

 ${\bf 2}$  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	8
3.1	. Obtain the certificates for the root and subordinate Certification Authorities	8
3.2	. Install the root Certification Authority	8
3.3	. Install the subordinate Certification Authorities1	1

Project name:	ESCB-PKI
Author:	ESCB-PKI team
File name:	ESCB-PKI - Install Root and Subordinate CAs.pdf
Version:	3.0
Date of issue:	31.10.2024
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
2.0	Final	11.09.2018	BdE Revision
2.1	Final	06.02.2024	Updated http links to ESCB-PKI website to https
3.0	Final	31.10.2024	Addition of ESCB-PKI Online CA V1.2

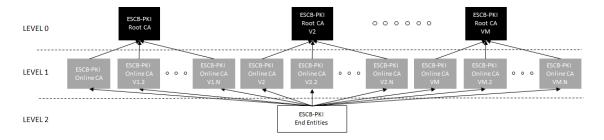
# 1. INTRODUCTION

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:

- **ESCB-PKI 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
lssuer	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
Thumbprint (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB

- **ESCB-PKI 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
Thumbprint (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700

• **ESCB-PKI Online CA V1.2**: Certification Authority subordinated to the ESCB-PKI Root CA. It is responsible for issuing the ESCB-PKI end entities certificates in order to replace the current ESCB-PKI Certification Authority when it is near its expiration date. Its most significant data are:

SHA-256 certificate:

Distinguished Name	CN = ESCB-PKI ONLINE CA V1.2, O= European System of Central Banks, C=EU
Serial Number	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
Distinguished Name of Issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity Period	From 08-06-2023 17:07:00 to 08-06-2038 17:07:00
Message Digest (SHA-1)	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Message Digest (SHA-256)	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Cryptographic algorithms	SHA-256 / RSA 4096

- 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 organization.

Below you can find the necessary steps 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, https://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:

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		
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:

📃 Certifi	cate 🛛 🗙
General Details Certification Path	
Show: <a>All&gt;</a>	~
Field Va	lue
Signature algorithm sh Signature hash algorithm sh Issuer ES Valid from ma Valid from vie	31 9c 5F 91 e8 16 2f 4e 00         ■           a256RSA         ■           a256         CB-PKI ROOT CA, EUROPE           rtes, 21 de junio de 2011 1         ■           cB-PKI ROOT CA, EUROPE         ▼
44 31 9c 5f 91 e8 16 2f d8	4e 00 73 f6 6a b8 71
Edit Pi	Copy to File
	OK

- 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	
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, click Next.
	< Back Next > Cancel

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



- Press Next. The following screen will be shown:

Certificate Import Wizard	And and a second second	×
	Completing the Certifi Wizard	cate Import
	The certificate will be imported after	r you click Finish.
	You have specified the following set	ttings:
	Certificate Store Selected by User Content	Trusted Root Certifica Certificate
	•	4
	< Back F	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 AUTHORITIES

- Double-click on the subordinate CA certificate file. 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 certificates		
ОК		

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

📃 Cei	rtificate
General Details Certification Path	1
Show: <all></all>	~
Field	Value ^
🛅 Version	V3
Serial number	66 0c 9b 12 9a 0a 6c 21 55 09 🔳
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
	ESCB-PKI ROOT CA, EUROPE
📴 Valid from	viernes, 22 de julio de 2011 1
Valid to	miércoles, 22 de julio de 2026
E Subject	ESCB-PKI ONLINE CA, EUROP 🗸
66 Oc 9b 12 9a Oa 6c 2d	21 55 09 38 dd 54 a0 ed
E	dit Properties Copy to File
	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	×
General Details Certification Path	
Certification path	
SCB-PKI ROOT CA	
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	
	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 "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.
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 dick Finish.
	You have specified the following settings:          Certificate Store Selected by User       Intermediate Certificate         Content       Certificate          III
	< Back Finish Cancel

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

Repeat all the steps at point 3.3 Install the subordinate Certification Authorities for the subordinate CA v1.2 certificate file.