BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

USER GUIDE:

IMPORTING AND EXPORTING STANDARD CERTIFICATES

VERSION 1.1

ECB-PUBLIC
24-Nov-2011

TABLE OF CONTENTS

1. Introduction 5
2. The ESCB-PKI Certification Authorities 5
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 1.1.docx
Version:	1.1
Date of issue:	26.11.2011
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

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[1] 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.

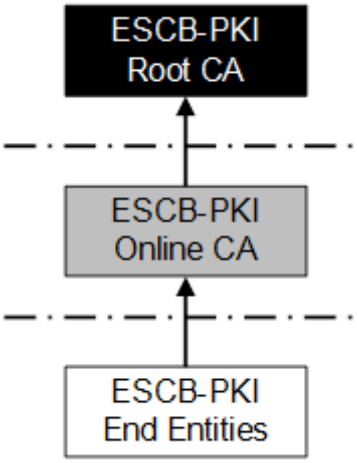
The screen shots are included only as a reference. Depending on the operating system version and web browser configuration used, the real screens could be slightly different.

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.

[1] 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.

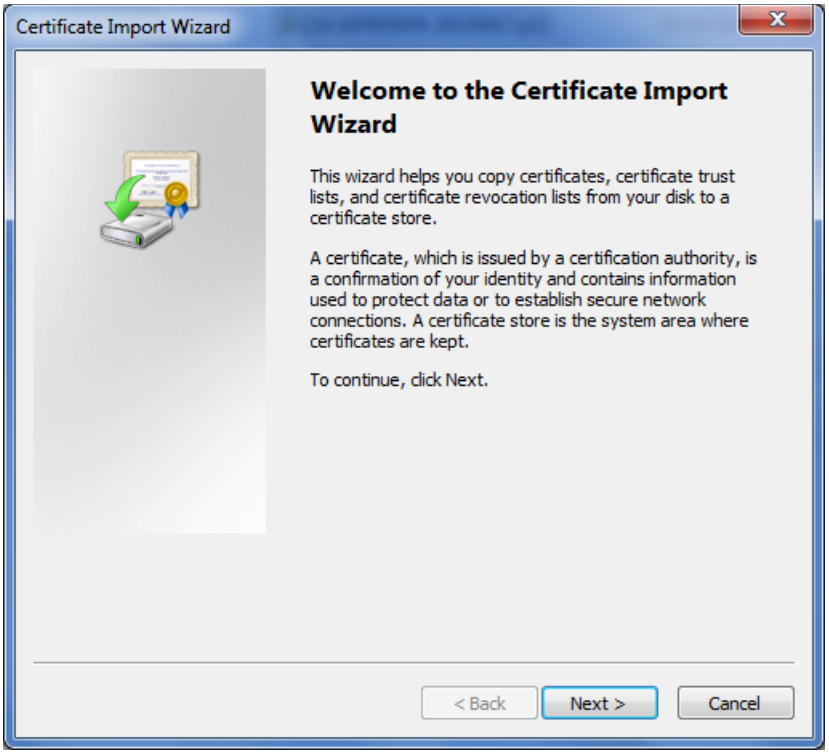
Before using any ESCB-PKI certificate, it is required to install the root and subordinate CA certificates; otherwise the computer will not trust the certificate.

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

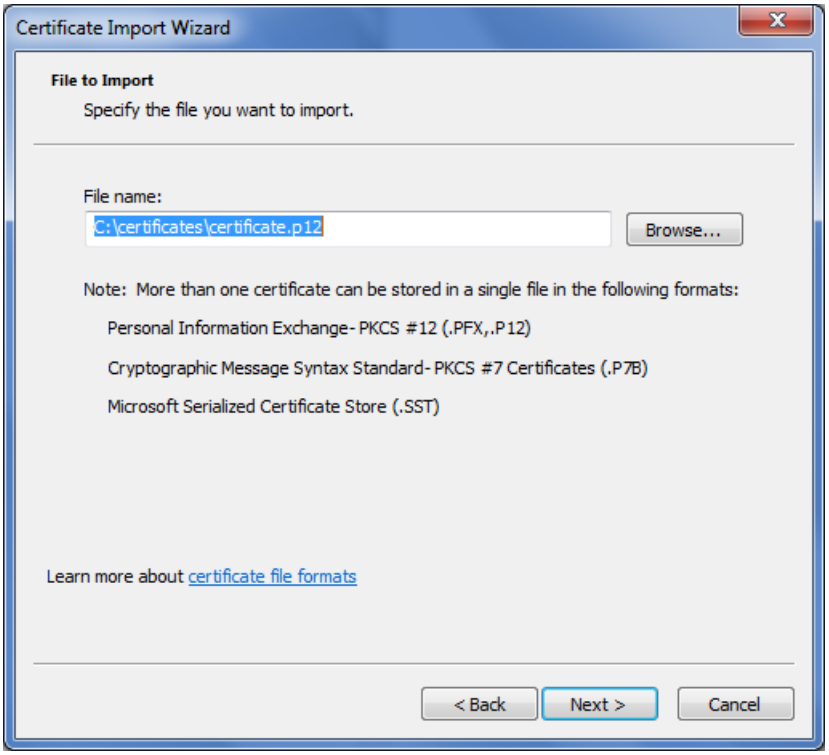
3. IMPORTING AN ESCB-PKI STANDARD CERTIFICATE

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.

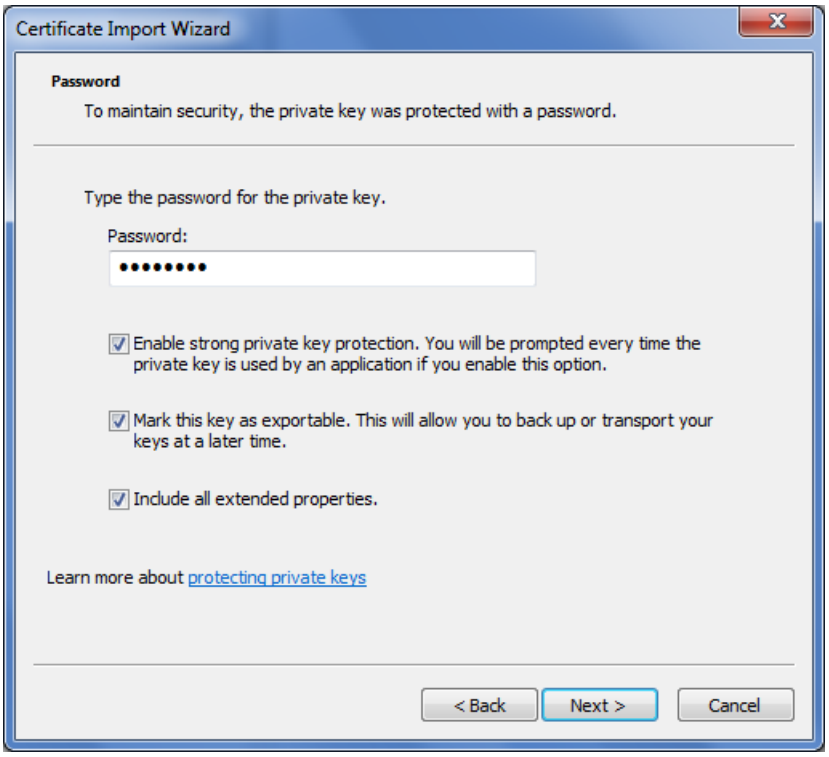
- Double-click on the .p12 or .pfx file (e.g. certificate.p12 or certificate.pfx). The Certificate Import Wizard will be started:



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



- Press Next. You will see the following screen:



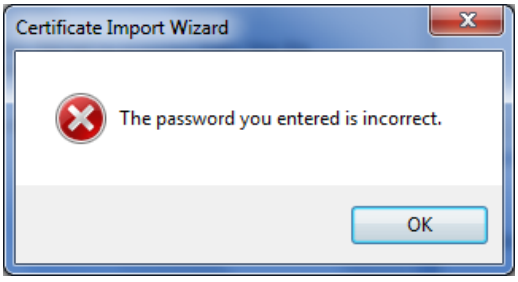
- Type the password of the .p12 o .pfx file.

- 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.

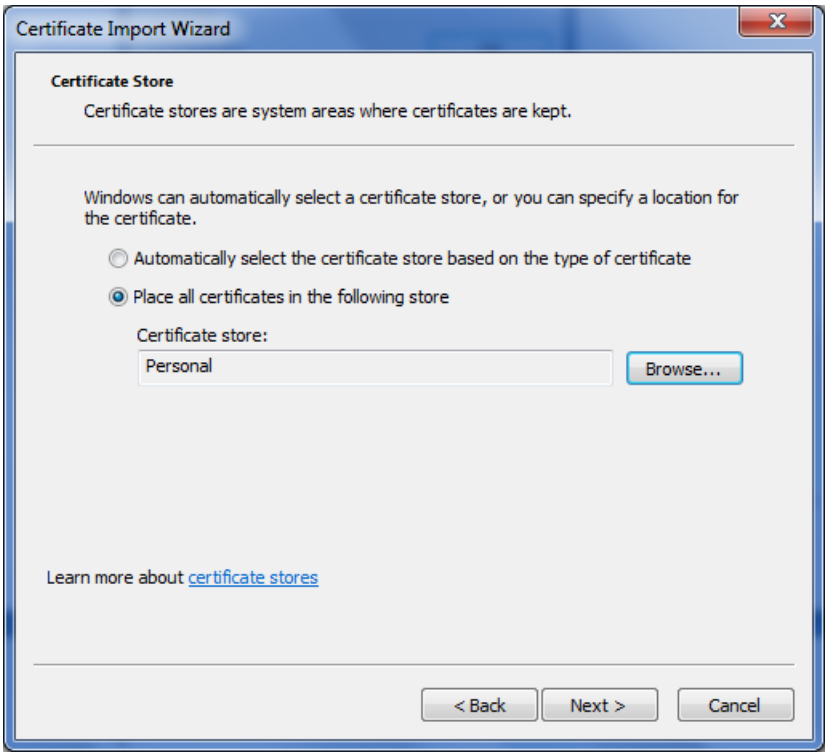
- Check the option “Mark this key as exportable” if you want that the copy of the private key that is going to be installed in the MS Windows account is ready to be exported again in the future to a new .p12 or .pfx file.

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

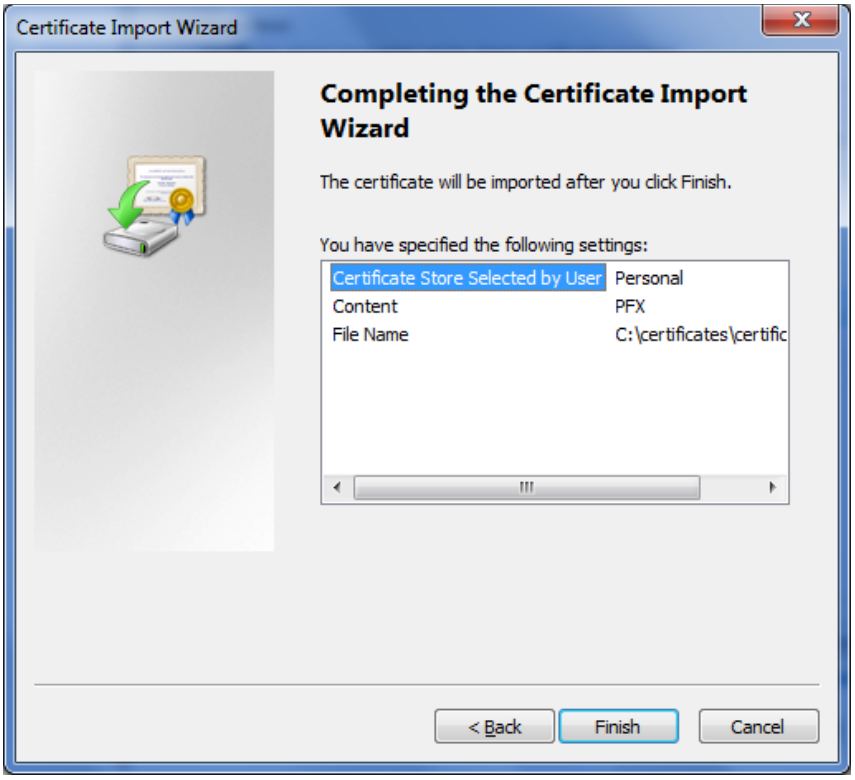
- Press Next. If you have typed a wrong password, the following message will appear:



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



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



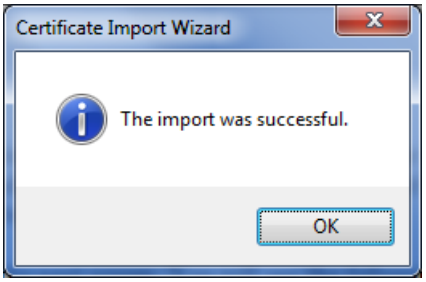
- Press Finish. You will see the following screen to confirm the installation of the private key:

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

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

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.

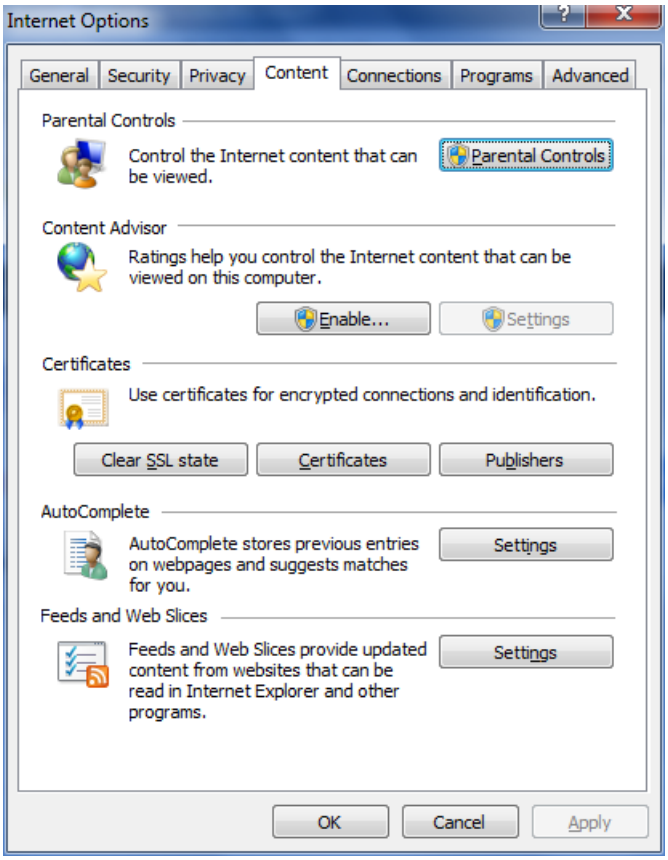
- Press Finish and OK in the next screen. You will see the following message:



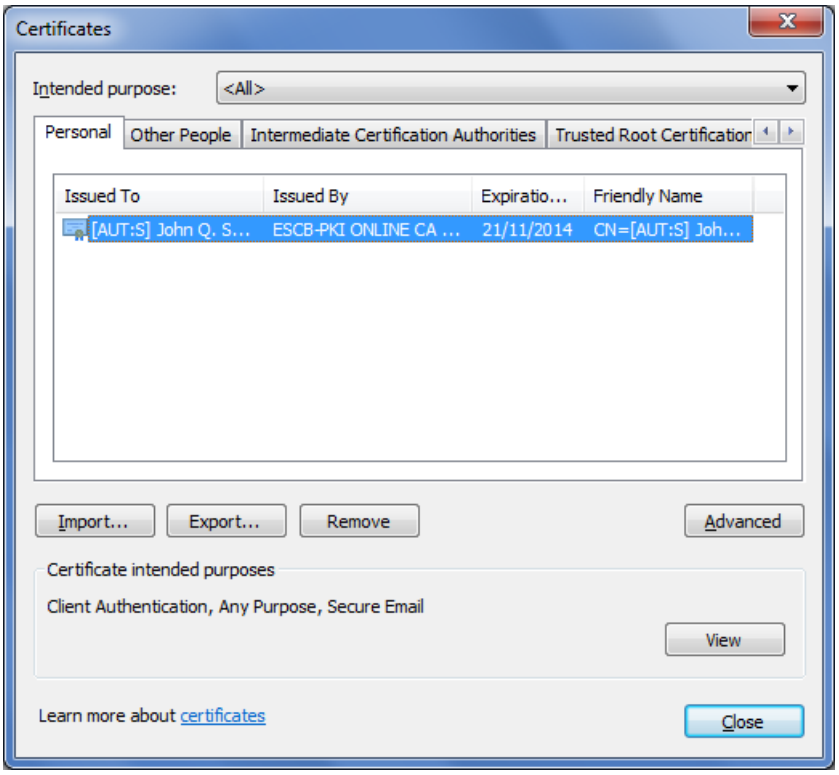
4. VERIFYING THE CERTIFICATE INSTALLATION

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

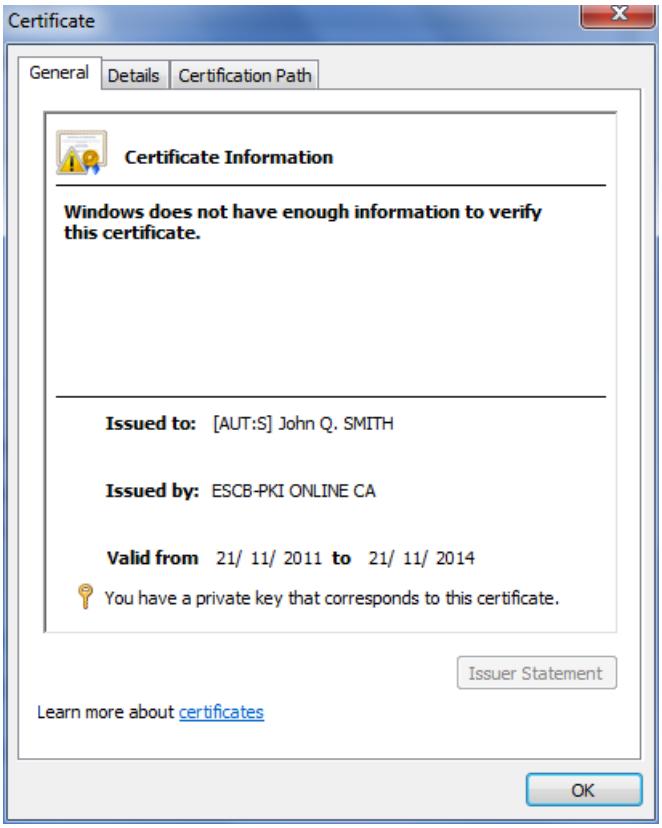
- Select the menu Tools > Internet Options and click on the Content tab:



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



- 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":

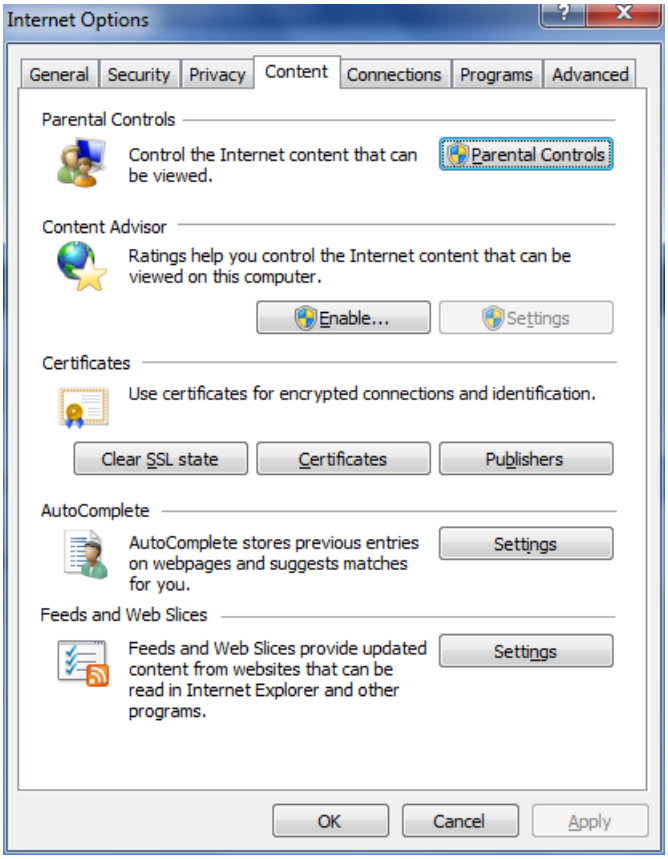


5. EXPORTING AN ESCB-PKI STANDARD CERTIFICATE

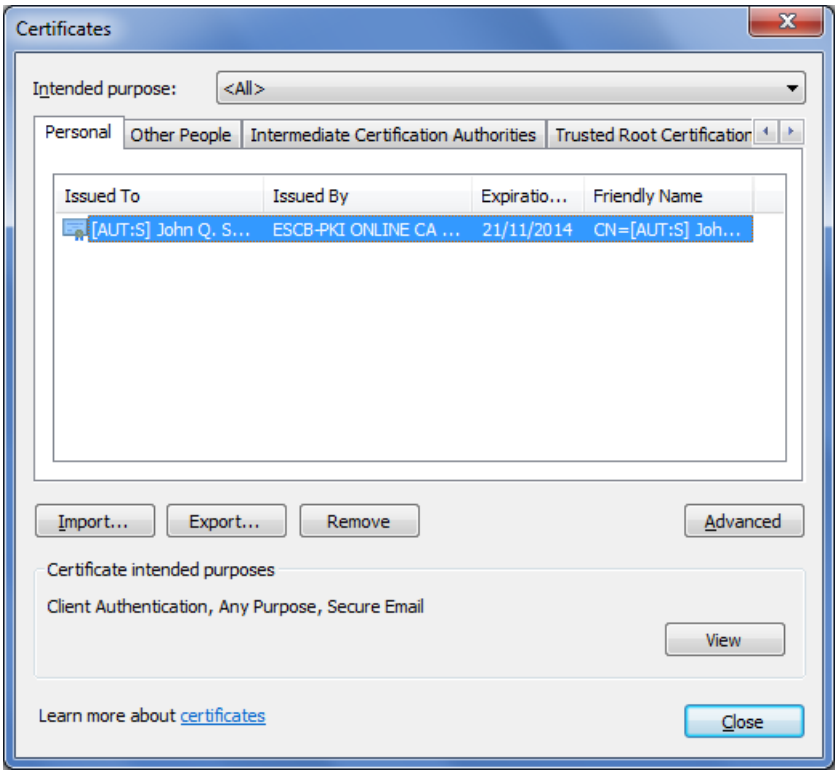
This section describes the steps necessary to export an ESCB-PKI standard certificate that is installed in your MS Windows user account to a password-protected file. You can use this password-protected file as a backup copy of your certificate and associated private key.

- Open the MS Internet Explorer browser:

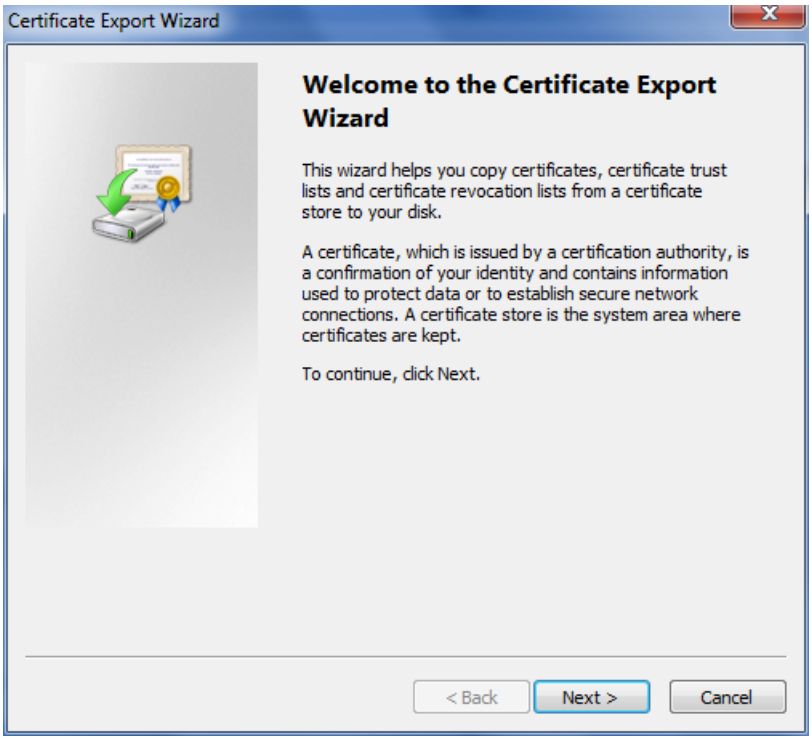
- Select the menu Tools > Internet Options and click on the Content tab:



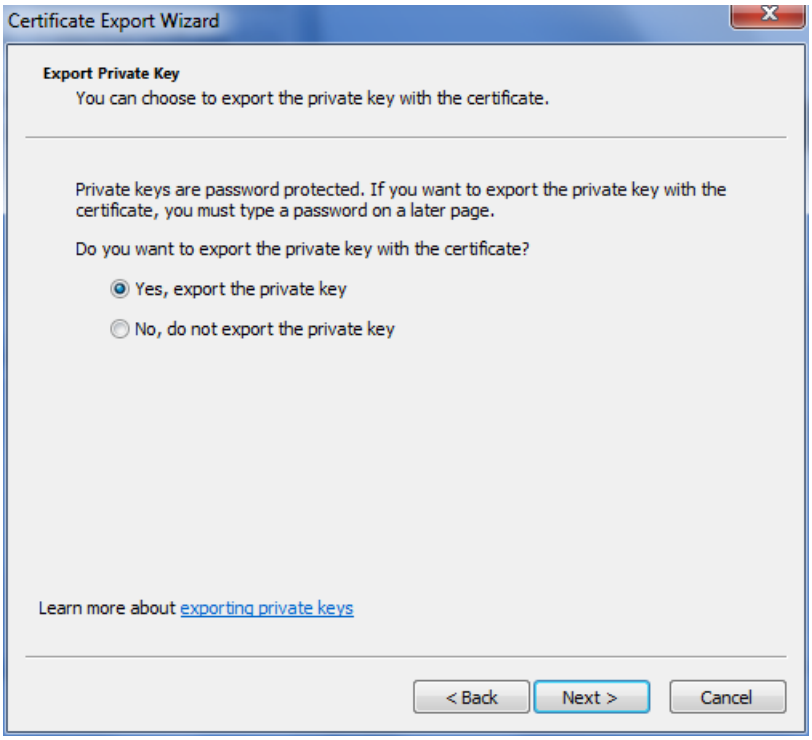
- Press the Certificates button and ensure that the Personal tab is displayed:



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

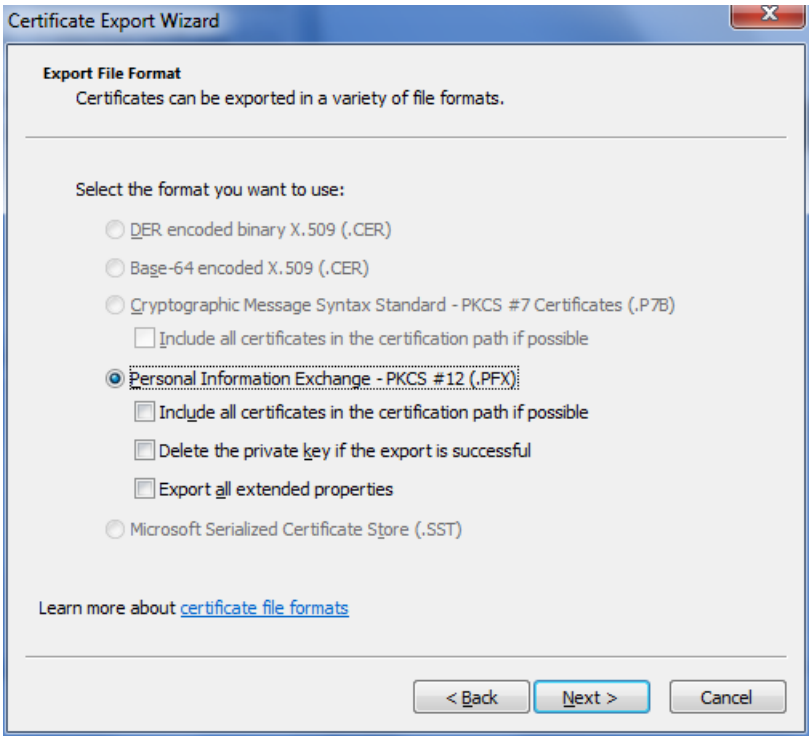


- Press Next and select the option “Yes, export the private key”:



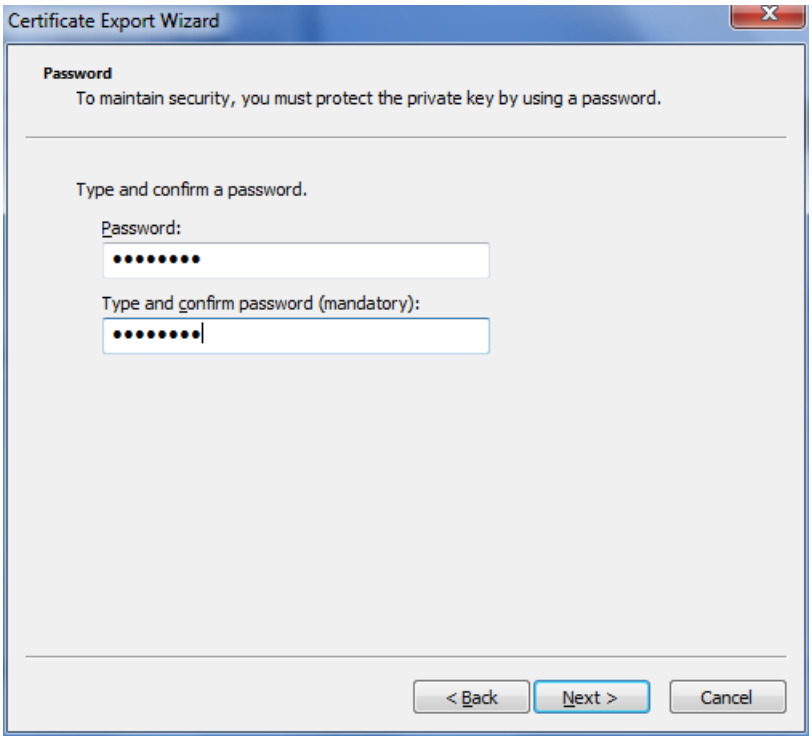
In case that the “Yes, export the private key” option cannot be selected this is because either you have not got a private key associated to the certificate, or because the “mark this key as exportable” option was not selected when you installed the certificate in the past. In this case you will not 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:



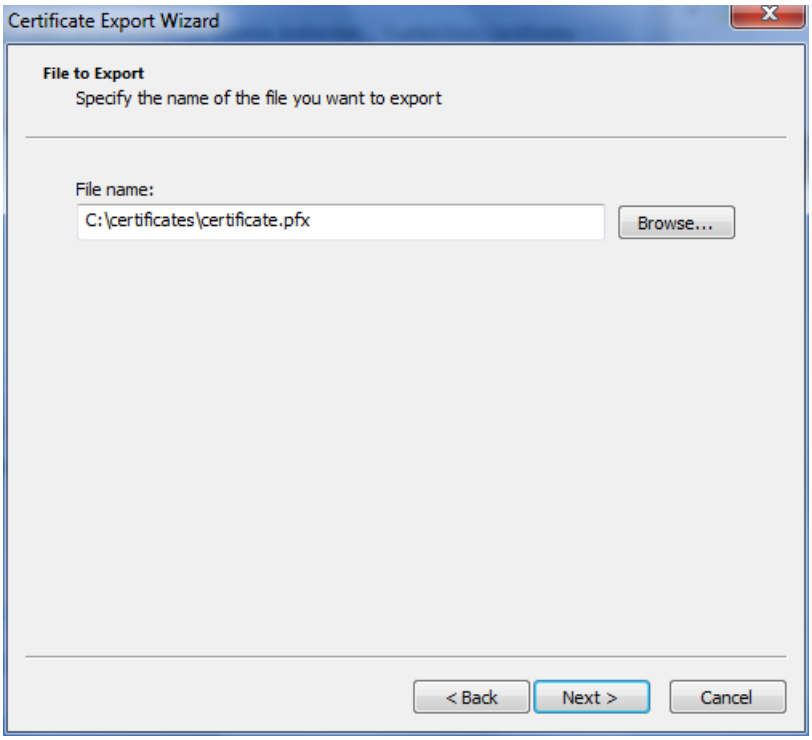
It is not necessary to select any of the options under the .PFX file format.

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

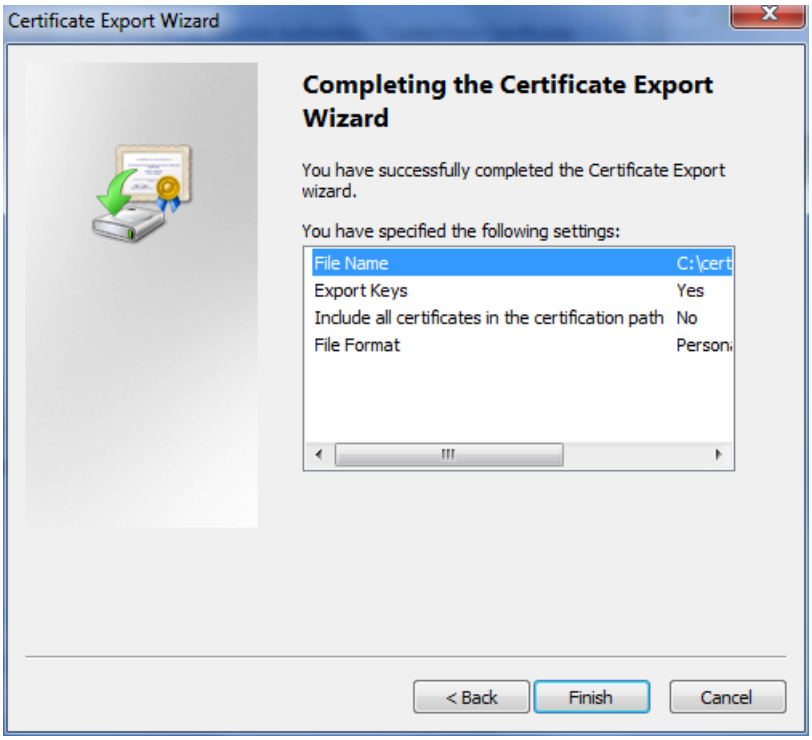


Very important notice: choose a strong password that is easy to remember. Take into account that you will need this password when you want to import your certificate and corresponding private key.

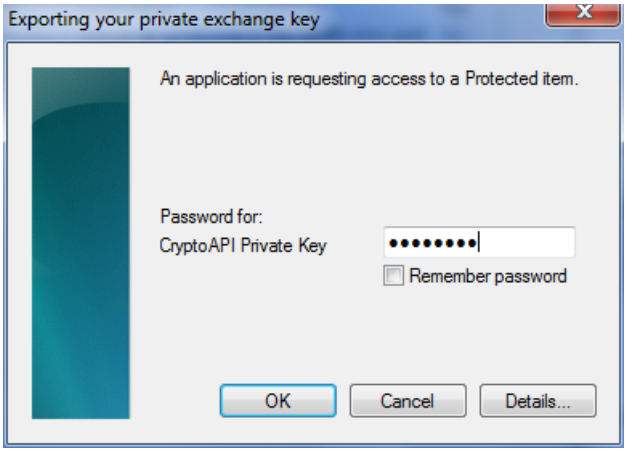
- Press Next and choose the path and name of the file that will be generated:



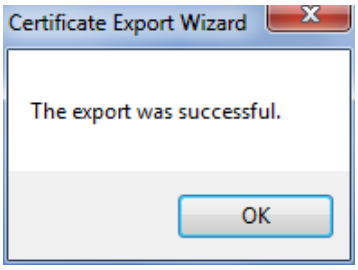
- Press Next. The following confirmation screen will be displayed:



- 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:



- 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.