



# FSB-COMPLIANT KEYS AND CERTIFICATES MANAGEMENT: PRACTICAL GUIDELINES

## Table of Content

<b>1</b>	<b>Context and objectives</b>	<b>3</b>
<b>2</b>	<b>Procedures and tools</b>	<b>4</b>
<b>2.1</b>	<b>Workstation preparation: install openssl and Keystore explorer</b>	<b>4</b>
2.1.1	OpenSSL for Windows	4
2.1.2	OpenSSL for Linux	4
2.1.3	Keystore explorer installation	5
<b>2.2</b>	<b>Generate the CSR</b>	<b>6</b>
<b>2.3</b>	<b>Send the CSR files to fsb@bosa.fgov.be</b>	<b>6</b>
<b>2.4</b>	<b>After receiving the key files</b>	<b>8</b>
<b>2.5</b>	<b>After receiving the key files</b>	<b>8</b>

# 1 Context and objectives

In order to meet the required level of security, the Federal Service Bus (FSB), just like in other technologies, requires its consumers to sign their messages. Signing message requires using a private key and associated certificate(s). Managing this technical layer is the responsibility of the consumer. Since keys and certificates are in used in many IT domains, they usually have directives, procedures and tools in place to manage this. However, (1°) sometimes these directives, procedures and tools may not be designed to encompass message signing, and (2°) even if they do, they may fail to support some FSB-specific detailed specifications.

Consequently, the FSB team decided to produce the current document. It provides practical instructions how to:

1. Prepare a workstation (install openssl)
2. generate an fsb-compliant key and a certificate signing request (CSR)
3. send the CSR to the FSB team for production of the certificate
4. once you have received the certificate, link it to the private key
5. create an java Keystore (JKS)
6. properly store the key pair and all necessary certificates into the JKS
7. perform an end-to-end test

Remarks:

- The target audience of this document are (a) the technical operators in charge of the management of the keypair, (b) the operators in charge of running the application servers, and (c) their managers. They are supposed to know the principles of public and private keys and to be experienced with the use of the related technology.
- This document provides practical instructions how to proceed, based on existing freeware tools. It must be understood as purely informative. It is the responsibility of the service consumer team to decide to follow them strictly, to adapt them, or to meet other practices.
- We assume that the service consumer is a java application. In other situations, several aspects of the process may need to be altered (eg other keystore format).
- Users of this document are invited to send questions, issue remarks and improvement suggestions to this document.

## 2 Procedures and tools

### 2.1 Workstation preparation: install openssl and Keystore explorer

#### 2.1.1 OpenSSL for Windows

Go to <http://slproweb.com/products/Win32OpenSSL.html>

1. Download the release relative to your machine configuration. Run the installer and accept default settings

File	Type	Description
<a href="#">Win64 OpenSSL v3.0.5 Light EXE   MSI</a>	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.0.5 (Recommended for users by the creators of <a href="#">OpenSSL</a> ). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
<a href="#">Win64 OpenSSL v3.0.5 EXE   MSI</a>	140MB Installer	Installs Win64 OpenSSL v3.0.5 (Recommended for software developers by the creators of <a href="#">OpenSSL</a> ). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
<a href="#">Win32 OpenSSL v3.0.5 Light EXE   MSI</a>	4MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v3.0.5 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
<a href="#">Win32 OpenSSL v3.0.5 EXE   MSI</a>	116MB Installer	Installs Win32 OpenSSL v3.0.5 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

further instructions assume OpenSSL is installed in C:\OpenSSL

2. Add C:\OpenSSL\bin to your system path (Control Panel, System, Advanced, Environment Variables, System Variables) - this isn't strictly necessary but it makes things a lot easier.

3. Create a working directory - here, we will use c:\ssl as our working folder.

Note: If your are using the .net environment, MMC certificate snap-in(mcc.exe) can be used instead of OpenSSL

More info on : <https://knowledge.digicert.com/solution/SO29005.html>

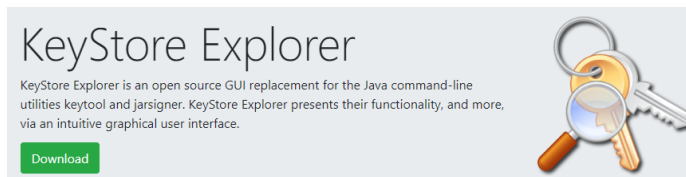
For .net consumers that want to use SOAP UI, export the key-pair from mmc.exe to a pkcs12 format.

#### 2.1.2 OpenSSL for Linux

Open SSL is shipped with most LINUX distributions Open SSL.

## 2.1.3 Keystore explorer installation

Go to <http://keystore-explorer.sourceforge.net> and download the right version for your platform



Install the tool. Follow the screen, no special configuration needed.

## 2.2 Generate the CSR

<OrganisationProject> is your Organisation & project name (Example fedorest-invoiceSys)

```
set openssl_conf=Drive:\...\openssl-1.1.1d-win64\openssl.cfg
```





```
// for INT environment
```

```
openssl req -new -newkey rsa:4096 -nodes -out <OrganisationProject>-test.bosa.be.csr -
keyout <OrganisationProject>-test.bosa.be.key -subj "/C=BE/ST=Brussel/L=Brussel/O=FOD
BOSA/CN=<OrganisationProject>-test.bosa.be"
```

```
// for PRD environment
```

```
openssl req -new -newkey rsa:4096 -nodes -out <OrganisationProject>.bosa.be.csr -keyout
<OrganisationProject>.bosa.be.key -subj "/C=BE/ST=Brussel/L=Brussel/O=FOD
BOSA//CN=<OrganisationProject>.bosa.be"
```

output:

 OrganisationProject.bosa.be	13/09/2022 13:59	CSR File	2 KB
 OrganisationProject.bosa.be	13/09/2022 13:59	KEY File	4 KB
 OrganisationProject-test.bosa.be	13/09/2022 13:35	CSR File	2 KB
 OrganisationProject-test.bosa.be	13/09/2022 13:35	KEY File	4 KB

It will generate 2 private key files and 2 CRS files. Store the .key files on a secure place.

If these files are compromised, you will need to restart the process.

## 2.3 Send the CSR files to [fsb@bosa.fgov.be](mailto:fsb@bosa.fgov.be)

Send the generated CSR (Certificate Signing Request) to [fsb@bosa.fgov.be](mailto:fsb@bosa.fgov.be) together with the required certificate request form(s) and the certificate requestor form.

Read more on:

<https://dtservices.bosa.be/nl/services/service-integrator-fsb/ik-wil-aansluiten>

<https://dtservices.bosa.be/fr/services/service-integrator-fsb/je-veux-me-connecter>

**Mail template for a Certificate request::**

to [fsb@bosa.fgov.be](mailto:fsb@bosa.fgov.be)

subject: CSR files to access FSB Services for <Your organization> for the environment INT/PRD

Dear,

As a consumer for FSB services, I would like to receive certificates for INT and PR.

In attachment you will find the 2 **Certificate Signing Request** files performed.

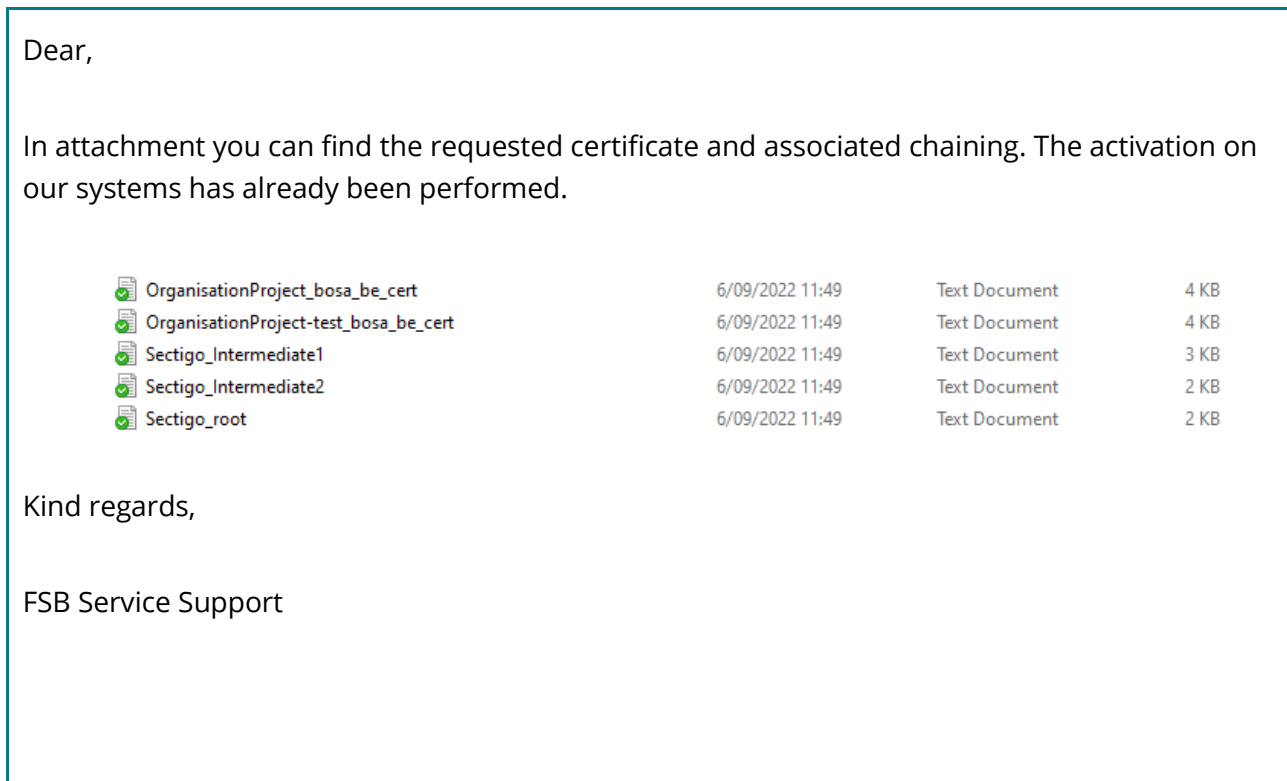
 OrganisationProject.bosa.be	27/06/2022 13:39	CSR File	2 KB
 OrganisationProject-test.bosa.be	27/06/2022 13:39	CSR File	2 KB

Kind regards,

<contact info>

## 2.4 Requested certificate and associated chaining

As answer you will receive the requested certificates via mail:



Rename the files with the relevant **.crt** extension (The files attached to the eMail have **.txt** extension to prevent your email server to block the attachments):

- OrganisationProject-test.bosa.be.**.crt**
- OrganisationProject.bosa.be.**.crt**

## 2.5 After receiving the certificate files, link the certificate to the private key

Link the certificate to the private key:

**Remark :** The tool will ask you for a password, type a strengthened password and store it safely for later use in step 2.7.



**// for INT environment**

```
openssl pkcs12 -export -out <OrganisationProject>-test.bosa.be.pkcs12 -inkey
<OrganisationProject>-test.bosa.be.key -in <OrganisationProject>-test.bosa.be.crt
```

**// for PRD environment**

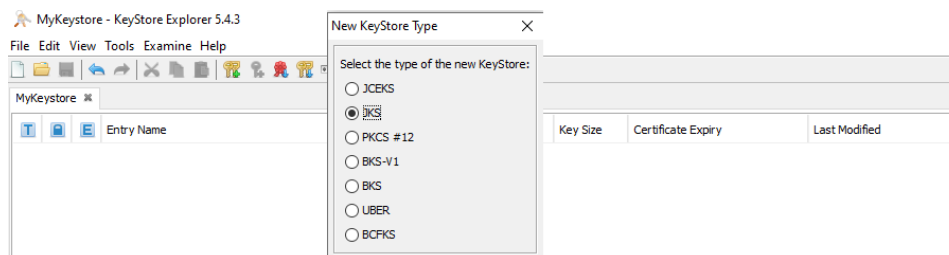
```
openssl pkcs12 -export -out <OrganisationProject>.bosa.be.pkcs12 -inkey
<OrganisationProject>.bosa.be.key -in <OrganisationProject>.bosa.be.crt
```

\*.pkcs12 will be created : (example for INT environment)

OrganisationProject-test.bosa.be	4/07/2022 14:45	Security Certificate	4 KB
OrganisationProject-test.bosa.be	27/06/2022 13:39	CSR File	2 KB
OrganisationProject-test.bosa.be	27/06/2022 13:39	KEY File	4 KB
OrganisationProject-test.bosa.be.pkcs12	13/09/2022 14:36	PKCS12 File	5 KB

## 2.6 Creating a keystore

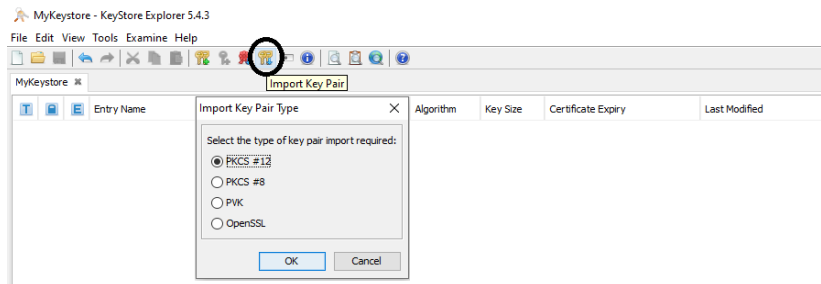
Start the Keystore Explorer application. Create a password protected keystore file of the type "JKS"



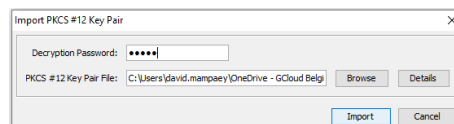
## 2.7 Store the key pair and all necessary certificates into the JKS

The process is almost complete. You still need to (1°) import the key pair, and (2°) append chaining certificates. The following instructions drive you into these last steps.

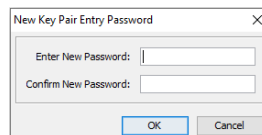
- Keystore explorer now asks you to select a type for the key pair to be imported. Accept default (PKCS #12) :



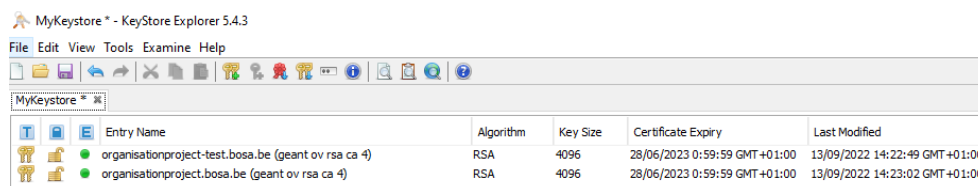
- Browse to your working directory, select **OrganisationProject-test.bosa.be.pkcs12** In the field "Decryption Password", Type the password you used when generating it (see step 2.5)



- This password is used by the keystore to use .pkcs12, the keystore will protect the keypair with a new password, please feel free to use the same password, and store it safely for later use in the application configuration files and/or further certificates maintenance duties using the keystore.



- Result: (in this case the INT and PRD certificate pair is stored in the same keystore.)



- Optional: It is possible to append the certificate chain to the keypair in the keystore. This is not required because the FSB uses its own copy of the certificate chain to validate incoming requests.

## 2.8 Perform an end to end test

In order to control that applications on your server are able to properly use this security infrastructure, you can perform a test with the securedEchoService – or ask to your application team to do so, if this falls out of your scope of responsibility.

The securedEchoService is a simple service exposed by the fsb to allow service consumers to control that the basic secure connectivity is OK. The test consists in issuing a request from the server, and controlling the response.

All additional information and resources required to perform the test can be found at the

<https://dtservices.bosa.be/nl/services/service-integrator-fsb/catalogue-service-integrator/utilityservices-s137/documentatie>

<https://dtservices.bosa.be/fr/services/service-integrator-fsb/catalogue-service-integrator/utilityservices-s137/documentation>

Once this step is completed, you are certain that the security is properly set up. You can move on to the development of your application.

Samples of service requests are available upon request in the project format of SOAPUI. Contact BOSA DGDT via [fsb@bosa.fgov.be](mailto:fsb@bosa.fgov.be).