

**09.04.2010**

**Servicios electrónicos del Banco de España**

Verificación de la firma electrónica de documentos en formato PDF

---



## ÍNDICE

- 1 Introducción 1
- 2 Actualización de las entidades de confianza de Adobe Reader 2
  - 2.1 Descarga de los certificados de la AC Raíz y AC Corporativa de PKIBDE 2
  - 2.2 Alternativa 1: Instalar certificados de PKIBDE en Windows 3
  - 2.3 Alternativa 2: Instalar certificados de PKIBDE en Adobe Reader 8
- 3 Verificación de firmas electrónicas en documentos PDF 12
  - 3.1 Configuración de Adobe Reader 12
  - 3.2 Panel de firmas de Adobe Reader 14
  - 3.3 Verificar una firma 15



## 1 Introducción

Determinados servicios electrónicos ofrecidos por el Banco de España proporcionan información mediante documentos en formato PDF (Portable Document Format). Cuando la naturaleza de la información lo requiere, los documentos pueden estar firmados electrónicamente.

Este documento constituye una guía de configuración y utilización de la aplicación Adobe Reader para validar la firma electrónica de dichos documentos.

Para la elaboración del manual se ha utilizado la versión 9 de Adobe Reader sobre sistema operativo Microsoft Windows. El documento puede también utilizarse como referencia en el caso de otras versiones de la aplicación o de plataformas distintas de Microsoft Windows.

En instalaciones corporativas de Adobe Reader y Microsoft Windows, algunas de las opciones de configuración descritas en este documento podrían no estar disponibles. Si se da tal circunstancia, contacte con el servicio técnico de su organización.

Para más información consulta la ayuda de la aplicación Adobe Reader o la [página web de Adobe](#).

## 2 Actualización de las entidades de confianza de Adobe Reader

Los certificados electrónicos utilizados por los servicios electrónicos del Banco de España para firmar documentos PDF han sido emitidos por la [Infraestructura de Clave Pública del Banco de España](#) (PKIBDE).

PKIBDE está constituida en base a la siguiente estructura jerárquica:

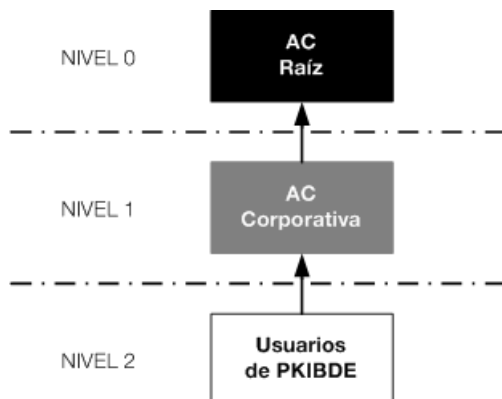


Ilustración 1

La Autoridad de Certificación Raíz (AC Raíz) ha emitido el certificado de la Autoridad de Certificación Corporativa (AC Corporativa), la cual a su vez es la encargada de emitir los certificados de los usuarios de PKIBDE, entre ellos los utilizados para firmar electrónicamente los documentos PDF.

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

Se puede obtener una copia de los certificados de la AC Raíz y la AC Corporativa de PKIBDE en la página [web de PKIBDE](#) o en la [Oficina Virtual del Banco de España](#). Los ficheros que contienen dichos certificados son ACraiz.crt y ACcorporativa.crt, respectivamente. Para asegurar que los certificados descargados son los correctos se puede comprobar la siguiente información:

#### Autoridad de Certificación Raíz

- Emisor: CN=BANCO DE ESPAÑA-AC RAIZ,O=BANCO DE ESPAÑA,C=ES
- Titular: CN=BANCO DE ESPAÑA-AC RAIZ,O=BANCO DE ESPAÑA,C=ES
- Número de serie: F1:6D:75:86:5D:7C:CF:92:41:AD:A1:7A:CD:9A:3D:E2
- Huella digital SHA1: 2B:60:DE:7D:33:37:8B:F7:5B:67:8B:10:77:BB:F9:51:60:29:D6:A8
- Huella digital MD5: 19:B8:11:18:37:E3:F7:57:23:D0:2E:CF:37:B8:8E:22

#### Autoridad de Certificación Corporativa

- Emisor: CN=BANCO DE ESPAÑA-AC RAIZ,O=BANCO DE ESPAÑA,C=ES
- Titular: CN=BANCO DE ESPAÑA-AC CORPORATIVA,O=BANCO DE ESPAÑA,C=ES
- Número de serie: 36:6A:52:4D:A5:E4:4A:F8:41:08:A1:40:9B:9B:76:EB
- Huella digital SHA-1: AB:E6:1E:D2:5A:F6:42:53:F7:7B:32:2F:6F:21:37:29:B5:39:1B:DA
- Huella digital MD5: CE:F6:88:59:37:7F:E4:25:C8:27:DC:01:32:CB:5E:FB

Esta información fue también publicada en la Resolución de 30 de junio de 2006, del Banco de España (BOE de 16 de septiembre), considerando también la corrección de erratas del BOE de 20 de septiembre.

Para la validación de las firmas electrónicas de los documentos PDF se requiere por tanto que la aplicación Adobe Reader considere a la AC Raíz y AC Corporativa del Banco de España como identidades de confianza. A continuación se describen las dos alternativas existentes para realizar esta operación.

## 2.2 Alternativa 1: Instalar certificados de PKIBDE en Windows

Adobe Reader tiene la posibilidad de confiar en las entidades de confianza disponibles en el sistema operativo Microsoft Windows. Por ello, es posible instalar los certificados de la AC Raíz y AC Corporativa de PKIBDE en el almacén de entidades de confianza de Microsoft Windows y, posteriormente, configurar Adobe Reader para confiar en dicho almacén.

Importante: Adobe Reader confiará en las firmas incluidas en documentos PDF generadas no sólo con certificados de PKIBDE, sino también con los emitidos por cualquiera de las Autoridades de Certificación incluidas en el almacén de certificados de Microsoft Windows.

Los pasos a seguir son los siguientes:

### Instalar el certificado de la AC Raíz

Hacer doble click sobre el fichero ACraiz.crt. Se mostrará la siguiente ventana:

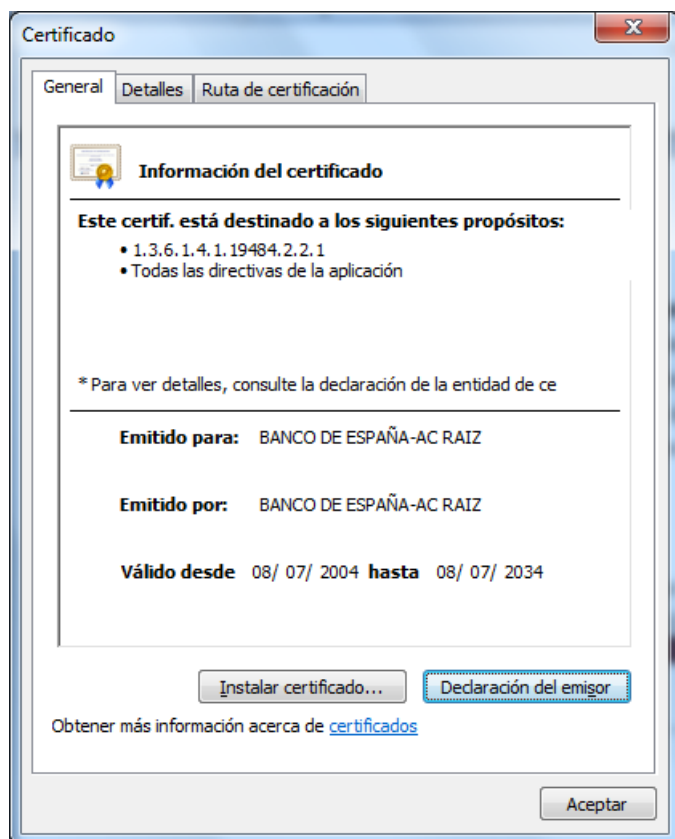


Ilustración 2

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, pulsar “Instalar certificado...”.

Se iniciará el “Asistente para la importación de certificados”:

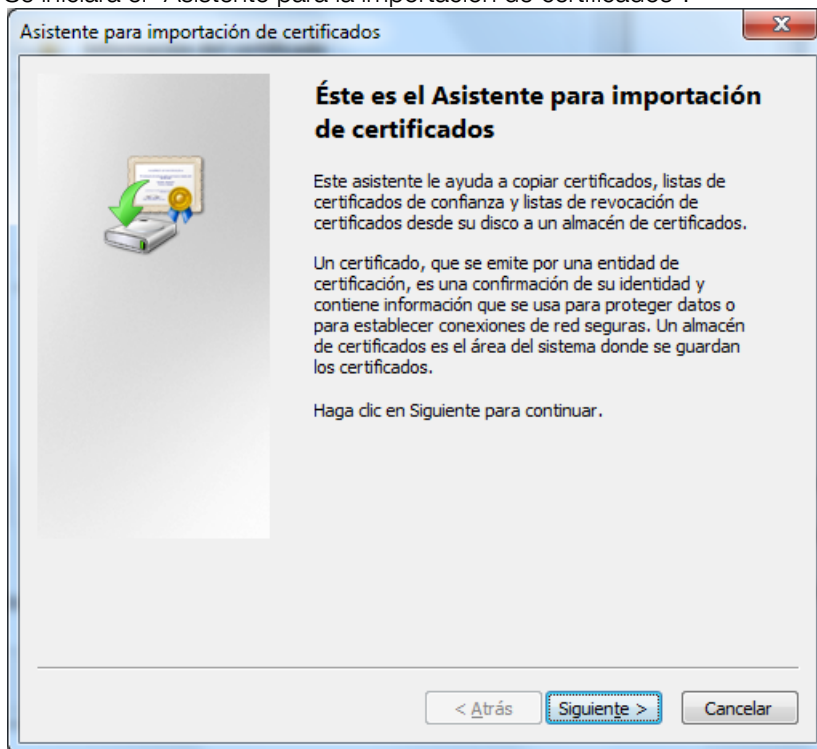


Ilustración 3

Pulsar Siguiente.

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

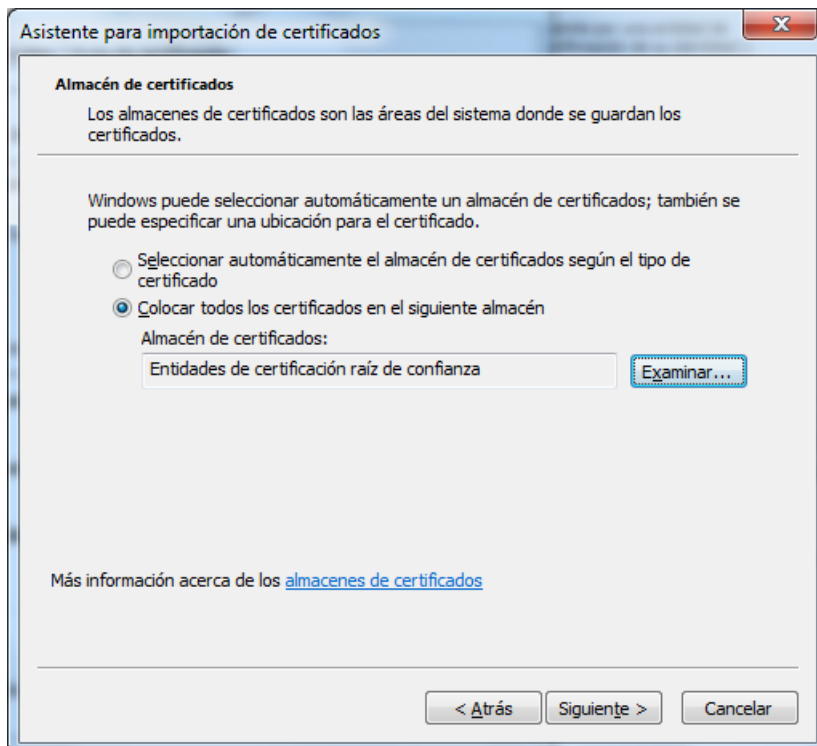


Ilustración 4

Pulsar Siguiente.



Aparecerá la siguiente pantalla:

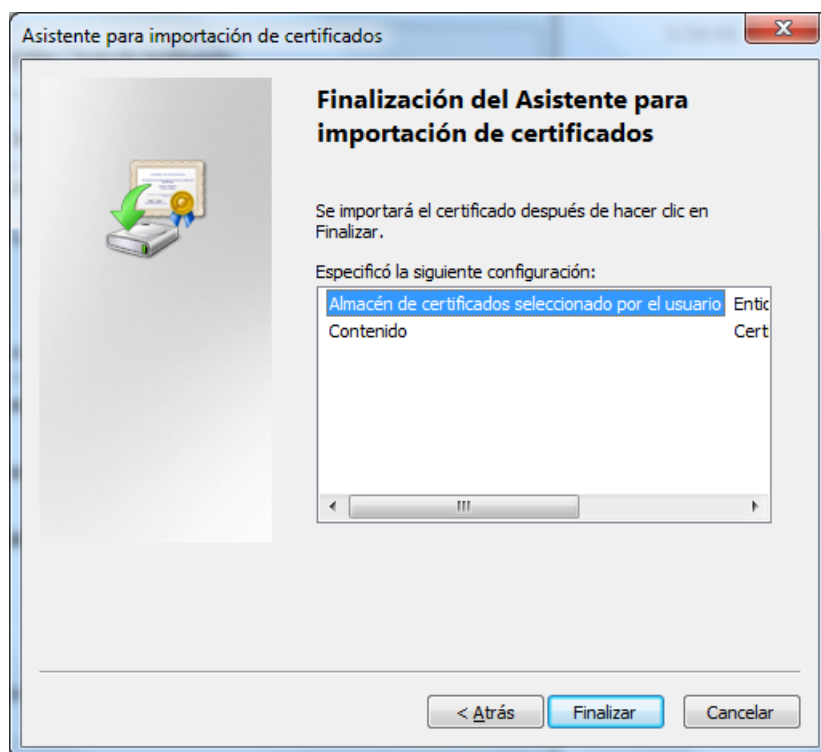


Ilustración 5

Pulsar Finalizar.

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

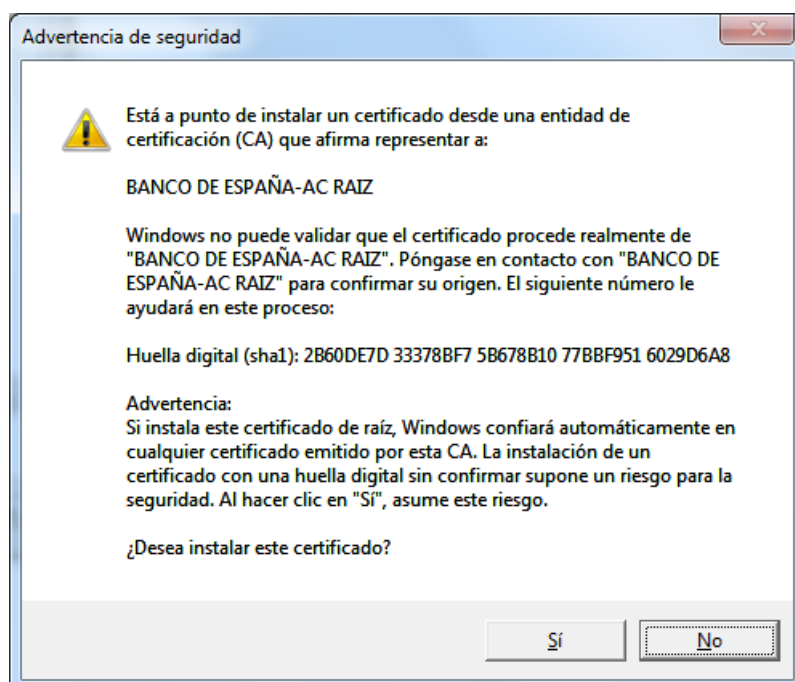


Ilustración 6

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

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

## Instalar el certificado de la AC Corporativa

Hacer doble click sobre el fichero ACcorporativa.crt. Se mostrará la siguiente ventana:

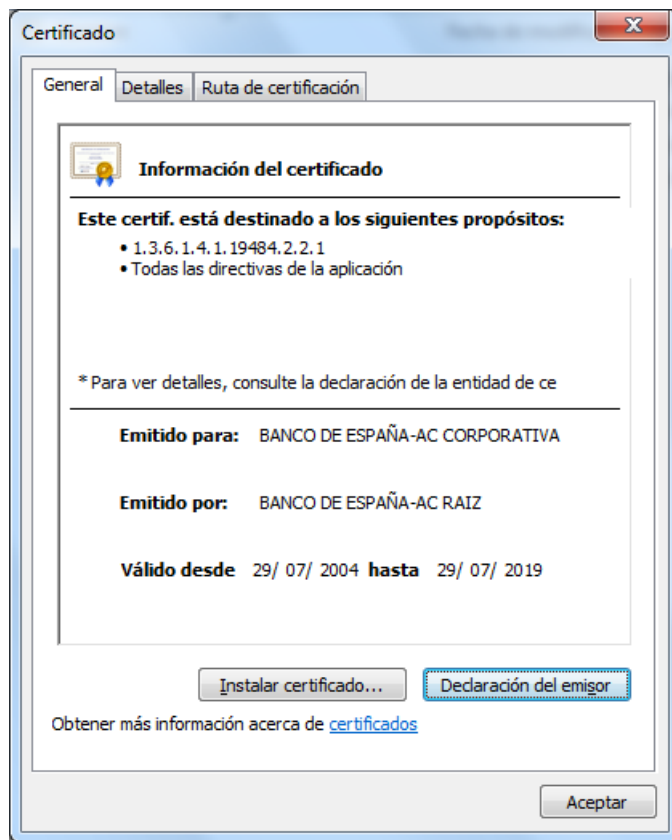


Ilustración 7

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

Pulsar “Instalar certificado...”.

Se iniciará el “Asistente para la importación de certificados”.

Repetir el procedimiento descrito arriba para el certificado de la AC Raíz, 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 pantalla de la ilustración 6.

## Configurar Adobe Reader para confiar en el almacén de Windows

Iniciar Adobe Reader y elegir el menú Edición > Preferencias.

Seleccionar la sección Seguridad y pulsar el botón “Preferencias Avanzadas”.

Elegir la pestaña “Integración de Windows” y pinchar en la opción “Validando firmas” bajo el epígrafe “Confiar en TODOS los certificados raíz del almacén de certificados de Windows para las siguientes operaciones”:

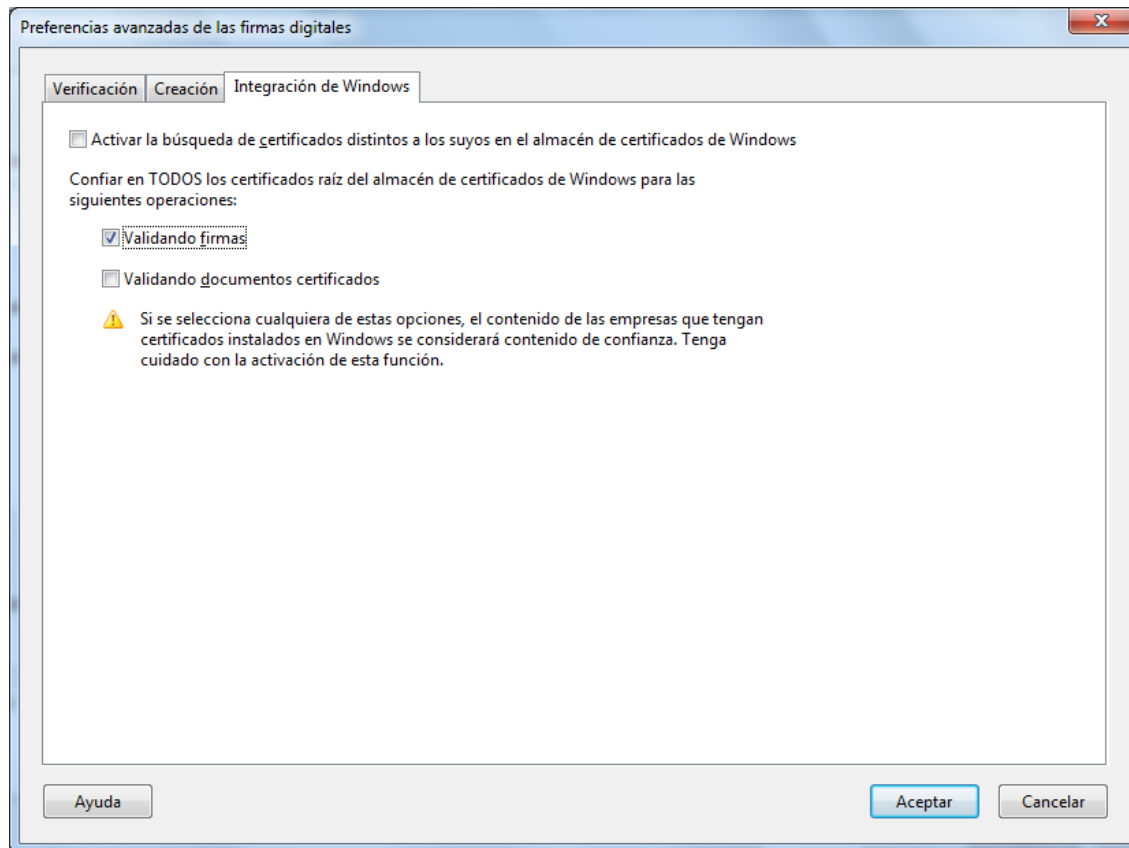


Ilustración 8

Pulsar Aceptar.

### 2.3 Alternativa 2: Instalar certificados de PKIBDE en Adobe Reader

Adobe Reader dispone de su propio almacén de certificados de confianza, por lo que es posible instalar en él los certificados de la AC Raíz y AC Corporativa de PKIBDE para que, de esta forma, la aplicación confíe en las firmas de los documentos PDF.

Los pasos a seguir son los siguientes:

#### Instalar el certificado de la AC Raíz

Iniciar Adobe Reader y elegir el menú Documento > Administrar identidades de confianza...

Aparecerá la siguiente pantalla:

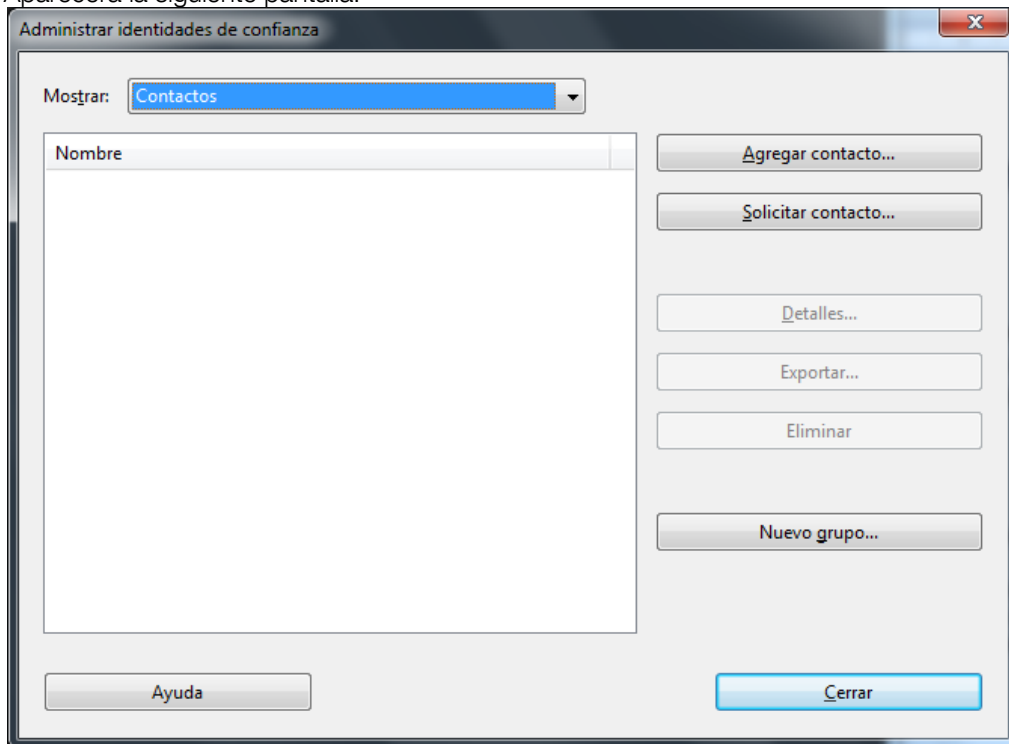


Ilustración 9

Pulsar el botón “Agregar contacto...”

Aparecerá la siguiente pantalla:

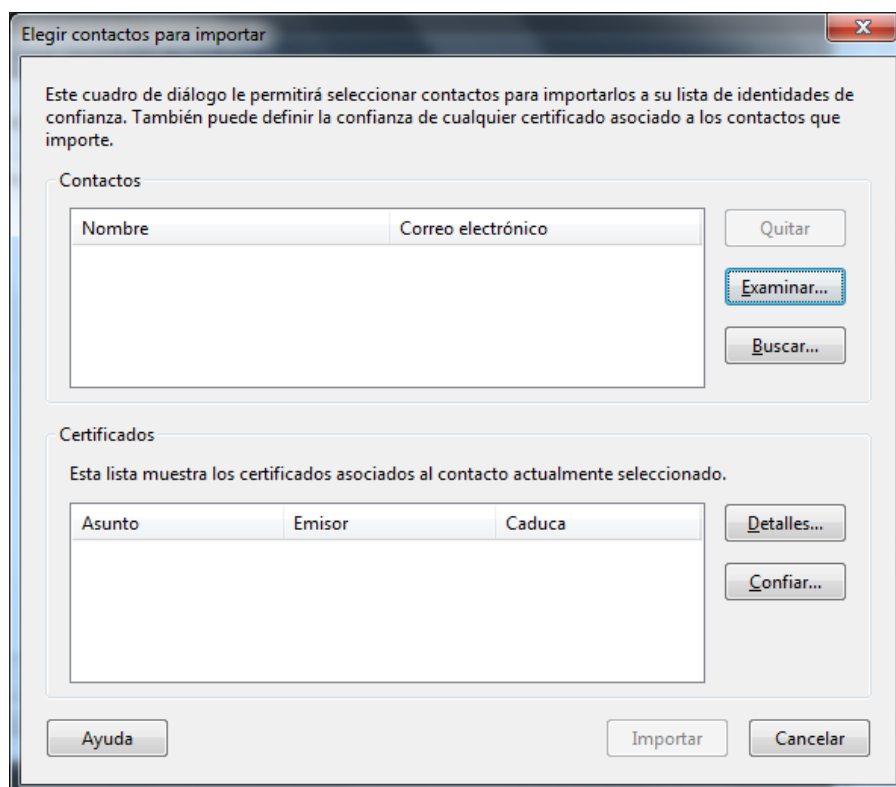


Ilustración 10

Pulsar el botón Examinar y seleccionar el fichero ACraiz.crt:

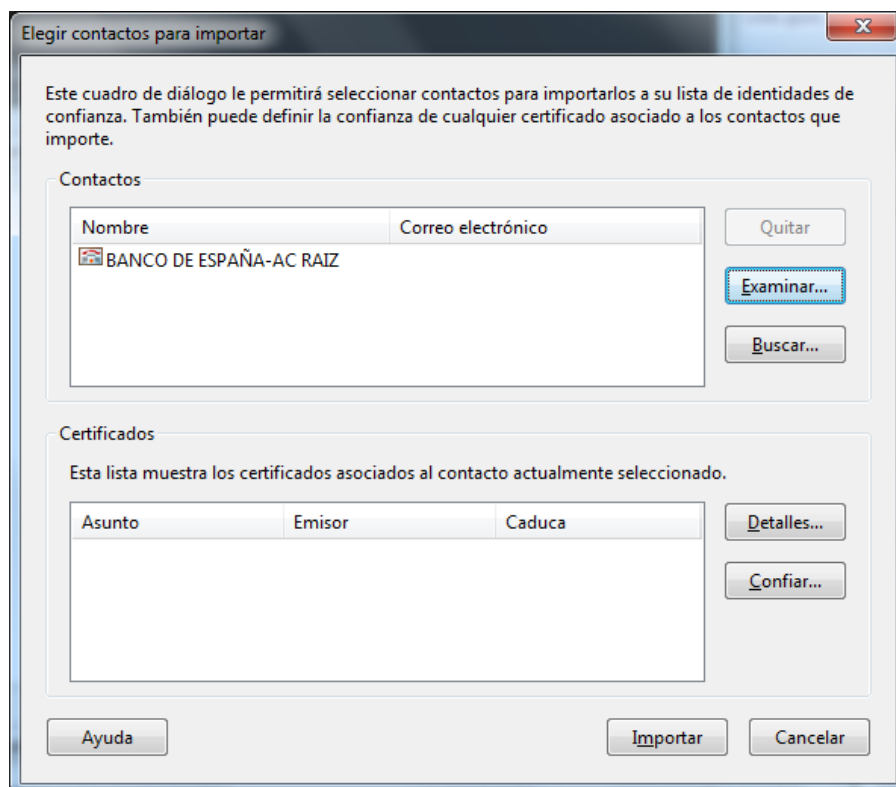


Ilustración 11

En la parte superior de la ventana seleccionar el contacto recién importado y, a continuación, en la parte inferior de la ventana seleccionar el certificado:

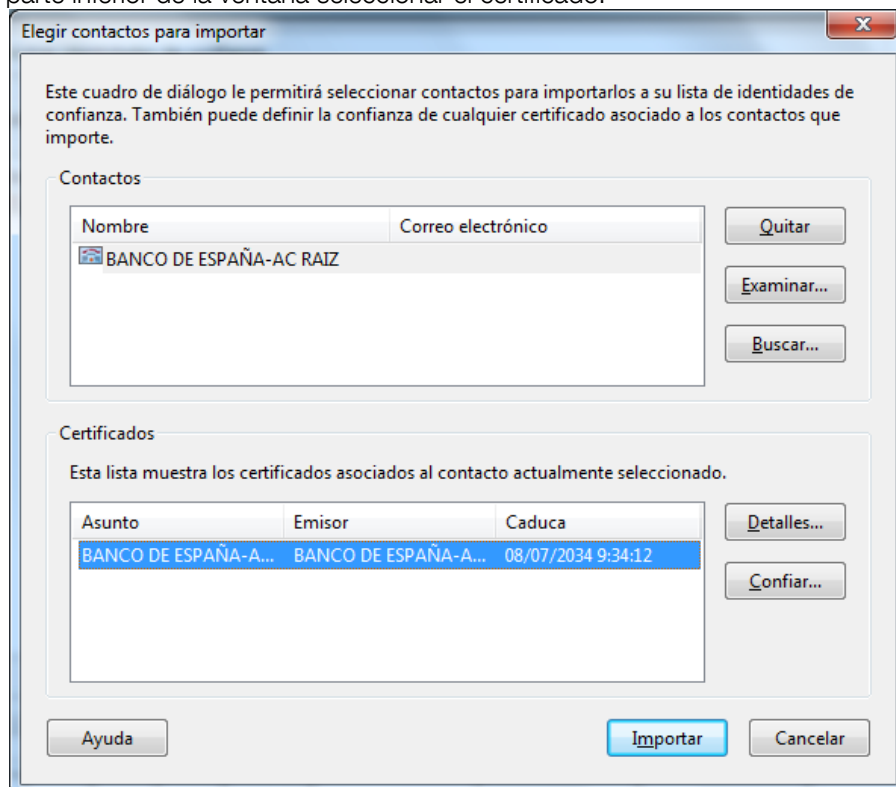


Ilustración 12

Pulsar el botón Confiar:

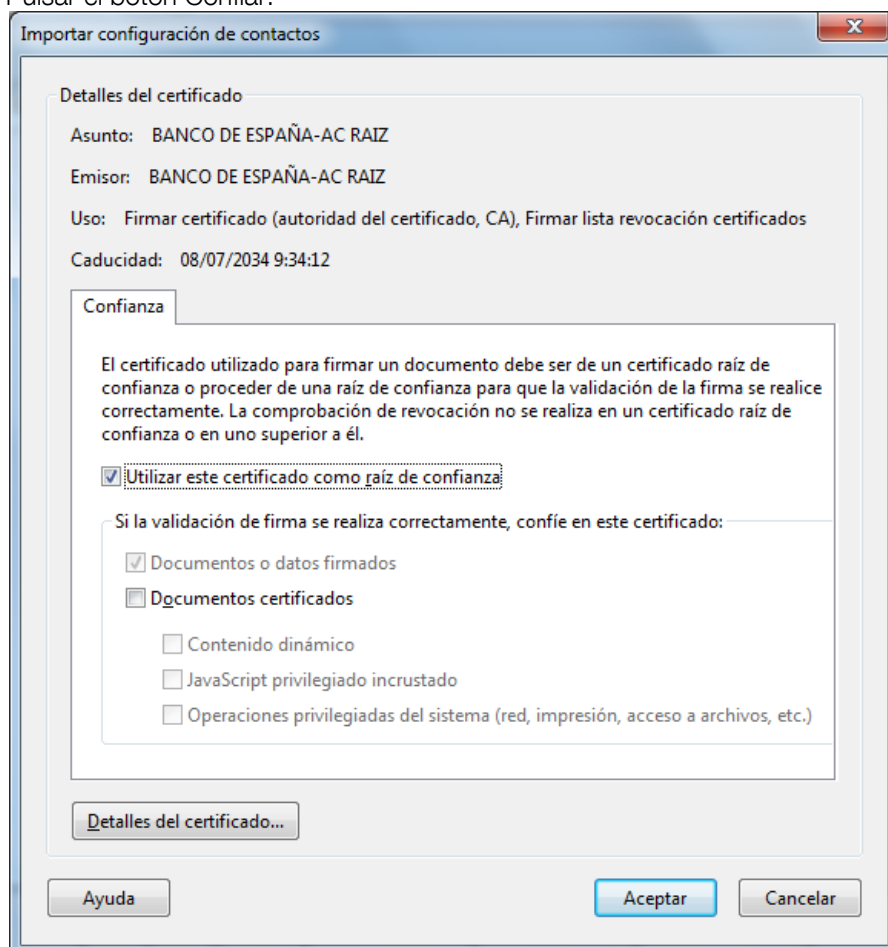


Ilustración 13

Elegir la opción “Utilizar este certificado como raíz de confianza” y pulsar Aceptar.

Aparecerá de nuevo la pantalla de la ilustración 12. Pulsar el botón Importar.

Se mostrará el siguiente mensaje:

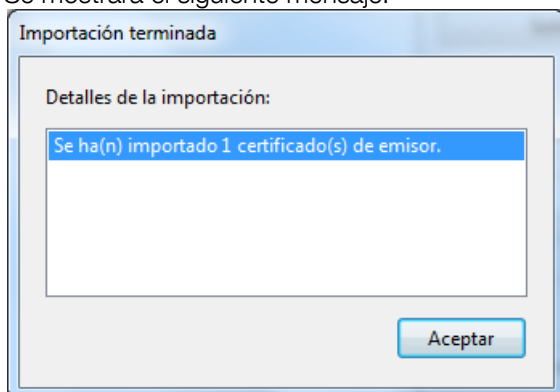


Ilustración 14

### Instalar el certificado de la AC Corporativa

En el menú Documento > Administrar identidades de confianza, de Adobe Reader (ver ilustración 9), repetir el procedimiento descrito para la AC Raíz pero, en esta ocasión, elegir el fichero ACCorporativa.crt. No es necesario confiar en este certificado como raíz de confianza en la ventana de la ilustración 13.

Para confirmar que se han instalado los dos certificados correctamente, en la pantalla de la ilustración 9 elegir “mostrar Certificados”:

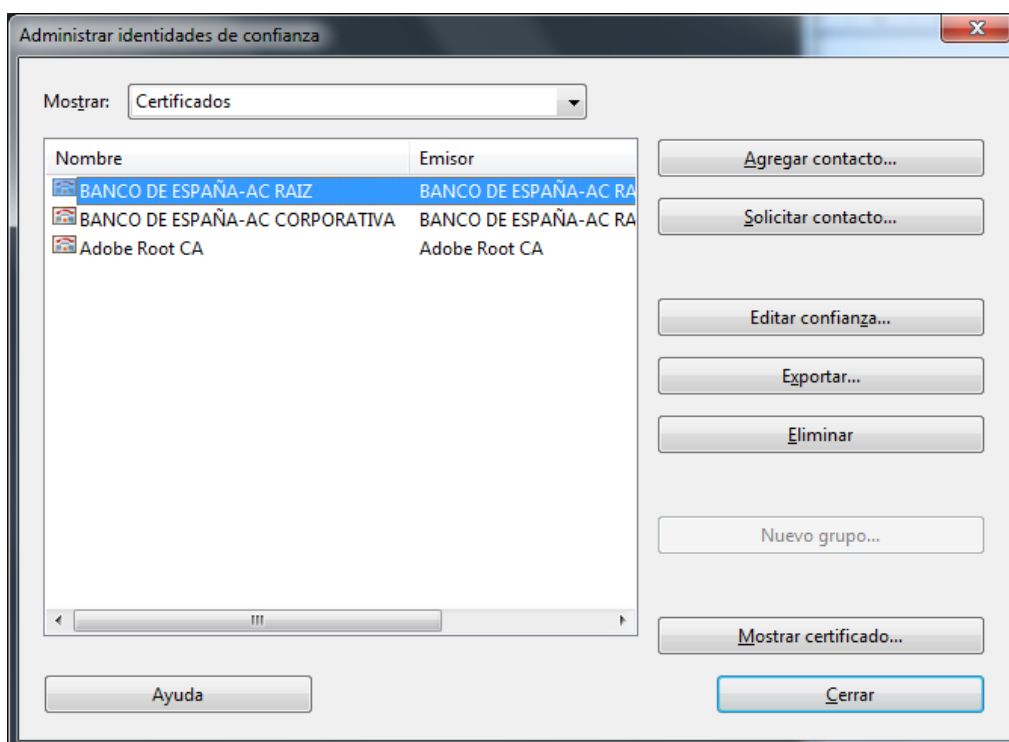


Ilustración 15

Deberán aparecer los certificados de nombre “BANCO DE ESPAÑA – AC RAIZ” y “BANCO DE ESPAÑA – AC CORPORATIVA”. Para confirmar que se trata de los certificados correctos, se puede seleccionar cada uno de ellos y pulsar el botón “Mostrar certificado...”. Se podrá comprobar en la pestaña detalles que los atributos de cada certificado se corresponden con los indicados en el apartado 2.1.

### 3 Verificación de firmas electrónicas en documentos PDF

En este apartado se describe las opciones de configuración de Adobe Reader para la verificación de firmas electrónicas, así como el procedimiento a seguir para realizar la verificación.

#### 3.1 Configuración de Adobe Reader

Iniciar Adobe Reader y elegir el menú Edición > Preferencias.

Seleccionar la sección Seguridad aparecerá la siguiente pantalla:

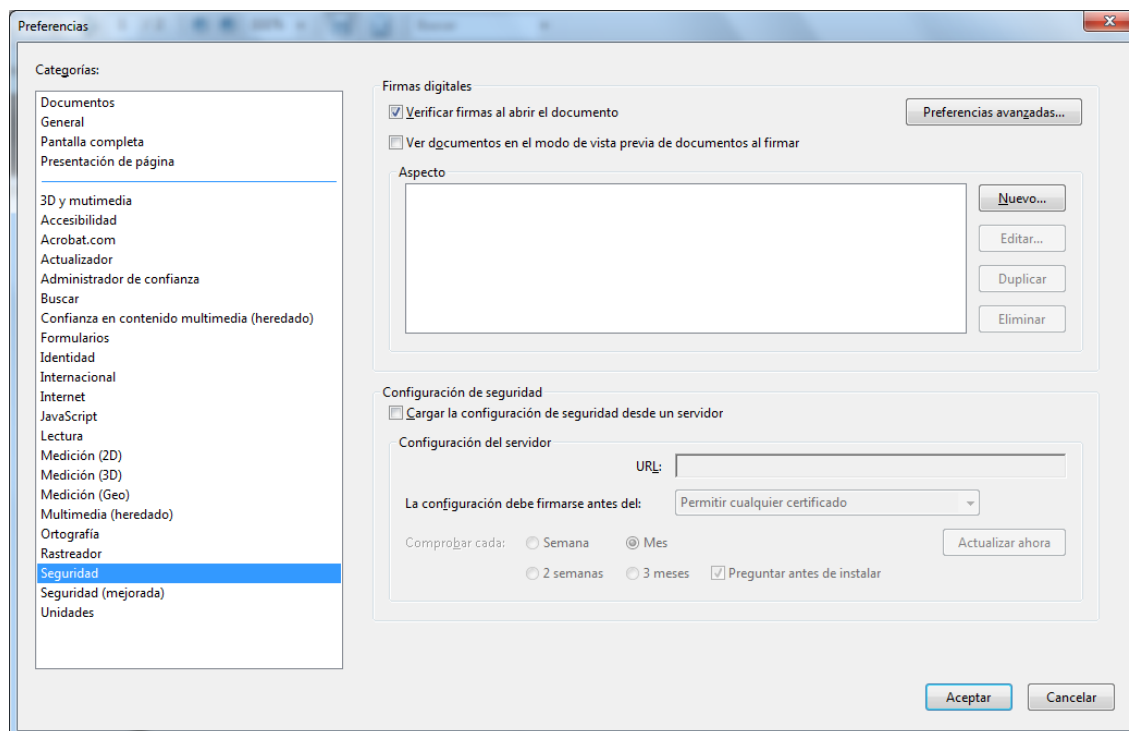


Ilustración 16

Si se desea que Adobe Reader verifique las firmas electrónicas en el momento de abrir los documentos PDF, seleccionar la opción correspondiente. Si no se elige esta opción, se requerirá ejecutar manualmente la opción de menú “Validar firma” en el panel de firma, según se describe en el apartado 3.3.

A continuación, en la ventana de la ilustración 16, pulsar el botón “Preferencias avanzadas...” y seleccionar la pestaña Verificación.



Aparecerá la siguiente pantalla:

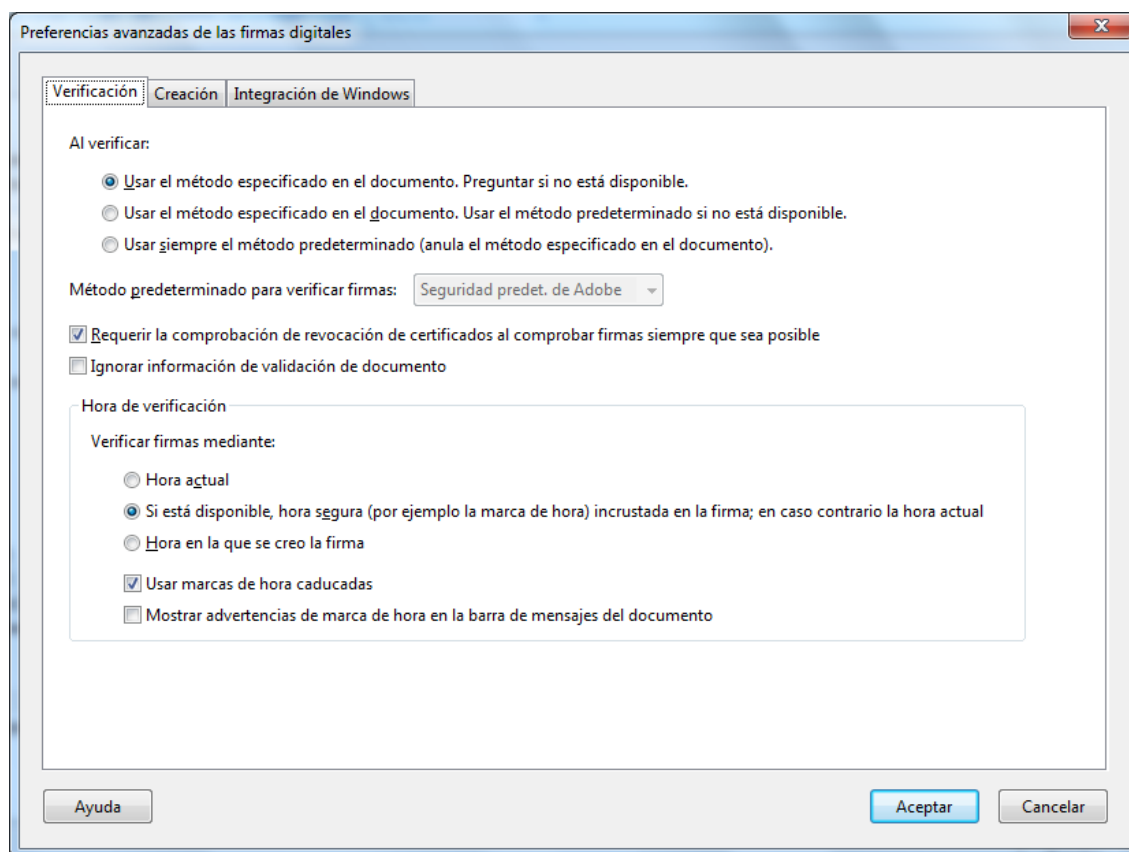


Ilustración 17

Seleccionar las siguientes opciones de configuración:

- Al verificar: usar el método especificado en el documento. Preguntar si no está disponible.
- Requerir la comprobación de revocación de certificados al comprobar firmas siempre que sea posible.
- Hora de verificación. Verificar firmas mediante: si está disponible, hora segura (por ejemplo la marca de hora) incrustada en la firma; en caso contrario la hora actual.

Pulsar Aceptar.

### 3.2 Panel de firmas de Adobe Reader

Para verificar la firma electrónica de un documento PDF y acceder a la información sobre el firmante, se requiere utilizar el panel de firmas.

Dicho panel habitualmente se muestra de forma automática si el documento PDF está firmado. En cualquier caso, puede accederse al panel de firma mediante el menú Ver > Paneles de navegación > Firmas

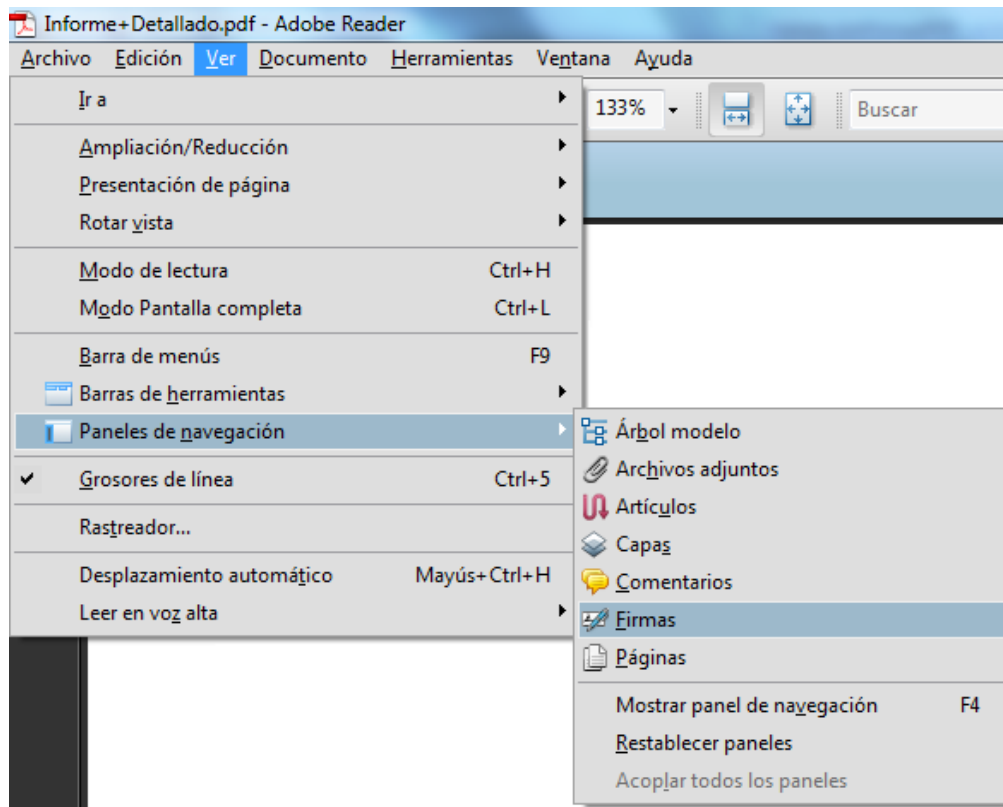


Ilustración 18

El panel de firmas aparecerá situado a la izquierda de la pantalla:

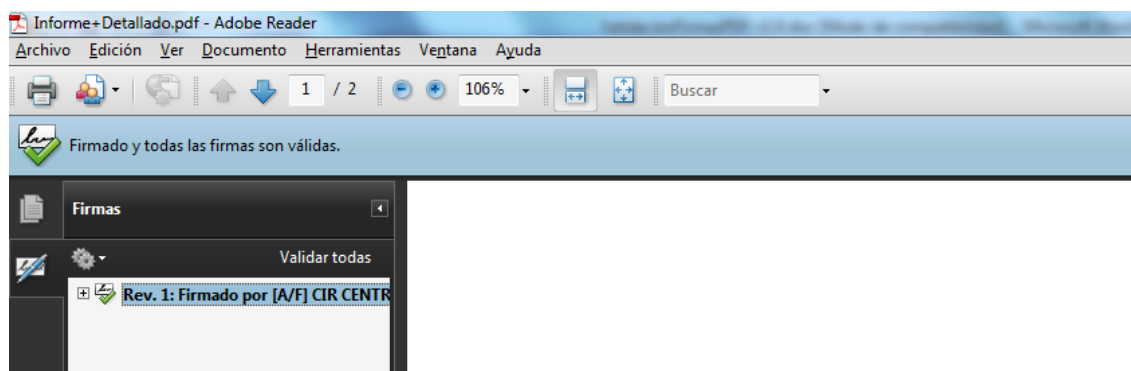


Ilustración 19

Nota: si el panel de firmas no está disponible será debido a que el documento PDF no está firmado electrónicamente.

### 3.3 Verificar una firma

Para verificar una firma se ha de pulsar con el botón derecho del ratón sobre la firma a verificar en el panel de firmas (pantalla de la ilustración 19) y elegir la opción “Validar firma”:

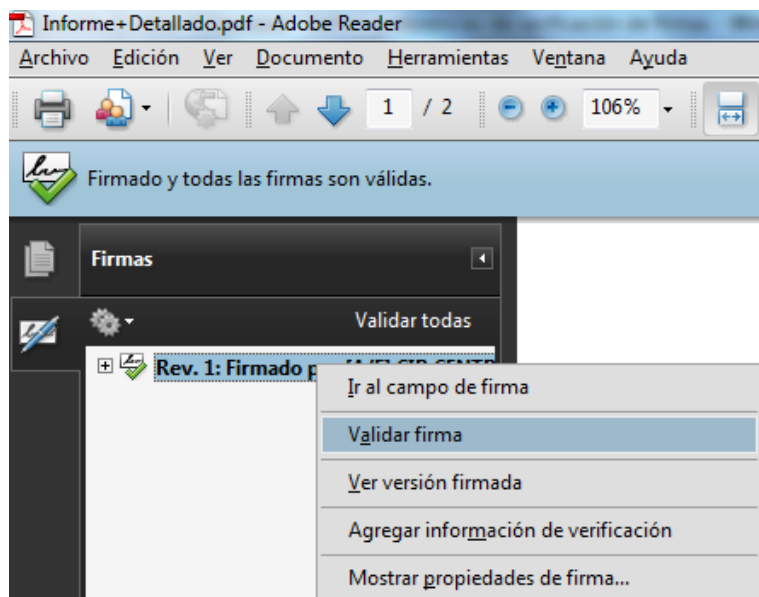


Ilustración 20

Pasados unos segundos, requeridos para que Adobe Reader obtenga la información de revocación publicada por la Autoridad de Certificación, aparecerá la una ventana que informa sobre el resultado de la verificación:

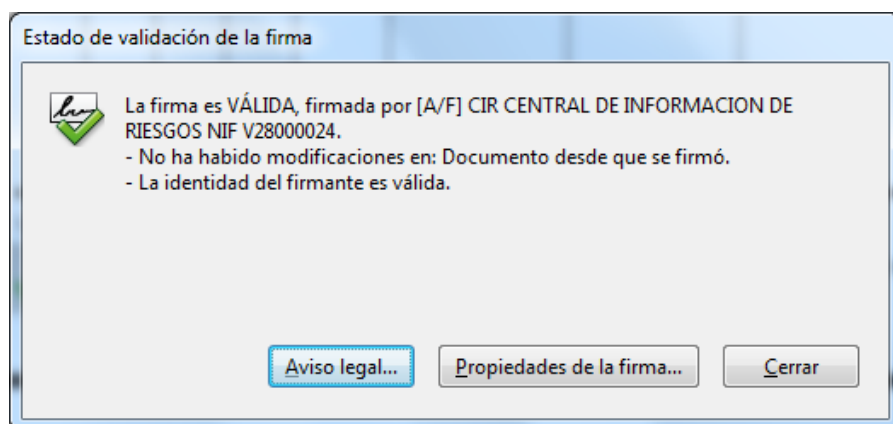


Ilustración 21

Al pulsar el botón “Propiedades de la firma...” aparecerá la siguiente ventana, que permite obtener información detallada sobre la verificación de la firma, el certificado del firmante incluyendo su estado de revocación, y la fecha y hora en la que se firmó el documento:

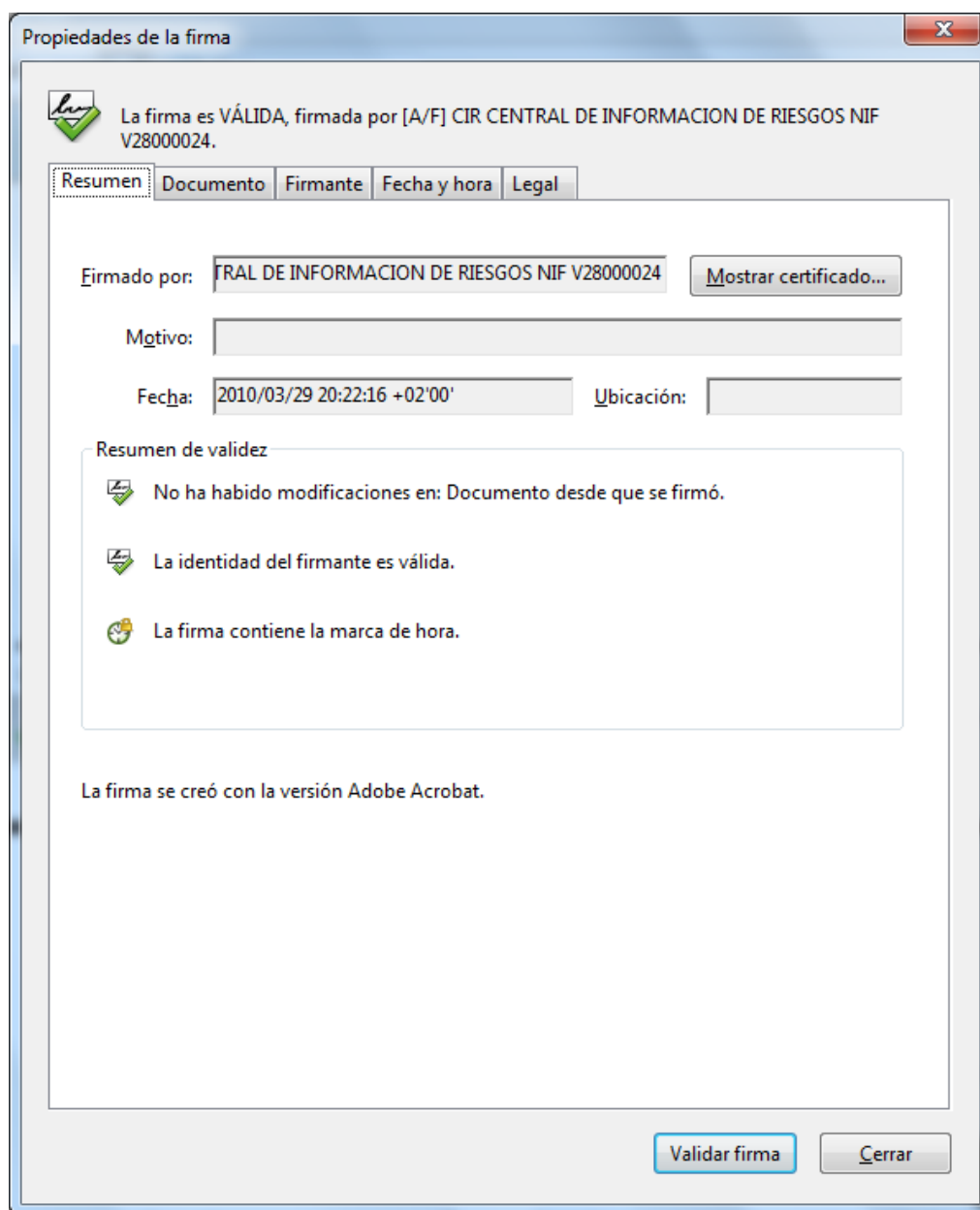


Ilustración 22