

ECB - Public

# TABLE OF CONTENTS

1.	Introduction	5
2.	The ESCB-PKI Certification Authorities	6
3.	Importing an ESCB-PKI standard certificate	7
4.	Verifying the certificate installation	12
5.	Exporting an ESCB-PKI standard certificate	14
6.	Changing the password of a .P12 or .PFX file	19

Project name:	ESCB-PKI
Author:	ESCB-PKI team
File name:	ESCB-PKI - Import Export Standard Certificates v 2.0.docx
Version:	2.0
Date of issue:	11.09.2018
Status:	First version
Approved by:	
Distribution:	

### **RELEASE NOTES**

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	Status	Date of issue	Revisions
0.1	Draft	07.10.2011	Initial version.
1.0	Draft	05.11.2011	BdE Revision
1.1	Draft	25.11.2011	BdE Revision
2.0	Final	11.09.2018	BdE Revision

### 1. INTRODUCTION

ESCB-PKI standard certificates are software-based certificate, that is to say, the certificate and the corresponding private key has been delivered in a password-protected file (software keystore).

The format for this type of files is based on the PKCS#12 standard, and they have the extensions **.p12** or **.pfx** (they are equivalent)

This guide describes how to import into a MS Windows user account<sup>1</sup> an ESCB-PKI standard certificate from a password-protected file. Moreover, the guide describes the reverse operation: how to generate a password-protected file from an ESCB-PKI standard certificate and the corresponding private key that are installed in a MS Windows user account. Finally, the guide explains how to change the password of a password-protected file.

The screen shots are included only as a reference. Depending on the operating system version and web browser configuration used, the real screens could be slightly different.

**Note**: The last version of this document can be found in the Support tab of the ESCB-PKI Website, along with other ESCB-PKI guides and manuals.

<sup>&</sup>lt;sup>1</sup> Certificates that are installed in a MS Windows user account are also handled by the MS Internet Explorer browser.

## 2. THE ESCB-PKI CERTIFICATION AUTHORITIES

The ESCB Public Key Infrastructure is based on the following certificate chain:



#### Where:

- **Root CA**: is the first-level Certification Authority. This CA only issues certificates for itself and its Subordinate CA.

- **Online CA**: this second-level Certification Authority is subordinate to the Root CA. It is responsible for issuing certificates for the ESCB-PKI end entities.

- End entities: they are the ESCB-PKI users that hold one or several digital certificates.

Before using any ESCB-PKI certificate, it is required to install the root and subordinate CA certificates; otherwise the computer will not trust the certificate.

**Therefore:** before importing or exporting an ESCB-PKI standard certificate, please follow the required user guide to install the ESCB-PKI Certification Authorities.

### 3. IMPORTING AN ESCB-PKI STANDARD CERTIFICATE

This section describes the steps necessary to import into a MS Windows user account an ESCB-PKI standard certificate (and its corresponding private key) from a password-protected .p12 or .pfx file.

- Double-click on the .p12 or .pfx file (e.g. certificate.p12 or certificate.pfx). The Certificate Import Wizard will be started:

Certificate Import Wizard	
	Welcome to the Certificate Import Wizard
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
4	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	To continue, click Next.
	< Back Next > Cancel

- Press Next. The file path will be displayed for confirmation:

Certificate Import Wizard		
File to Import		
Specify the file you want to import.		
File name:		
C:\certificates\certificate.p12 Browse		
Note: More than one certificate can be stored in a single file in the following formats:		
Personal Information Exchange- PKCS #12 (.PFX,.P12)		
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)		
Microsoft Serialized Certificate Store (.SST)		
Learn more about <u>certificate file formats</u>		
< Back Next > Cancel		

- Press Next. You will see the following screen:

Certificate Import Wizard
Password To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
•••••
<ul> <li>Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.</li> <li>Mark this key as exportable. This will allow you to back up or transport your keys at a later time.</li> <li>Include all extended properties.</li> <li>Learn more about protecting private keys</li> </ul>
<pre>&lt; Back Next &gt; Cancel</pre>

- Type the password of the .p12 o .pfx file.

- Check the option "Enable strong private key protection" to protect the copy of the private key that is going to be installed in the MS Windows account.

- Check the option "Mark this key as exportable" if you want that the copy of the private key that is going to be installed in the MS Windows account is ready to be exported again in the future to a new .p12 or .pfx file.

- The option "Include all extended properties" is not relevant and could be not available depending on the operating system version and configuration.

- Press Next. If you have typed a wrong password, the following message will appear:

Certificate In	nport Wizard 📃	x
8	The password you entered is incorrect.	
	ОК	

- Otherwise, select the "Personal" certificate store to install the certificate and corresponding private key:



- Press Next. The following confirmation screen will be displayed:

Certificate Import Wizard		
	Completing the Certificate Import Wizard The certificate will be imported after you click Finish.	
	You have specified the follo Certificate Store Selected Content File Name	wing settings: by User Personal PFX C:\certificates\certific
	۲ <u>ااا</u>	
	< <u>B</u> ack	Finish Cancel

- Press Finish. You will see the following screen to confirm the installation of the private key:

Importing a new private exchange key		
	An application is creating a Protected item.	
	CryptoAPI Private Key	
	Security level set to Medium Set Security Level	
	OK Cancel Details	

- Press the "Set Security Level" button and select the High security level:

Choose a Security Level	
	Choose a security level appropriate for this item.
	High Request my permission with a password when this item is to be used.
	Medium Request my permission when this item is to be used.
	< Back Next > Cancel

- Choose a password to protect the private key once installed into your Windows account:

Create a password to	o protect this item.
Create a new passw Password for:	ord for this item. CryptoAPI Private Key
Password:	•••••

You will be asked for this password whenever you use the private key (e.g. while authenticating in an application). Do not mistake this password with the one of the password-protected file, although both can be the same if you wish.

- Press Finish and OK in the next screen. You will see the following message:



# 4. VERIFYING THE CERTIFICATE INSTALLATION

- Confirm that the certificate and private key have been successfully imported. For this, open the MS Internet Explorer browser:



- Select the menu Tools > Internet Options and click on the Content tab:

Internet Options
General Security Privacy Content Connections Programs Advanced
Parental Controls
Control the Internet content that can Be viewed.
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
🛞 Enable 🛞 Se <u>t</u> tings
Certificates
Use certificates for encrypted connections and identification.
Clear <u>S</u> SL state         Certificates         Publishers
AutoComplete
AutoComplete stores previous entries Settings on webpages and suggests matches for you.
Feeds and Web Slices
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.
OK Cancel Apply

- Press the Certificates button and ensure that the Personal tab is displayed:

Certificates							
I <u>n</u> te	nded pu	irpose: (	<all></all>				•
Pe	rsonal	Other Peopl	e Intermedia	te Certification A	uthorities T	rusted Root Certificatio	on 4 🕨
	Issued '	То	Issued B	у	Expiratio	. Friendly Name	
	E [AU	Ր։Տ] John Q.	S ESCB-PK	I ONLINE CA	21/11/201	4 CN=[AUT:S] Joh	
Ī	import	. Exp	ort	emove		Adva	anced
Ce	Certificate intended purposes						
Cli	Client Authentication, Any Purpose, Secure Email						
Lea	arn more	about <u>certif</u>	cates				ose

- Double-click on your certificate and confirm the most relevant information of the ESCB-PKI standard certificate and that "you have a private key that corresponds to this certificate":

Certificate				
General Details Certification Path				
Certificate Information				
Windows does not have enough information to verify this certificate.				
Issued to: [AUT:S] John Q. SMITH	_			
Issued by: ESCB-PKI ONLINE CA				
Valid from 21/ 11/ 2011 to 21/ 11/ 2014				
$\ref{eq:product}$ You have a private key that corresponds to this certificate.				
Issuer Statement				
Learn more about <u>certificates</u>				
	ОК			

### 5. EXPORTING AN ESCB-PKI STANDARD CERTIFICATE

This section describes the steps necessary to export an ESCB-PKI standard certificate that is installed in your MS Windows user account to a password-protected file. You can use this password-protected file as a backup copy of your certificate and associated private key.

- Open the MS Internet Explorer browser:



- Select the menu Tools > Internet Options and click on the Content tab:

Internet Options
General Security Privacy Content Connections Programs Advanced
Parental Controls
Control the Internet content that can Be viewed.
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
🛞 Enable 🔞 Settings
Certificates
Use certificates for encrypted connections and identification.
Clear <u>SSL</u> state <u>C</u> ertificates         Publishers
AutoComplete
AutoComplete stores previous entries Settings on webpages and suggests matches for you.
Feeds and Web Slices
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.
OK Cancel Apply

- Press the Certificates button and ensure that the Personal tab is displayed:

C	Certificates					
	I <u>n</u> tended p	urpose: <	All>			•
	Personal	Other People	Intermediate Certification	Authorities Tru	isted Root Certification	4 >
	Issued	То	Issued By	Expiratio	Friendly Name	
	E [AU	T:S] John Q. S.	ESCB-PKI ONLINE CA	. 21/11/2014	CN=[AUT:S] Joh	
	Import	Expor	Remove		Advar	nced
	Certificate intended purposes					
	Client Authentication, Any Purpose, Secure Email					
	Learn more about <u>certificates</u>				se	

- Select your ESCB-PKI standard certificate and press the Export button. The Certificate Export Wizard will be displayed:

Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard
Ģ	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
4	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	To continue, dick Next.
	< Back Next > Cancel

- Press Next and select the option "Yes, export the private key":

Certificate Export Wizard				
Export Private Key You can choose to export the private key with the certificate.				
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	÷			
Do you want to export the private key with the certificate?				
Yes, export the private key				
$\bigcirc$ No, do not export the private key				
Learn more about <u>exporting private keys</u>				
< Back Next > Ca	ncel			

In case that the "Yes, export the private key" option cannot be selected this is because either you have not got a private key associated to the certificate, or because the "mark this key as exportable" option was not selected when you installed the certificate in the past. In this case you will not be able to generate a password-protected file with your certificate and corresponding private key.

- Press Next and ensure that the "Personal Information Exchange – PKCS #12 (.PFX)" file format is selected in the following screen:

Certificate Export Wizard				
Export File Format Certificates can be exported in a variety of file formats.				
Select the format you want to use:				
DER encoded binary X.509 (.CER)				
Bage-64 encoded X.509 (.CER)				
Oryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)				
Include all certificates in the certification path if possible				
Personal Information Exchange - PKCS #12 (.PFX) Indude all certificates in the certification path if possible				
Delete the private key if the export is successful				
Export all extended properties				
Microsoft Serialized Certificate Store (.SST)				
Learn more about <u>certificate file formats</u>				
< <u>B</u> ack <u>N</u> ext > Cancel				

It is not necessary to select any of the options under the .PFX file format.

- Press Next and choose a password to protect the file:

Certificate Export Wizard				
Password To maintain security, you must protect the private key by using a password.				
Type and confirm a password.				
Password:				
•••••				
Type and confirm password (mandatory):				
•••••				
< <u>B</u> ack <u>N</u> ext > Cancel				

**Very important notice**: choose a strong password that is easy to remember. Take into account that you will need this password when you want to import your certificate and corresponding private key.

- Press Next and choose the path and name of the file that will be generated:

Certificate Export Wizard			
File to Export Specify the name of the file you want t	to export		
File name:			
C:\certificates\certificate.pfx	Browse		
	< Back Next > Cancel		
	< Back Next > Cancel		

- Press Next. The following confirmation screen will be displayed:

Certificate Export Wizard				
	Completing the Certificate Exp Wizard	port		
	You have successfully completed the Certificate wizard.	Export		
	You have specified the following settings:			
	File Name	C:\cert		
	Export Keys	Yes		
	Include all certificates in the certification path	No		
	File Format	Personi		
	< <u> </u>	ł		
	< Back Finish	Cancel		

- Press Finish. Since access to the private key is required to generate the file, in case that the private key is protected with a password you will be prompted for this password:

Exporting your private exchange key				
	An application is requesti	ng access to a Protected item.		
	Password for: CryptoAPI Private Key	Remember password		
	ОК	Cancel Details		

- Press OK. The following confirmation message will be shown:



- Confirm that the password-protected file (.PFX extension) has been generated in the directory you chose.

### 6. CHANGING THE PASSWORD OF A .P12 OR .PFX FILE

In case you want to change the password of a **.p12** or **.pfx** file containing an ESCB-PKI standard certificate and the corresponding private key, all you need to do is:

- First, import the **.p12** or **.pfx** file into your MS Windows account as described in section 3.

- Second, export the certificate and private key from your MS Windows account to a new **.pfx** file, as described in section 5.