BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

USER GUIDE:

INSTALLING THE ROOT AND SUBORDINATE

ACCEPTANCE CERTIFICATION AUTHORITIES

VERSION 3.0

ECB-PUBLIC
31-Oct-2024

TABLE OF CONTENTS

1. Introduction ... 5

2. The ESCB-PKI acceptance certification hierarchy ... 6

3. Installing the ESCB-PKI acceptance root and subordinate CAs ... 8

3.1. Obtain the certificates for the acceptance root and subordinate Certification Authorities ... 8

3.2. Install the acceptance root Certification Authority ... 8

3.3. Install the acceptance subordinate Certification AuthoritIES ... 12

Project name:	ESCB-PKI
Author:	ESCB-PKI team
File name:	ESCB-PKI - Install Root and Subordinate CAs - acceptance v.3.0.docx
Version:	3.0
Date of issue:	31.10.2024
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	Format Revision
3.0	Final	31.10.2024	Addition of *ESCB-PKI Online CA ACCEPTANCE V1.2*

1. INTRODUCTION

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

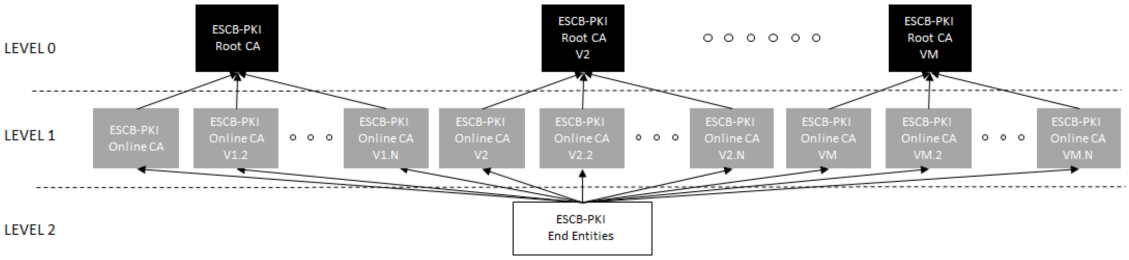
Very important notice: certificates issued by the ESCB-PKI acceptance environment are only valid for acceptance tests since no formal registration procedures are followed to issue them. Therefore, you should only install the root and subordinate Certification Authorities to carry out acceptance tests, **not for production purposes**.

The screen shots are included only as a reference. Depending on the operating system version and configuration, 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 ACCEPTANCE CERTIFICATION HIERARCHY

The ESCB Public Key Infrastructure for the acceptance environment 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 ACCEPTANCE, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	699B 8B06 6486 42A5 5506 B0FD 220F EAF8
Issuer	CN= ESCB-PKI ROOT CA ACCEPTANCE, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity	From 27-06-2011 16:33:18 to 27-06-2041 16:33:18
Thumbprint (SHA-1)	6942 03B2 BE0F 3A98 4DA5 1A80 E21B 77A2 389B 5C6A
Thumbprint (SHA-256)	B3DF FA18 2B1F 4DDA A887 8A2E C291 9FE3 5567 9990 159D FDCC 7F51 D587 A0AA 4260

- **ESCB-PKI Online CA Acceptance**: 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 ACCEPTANCE, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	157A 1105 AB2C D266 5506 B420 053E E889
Issuer	CN=ESCB-PKI ROOT CA ACCEPTANCE, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity	From 27-06-2011 16:36:14 to 27-06-2026 16:36:14
Thumbprint (SHA-1)	5737 6929 D09B 868A 5AFD EF84 A364 F383 1B88 2C6A
Thumbprint (SHA-256)	7651 6996 902E DEA3 8A94 27A3 F3F7 C78F B425 D06A 308C 089B 97C2 11BD ED4C 4043

- **ESCB-PKI Online CA Acceptance V1.2**: 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 ACCEPTANCE V1.2, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	1121 0309 84C7 9C1F D607 339E 1A7F 7B7B EC62
Issuer	CN=ESCB-PKI ROOT CA ACCEPTANCE, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity	From 14-03-2023 14:05:00 to 14-03-2038 14:05:00
Thumbprint (SHA-1)	390F B137 BBB8 405A 76BD B2CC 80FE 25C4 2915 E285
Thumbprint (SHA-256)	C548 B60B 8398 2146 5B05 9821 9AD1 2DB0 A61A 5E68 E1D6 3738 0795 9FF4 C290 7844

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

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

3. INSTALLING THE ESCB-PKI ACCEPTANCE ROOT AND SUBORDINATE CAS

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

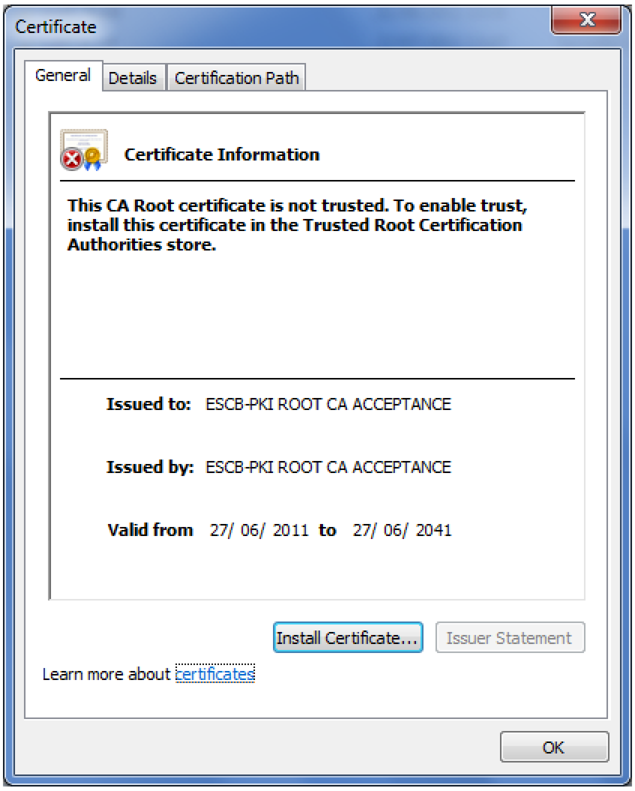
Below you can find the necessary steps to install the root and subordinate CA certificates in your computer for the Windows user account you use to log in. In case you require installing these certificates among several computers or for several user accounts, ask your local Help Desk.

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

These certificates can be downloaded at the ESCB-PKI acceptance website, https://a-pki.escb.eu

3.2. INSTALL THE ACCEPTANCE ROOT CERTIFICATION AUTHORITY

- Double-click on the acceptance root CA certificate file (a-rootCA-sha256.crt). You will see the following screen indicating that the certificate is not trusted:



This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

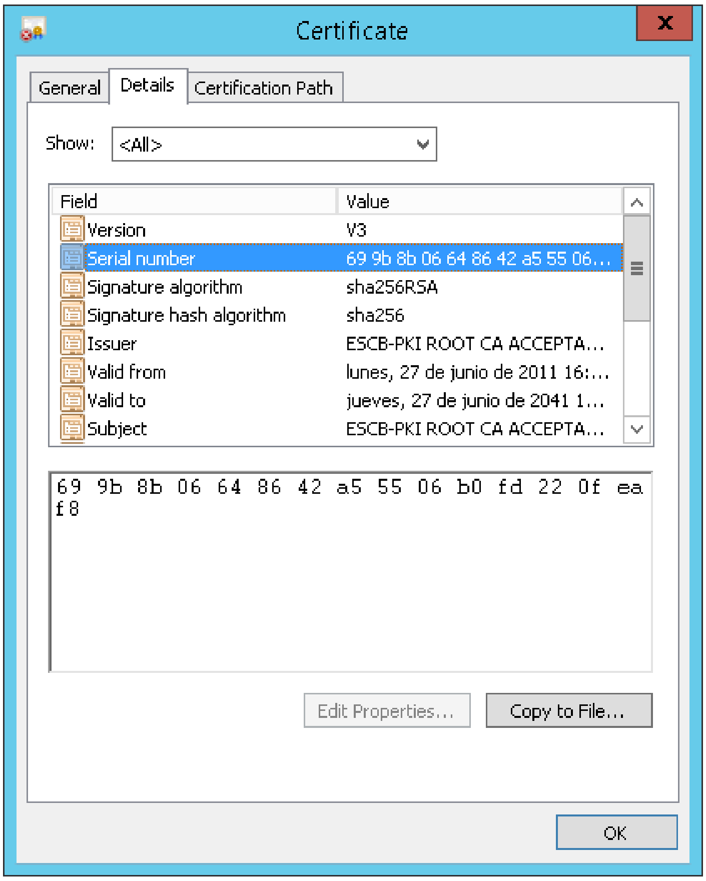
Issued to: ESCB-PKI ROOT CA ACCEPTANCE

Issued by: ESCB-PKI ROOT CA ACCEPTANCE

Valid from 27/ 06/ 2011 to 27/ 06/ 2041

- 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

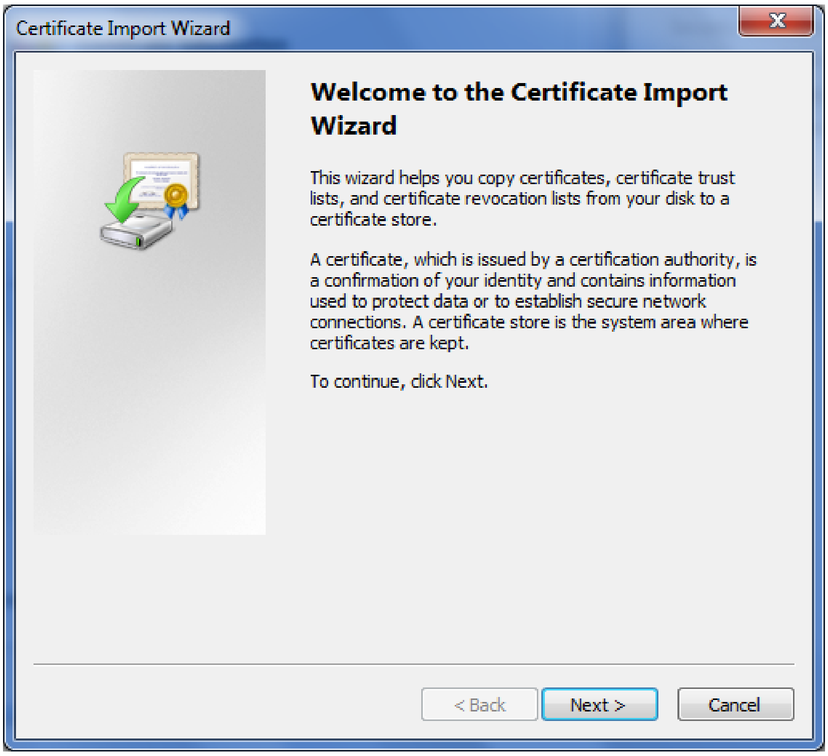
- Click on the Details tab and check the most significant data against the certificate information provided in section 2:



Field	Value
Version	V3
Serial number	69 9b 8b 06 64 86 42 a5 55 06...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ESCB-PKI ROOT CA ACCEPTA...
Valid from	lunes, 27 de junio de 2011 16:...
Valid to	jueves, 27 de junio de 2041 1...
Subject	ESCB-PKI ROOT CA ACCEPTA...

```
69 9b 8b 06 64 86 42 a5 55 06 b0 fd 22 0f ea
f8
```

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



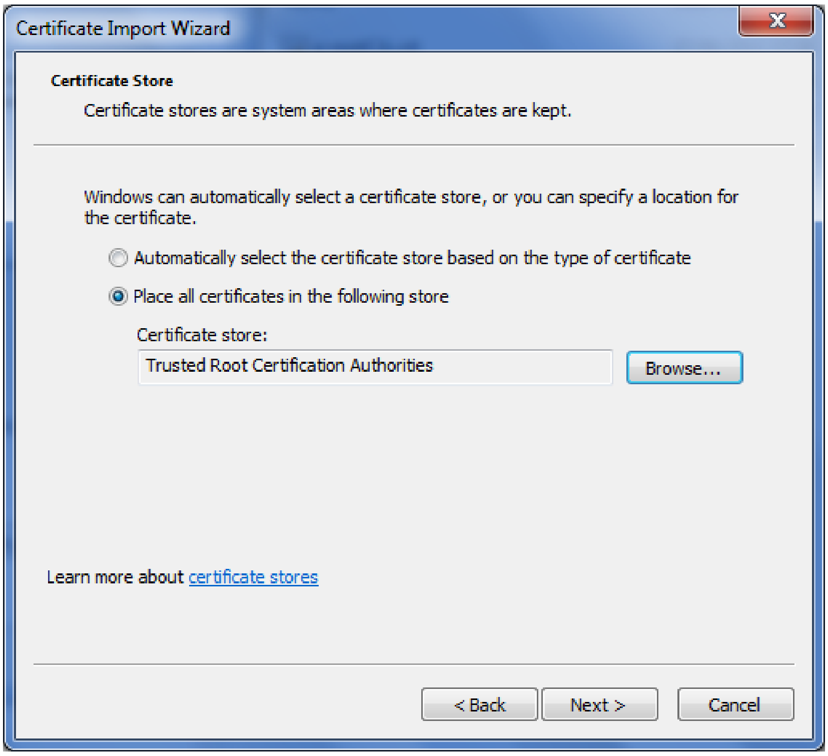
Welcome to the Certificate Import Wizard

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.

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



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

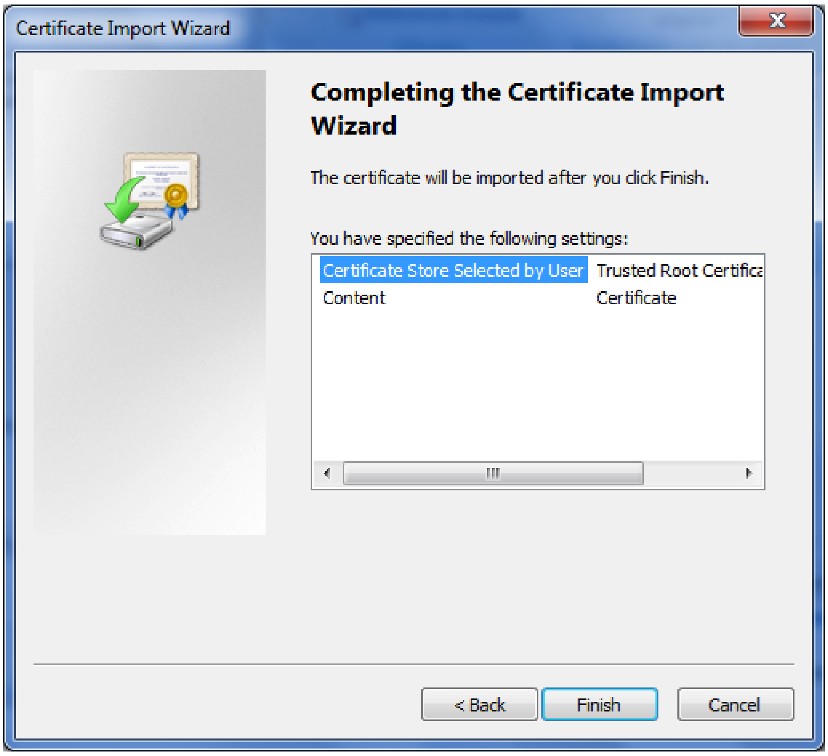
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

- Press Next. The following screen will be shown:



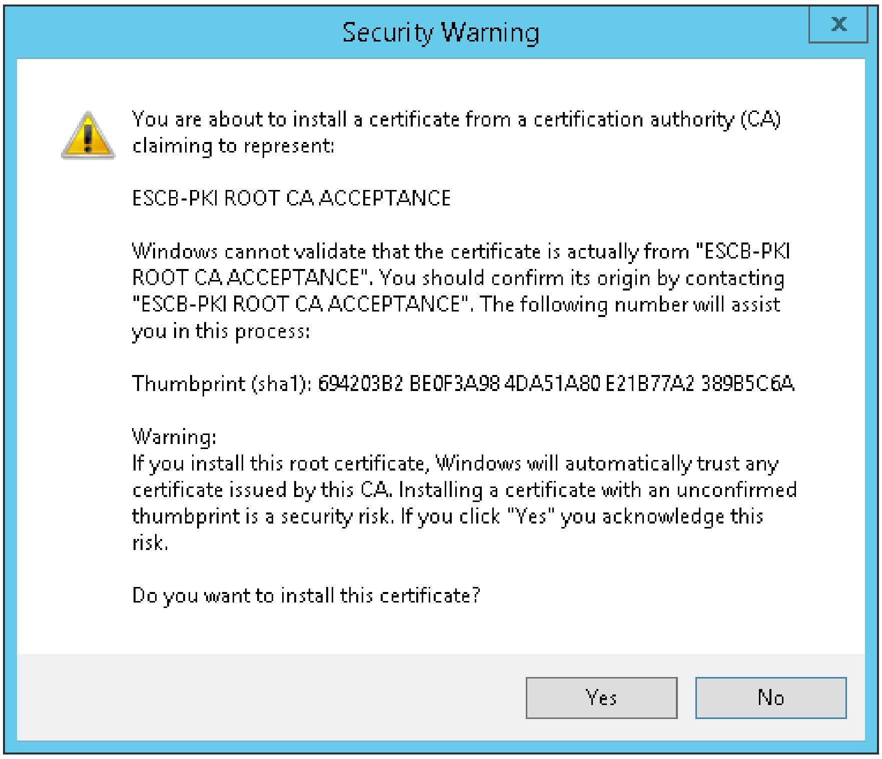
Completing the Certificate Import Wizard

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

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



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

ESCB-PKI ROOT CA ACCEPTANCE

Windows cannot validate that the certificate is actually from "ESCB-PKI ROOT CA ACCEPTANCE". You should confirm its origin by contacting "ESCB-PKI ROOT CA ACCEPTANCE". The following number will assist you in this process:

Thumbprint (sha1): 694203B2 BE0F3A98 4DA51A80 E21B77A2 389B5C6A

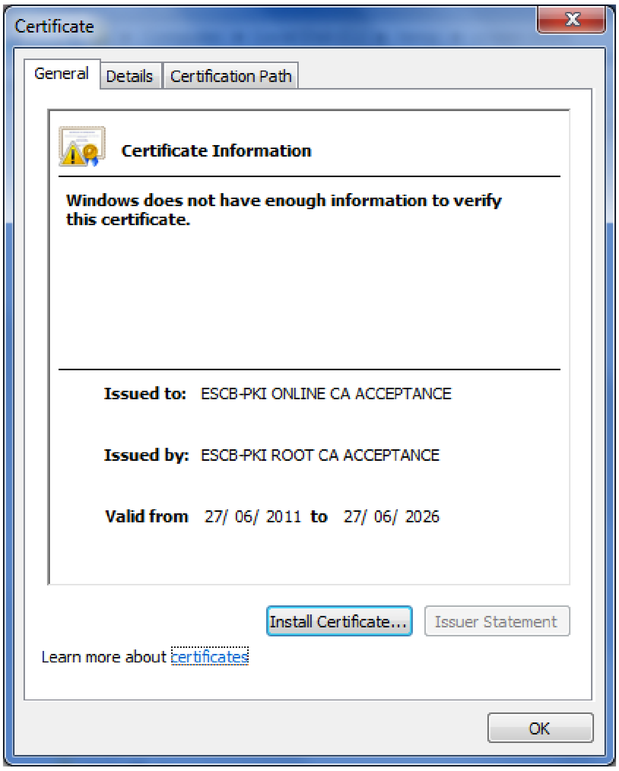
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

- 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 ACCEPTANCE SUBORDINATE CERTIFICATION AUTHORITIES

- Double-click on the acceptance subordinate CA certificate file. You will see the following screen:



Certificate

General | Details | Certification Path

Certificate Information

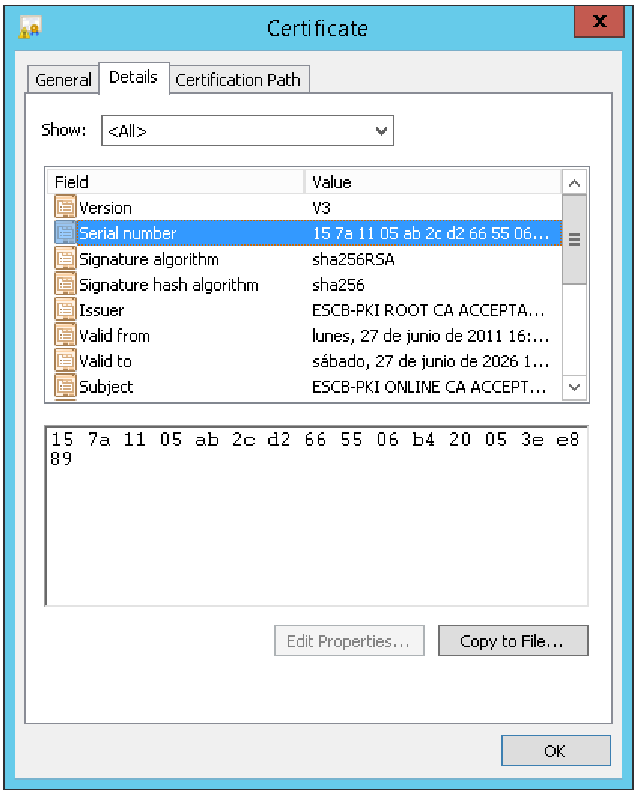
Windows does not have enough information to verify this certificate.

Issued to: ESCB-PKI ONLINE CA ACCEPTANCE

Issued by: ESCB-PKI ROOT CA ACCEPTANCE

Valid from 27/ 06/ 2011 **to** 27/ 06/ 2026

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



Certificate

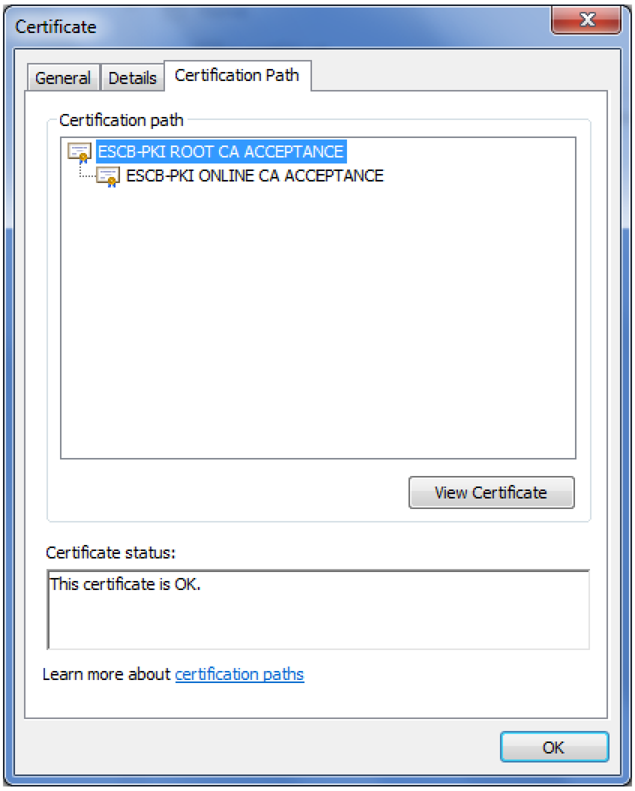
General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	15 7a 11 05 ab 2c d2 66 55 06...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ESCB-PKI ROOT CA ACCEPTA...
Valid from	lunes, 27 de junio de 2011 16:...
Valid to	sábado, 27 de junio de 2026 1...
Subject	ESCB-PKI ONLINE CA ACCEPT...

```
15 7a 11 05 ab 2c d2 66 55 06 b4 20 05 3e e8
89
```

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

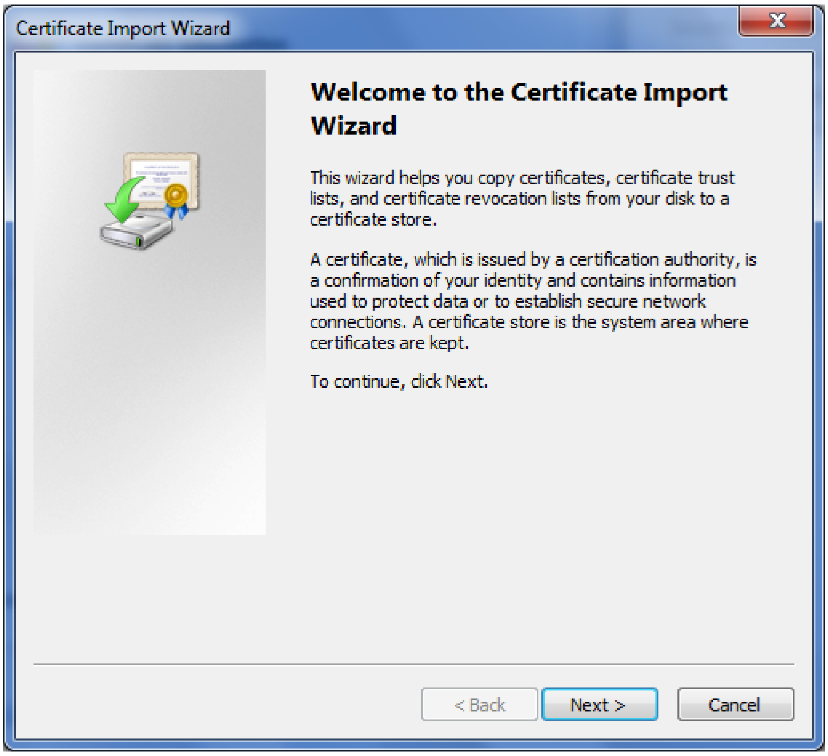


Certificate status:

This certificate is OK.

Learn more about certification paths

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



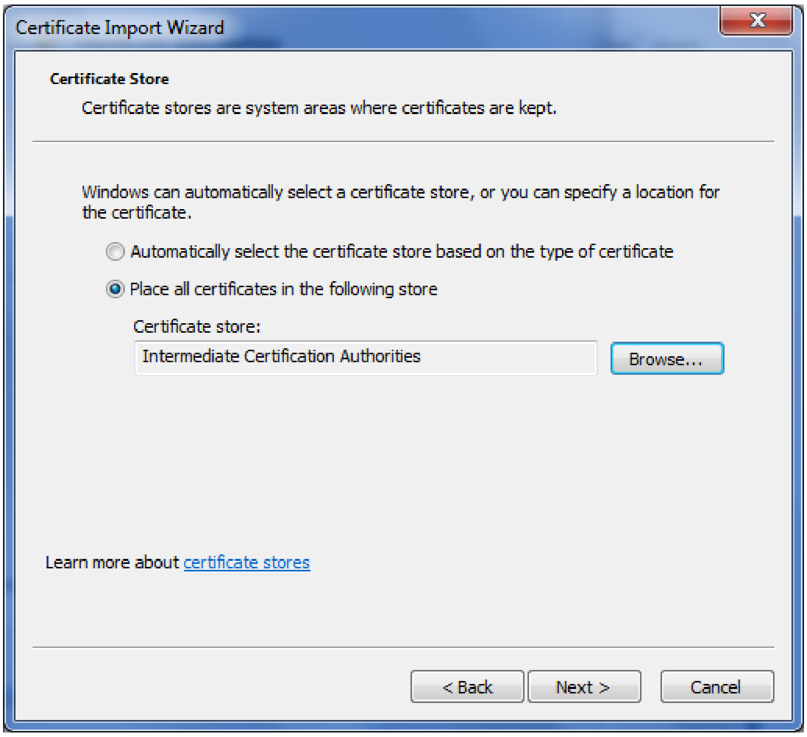
Welcome to the Certificate Import Wizard

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.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

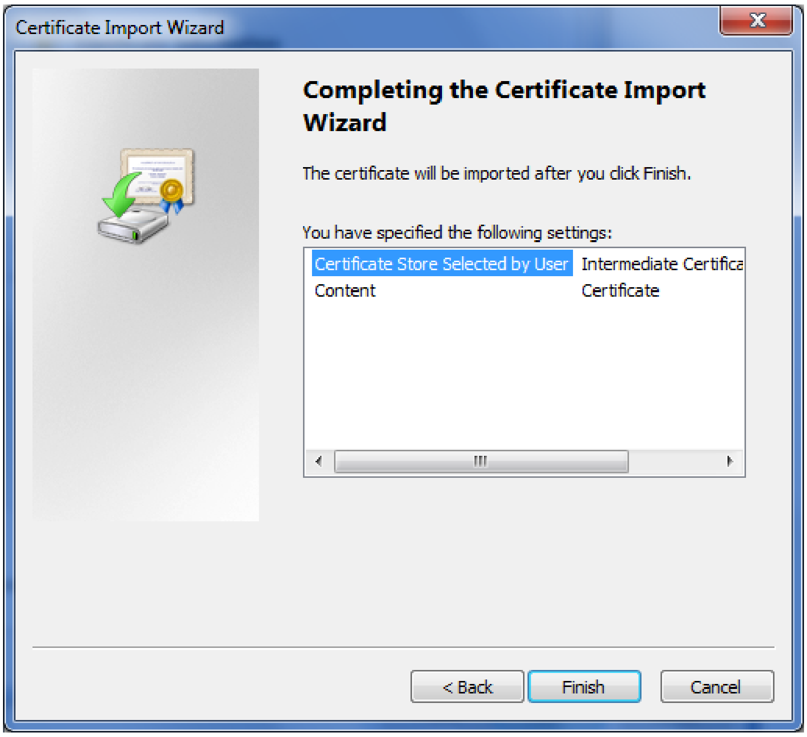
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Intermediate Certification Authorities

- 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

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