

Eurosistema

Departamento de Sistemas de Información

03.09.2018

# Servicios electrónicos del Banco de España

Instalación de la jerarquía de certificación de Banco de España

## ÍNDICE

- 1 Introducción 1
- 2 Instalación de los certificados de las Autoridades de Certificación de BE 1
  - 2.1 Descarga de los certificados de la AC Raíz v2 y AC Corporativa v2 de PKIBDE 1
  - 2.2 Instalación del certificado de la AC Raíz v2 1
  - 2.3 Instalación del certificado de la AC Corporativa v2 4

#### 1 Introducción

Este documento constituye una guía para la instalación, en sistemas operativos Microsoft Windows (aunque puede también utilizarse como referencia en el caso de otras plataformas), de la jerarquía de certificación de la Infraestructura de Clave Pública de Banco de España (en adelante PKIBDE).

#### 2 Instalación de los certificados de las Autoridades de Certificación de BE

El acceso a los servicios telemáticos de Banco de España puede requerir tener instalado, en el equipo de los usuarios finales, los certificados de las Autoridades de Certificación que conforman la jerarquía de certificación de PKIBDE.

PKIBDE está constituida en base a la siguiente estructura jerárquica:



La Autoridad de Certificación Raíz (AC Raíz v2) ha emitido el certificado de la Autoridad de Certificación Corporativa (AC Corporativa v2), la cual a su vez es la encargada de emitir los certificados de los usuarios de PKIBDE. Las Autoridades de certificación anteriores, sin número de versión, dejaron de ser utilizadas para la emisión de certificados en 2015.

#### 2.1 Descarga de los certificados de la AC Raíz v2 y AC Corporativa v2 de PKIBDE

Se puede obtener una copia de los certificados de la AC Raíz v2 y la AC Corporativa v2 en la sección *Certificados PKIBDE* de la página <u>web de PKIBDE</u>. Los ficheros que contienen dichos certificados son ACraizv2-sha256.crt y ACcorporativav2-sha256.crt, respectivamente. Para asegurar que los certificados descargados son los correctos se puede comprobar la siguiente información:

#### Autoridad de Certificación Raíz v2

- Emisor: CN=BANCO DE ESPAÑA-AC RAIZ V2,O=BANCO DE ESPAÑA,C=ES
- Titular: CN=BANCO DE ESPAÑA-AC RAIZ V2,O=BANCO DE ESPAÑA,C=ES
- Número de serie: 45:54:22:D4:E8:76:1B:FC:55:47:4D:19:4E:85:6E:37
- Huella digital SHA1: AC:BC:CB:74:40:6A:55:88:EB:88:2F:5F:59:94:9D:DC:B8:31:79:86

## Autoridad de Certificación Corporativa v2

- Emisor: CN=BANCO DE ESPAÑA-AC RAIZ V2,O=BANCO DE ESPAÑA,C=ES
- Titular: CN=BANCO DE ESPAÑA-AC CORPORATIVA V2,O=BANCO DE ESPAÑA,C=ES
- Número de serie: 18:D8:76:5B:E6:81:86:C6:55:47:76:F5:92:27:24:80
- Huella digital SHA-1: A8:F0:5C:AC:9C:65:18:C0:8F:F6:3F:82:C3:38:DE:46:D8:B9:3E:38

#### 2.2 Instalación del certificado de la AC Raíz v2

Haga doble click sobre el fichero ACraizv2-sha256.crt. Se mostrará la siguiente ventana:

Certificado				
General Detalles Ruta de certificación				
Información del certificado				
Este certificado raíz de la entidad de certificación no es de confianza. Para habilitar la confianza, instale este certificado en el almacén de entidades de certificación raíz de confianza.				
Emitido para: BANCO DE ESPAÑA-AC RAIZ V2				
Emitido por: BANCO DE ESPAÑA-AC RAIZ V2				
Válido desde 04/05/2015 hasta 04/05/2045				
Instalar certificado         Declaración del emisor           Obtener más información acerca de certificados				
Aceptar				

En la pestaña "Detalles" se podrán comprobar los atributos indicados en el apartado 2.1 para confirmar que se trata del certificado correcto.

A continuación, pulse "Instalar certificado...".

Se iniciará el "Asistente para la importación de certificados":

certificados
<ul> <li>Éste es el Asistente para importación de certificados</li> <li>Este asistente le ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde su disco a un almacén de certificados.</li> <li>Un certificado, que se emite por una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados.</li> <li>Haga clic en Siguiente para continuar.</li> </ul>
< <u>A</u> trás Siguiente > Cancelar

Pulse Siguiente.

En la siguiente pantalla, para asegurar que el certificado se instala en el almacén correcto, elija manualmente el de nombre "Entidades de certificación raíz de confianza":

Asistente para importación de certificados				
Almacén de certificados				
Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.				
Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.				
Seleccionar automáticamente el almacén de certificados según el tipo de certificado				
Colocar todos los certificados en el siguiente almacén				
Almacén de certificados:				
Entidades de certificación raíz de confianza Examinar				
Más información acerca de los <u>almacenes de certificados</u>				
< <u>A</u> trás Siguien <u>t</u> e > Cancelar				

Pulse Siguiente.

Aparecerá la siguiente pantalla:

Asistente para importación de certificados				
	Finalización del Asistente para importación de certificados			
	Se importará el certificado después de hacer dic en Finalizar.			
	Especificó la siguiente configuración:			
	Almacen de certificados seleccionado por el usuario Contenido	Cert		
	< <u> </u>	Þ		
	< <u>A</u> trás Finalizar C	Cancelar		

Pulse Finalizar.

Dado que se trata del certificado de una Autoridad de Certificación raíz de una jerarquía, aparecerá la siguiente advertencia de seguridad para solicitar confirmación:

Advertenci	a de seguridad	A later	x
	Está a punto de instalar un certifica certificación (CA) que afirma repre BANCO DE ESPAÑA-AC RAIZ V2 Windows no puede validar que el o "BANCO DE ESPAÑA-AC RAIZ V2" DE ESPAÑA-AC RAIZ V2" para con le ayudará en este proceso: Huella digital (sha1): ACBCCB74 40 B8317986	ado desde una entidad de esentar a: certificado procede realmente de . Póngase en contacto con "BANCO firmar su origen. El siguiente númer D6A5588 EB882F5F 59949DDC	o
	Advertencia: Si instala este certificado de raíz, W cualquier certificado emitido por e certificado con una huella digital s seguridad. Al hacer clic en "Sí", asu ¿Desea instalar este certificado?	/indows confiará automáticamente esta CA. La instalación de un in confirmar supone un riesgo para ume este riesgo.	en la
		<u>S</u> í <u>N</u> o	

Se puede comprobar que la huella digital basada en el algoritmo SHA1 coincide con la indicada en el apartado 2.1.

Pulse Sí. Aparecerá un mensaje confirmando la instalación del certificado.

## 2.3 Instalación del certificado de la AC Corporativa v2

Haga doble click sobre el fichero ACcorporativav2-sha256.crt. Se mostrará la siguiente ventana:

Certificado
General Detalles Ruta de certificación
Información del certificado
Este certif. está destinado a los siguientes propósitos: • 1.3.6.1.4.1.19484.2.2.1 • Todas las directivas de la aplicación
* Para ver detalles, consulte la declaración de la entidad de ce
Emitido para: BANCO DE ESPAÑA-AC CORPORATIVA V2
Emitido por: BANCO DE ESPAÑA-AC RAIZ V2
Válido desde 04/05/2015 hasta 04/05/2030
Instalar certificado Declaración del emisor Obtener más información acerca de <u>certificados</u>
Aceptar

En la pestaña "Detalles" se podrán comprobar los atributos indicados en el apartado 2.1 para confirmar que se trata del certificado correcto.

Pulse "Instalar certificado...".

Se iniciará el "Asistente para la importación de certificados".

Repita el procedimiento descrito arriba para el certificado de la AC Raíz v2 con la diferencia de que, en esta ocasión, el almacén a elegir ha de ser el de nombre "**Entidades de certificación intermedias**". Además, por no tratarse de la AC raíz de una jerarquía, no aparecerá la advertencia de seguridad.