BANCO DE ESPAÑA
Eurosistema

Information Systems Department

03.09.2018

Banco de España electronic services

Installation of Banco de España certification hierarchy

CONTENTS

1 Introduction 1

2 Installation of the certification hierarchy 1

2.1 Downloading the certificates 1

2.2 Installing Root CA v2 certificate 2

2.3 Installing Corporate CA v2 certificate 4

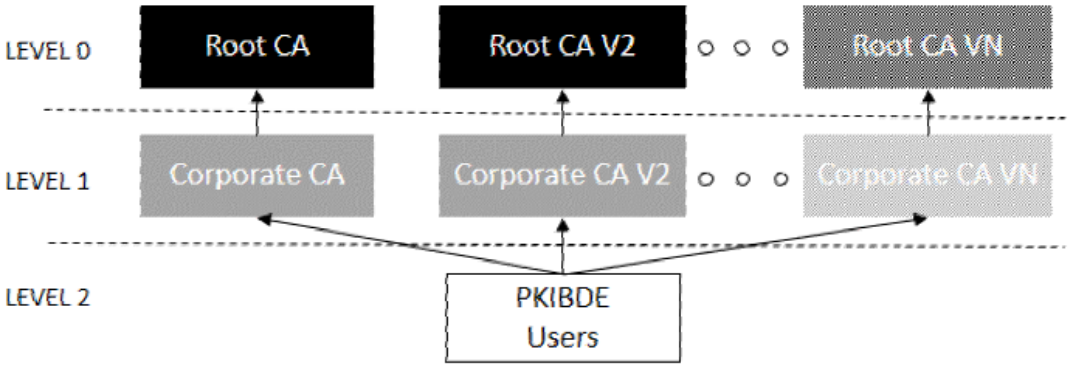
1 Introduction

This document shows how to install, in Microsoft Windows Operating Systems (although it can be also used as a reference guide for other OSs), the hierarchy of the Certification Authorities of Banco de España's Public Key Infrastructure (PKIBDE).

2 Installation of the certification hierarchy

Access to the Banco de España's on-line services may require the installation, onto the final user PC, of the certificates of the Certification Authorities of PKIBDE.

The general architecture, in terms of hierarchy, of Banco de España's PKI is as follows:



2.1 Downloading the certificates

These certificates are available for downloading at PKIBDE certification hierarchy.
The file names are ACraizv2-sha256.crt and ACcorporativav2-sha256.crt. To ensure that the certificates are the correct ones, you must confirm this information:

Root CA v2

First-level Certification Authority. This CA only issues certificates for itself and its Subordinate CAs. It will only be in operation whilst carrying out the operations for which it is established. Its most significant data are:

- Issuer: CN=BANCO DE ESPAÑA-AC RAIZ V2,O=BANCO DE ESPAÑA,C=ES
- DN: CN=BANCO DE ESPAÑA-AC RAIZ V2,O=BANCO DE ESPAÑA,C=ES
- Serial number: 45:54:22:D4:E8:76:1B:FC:55:47:4D:19:4E:85:6E:37
- Message digest (SHA1): AC:BC:CB:74:40:6A:55:88:EB:88:2F:5F:59:94:9D:DC:B8:31:79:86

Corporate CA v2

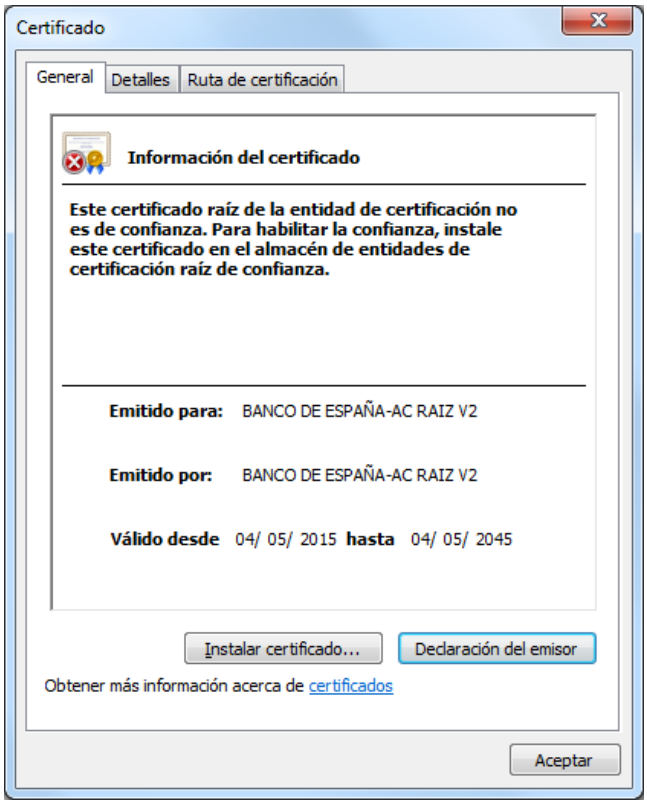
Certification Authority subordinate to the Root CA v2. It is responsible for issuing certificates for PKIBDE end-users.

- Issuer: CN=BANCO DE ESPAÑA-AC RAIZ V2,O=BANCO DE ESPAÑA,C=ES
- DN: CN=BANCO DE ESPAÑA-AC CORPORATIVA V2,O=BANCO DE ESPAÑA,C=ES
- Serial number: 18:D8:76:5B:E6:81:86:C6:55:47:76:F5:92:27:24:80
- Message digest (SHA-1): A8:F0:5C:AC:9C:65:18:C0:8F:F6:3F:82:C3:38:DE:46:D8:B9:3E:38

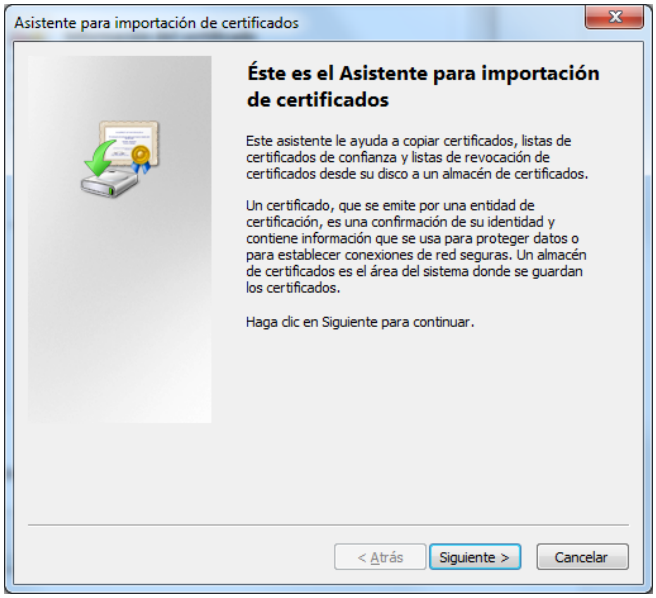
The next section summarises the steps required to install these certificates in your computer. Please note that the procedure to install the certificates depends on the OS and browser used, so only the procedure for the most used browser is described.

2.2 Installing Root CA v2 certificate

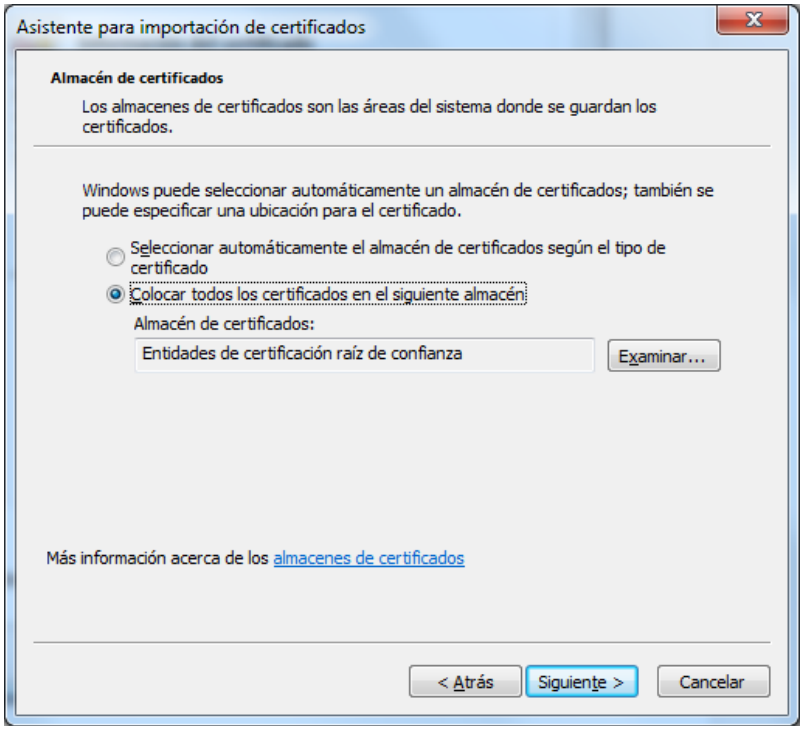
Double click the file ACraizv2-sha256.crt. The following window will be shown:



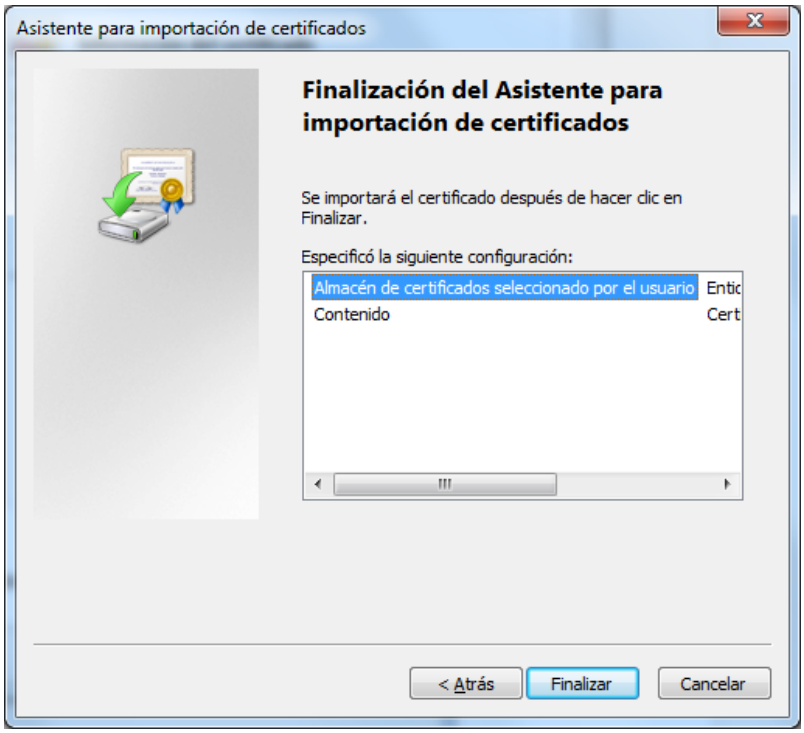
Press the button *Install certificate… (Instalar certificado…* in the above screenshot) and the certificate import wizard will be initiated.



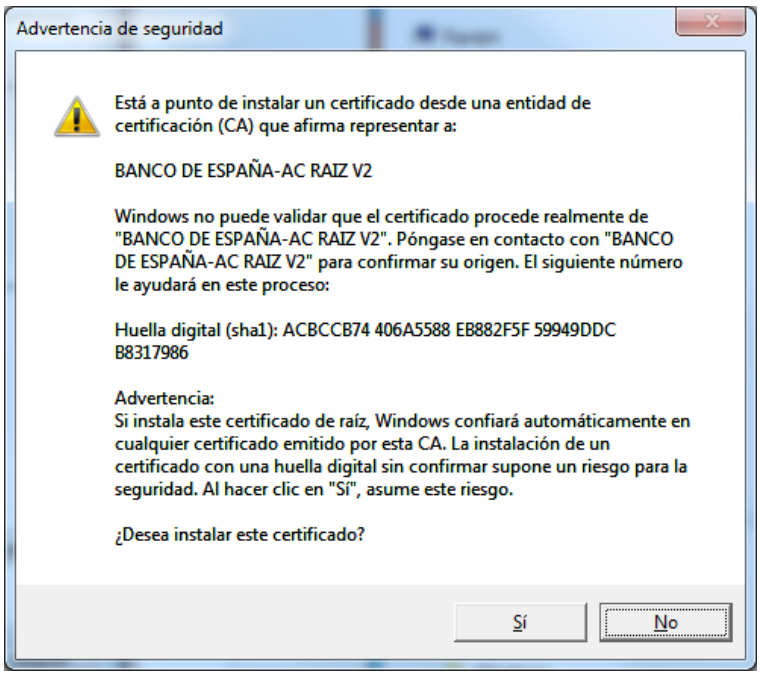
Press the button *Next* (*Siguiente* in the above screenshot) and select manually the *Trusted Root Certification Authority store (Entidades de certificación raíz de confianza in the following screenshot).*



Press the button *Next* and a window summarising the installation will be shown:



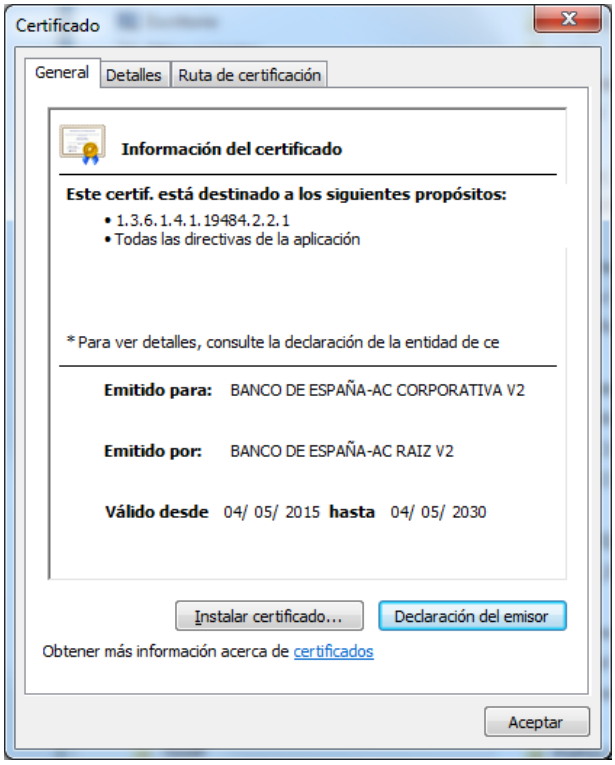
Press the button *Finalise* (*Finalizar* in the above screenshot) and the following confirmation window will be shown:



Press *Yes* (*Sí* in the above screenshot) once you have confirmed that the message digest is the same as the one shown in section 2.1

2.3 Installing Corporate CA v2 certificate

Double click the file ACcorporativav2-sha256.crt. The following window will be shown:



On the *Details* tab (*Detalles* in the above screenshot) you can confirm the attributes shown in section 2.1 in order to confirm that the certificate is the correct one.

Press the button *Install certificate… (Instalar certificado…* in the above screenshot) and the certificate import wizard will be initiated.

Repeat the procedure described for the Root CA v2 certificate, but bear in mind that the store to select has to be "*Intermediate Certification Authority*".