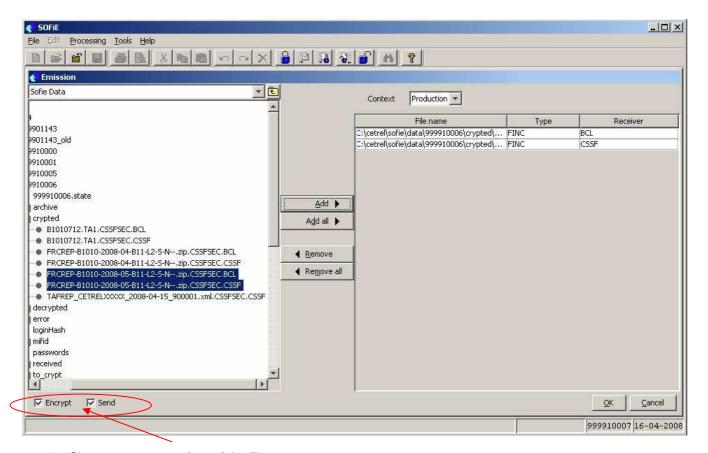
!!!! Print out the report immediately, you will not have the opportunity to request the reprint of the report!!!

Sending to CSSF and BCL with your SOFiE Transport client

The Emission function allows you to send your reporting files to CSSF and BCL.

1. Start the sending process

1. Choose on the toolbar the **Emission** option



2. Choose encrypt and send the files

The CSSF and BCL impose a new encryption for the sending, it's the reason that you must choose encrypt option

3. Choose the **context** in which you want to use SOFiE.

!!!! Be aware that when you use the test mode, the receiver will probably not automatically treat your files. The test context mode should only be used to exchange files for test purposes!!!!

4. Establish the list of files you want SOFiE to treat

Select the directory where your files are located and use the button to add all the files contained in the directory to your list

or

Select the specific file and use the Add button to add the file to your list.

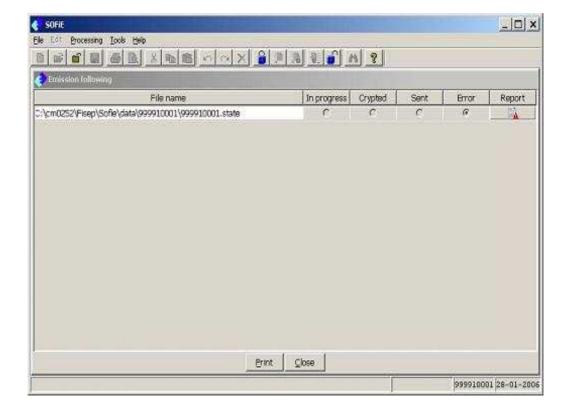
You can also use the normal Windows options for selecting directories and files (Shift + select, Ctrl + select,)

Only encrypted files with SOFiE Crypt or another crypt tool can be sent to CSSF and BCL. If files that are not secured by SOFiE Crypt or another crypt tool have been selected, and you request the sending, the files are not transferred.

5. Confirm with or , to start the encryption/send process.

2. Follow the sending process

1. After starting the emission process, SOFiE Transport client attaches the Follow-up screen.



2. The complete list of all the selected files is attached.

According to the automatic processing of SOFiE, the status of the files is attached.

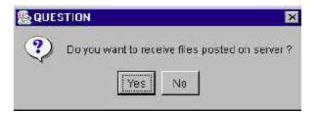
In progress : The file is about to be treated by SOFiE

Crypted: The file is crypted (only if the Crypt option has been set)
 Sent: The file is sent (only if the sent option has been set)
 Error: The file, that for any reason could not be treated correctly
 Report: Have direct access to the informations, that allow you to find out why the processing of your file did not work

3. When the processing of all the files completes, you can print a report containing the information of all processed files.

!!!! Print out the report immediately, you will not have the opportunity to request the reprint of the report!!!

4. When you close the window, SOFiE is asking you if you want to start the Receipt.



Notices:

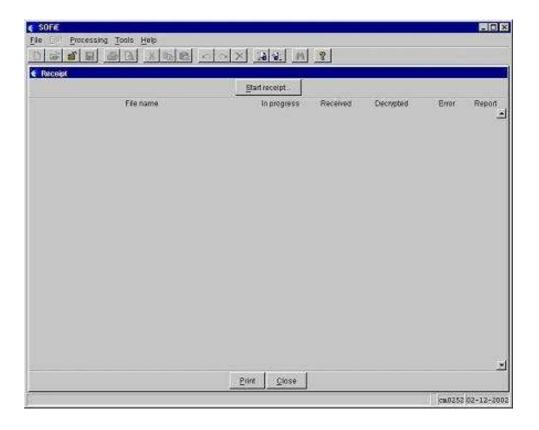
- 1. The original files are not deleted by SOFiE.
- 2. When the Emission process is interrupted, SOFiE does not fulfill a rollback, meaning that files that are sent have arrived to CETREL. Files that are encrypted are in the encrypted Directory.
- 3. The files that have been treated with an error are put into the Error Directory of your Participant Id.
- 4. The files that result from an encryption process are stored in the Crypted Directory.
- 5. All treated files (the original version) are stored in the Archive\to_crypt directory.
- 6. All sent files are stored in the Archive\to_send directory.
- 7. If you need your report in an electronic way, use the possibilities of the printer configuration.
- 8. All the files are renamed along a specific SOFiE rule, when they are encrypted. The standard is <<SOFIE.timestamp.ld destinator>>.
- 9. As a user you need to know the receiver of your file in terms of "who will have access to the content of the file". The potential intermediary (Routing concept) on the receiver's side is not an important information for you.

Receive from CSSF and BCL with your SOFiE Transport client

The Receive function allows you to receive all the feedback reports that have been sent to you.

1. Start the receive process

1. Choose the Receipt/Receive function

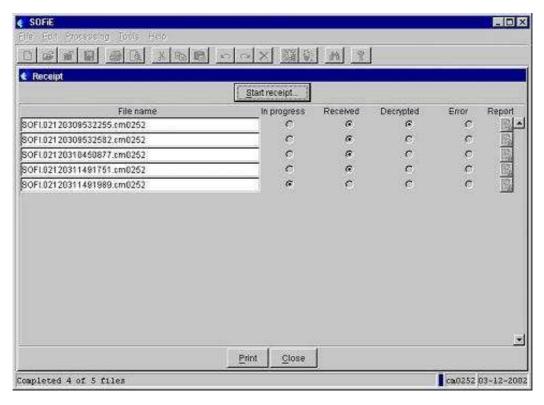


2. Start the Receipt by pushing on the button

3. The following message informs you, in case no file is available for you



4. Otherwise the files with their respective processing status are attached



• In progress : The file is about to be treated

Received : The file is received

• Decrypted : The deciphering process is executed

• Error : An error occurred and the error report should be considered

5. Files sent to you are stored as follows

\Decrypted\

\production files sent in production context are stored here

\test files sent in test context are stored here

\Received\9999.... files that are to be routed to another destinator are stored in a seperate directory

6. When the processing of all the files completes, you can **print** a report containing the information of the files that have been processed.

!!!! Print out the report immediately, you will not have the opportunity to request the reprint of the report!!!

Notices:

- If any problem occurs after the receiving process, the secured file is copied in your ...\to_decrypt
 directory. Consult the error report to find out the reason for the problem. Use the <u>Decryption</u>
 <u>Functionality</u> after resolving the problem.
- 2. All the files that have been received are named along a specific SOFiE rule. The standard is <<SOFIE.timestamp.Id Destinator>>. When the file has been deciphered, it will get a name according to the SOFiE Naming functions

Routing between your SOFiE Crypt client and your SOFiE Transport client

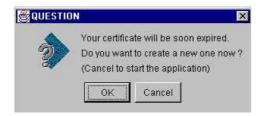
The routing between your SOFiE Crypt client and your SOFiE Transport client must be defined by you following your intern and security procedures.

In fact, the CSSF and BCL imposes that the encryption tool is separated of the sending tool and any vendor can sell a encryption tool with the direct connection with the sending tool.

Certificate expiration

1. Certificate has reached limit date and renewal was not requested

SOFiE detects that your certificate will soon expire (1 month), and asks if you want to renew your Certifiacte





will start the application

will Generate a new private/public key

2. Certificate expired

SOFiE detects that the certificate has expired.



will start the application, but you will not be able to encrypt and send any file

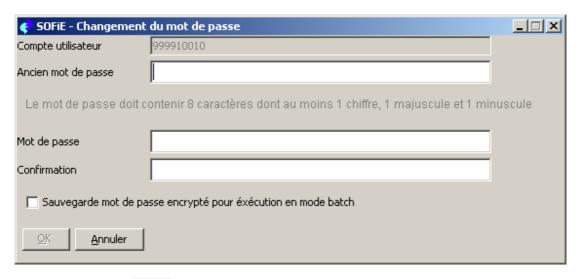
will either invite you to load a requested certificate, or to renew your certificate

Change password

It is recommended that you change your password regularly.

If you think that someone else was able to access your password, modify it immediately.

1. After starting the application, choose the option Change Password

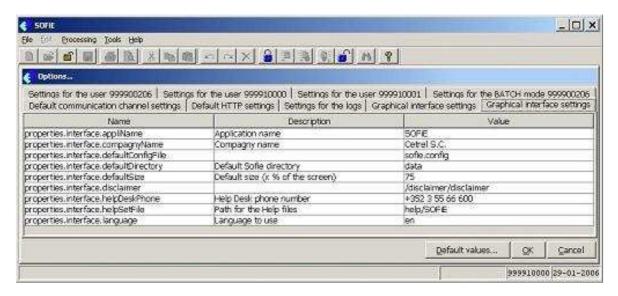


2. Fill in and confirm with your new Password.

Options

1. Options - Gui Settings

Choose on the Tools Menu, the Options

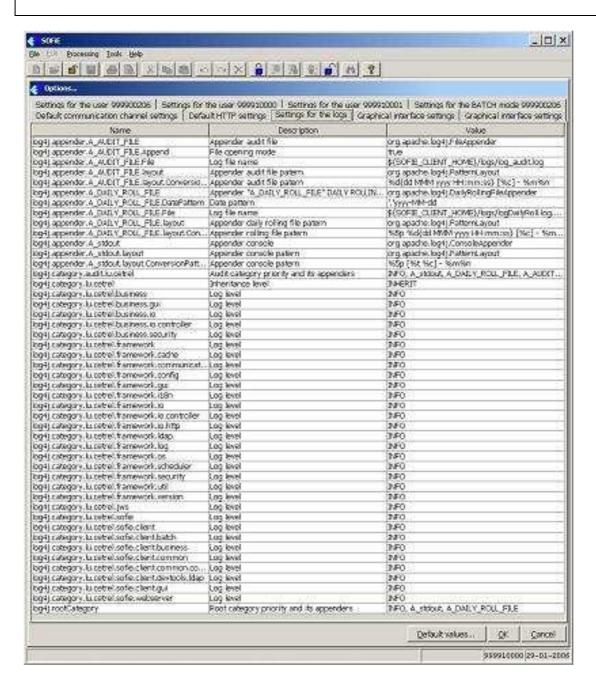


!!!!If you have any doubt concerning the correct understanding of a property, don't hesitate to contact CETREL!!!!

2. Options - Log Settings

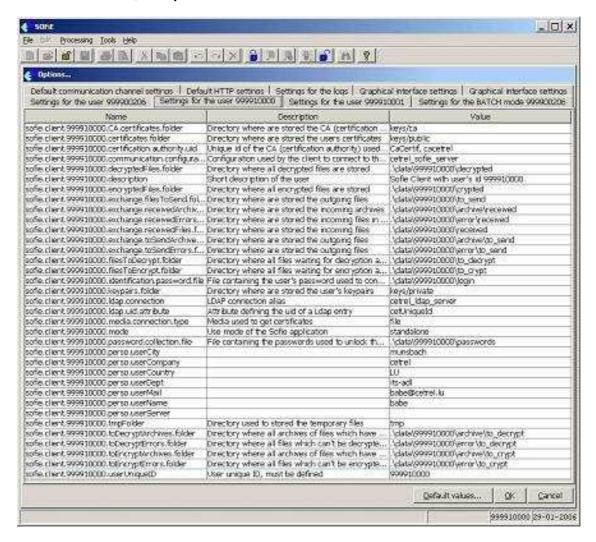
Choose on the Tools Menu, the Options

!!!!You should have good knowledge of the LOG4J tool, if you want to change the configuration for the log management. Contact CETREL in case you have special needs!



3. Options - Users Settings

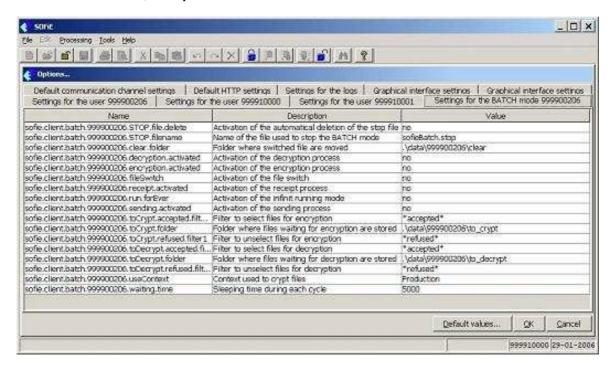
Choose on the Tools Menu, the Options



!!!!If you have any doubt concerning the correct understanding of a property, don't hesitate to contact CETREL!!!!

4. Options - Batch Settings

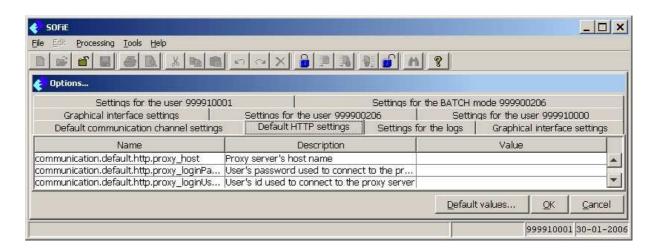
Choose on the Tools Menu, the Options



!!!!If you have any doubt concerning the correct understanding of a property, don't hesitate to contact CETREL!!!!

5. Options - HTTP Settings

Choose on the Tools Menu, the Options



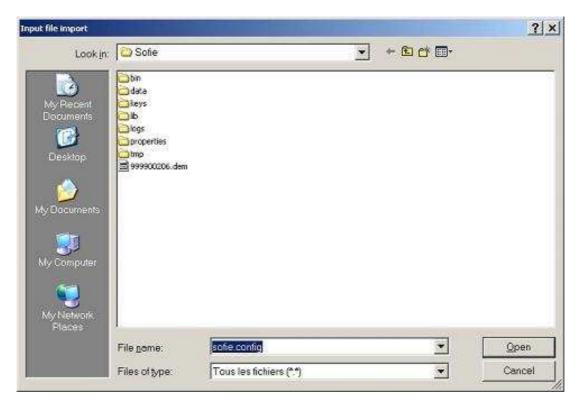
Input file import

In standalone mode, a set of configuration parameters allow you to configure SOFiE in order to use the encryption functionality (certificates).

CETREL put in place a simple way to allow you to change the configuration. In the case (key renewal of your destinator, change of your contract,), your configuration has to be changed, CETREL automatically sends you a new configuration file.

The file is sent by mail, and mentions all the steps you have to execute.

1. Select the configuration file SOFIE.CONFIG



2. SOFiE imports the file and updates your configuration

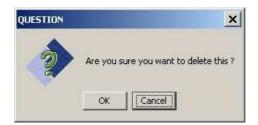
Cancel Certificate Request

As already mentioned, SOFiE manages the status of your user (refer to Login).

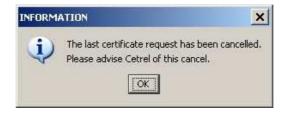
If you did launch a Certificate Request using the Key Renewal function, you can cancel the certificate requestion.

Choose in the tools menu the "Cancel Certificate Request" option.

SOFiE asks you to confirm



After confirming, please contact the **CA-Cetrel** as requested

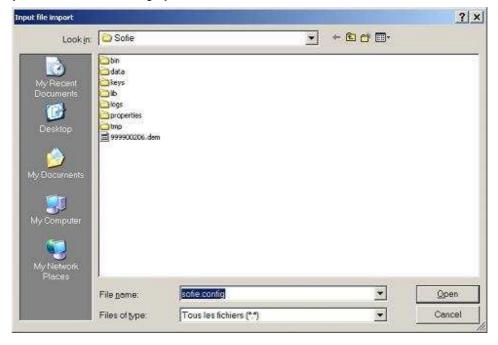


User Configuration File Input

The usage of this function may be useful in two circumstances:

- You have been renewing your key and when logging to SOFiE you did not yet have received your sofie.config file or you asked SOFiE to continue logging in. Now you want to finalize your key renewal by importing the new certificate, included in the new sofie.config file.
- You are working in non-LDAP or stand-alone mode and some modification of your interaction with other SOFiE participants has changed. Cetrel is sending you a new sofie.config file. You have to import this file as soon as possible. Otherwise it may be possible that your next sending of files may cause problems (at the destinator).

When using on the tools menu the user configuration file input, SOFiE requests you to confirm the location of the sofie.config file you have been receiving by mail from Cetrel.



!!! We highly recommend you to install as soon as possible any sofie.config file, Cetrel is sending you.

The non-installation may have impacts on your next file transfer.

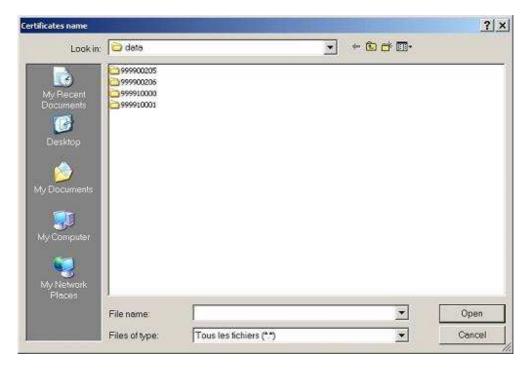
Cetrel may not me hold responsible for any damage if you do not following this instruction!!!

Import Certificates

This function allows you to import new root Certificates form the Cetrel Certification Authority.

The new root Certificate of CA-Cetrel has been sent by mail or is awailable on www.cetrel.lu

When using on the tools menu the option "Import Certificates",



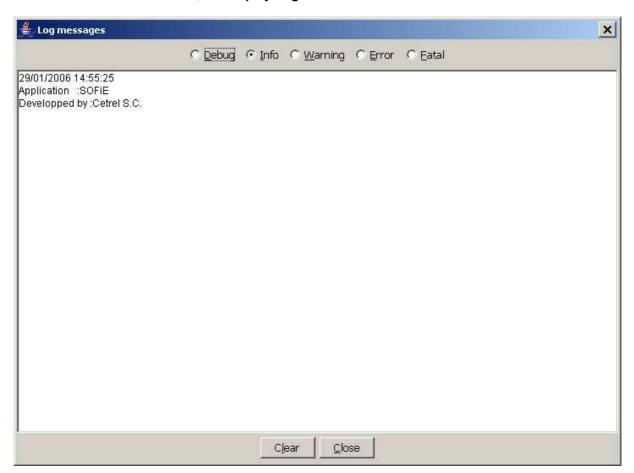
Use the import function and select the file containing the certificate

Logs

1. Technical Log

SOFiE manages a log, where all the errors/warnings generated by the program are saved. The log can be accessed either by the GUI or directly by a Text editor in the directory ...\logs\.

1. Choose on the **Tools** Menu, the **Display Log Console**



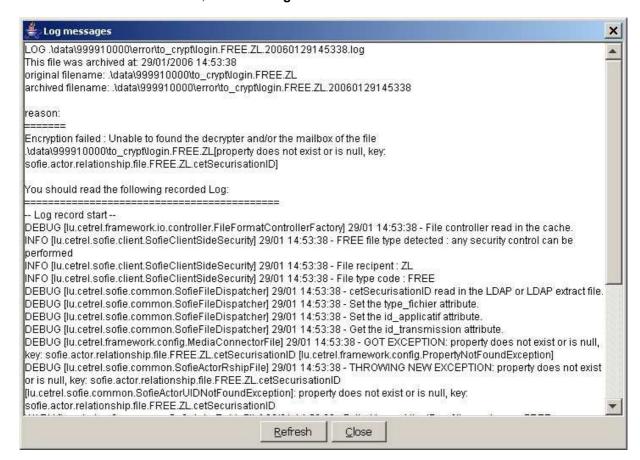
- 2. You can change the type of messages, that the Log Console attaches, by selecting the desired **Message Level** .
- 3. With Clear you can reinitialize the Log console

2. Audit Log

SOFiE manages a special log, which traces for you all the file exchanges that occur.

The log can be accessed either by the GUI or directly by a Text editor in the directory ...\logs\log_audit.

1. Choose on the Tools Menu, the Audit Log



3. The log files

SOFiE uses the LOG4J utility to generate and organize logging. It is possible to configure the logging according to specific needs. Such an action should only be done in collaboration with CETREL S.C.

Different levels for logs are generated according to the properties settings.

Log level	Explanation
« debug »	Detailled information of the processing
	• Is normally used in development, testing or problem resolution to find and
	resolve a particular problem in the processing

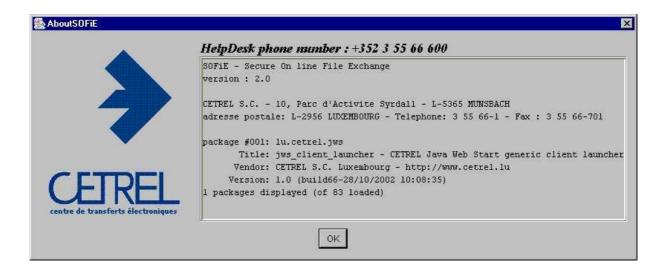
« info »	Synthetic information about the processing	
	Informs that a praticular step in the processing has been executed	
	Is normally used to have an overview of the processing	
« warn »	 Information that the application got an error that does however not make any doubt about the correct processing. 	
	The message should be investigated to find the precise reason	
« error »	An error occured, but the application continues to work	
« fatal »	Critical error message that normaly ends up in stopping the application	

Differents logs are produced in the directory ..\cetrel\sofie\logs.

!!!! We recommend that you backup the log regularly. It can be used as a tracing tool for all your activities. It could be useful if you are at odds with another participant about a file exchange.!!!!

About

The About screen gives you a reference of all the program modules, which are installed for SOFiE



Batch mode

The functions of SOFiE can also be integrated into an automated working environment, as it is often necessary for files that are processed in an automatical way by external systems.

To work in an automated way, SOFiE has created during your <u>first Login</u> the basics for the Batch mode usage. In batch mode, you can only access to non-interactive functions, being the emission/receipt and the receive/decryption functions.

These basics consist in creating a script, putting your passwords in a securized file, and creating a properties file, that can be modified by the <u>User Batch Settings</u>.

The script is located in the ...\bin directory, and is names run_batch_participant ID.bat

1. Batch execution using the config file

To existe the batch mode in this form, start the run_batch_userid.bat/ksh script.

It will execute SOFiE using the batch.config file.

Description of the batch.config file		
sofie.client.batch.999910003.useContext=Production		
Context used for encrypting files (Production or Test). After decryption, the required		
directories are created automatically and files stores according to the context. sofie.client.batch.999910003.STOP.filename=sofieBatch.stop		
Name of the file that indicates to SOFiE to stop the processing.		
sofie.client.batch.999910003.toDecrypt.refused.filter1=*refused		
Filter of files that are refused for decryption		
sofie.client.batch.999910003.receipt.activated=yes		
Activate the receipt of files		
sofie.client.batch.999910003.encryption.activated=yes		
Activate the encryption of files		
sofie.client.batch.999910003.decryption.activated=yes		
Activate the decryption of files		
sofie.client.batch.999910003.waiting.time=5000		
Waiting time (milliseconds) in the processing		
sofie.client.batch.999910003.fileSwitch=no		
Activation of fileswitch		
sofie.client.batch.999910003.toCrypt.folder=\\cetrel\\sofie\\data\\999910003\\to_crypt		
Directory containing the files that are encrypted and sent		
sofie.client.batch.999910003.toDecrypt.folder=\cetrel\\sofie\\data\\999910003\\to_decrypt		
Directory containing the files to decrypt		

sofie.client.batch.999910003.clear.folder=\\cetrel\\sofie\\data\\999910003\\clear
Directory containing files that are not treated by the batch (if fileswitch activated)
sofie.client.batch.999910003.toCrypt.refused.filter1=*refused*
Filter of refused files to be encrypted
sofie.client.batch.999910003.STOP.file.delete=yes
Flag indicating the deletion of the stopping file for the batch mode
sofie.client.batch.999910003.toDecrypt.accepted.filter1=SOFI.*
Filter of files accepted for decryption
sofie.client.batch.999910003.run.forEver=yes
Flag for activating/deactivating the processing of the batch
sofie.client.batch.999910003.toCrypt.accepted.filter1=*.*
Filter of files accepted for encryption
sofie.client.batch.999910003.sending.activated=yes
Activation fla for the sending of encrypted files

Remarks: This form of using the batch mode allows the automatic synchronization of your SOFIE software with the reference at Cetrel.

The first time the complete SOFIE executables are downloaded. Afterwards, only upgraded modules are loaded.

2. Manual batch execution

To execute the batch mode, start SOFiE using the _run lu.cetrel.sofie.client.SofieMain #options# command. The options that can be given are:

Parameter	Possible Values	Default	Description
-mode	gui batch	gui	execution mode
-user	your Userid		profile that has to be used to execute the batch
-file	filename		name of the file that has to be treated
-e			Encrypt
-S			Send file
-d			Decrypt file
-ctx	Production Test		

One of the 3 actions must be indicated.

Remember the following rules:

- you can only encrypt files that have not been encrypted by SOFiE before
- · you can only send files that have been encrypted
- you can only decrypt files that have been encrypted before

In all cases, SOFiE searches the default folder you indicated in your <u>Properties</u> for other files to treat and acts according to the configured parameters.

Ex.:

run_batch -mode batch -user cm0252

--> will launch SOFiE and treat all the files you put in the configured directories

run_batch -mode batch -user cm0252 -e simple_file.FREE.99990003

--> will launch SOFiE and encrypt the file simple_file.FREE.99990003 with the private key of cm0252 and the certificate of 99990003. The resulting file will be named SOFIE.timestamp.99990003 and must be transmitted to the destinator.

run batch -mode batch -user cm0252 -d SOFI.200212091211001.cm0252

--> will launch SOFiE and decrypt the file SOFI.200212091211001.cm0252 as far and the private key of cm0252 corresponds to the certificate that has been used by the sender to encrypt the file. The resulting file will be named according to the original name, or if a special naming convention has been implemented for the user cm0252.

Remark: This form of using the batch mode allows the automatic synchronization of your SOFiE software with the reference at Cetrel.

The first time the complete SOFIE executables are downloaded. Afterwards, only upgraded modules are loaded.

3. Tracking the batch processing using the return code

Also in batch mode, SOFiE is generating messages that are put in the same log as the user-interface execution.

When stopping, SOFiE is returning a system code, indicating whether file(s) have been treated without errors. The values of the return code are:

- 0 if no error occurs
- the number of files in error

Specific reports concerning the processing of each file can be found in the Userla\text{derror}\text{....} Directories.

They are the equivalent of the Emission/Receive Report.

4. Tracking the batch processing using the Audit Log

The audit log (...\logs\log_audit.log) contains all the information that allows a tracking of the processing of SOFIE.

The explanation of the different messages are:

<<

24 mars 2005 13:02:33 [audit.lu.cetrel.sofie.client.SofieClientSideCommunication] - 0 files available on server for user login: 999910003 :

>>

No file was available on the server for the requesting user

<<

25 mars 2005 09:57:36 [audit.lu.cetrel.sofie.client.SofieClientSideCommunication] - 1 files available on server for user login: 999910003 : SOFI.05032508402466.999910003
25 mars 2005 09:57:37 [audit.lu.cetrel.sofie.client.SofieClientSideCommunication] - < < received file: SOFI.05032508402466.999910003 (acknowledgement sent), login: 999910003, size: 7135 bytes, saved as: \cetrel\sofie\data\999910003\received\SOFI.05032508402466.999910003
25 mars 2005 09:57:37 [audit.lu.cetrel.sofie.client.SofieClientSideCommunication] - < SOFiE file name = SOFI.05032508402466.999910003 - Original file name = RLAE.2005032527083801.999910003

SOFiE received an information from the server that there is one file available SOFiE receives the file from the server and saves it on the platform

SOFiE verifies the file and saves it it's final form on the server

<<

6 avr. 2005 11:51:04 [audit.lu.cetrel.sofie.client.SofieClientSideCommunication] - >> SOFiE file name = SOFI.05040611505280.999910003 - Original file name = SNOCS.DTA
06 avr. 2005 11:51:05 [audit.lu.cetrel.sofie.client.SofieClientSideCommunication] - >> sent to:
cetrel_sofie_server, login: 999910003, file:
\cetrel\sofie\data\999910003\to_send\SOFI.05040611505280.999910003, size: 21122 bytes
>>

SOFIE has detected a file to encrypt and send SOFIE has encrypted and sent the file

Useful information

Sending	After sending, the files are not deleted in the original directory	
Receiving	You must delete yourself the files from the receiving directory. Otherwise SOFiE may not be able to receive another file containing the same name	
Multiple users/install ations	You need to install SOFiE once on a computer. You may declare multiple users on the same computer, with the same SOFiE installation	
Backup	Informations in these directories must be backed up regularly \data\user1*.* \keys**.* \logs*.*	
Status	The status of every user is maintained and is a basis for SOFiE to manage the different configuration steps the user has to fulfill before accessing to the de/encryption and sending/receiving functions. SOFiE distinguishes: User not declared User in configuration process Certificate has reached limit date and renewal was not requested New Certificate was requested Certificate expired User defined and certificate valid	

1. Packages

SOFiE integrates (refer to the SOFiE Architecture) a certain intelligence for recognizing, validating and naming files.

Before version 2.5 of SOFiE, this functionality was attached to the concept of file type. Indeed, to every file type, SOFiE attached a required naming convention for the sender, a required format of the content of the file and finally used a defined naming convention for the receiver.

The main idea behind this function is, according to the requirements of the receiver given to Cetrel, to refuse invalid files at the sender's premises. Thus avoiding the unnecessary phone calls and retrials.

In the end, SOFiE had to support plenty of file types, and it became difficult to maintain a good understanding of them all.

Beginning with version 2.5. SOFiE is bundling the multiple file types into packages. So a package:

- is a particular service, the SOFiE participant is subscribing in his contract
- is a particular service that may be billed (refer to the official price list)
- is a particular service, allowing the exchange of files between defined participants (Closed User Group)
- is a particular service, where only defined file types may be exchanged

A list of all the packages and a detailled description of all the packages is awailable at Cetrel.

2. Standalone/Connected mode

The concept of the standalone/connected mode has been introduced to respond to very high security needs that may occur.

It may happen that the data you want to exchange with another SOFiE participant is located in a very highly secured environment. This environment is even not connected to a network.

Nevertheless in certain cases you have to exchange data with someone else. Using a standalone installation or combining it with the SOFiE's routing concept, you can nevertheless exchange data with other people in confidence.

In the standalone mode, the functions needing a network connection are de-activated, and are replaced by manual functions.

	Standalone	Connected	
Installation	Same installation process		
Version synchronization	Synchronized to a local reference version> no automatic version update	Synchronization is done to the reference version at CETREL	

Configuration	No access to the Webserver No access to the LDAP> Requires the import of configuration date (Input file import)	Access to the Webserver Access to the LDAP
Send/Receive	Not possible> only encryption/decryption	Possible
Certificate	Certificate request is saved as a file and sent to CA-CETREL by another station	Automatic sending of certificate request
Exchange of data	data is not exchanged by network, but by another medium (diskette)	Date is exchange via the network (send, receive)
Input file import	Imports your certificate, certificates of your destinators and configuration file to define your destinator	Imports only your certificate, as other informations are on the LDAP

!!!!! It is recommended to use the standalone mode only for special purpose!!!!!

3. Change the mode

You can change the mode, but you must respect the procedure, otherwise your installation will no longer work.

Change from standalone to connected mode

- 1. Contact CETREL and proceed to a change of contract
- 2. Modify the parameter in the options
- 3. Verify that you are connected to a network

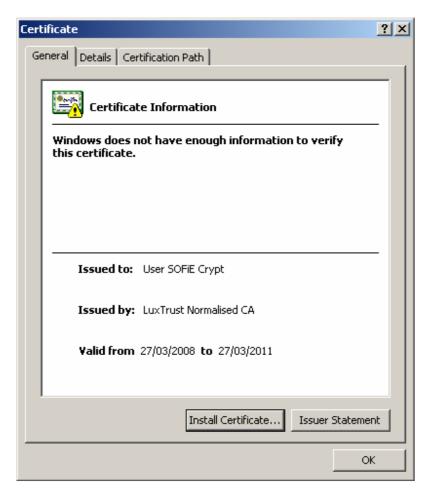
Change from connected mode to standalone

- 4. Contact CETREL and proceed to a change of contract
- 5. Modify the parameter in the options
- 6. You will receive from CETREL a mail, giving your configuration file. Use the input file import functionality.
- 7. SOFiE will no longer give you access to the send/receive function.

4. Verify Certificates

To verify if Certificates delivered by LuxTrust are really delivered by LuxTrust, you can verify the contents of a certificate.

Double-click on the Certificate file



Attach the **Details** and choose the **Fingerprint contents**

