

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT



USER GUIDE:

INSTALLING THE ROOT AND SUBORDINATE CERTIFICATION AUTHORITIES

VERSION 1.2

TABLE OF CONTENTS

1.	Introduction	5
2.	The ESCB-PKI certification hierarchy	6
3.	Installing the ESCB-PKI root and subordinate Certification Authorities.....	7
3.1.	Obtain the certificates for the root and subordinate Certification Authorities	7
3.2.	Install the root Certification Authority	7
3.3.	Install the subordinate Certification Authority	10

Project name:	ESCB-PKI
Author:	ESCB-PKI team
File name:	ESCB-PKI - Install Root and Subordinate CAs v.1.2.docx
Version:	1.2
Date of issue:	26.11.2011
Status:	Final
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
1.2	Final	26.11.2011	Format

1. INTRODUCTION

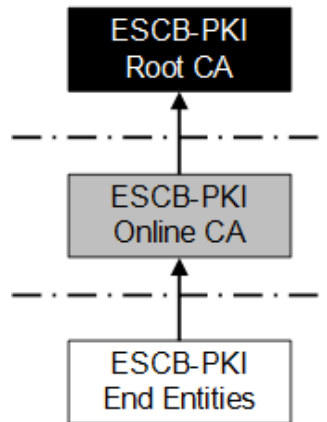
This guide describes how to install the ESCB-PKI root and subordinate Certification Authorities.

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.

2. THE ESCB-PKI CERTIFICATION HIERARCHY

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. Its most significant data are:

Subject	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8
Issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Thumbprint (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B

- **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. Its most significant data are:

Subject	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Thumbprint (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC

- **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.

3. INSTALLING THE ESCB-PKI ROOT AND SUBORDINATE CERTIFICATION AUTHORITIES

There are many technical possibilities to trust a Certificate Authority certificate. Check with your local Help Desk which options are available at your organisation.

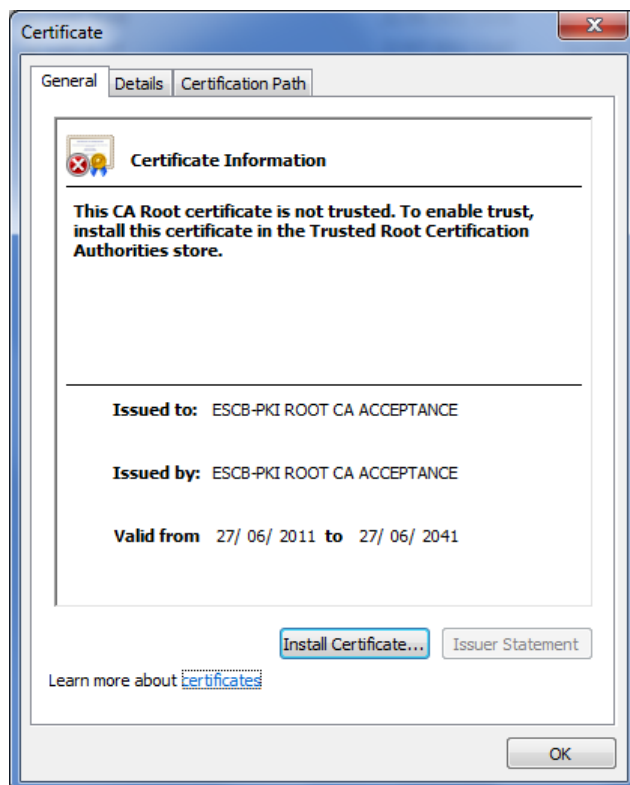
Below you can find the steps necessary to install the root and subordinate CA certificates in your computer for the Windows user account you use to log in. In case you require installing these certificates among several computers or for several user accounts, ask your local Help Desk.

3.1. OBTAIN THE CERTIFICATES FOR THE ROOT AND SUBORDINATE CERTIFICATION AUTHORITIES

These certificates can be downloaded at the ESCB-PKI website, <http://pki.escb.eu>

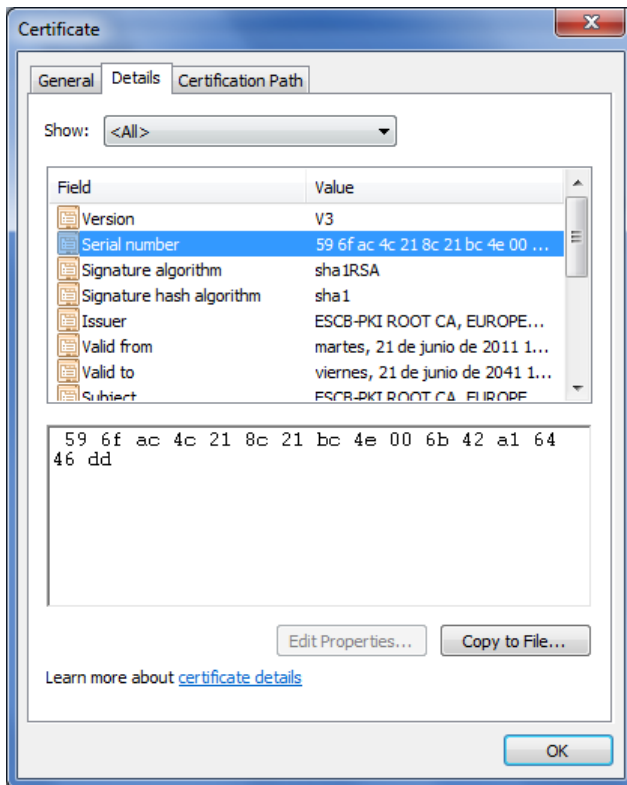
3.2. INSTALL THE ROOT CERTIFICATION AUTHORITY

- Double-click on the root CA certificate file (rootCA.crt). You will see the following screen indicating that the certificate is not trusted:



- In case the certificate is not tagged as “not trusted”, it means that your computer already trusts the certificate and you can skip the rest of the steps.

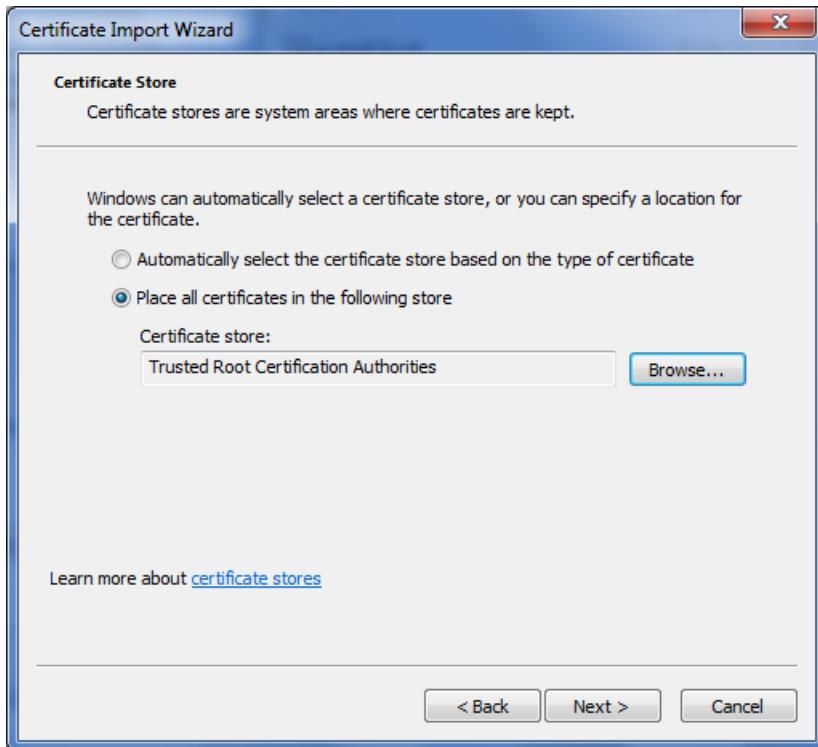
- Click on the Details tab and check the most significant data against the certificate information provided in section 2:



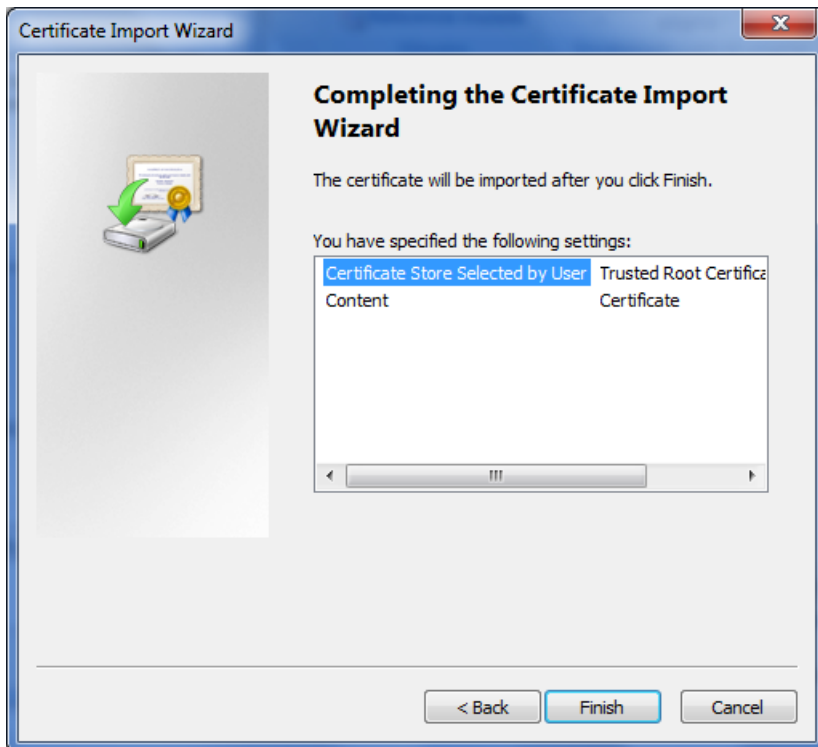
- If all the information matches, click on the General tab again and press the Install Certificate button. The Certificate Import wizard will start:



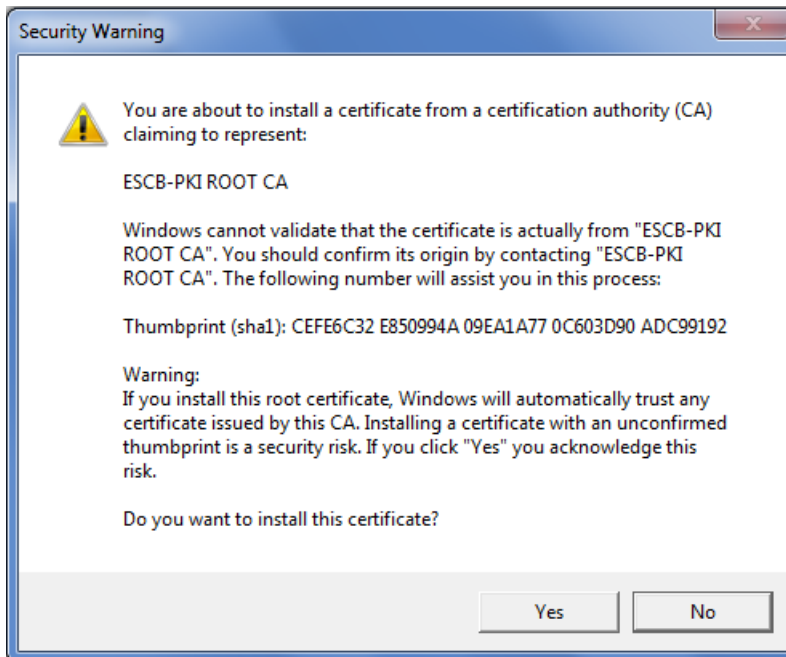
- Press Next. Select the “Trusted Root Certification Authorities” store:



- Press Next. The following screen will be shown:



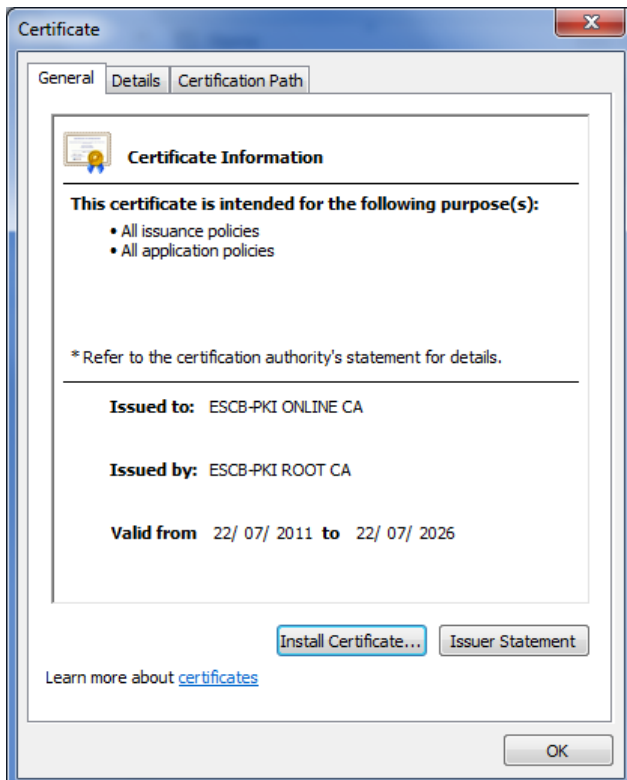
- Press Finish. The following security warning will be shown:



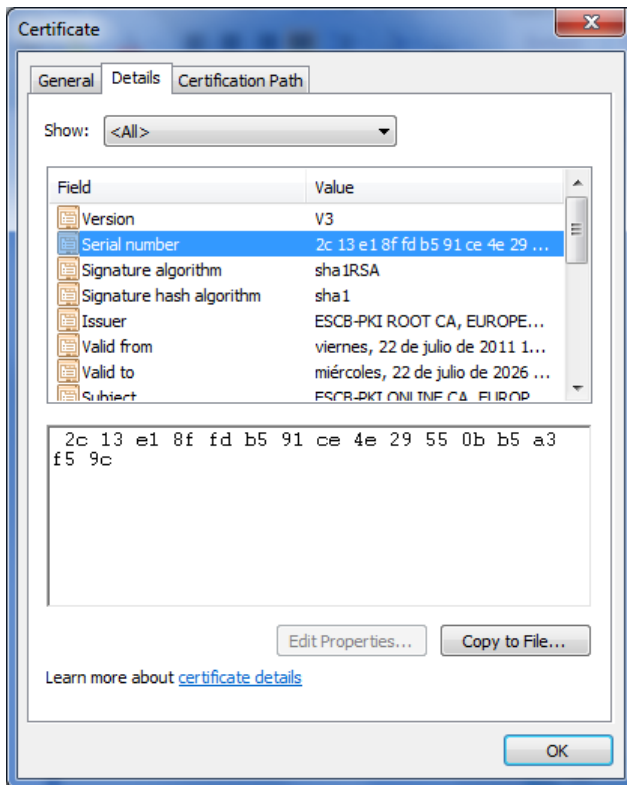
- Check the SHA-1 thumbprint against the one in section 2. Press Yes and then OK in the "The import was successful" pop-up message.

3.3. INSTALL THE SUBORDINATE CERTIFICATION AUTHORITY

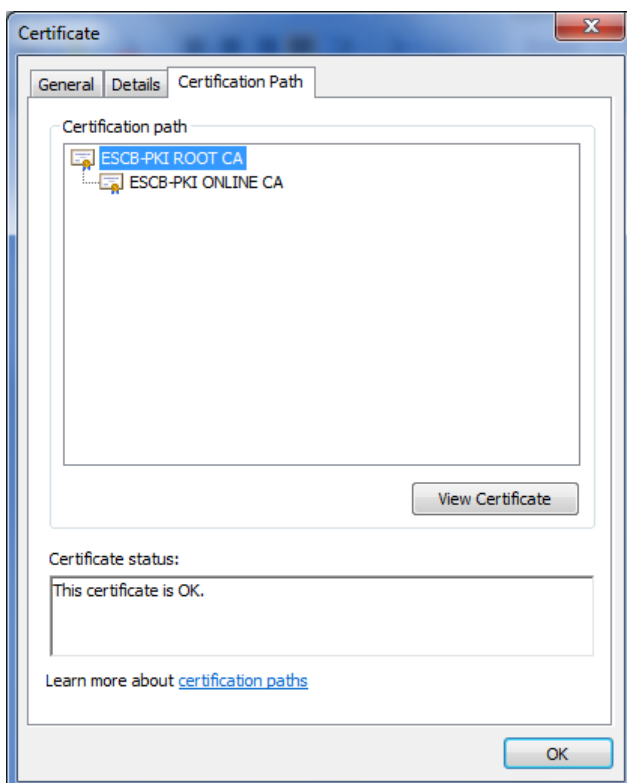
- Double-click on the subordinate CA certificate file (subCA.crt). You will see the following screen:



- Click on the Details tab and check the most significant data against the certificate information provided in section 2:



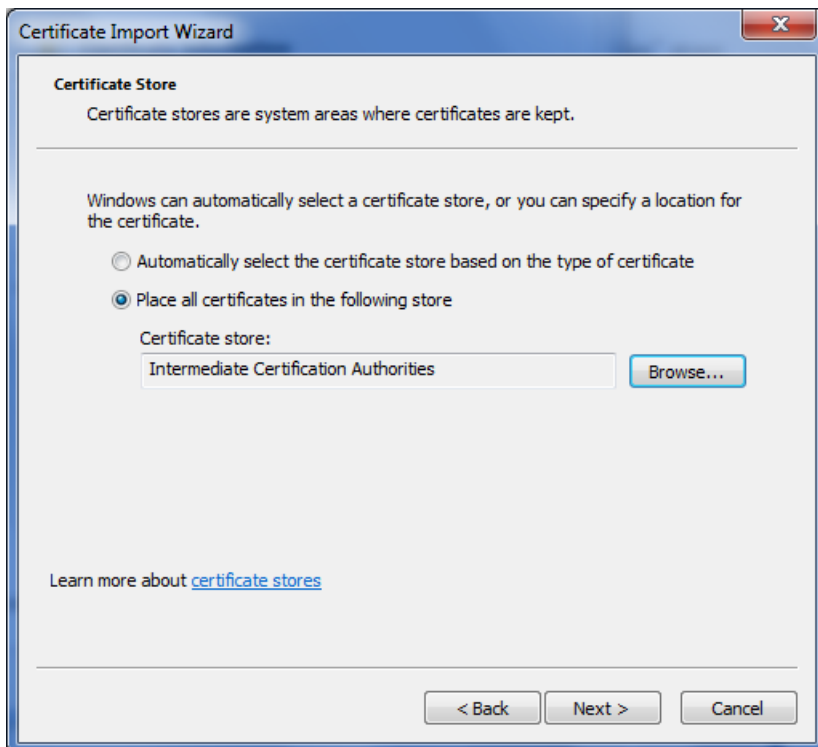
- Click on the Certification Path tab to make sure that the root CA certificate is properly installed in your computer (if that is not the case, install it again):



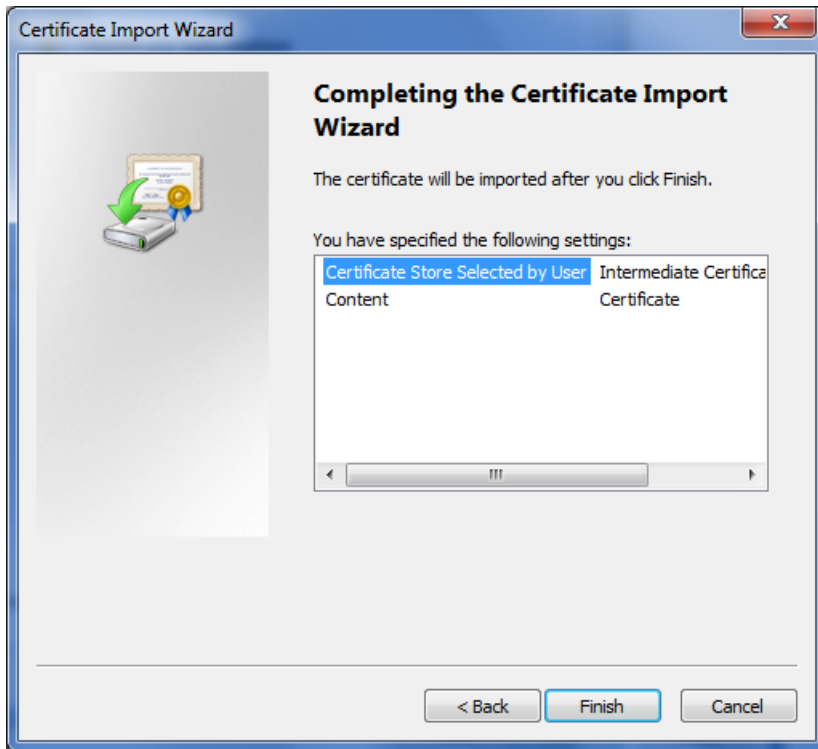
- Click on the General tab again and press the Install Certificate button. The Certificate Import wizard will start:



- Press Next. Select the "Intermediate Certification Authorities" store:



- Press Next. The following screen will be shown:



- Press Finish and OK in the "The import was successful" screen.