

ECB - Unrestricted

 ${\bf 2} \ {\rm user \ Guide: \ installing \ the \ escb-pki \ root \ and \ subordinate \ certification \ authorities}$

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

ECB - Unrestricted

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

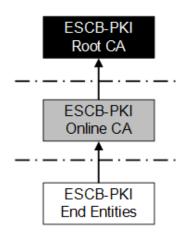
This guide describes how to install the ESCB-PKI root and subordinate Certification Authorities.

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
lssuer	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, <u>http://pki.escb.eu</u>

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:

Certificate		
General Details Certification Path		
Certificate Information		
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.		
Issued to: ESCB-PKI ROOT CA ACCEPTANCE		
Issued by: ESCB-PKI ROOT CA ACCEPTANCE		
Valid from 27/06/2011 to 27/06/2041		
Install Certificate Issuer Statement Learn more about tertificates		
ОК		

- 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:

Certificate	×
General Details Certification Path	
Show: <all></all>	•
Field	Value
Version	V3
Serial number	59 6f ac 4c 21 8c 21 bc 4e 00
Signature algorithm	sha 1RSA
Signature hash algorithm	sha1
Issuer	ESCB-PKI ROOT CA, EUROPE
Valid from	martes, 21 de junio de 2011 1
Valid to	viernes, 21 de junio de 2041 1
Subject	
59 6f ac 4c 21 8c 21 46 dd	bc 4e 00 6b 42 al 64
Ed	it Properties Copy to File
	ОК

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

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.
~	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

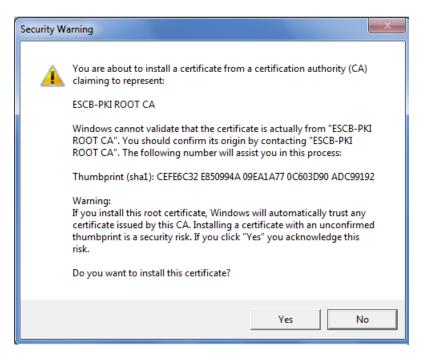
- Press Next. Select the "Trusted Root Certification Authorities" store:



- Press Next. The following screen will be shown:

Certificate Import Wizard	
	Completing the Certificate Import Wizard
	The certificate will be imported after you click Finish.
	You have specified the following settings:
	Certificate Store Selected by User Trusted Root Certifica
	Content Certificate
	۰ III ا
	< Back Finish Cancel

- 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:

Certificate		
General Details Certification Path		
Certificate Information		
This certificate is intended for the following purpose(s): • All issuance policies • All application policies		
* Refer to the certification authority's statement for details.		
Issued to: ESCB-PKI ONLINE CA		
Issued by: ESCB-PKI ROOT CA		
Valid from 22/ 07/ 2011 to 22/ 07/ 2026		
Install Certificate Issuer Statement Learn more about <u>certificates</u>		
ОК		

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

General Details Certification Path Show: <all> Field Value Wersion V3 Serial number 2c 13 e1 8f fd b5 91 ce 4e 29 Signature algorithm sha 1RSA Signature hash algorithm sha 1 Issuer ESCB-PKI ROOT CA, EUROPE Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subject PSCR-PKI ONI INF CA EUROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c Edit Properties Copy to File Learn more about certificate details</all>	Certificate	X		
Field Value Version V3 Serial number 2c 13 e1 8f fd b5 91 ce 4e 29 Signature algorithm sha1RSA Signature hash algorithm sha1 Issuer ESCB-PKI ROOT CA, EUROPE Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subject FSCR-PKI ONI TNE CA FIROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c Edit Properties Copy to File	General Details Certification Path			
Field Value Version V3 Serial number 2c 13 e1 8f fd b5 91 ce 4e 29 Signature algorithm sha1RSA Signature hash algorithm sha1 Issuer ESCB-PKI ROOT CA, EUROPE Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subiect FSCR-PKI ONI TNE CA ELIROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c Edit Properties Copy to File	Show: <			
Version V3 Serial number 2c 13 e1 3f fd b5 91 ce 4e 29 Signature algorithm sha1RSA Signature hash algorithm sha1 Issuer ESCB-PKI ROOT CA, EUROPE Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subject FSCR-PKI ONI TNE CA FIROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c				
Serial number 2c 13 e1 8f fd b5 91 ce 4e 29 Signature algorithm sha 1RSA Signature hash algorithm sha 1 Issuer ESCB-PKI ROOT CA, EUROPE Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subject FSCR-PKI ONI INF CA FUROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c	Field	Value 🔺		
Serial number 2c 13 e1 8f fd b5 91 ce 4e 29 Signature algorithm sha1RSA Signature hash algorithm sha1 Issuer ESCB-PKI ROOT CA, EUROPE Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subject FSCR-PKT ONI TNE CA ELIROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c	📴 Version	V3 =		
Signature hash algorithm sha1 Issuer ESCB-PKI ROOT CA, EUROPE Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subject FSCR-PKI ONI INF CA FUROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c Edit Properties Copy to File	📕 Serial number	2c 13 e1 8f fd b5 91 ce 4e 29		
Edit Properties				
Valid from viernes, 22 de julio de 2011 1 Valid to miércoles, 22 de julio de 2026 Subject FSCB-PKT ONU TNE CA FUROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c Edit Properties Copy to File				
Valid to miércoles, 22 de julio de 2026 Subject ESCB-PKT ONU TNE CA FUROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c Edit Properties Copy to File				
Subject FSCR-DKT ONLITNE CA FLIROP 2c 13 e1 8f fd b5 91 ce 4e 29 55 0b b5 a3 f5 9c Edit Properties				
f 5 9c Edit Properties Copy to File				
f 5 9c Edit Properties Copy to File				
Edit Properties Copy to File		ce 4e 29 55 UD D5 a3		
Learn more about <u>certificate details</u>	Ed	It Properties Copy to File		
	Learn more about <u>certificate details</u>			
ОК		ОК		

- 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):

Certificate	3
General Details Certification Path	
Certification path	
View Certificate	
Certificate status:	
This certificate is OK.	
Learn more about <u>certification paths</u>	
ОК	

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

Certificate Import Wizard	X
	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a
	A certificate store. 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. Select the "Intermediate Certification Authorities" store:

Certificate Import Wizard		
Certificate Store Certificate stores are system areas where certificates are kept.		
Windows can automatically select a certificate store, or you can specify a location for the certificate.		
O Automatically select the certificate store based on the type of certificate		
Place all certificates in the following store		
Certificate store: Intermediate Certification Authorities Browse		
Learn more about <u>certificate stores</u>		
< Back Next > Cancel		

- Press Next. The following screen will be shown:

Certificate Import Wizard	
	Completing the Certificate Import Wizard
	The certificate will be imported after you click Finish.
	You have specified the following settings:
	Certificate Store Selected by User Intermediate Certifica Content Certificate
	4
	< Back Finish Cancel

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