JUNTA DE ANDALUCIA

CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Expedición de copias autenticadas electrónicamente

Autenticación de diligencias

Versión: v01r00

Fecha: 16/01/2015

HOJA DE CONTROL

Título	Expedición de copias autenticadas electrónicamente. Autenticación de diligencias.		
Nombre del Fichero	20150116 Autenticación_Diligencias_v01r00.doc		
Autor	DGPD		
Versión/Edición	v01r00	**Fecha Versión**	16/01/2015
		Nº Total Páginas	13

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Creación del documento	DGPD	DGPD	16/01/2015

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
Manuel Perera Domínguez	Jefe de Servicio	CHAP	1
Francisco Mesa Villalba	Director de Proyecto	CHAP	1
José Ignacio Cortés Santos	Director de Proyecto	CHAP	1

ÍNDICE

1 INTRODUCCIÓN

Desde el 01/02/2015 las diligencias electrónicas de compulsa generadas por la herramienta (ficheros PDF) incorporan una firma electrónica en formato PaDES que permite verificar su autenticidad en cualquier sistema o aplicación que incorpore la capacidad de validar este formato de firma electrónica. Por ejemplo, el software Adobe Reader.

La firma electrónica de la diligencia (fichero PDF) se realiza mediante un certificado electrónico de componente de sello de entidad "HERRAMIENTA INFORMÁTICA GENÉRICA DE EXPEDICIÓN DE COPIAS AUTENTICADAS ELECTRÓNICAMENTE DE DOCUMENTOS EN SOPORTE PAPEL" emitido por la FNMT-RCM cuyo plazo de validez finaliza el 08/10/2017.

En el presente documento se describe cómo verificar una firma PaDES en el software Adobe Reader.

2 VERIFICACIÓN DE FIRMAS EN FORMATO PADES CON ADOBE READER

2.1 Configuración previa de Adobe Reader

La verificación de una firma PaDES realizada con un certificado electrónico de componente emitido por la FNMT-CRM requiere de una configuración previa en el software Adobe Reader para que éste considere a esta entidad como de confianza. Esta tarea previa de configuración debe realizarse una única vez y no es necesario repetirla cada vez que se desee verificar la autenticidad de una diligencia electrónica.

Es posible que un usuario no disponga de los permisos necesarios en su puesto de trabajo para realizar esta tarea de configuración previa por lo que en este caso deberá solicitar el apoyo del personal informático de su Consejería o entidad. Del mismo modo, dado que se trata de una tarea compleja para un usuario no familiarizado con los conceptos habituales de firma electrónica, es aconsejable en todo caso contar con el apoyo o asesoramiento de personal informático especializado.

1 - DESCARGA DEL CERTIFICADO AC RAÍZ FMNT-RCM

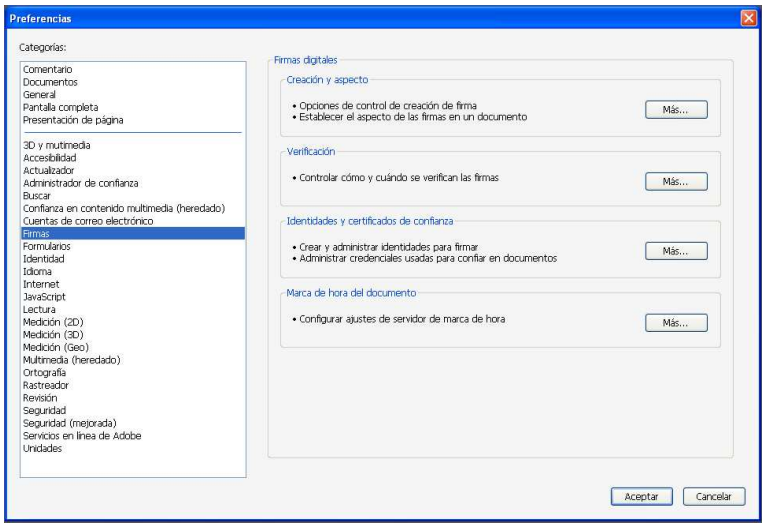
En primer lugar, deberemos descargar en nuestro equipo el certificado AC Raíz FNMT-RCM desde la siguiente dirección:

https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Raiz_FNMT-RCM.crt/7b177693-5387-40b9-afd4-32264998bd56

2 - INSTALACIÓN DEL CERTIFICADO AC RAÍZ FMNT-RCM COMO ENTIDAD DE CONFIANZA

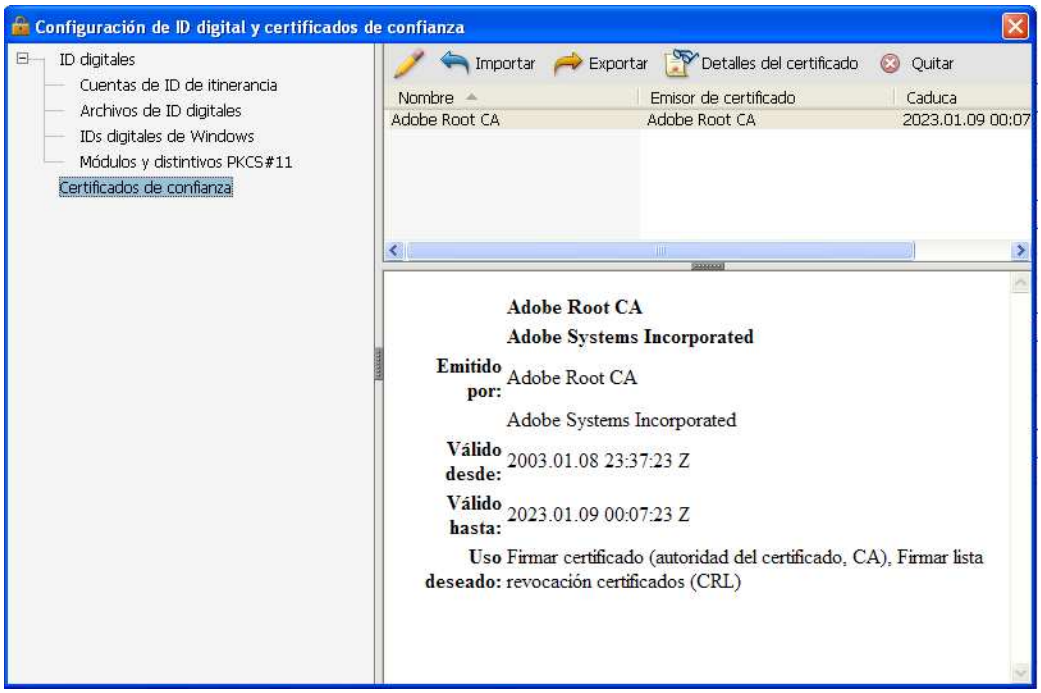
Para incorporar en Adobe Reader el certificado raíz de FNMT-CRM como entidad de confianza deben realizarse los siguientes pasos:

1. Iniciar Adobe Reader
2. Acceder al menú Edición => Preferencias
3. Seleccionar la opción "Firmas"

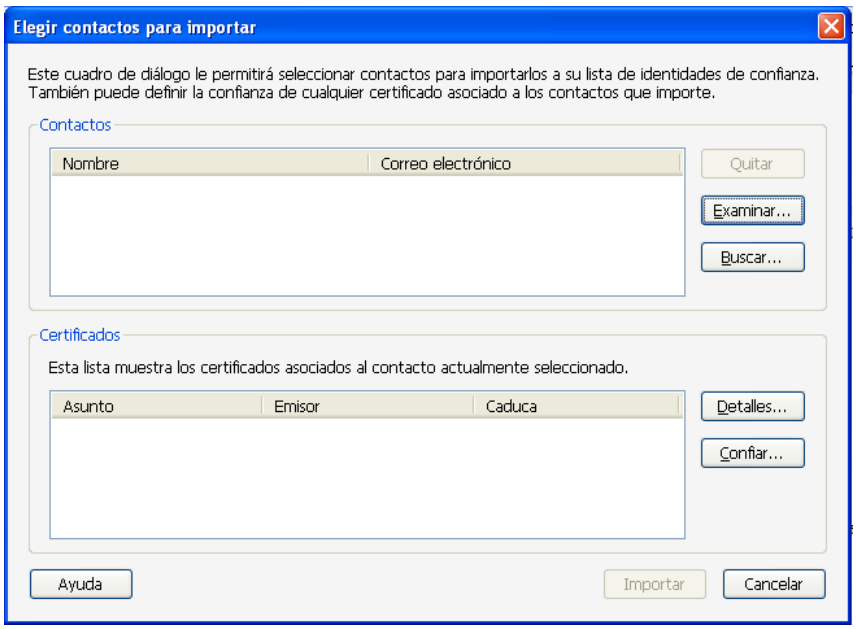


4. En la zona derecha, seleccionar la opción "*Identidades y certificados de confianza*" => "*Más*"

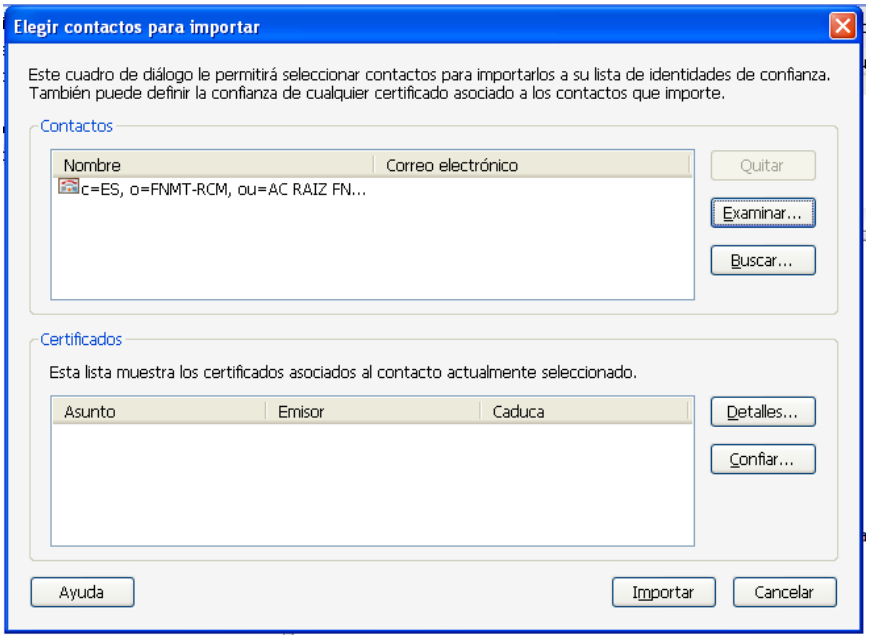
5. En la zona izquierda, seleccionar "*Certificados de confianza*":



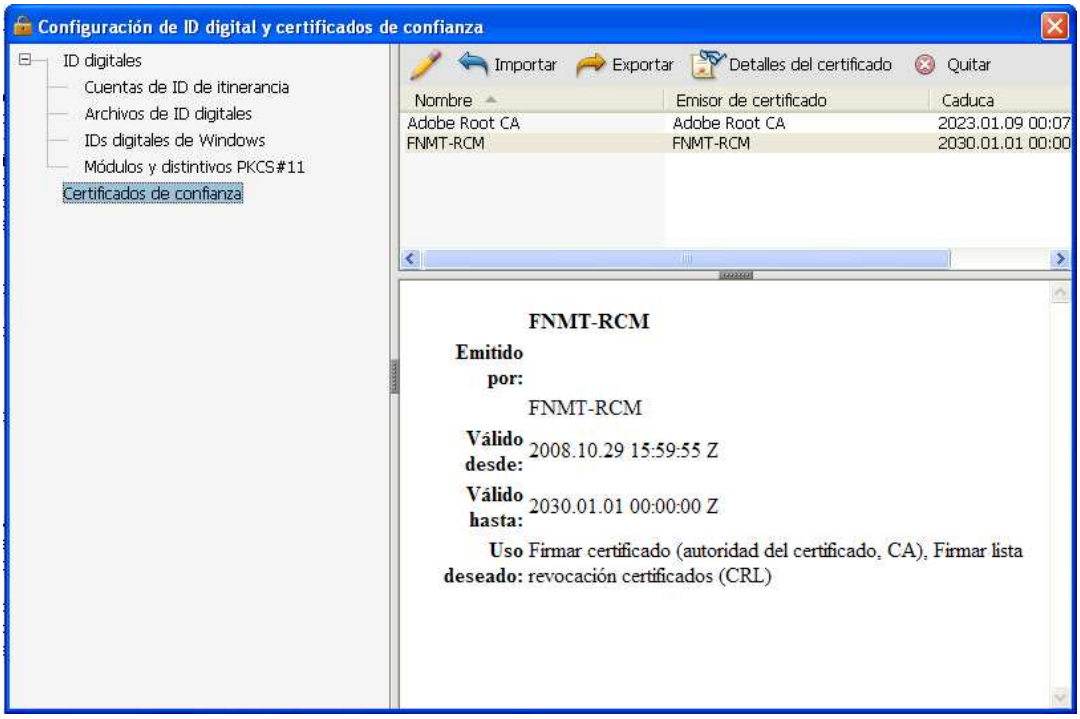
6. Tras seleccionar la opción "*Importar*" del menú superior, se accede a la siguiente pantalla:



7. Ahora se deberá pulsar el botón "*Examinar*", tras lo cual se podrá seleccionar el fichero que contiene el certificado AC Raíz FNMT-RCM:



8. Pulsando en este momento sobre el botón "*Importar*", aparecerá un mensaje informativo en el que se indica que se ha importado un certificado de emisor. Tras pulsar sobre "Aceptar", se volverá a la pantalla ya mostrada en el quinto paso, pero en esta ocasión aparecerá el certificado AC Raíz FNMT-RCM ya importado.



9. Antes de poder cerrar esta ventana, es necesario aún seleccionar el icono que contiene el dibujo de un lápiz, situado a la izquierda del botón "*Importar*", tras lo cual se accederá a una pantalla como la siguiente:

10. En la pantalla anterior, se deberá activar la opción "*Utilizar este certificado como raíz de confianza*" y ya se podrá cerrar esta ventana pulsando sobre "*Aceptar*", tras lo cual se podrá también cerrar la pantalla previa (paso 8) y posteriormente la pantalla de preferencias generales de Adobe.

3. CONECTIVIDAD DE RED CON EL SERVICIO OCSP DE VERIFICACIÓN DEL ESTADO DE REVOCACIÓN DEL CERTIFICADO

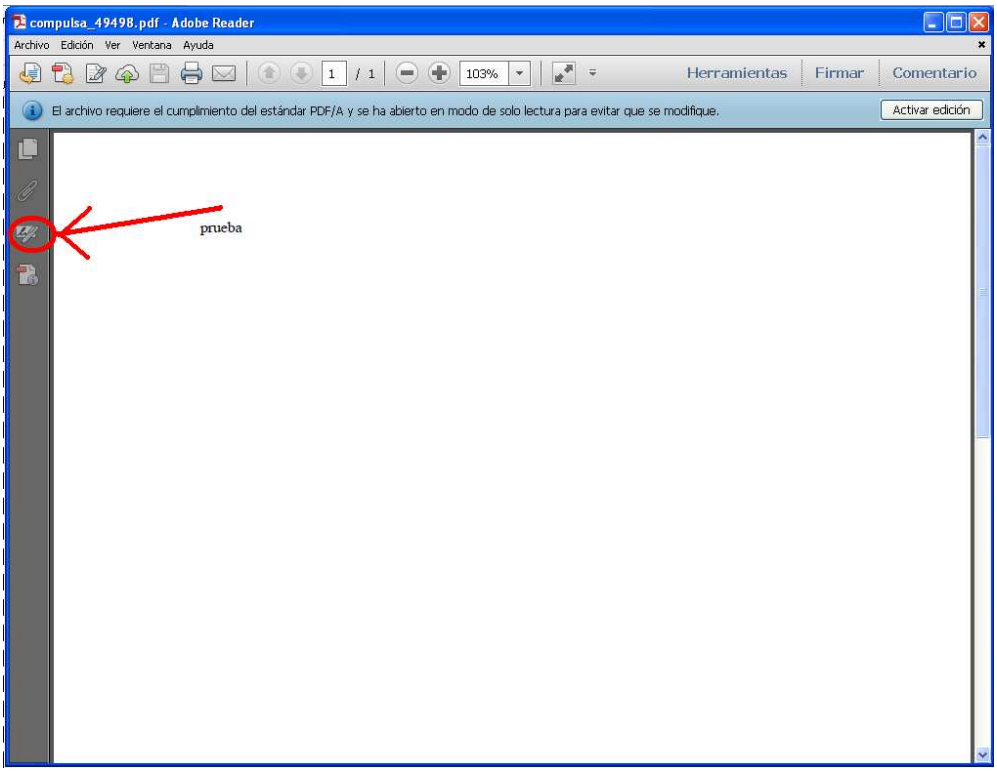
En el proceso de verificación de una firma electrónica en formato PaDES realizada sobre un archivo PDF, Adobe Reader verifica el que el certificado electrónico empleado para la firma no se encuentra revocado. Para ello, Adobe Reader necesita establecer una conexión con el servicio OCSP de verificación del estado de revocación de certificados de la FNMT-RCM. Será necesario que Adobe Reader tenga visibilidad de red con las siguientes direcciones:

- http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder
- http://www.cert.fnmt.es/certs/ACCOMP.crt

La visibilidad de red vendrá determinada por la política que al respecto se establezca en cada Consejería o entidad que las opciones para lograrla son múltiples: acceso mediante excepciones en el cortafuegos, configuración de un proxy, etc. Se recomienda que la tarea de verificación de conectividad de red con los servicios OSCP de FNMT-RCM sea realizada por personal técnico especializado.

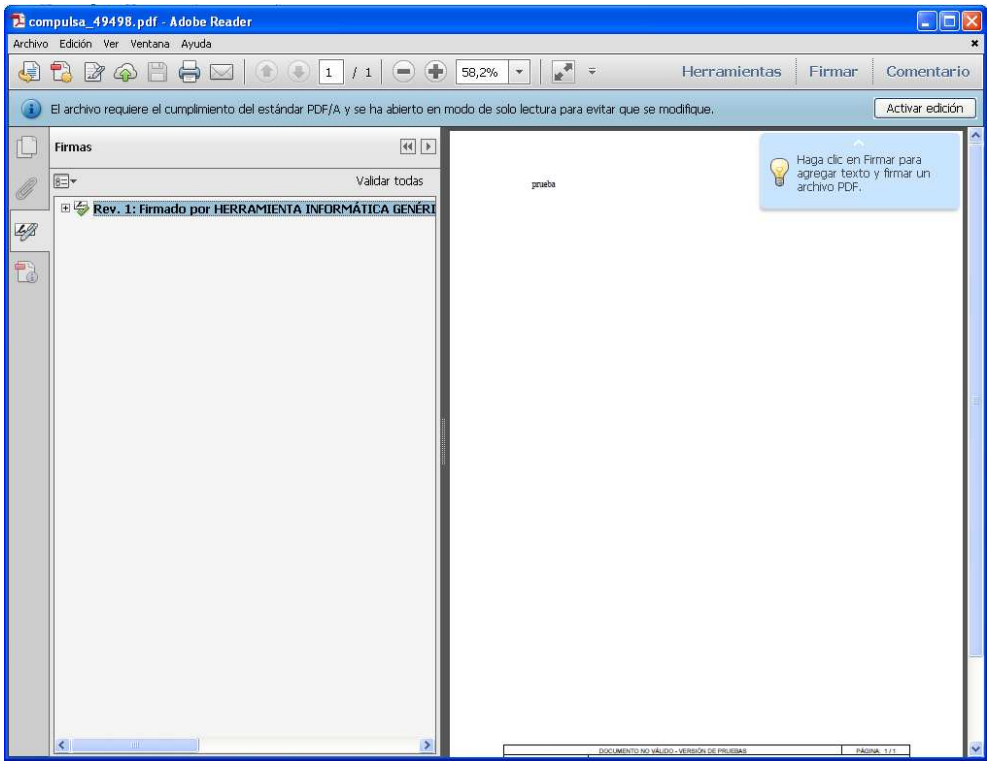
2.2 Verificación de una firma electrónica PaDES

Abrir el archivo PDF a comprobar con el software Adobe Reader y pulsar sobre el icono resaltado en la siguiente captura:

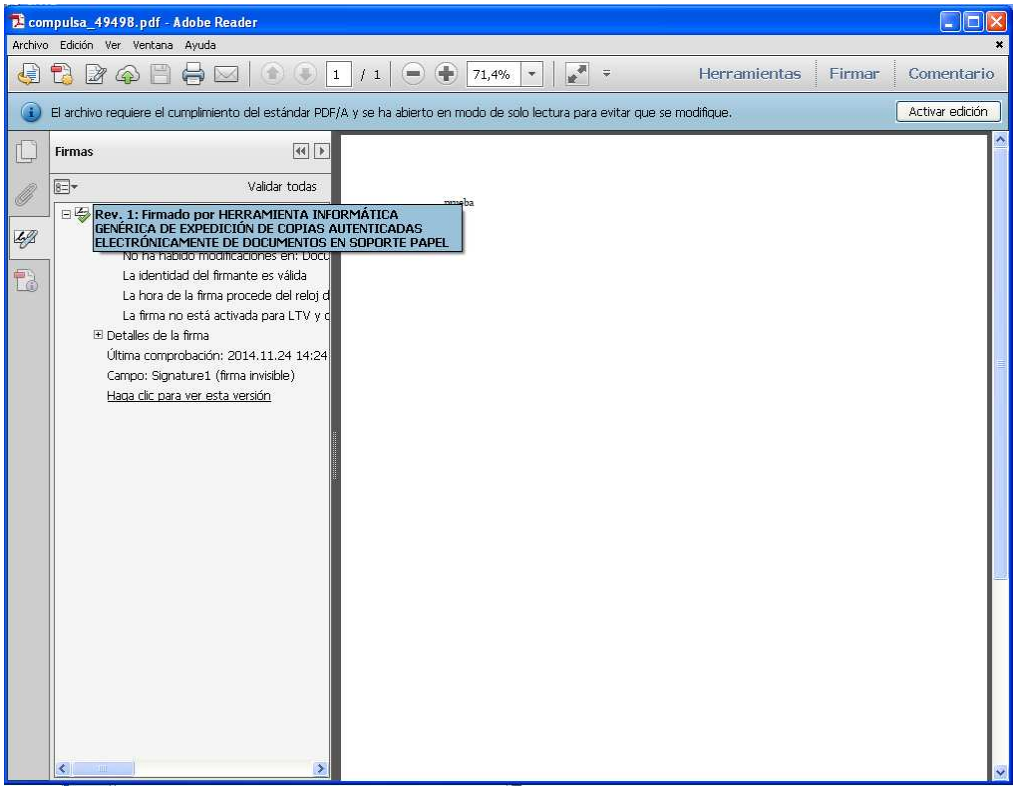


Este icono dará acceso a la información de firmas electrónicas en formato PaDES realizadas sobre el documento PDF. Se expondrán a continuación capturas de diferentes escenarios que se pueden dar tras pulsar sobre el icono resaltado en la pantalla precedente.

CASO 1: VERIFICACIÓN EXITOSA

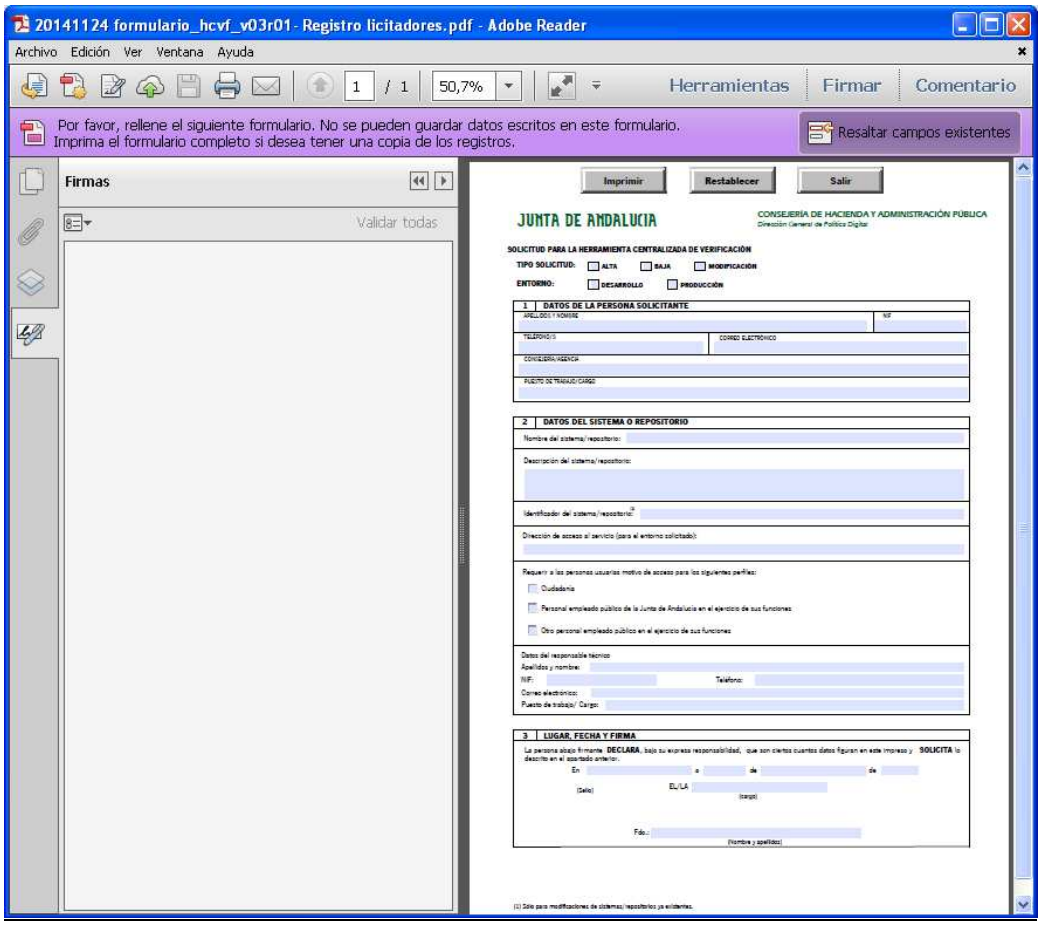


Puede verse un "check" de color verde que indica que la firma se ha validado correctamente. Ubicando sobre él el puntero del ratón observaremos la información del certificado con el que esta firma electrónica se realizó:



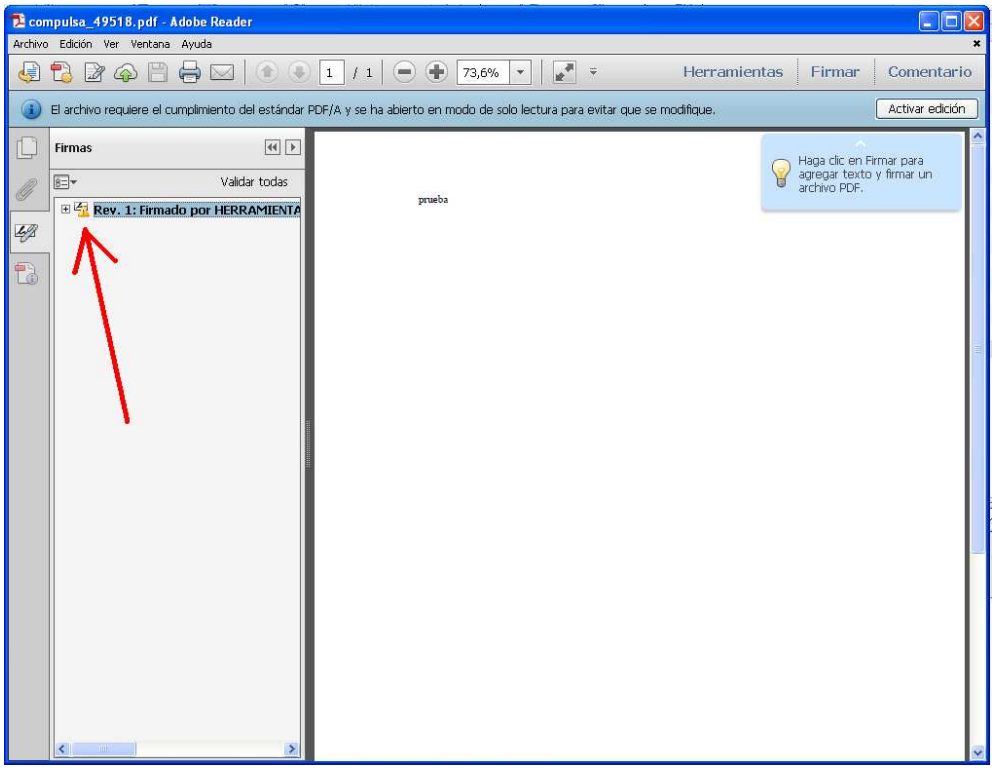
CASO 2: DOCUMENTO PDF SIN FIRMAS

En la siguiente captura muestra un documento PDF que no incorpora firma PaDES. En este caso, Adobe Reader mostrará vacía la zona de firmas.



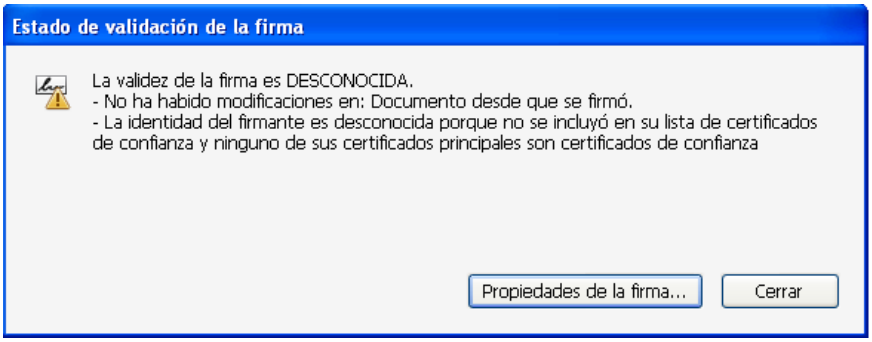
CASO 3: DOCUMENTOS CON FIRMAS QUE NO PUEDEN VERIFICARSE

Un icono de alerta de color amarillo indicará que no se ha podido verificar la firma electrónica.



Pinchando sobre el icono con el botón derecho del ratón, tendremos acceso a un menú en el que poder seleccionar la opción "Validar firma" para reintentar el proceso de validación y, en caso de no poderse realizar, conocer la causa.

Si la firma PaDES se ha efectuado con un certificado no emitido por una entidad de confianza obtendremos un mensaje como el siguiente:



Podría darse también que la firma no se validara incluso habiéndose realizado con un certificado válido. Esta situación se producirá cuando no se pudiera verificar el estado de revocación del certificado empleado para la firma, debido a un error puntual en el acceso al servicio OSCP de FNMT-RCM o bien debido a una configuración de conectividad de red del equipo que le impide el acceso al servicio. En esta situación, el mensaje de error obtenido será el siguiente: