BANCODE ESPAÑA

Eurosistema

Departamento de Sistemas de Información

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 <u>Infraestructura de Clave Pública del Banco de</u> <u>España</u> (PKIBDE).



PKIBDE está constituida en base a la siguiente estructura jerárquica:

llustración 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 <u>web de PKIBDE</u> o en la <u>Oficina Virtual del Banco de España</u>. 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:

| Certificado | x |
|--|-----|
| 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 RAIZ | |
| Emitido por: BANCO DE ESPAÑA-AC RAIZ | |
| Válido desde 08/07/2004 hasta 08/07/2034 | |
| Instalar certificado Declaración del emiso Obtener más información acerca de <u>certificados</u> | r |
| Асер | tar |

llustración 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...".

х Asistente para importación de certificados Éste es el Asistente para importación de certificados 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. 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 es el área del sistema donde se guardan los certificados. Haga clic en Siguiente para continuar. < <u>A</u>trás Siguien<u>t</u>e > Cancelar

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":

| As | sistente 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 |
| | Olocar todos los certificados en el siguiente almacén |
| | Almacén de certificados: |
| | Entidades de certificación raíz de confianza |
| | Más información acerca de los <u>almacenes de certificados</u> |
| | < <u>A</u> trás Siguien <u>t</u> e > Cancelar |

llustración 4

Pulsar Siguiente.

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

Aparecerá la siguiente pantalla:

| Asistente para importación de ce | ertificados | x |
|----------------------------------|--|-------------------------|
| | Finalización del Asi importación de cert | stente para ificados |
| | Se importará el certificado desp Finalizar. | ués de hacer dic en |
| | Especificó la siguiente configura | ición: |
| | Contenido | Cert |
| | | |
| | | |
| | | |
| | | |
| | | • |
| | | |
| | | |
| | | |
| | | |
| | < <u>A</u> trás | Finalizar Cancelar |
| | | |

llustración 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:

| Advertenci | a de seguridad |
|------------|---|
| | Está a punto de instalar un certificado desde una entidad de certificación (CA) que afirma representar a: BANCO DE ESPAÑA-AC RAIZ Windows no puede validar que el certificado procede realmente de "BANCO DE ESPAÑA-AC RAIZ". Póngase en contacto con "BANCO DE ESPAÑA-AC RAIZ" para confirmar su origen. El siguiente número le ayudará en este proceso: |
| | Huella digital (sha1): 2B60DE7D 33378BF7 5B678B10 77BBF951 6029D6A8 |
| | Advertencia: Si instala este certificado de raíz, Windows confiará automáticamente en cualquier certificado emitido por esta CA. La instalación de un certificado con una huella digital sin confirmar supone un riesgo para la seguridad. Al hacer clic en "Sí", asume este riesgo. |
| | ¿Desea instalar este certificado? |
| | Sí |

llustración 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:

| 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 |
| Emitido por: BANCO DE ESPAÑA-AC RAIZ |
| Válido desde 29/ 07/ 2004 hasta 29/ 07/ 2019 |
| Instalar certificado Declaración del emisor Obtener más información acerca de <u>certificados</u> |
| Aceptar |

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":

| Preferencias avanzadas de las firmas digitales | x |
|---|---|
| Verificación Creación Integración de Windows | |
| Activar la búsqueda de certificados distintos a los suyos en el almacén de certificados de Windows | |
| Confiar en TODOS los certificados raíz del almacén de certificados de Windows para las siguientes operaciones: | |
| Validando firmas | |
| Validando <u>d</u> ocumentos certificados | |
| Si se selecciona cualquiera de estas opciones, el contenido de las empresas que tengan certificados instalados en Windows se considerará contenido de confianza. Tenga cuidado con la activación de esta función. | |
| | |
| Ayuda Aceptar Cancelar | |

llustración 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: Administrar identidades de confianza Mosţrar: Contactos Nombre Agregar contacto... Solicitar contacto... Detalles... Exportar... Eiminar Nuevo grupo... Ayuda Cerrar

llustración 9

Pulsar el botón "Agregar contacto..."

Aparecerá la siguiente pantalla:

| egir contactos para imp | oortar | _ | |
|--|--|--|--|
| Este cuadro de diálogo confianza. También pi importe. Contactos |) le permitirá seleccion Jede definir la confian: | ar contactos para importarlos a za de cualquier certificado asoci | su lista de identidades de iado a los contactos que |
| Nombre | | Correo electrónico | Quitar |
| | | | <u>E</u> xaminar |
| | | | <u>B</u> uscar |
| Certificados Esta lista muestra lo | os certificados asociado | os al contacto actualmente sele | ccionado. |
| Asunto | Emisor | Caduca | Detalles |
| | | | <u>C</u> onfiar |
| Ayuda | | In | nportar Cancelar |

llustración 10

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

| Elegir contactos para imp | oortar | | X |
|---|--|---|--|
| Este cuadro de diálogo confianza. También p importe. Contactos | o le permitirá selecc uede definir la confi | ionar contactos para importarlos a su li ianza de cualquier certificado asociado | sta de identidades de a los contactos que |
| Nombre | | Correo electrónico | Quitar |
| Certificados Esta lista muestra lo | PAÑA-AC RAIZ | iados al contacto actualmente seleccior | Examinar Buscar |
| Asunto | Emisor | Caduca | Detalles |
| Ayuda | | Import | Confiar |

llustración 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:

| legir contactos para importar | _ | | × |
|---|--|--|---|
| Este cuadro de diálogo le per confianza. También puede de importe. Contactos | mitirá seleccionar contacto finir la confianza de cualq | os para importarlos a s uier certificado asocia | su lista de identidades de ado a los contactos que |
| Nombre | Correo elec | trónico | Quitar |
| 📾 BANCO DE ESPAÑA-A | AC RAIZ | | |
| | | | <u>E</u> xaminar |
| | | | <u>B</u> uscar |
| | | | |
| 0.00 | | | |
| Certificados | | | |
| Esta lista muestra los certif | ficados asociados al contac | to actualmente selec | cionado. |
| Asunto | Emisor | Caduca | Detalles |
| BANCO DE ESPAÑA-A | BANCO DE ESPAÑA-A | 08/07/2034 9:34:12 | |
| | | | <u>C</u> onfiar |
| | | | |
| | | | |
| | | | |
| Ayuda | | Im | portar Cancelar |
| | | | |

llustración 12

Pulsar el botón Confiar:

| Detalles del certificado Asunto: BANCO DE ESPAÑA-AC RAIZ Emisor: BANCO DE ESPAÑA-AC RAIZ Uso: Firmar certificado (autoridad del certificado, CA), Firmar lista revocación certificados Caducidad: 08/07/2034 9:34:12 Confianza El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. VIIIizar este certificado como raíz de confianza Si la validación de firma se realiza correctamente, confíe en este certificado: Documentos o datos firmados Degumentos certificados Contenido dinámico JavaScript privilegiada incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado | Importar configuración de contactos | × |
|---|--|-----|
| Asunto: BANCO DE ESPAÑA-AC RAIZ Emisor: BANCO DE ESPAÑA-AC RAIZ Uso: Firmar certificado (autoridad del certificado, CA), Firmar lista revocación certificados Caducidad: 08/07/2034 9:34:12 Confianza El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. Ø Utilizar este certificado como raíz de confianza Si la validación de firma se realiza correctamente, confíe en este certificado: Ø Documentos o datos firmados Ø Documentos certificados Operaciones privilegiado incrustado Ø Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Letalles del certificado | - Detaller del certificado | |
| Haundi, Banco DE ESPAÑA-AC RAIZ Uso: Firmar certificado (autoridad del certificado, CA), Firmar lista revocación certificados Caducidad: 08/07/2034 9:34:12 Confianza El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. ØUtilizar este certificado como raíz de confianza Si la validación de firma se realiza correctamente, confíe en este certificado: Ø Documentos o datos firmados Ogcumentos certificados Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado | Acusto: BANCO DE ESPAÑA-AC BAIZ | |
| Emisor: BANCO DE ESPANA-AC RAIZ Uso: Firmar certificado (autoridad del certificado, CA), Firmar lista revocación certificados Caducidad: 08/07/2034 9:34:12 Confianza El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. VUtilizar este certificado como raíz de confianza Si la validación de firma se realiza correctamente, confíe en este certificado: Documentos o datos firmados Documentos certificados Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado | | |
| Uso: Firmar certificado (autoridad del certificado, CA), Firmar lista revocación certificados Caducidad: 08/07/2034 9:34:12 Confianza El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. V Utilizar este certificado como raíz de confianza Si la validación de firma se realiza correctamente, confíe en este certificado: Documentos o datos firmados Documentos certificados Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado | Emisor: BANCO DE ESPANA-AC RAIZ | |
| Caducidad: 08/07/2034 9:34:12 Confianza El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. Utilizar este certificado como raíz de confianza Si la validación de firma se realiza correctamente, confíe en este certificado: Documentos o datos firmados Documentos certificados Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado Ayuda Aceptar Cancelar | Uso: Firmar certificado (autoridad del certificado, CA), Firmar lista revocación certificados | |
| Confianza El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. Image: Ima | Caducidad: 08/07/2034 9:34:12 | |
| El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. | Confianza | |
| Si la validación de firma se realiza correctamente, confíe en este certificado: Documentos o datos firmados Documentos certificados Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado Ayuda Aceptar Cancelar | El certificado utilizado para firmar un documento debe ser de un certificado raíz de confianza o proceder de una raíz de confianza para que la validación de la firma se realico correctamente. La comprobación de revocación no se realiza en un certificado raíz de confianza o en uno superior a él. | e |
| Documentos o datos firmados Documentos certificados Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado Ayuda Aceptar Cancelar | Si la validación de firma se realiza correctamente, confíe en este certificado: | _ |
| Documentos certificados Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado Ayuda | Documentos o datos firmados | |
| Contenido dinámico JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado Ayuda Aceptar Cancelar | Documentos certificados | |
| JavaScript privilegiado incrustado Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado Ayuda Aceptar Cancelar | Contenido dinámico | |
| Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) Detalles del certificado Ayuda Aceptar Cancelar | JavaScript privilegiado incrustado | |
| Detalles del certificado Ayuda Aceptar Cancelar | Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.) | |
| Detalles del certificado Ayuda Aceptar Cancelar | | |
| Ayuda Aceptar Cancelar | Detalles del certificado | |
| | Ayuda Aceptar Cance | lar |

llustración 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.

| 00 | montrará | | aiguianta | monooio |
|----|----------|----|-----------|----------|
| Se | mostrara | ei | siguiente | mensaje. |

| I | Importación terminada |
|---|--|
| | Detalles de la importación: |
| | Se ha(n) importado 1 certificado(s) de emisor. |
| | |
| | |
| | |
| | Aceptar |
| L | |

llustración 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":

| Administrar i | dentidades de confianza | | X |
|-------------------|--|---|---------------------------|
| Mos <u>t</u> rar: | Certificados | • | |
| Nombre | | Emisor | Agregar contacto |
| BANC BANC | O DE ESPANA-AC RAIZ O DE ESPAÑA-AC CORPORATIVA e Root CA | BANCO DE ESPANA-AC RA BANCO DE ESPAÑA-AC RA Adobe Root CA | Solicitar contacto |
| | | | Editar confian <u>z</u> a |
| | | | Exportar |
| | | | <u>E</u> liminar |
| | | | Nuevo grupo |
| • | III | | Mostrar certificado |
| | Ayuda | | <u>C</u> errar |

| Ilustración 15 | ción 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:

| <u>V</u> erificar firmas al abrir el documento <u> </u> | e documentos al firmar | Preferencias avan <u>z</u> adas |
|---|--|---|
| Ver d <u>o</u> cumentos en el modo de vista previa d Aspecto | e documentos al firmar | |
| Aspecto | | |
| Aspecto | | |
| | | |
| | | <u>N</u> uevo |
| | | |
| | | Editar |
| | | |
| | | Duplicar |
| | | |
| | | Eliminar |
| | | |
| | | |
| Configuración de seguridad | | |
| Cargar la configuración de seguridad desde u | in servidor | |
| | | |
| Configuración del servidor | | |
| UR <u>L</u> : | | |
| | | |
| La configuración debe firmarse antes del: | Permitir cualquier certificado | T |
| Complexity Officers Other | _ | A sturfferer shares |
| Comprogar cada: Semana @ Mes | 5 | Actualizar anora |
| 🔘 2 semanas 🛛 3 m | eses 🛛 📝 Preguntar antes de instalar | |
| | | |
| | | |
| | Configuración de seguridad Configuración de seguridad desde u Configuración del servidor URL: La configuración debe firmarse antes del: Comprobar cada: Semana @ Mer 2 semanas 3 m | Configuración de seguridad □ Cargar la configuración de seguridad desde un servidor Configuración del servidor URL: La configuración debe firmarse antes del: Comprobar cada: Comprobar ca |

llustración 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:

| Preferencias avanzadas de las firmas digitales |
|---|
| |
| Verricación Creación Integración de Windows |
| Al verificar: |
| Usar el método especificado en el documento. Preguntar si no está disponible. |
| O Usar el método especificado en el documento. Usar el método predeterminado si no está disponible. |
| ○ Usar siempre el método predeterminado (anula el método especificado en el documento). |
| Método <u>p</u> redeterminado para verificar firmas: Seguridad predet. de Adobe 👻 |
| Requerir la comprobación de revocación de certificados al comprobar firmas siempre que sea posible |
| Ignorar información de validación de documento |
| - Hora de verificación |
| Verificar firmas mediante: |
| ○ Hora a <u>c</u> tual |
| Si está disponible, hora segura (por ejemplo la marca de hora) incrustada en la firma; en caso contrario la hora actual |
| ○ Hora en la que se creo la firma |
| ☑ Usar marcas de hora caducadas |
| Mostrar advertencias de marca de hora en la barra de mensajes del documento |
| |
| |
| |
| |
| Ayuda Aceptar Cancelar |
| |

llustración 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

| 🔁 Informe+Detallado.pdf - Adobe Reader | | | |
|---|----------------------------------|---|--|
| <u>A</u> rchivo <u>E</u> dición <u>V</u> er <u>D</u> ocumento | <u>H</u> erramientas Ve <u>n</u> | tana A <u>y</u> uda | |
| <u>I</u> r a | • | 133% - 📑 🔂 Buscar | |
| <u>A</u> mpliación/Reducción | • | | |
| Presentación de página | + | | |
| Rotar <u>v</u> ista | • | | |
| Modo de lectura | Ctrl+H | | |
| M <u>o</u> do Pantalla completa | Ctrl+L | | |
| <u>B</u> arra de menús | F9 | | |
| 🔤 Barras de <u>h</u> erramientas | • | | |
| 🔲 Paneles de <u>n</u> avegación | • | 몉 Ár <u>b</u> ol modelo | |
| ✓ <u>G</u> rosores de línea | Ctrl+5 | Archivos adjuntos | |
| Ras <u>t</u> reador | | UL Artíc <u>u</u> los | |
| Decelaramiento automático | Mayoʻo Ctolu H | ∠ Sepas | |
| Less en une elle | wayus+Ctii+H | Comentarios | |
| Leer en vo <u>z</u> alta | | - <u>F</u> irmas | |
| | | 🕒 <u>P</u> áginas | |
| | | Mostrar panel de na <u>v</u> egación F4 | |
| | | <u>R</u> establecer paneles | |
| | | Acop <u>l</u> ar todos los paneles | |
| | | | |

llustración 18

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

| 🔁 Info | rme+Detallado.pdf - Adobe I | Reader | Table Control of | We class that is smaller | and manufacture |
|----------------|---|---|------------------|--------------------------|-----------------|
| <u>A</u> rchiv | o <u>E</u> dición <u>V</u> er <u>D</u> ocumer | nto <u>H</u> erramientas Ve <u>n</u> tana | Ayuda | | |
| 8 | 💩 • 🖏 🛧 🤻 | 1 / 2 💿 🖲 10 | 6% 🛛 🖶 🔂 Bus | car 🗸 | |
| lar | Firmado y todas las firmas so | on válidas. | | | |
| ľ | Firmas | 4 | | | |
| 1 | % - | Validar todas | | | |
| | 🗄 🗳 Rev. 1: Firmado por | [A/F] CIR CENTR | | | |

llustración 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":



llustración 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:

| Estado de | e validación de la firma |
|-----------|--|
| lu | La firma es VÁLIDA, firmada por [A/F] CIR CENTRAL DE INFORMACION DE RIESGOS NIF V28000024. - No ha habido modificaciones en: Documento desde que se firmó. - La identidad del firmante es válida. |
| | <u>Aviso legal</u> <u>P</u> ropiedades de la firma <u>C</u> errar |

llustración 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:

| Propiedades de la firma | × | | | |
|--|--------|--|--|--|
| La firma es VÁLIDA, firmada por [A/F] CIR CENTRAL DE INFORMACION DE RIESGOS NI V28000024. | F | | | |
| Resumen Documento Firmante Fecha y hora Legal | | | | |
| Eirmado por: FRAL DE INFORMACION DE RIESGOS NIF V28000024 | | | | |
| M <u>o</u> tivo: | | | | |
| Fec <u>h</u> a: 2010/03/29 20:22:16 +02'00' <u>U</u> bicación: | | | | |
| Resumen de validez | \neg | | | |
| No ha habido modificaciones en: Documento desde que se firmó. | | | | |
| 😂 La identidad del firmante es válida. | | | | |
| 🤭 La firma contiene la marca de hora. | | | | |
| La firma se creó con la versión Adobe Acrobat. | | | | |
| | | | | |
| Validar firma | errar | | | |

Ilustración 22