KeyFour Bit4id

Manual de usuario

Sumario

Revisiones

Revisión	Fecha	Cambios	Autor
1.0	26/06/2014	Primera redacción	GGM
2.0	26/08/2014	Opciones	GGM-RAV

Introducción

En sus manos tiene un dispositivo portátil ideal realizar firmas electrónicas con total libertad. Su utilización es muy simple ya que no precisa de ningún tipo de conocimiento previo ni instalación.

Este dispositivo criptográfico inteligente incluye diferentes aplicaciones a bordo para dotar al usuario de un instrumento verdaderamente útil y usable. Todas las aplicaciones se ejecutan en la memoria interna, sin ninguna dependencia externa.

Funciones y aplicaciones principales

Herramienta de Firma electrónica de documentos: Firme documentos de una manera rápida y sencilla con la misma garantía que la firma manuscrita. Elija el documento, el formato de firma y… ¡a firmar!

Validación de documentos firmados electrónicamente: Herramienta que permite la validación de documentos firmados electrónicamente.

Explorador de Internet Mozilla Firefox: Navegue sin problemas de dejar rastros utilizando el navegador portátil, además permite el uso de su certificado digital en cualquier Web.

Token Manager: modifique el PIN/PUK de su certificado de manera sencilla, importe certificados, etc.

Uso como lector de tarjetas tradicional en **modo CCID (Modo compatibilidad)**: Utilícelo como un token tradicional CCID.

Expulsar dispositivo con seguridad: extraiga el dispositivo con total comodidad y seguridad.

Ayuda y soporte: Completo manual de uso y ayuda. ¡Saque todo el partido a su smartTOKEN!

Información de interés sobre certificados digitales

El dispositivo contiene su certificado digital protegido por un código PIN personal y un código PUK de desbloqueo.

El certificado digital permite trabajar con más seguridad, rapidez y comodidad a la hora de realizar trámites con la Administración pública, instituciones, otras entidades, empresas y/o usuarios.

Podrá utilizarse como garantía de identidad y cualificación cuando se solicita la identificación de su propietario, así como para la firma electrónica de documentos, que según la legislación vigente, tiene el mismo valor que una firma manuscrita tradicional.

Permite la eliminación del papel a través de la firma de documentos electrónicos de una manera rápida y sencilla: facturas, contratos, nóminas, etc.

Tiene formato x509 que es el designado para las arquitecturas PKI, siendo la versión v3 la más actualizada, y tratándose de un estándar mundialmente aceptado y reconocido.

Los certificados incluyen una serie de campos con información sobre el emisor del certificado (Autoridad de Certificación) y el sujeto al que le ha sido emitido.

- General: Información general del certificado; titular, entidad emisora, fecha de expedición y caducidad…
- Detalles: Características avanzadas del certificado.
- Ruta de certificación: es una secuencia de uno o más puntos conectados entre el subscriptor y una CA raíz. Una CA raíz es una autoridad en la que confía la aplicación, ya que tiene almacenada de forma segura su clave pública.

Los elementos principales de un certificado X.509 v3 son:

- Versión: El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- Número de serie del certificado: Este campo es un entero asignado por la Autoridad de Certificación. Cada certificado emitido por una Autoridad de Certificación debe tener un número de serie único.
- Identificador del algoritmo de firmado: Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- Nombre del emisor. Este campo identifica la Autoridad de Certificación que ha firmado y emitido el certificado.
- Periodo de validez: Este campo indica el periodo de tiempo durante el cual el certificado es válido y la Autoridad de Certificación está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- Nombre del sujeto: Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una Autoridad de Certificación dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- Información de clave pública del sujeto: Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.

- Identificador único del emisor. Este es un campo opcional que permite reutilizar nombres de emisor.
- Identificador único del sujeto: Este es un campo opcional que permite reutilizar nombres de sujeto.
- Extensiones.

Puesta en marcha

Para empezar a utilizar el dispositivo, basta con conectarlo a su PC.

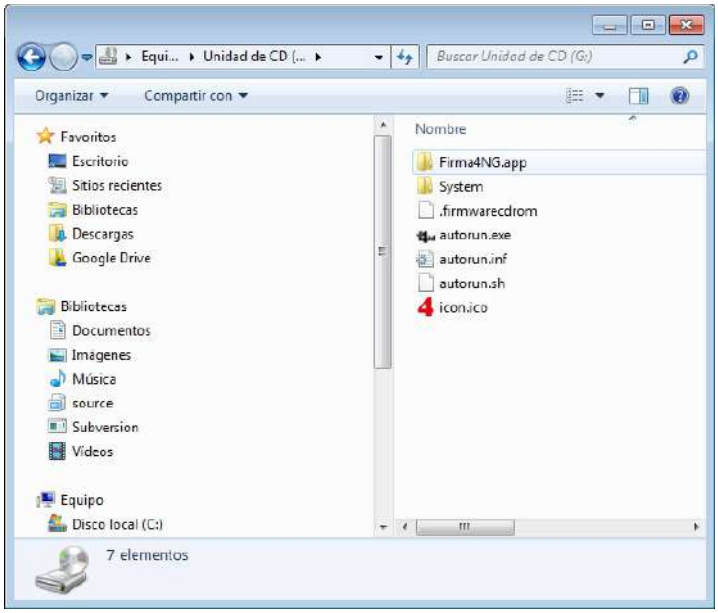
Una vez tenga su PC totalmente iniciado con el sistema operativo cargado, puede proceder a realizar la conexión en cualquier puerto USB que esté disponible.

En pocos segundos en la pantalla de su PC aparecerá automáticamente un menú con todas las funcionalidades y aplicaciones disponibles:

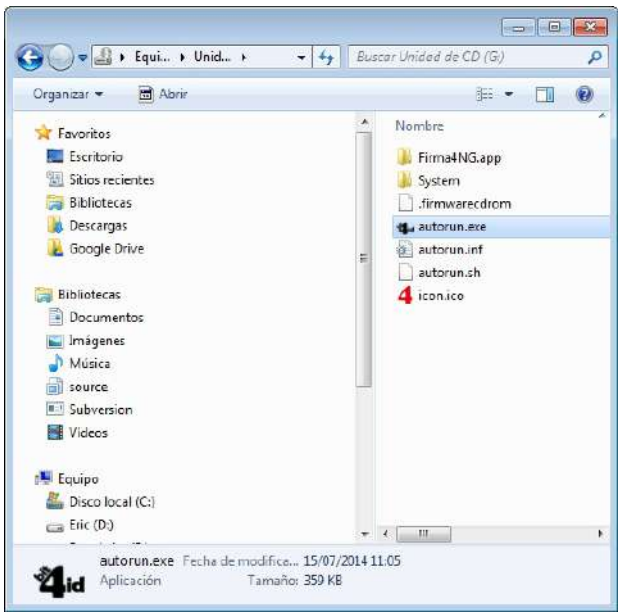
Si transcurrido medio minuto no aparece el menú citado anteriormente deberá acceder a él de la siguiente forma:

1. Pulse con el ratón en el menú inicio, en la parte inferior izquierda de su pantalla.
2. Busque el icono con el texto Mi PC y pulse sobre él.

3. Cuando aparezca una nueva ventana en el centro de su pantalla deberá pulsar dos veces sobre el icono.



4. Si sigue sin aparecer el menú mencionado deberá buscar en la nueva ventana el icono con el nombre autorun, ejecutándolo para que arranque el dispositivo.



Si sigue sin poder visualizar el menú, contacte con su administrador del sistema.

Menú principal

El dispositivo tiene un menú principal y un submenú desde donde puede acceder a todas sus funcionalidades.

A todas las funcionalidades se accede pulsando sobre los iconos.

Los controles generales son:

- Siempre visible: Mantiene el menú en todo momento visible.
- Minimizar: Oculta de la pantalla el menú, para volver a acceder a él se deberá buscar el icono al lado del reloj en la esquina inferior derecha.
- Cerrar: Cierra el menú

Este menú se divide en dos partes:

Menú principal

Herramientas: se accede pulsando sobre el icono Herramientas

Para volver al menú principal pulsaremos en el icono Menú.

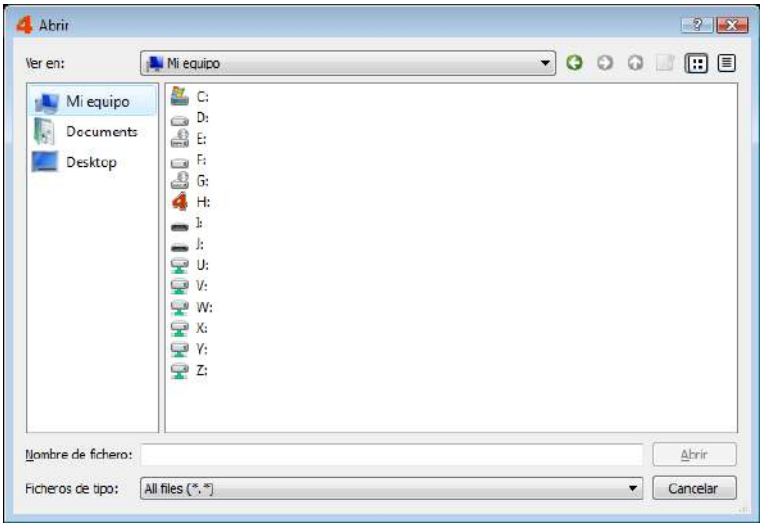
Firmar

Esta aplicación le permitirá firmar electrónicamente y en diferentes formatos cualquier tipo de documento, utilizando el certificado digital alojado en el dispositivo.

Iniciar el proceso de firma

Para lanzar el proceso de firma tiene dos opciones:

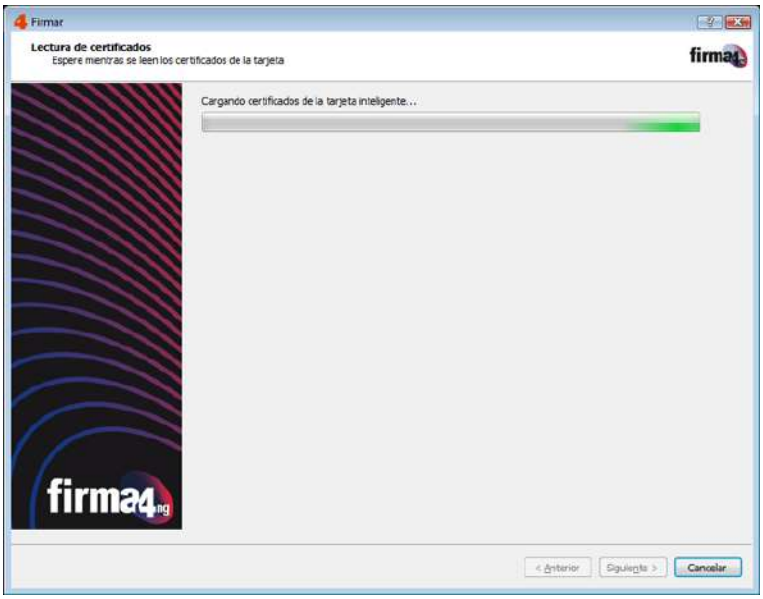
- Puede simplemente pulsar sobre el icono Firmar. Tenga en cuenta que de esta manera no podrá firmar varios documentos a la vez. A continuación abre una ventana donde deberá indicar o buscar la ruta del archivo a firmar. Una vez seleccionado el documento o archivo pulse en Abrir.



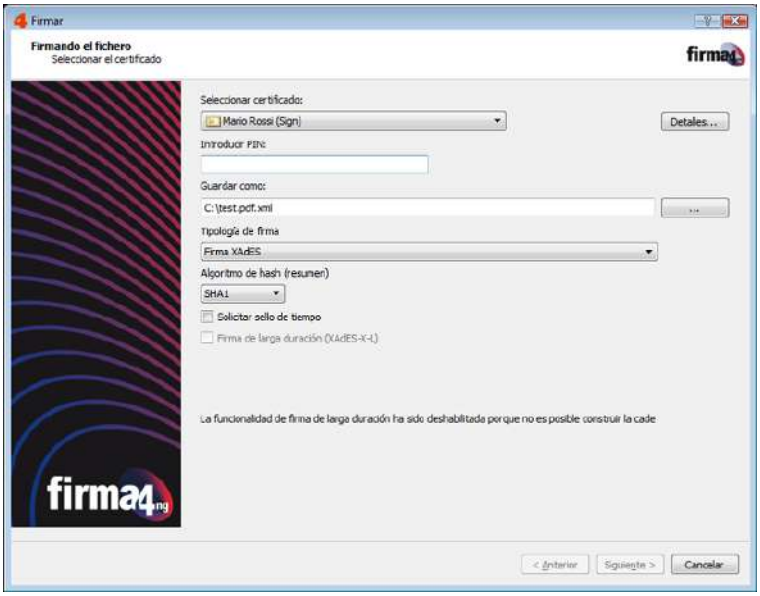
- Puede seleccionar uno o varios archivos de su PC y arrastrarlos encima del icono de Firmar.

Opciones de la firma

El programa mostrará una nueva ventana que le indicara que debe esperar un instante mientras carga sus certificados disponibles.



A continuación aparecerá la pantalla con la selección de las características.



- Seleccionar el certificado: en este control desplegable podrá explorar y elegir alguno de sus certificados disponibles (en caso de disponer de más de uno). En detalles verá la información del certificado.

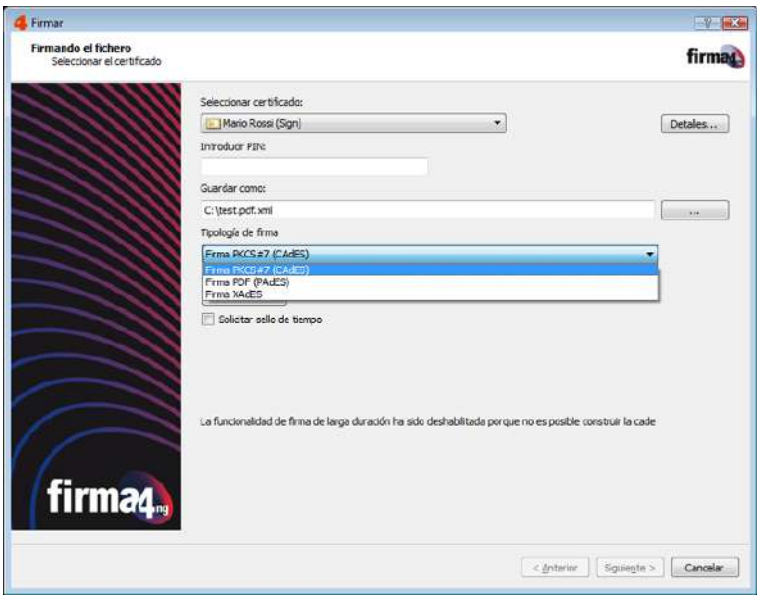
- Introducir PIN: Deberá introducir su PIN personal del certificado seleccionado.

- Guardar como: Es la ruta o dirección donde guardará el nuevo archivo firmado, por defecto se guarda en la misma ruta que el documento a firmar.

- Tipología de firma: Los formatos de firma soportados son CAdES (PKCS#7), PAdES (PDF) y XAdES (XML).
  El formato de firma PAdES sólo se encuentra disponible si el fichero origen es un PDF.

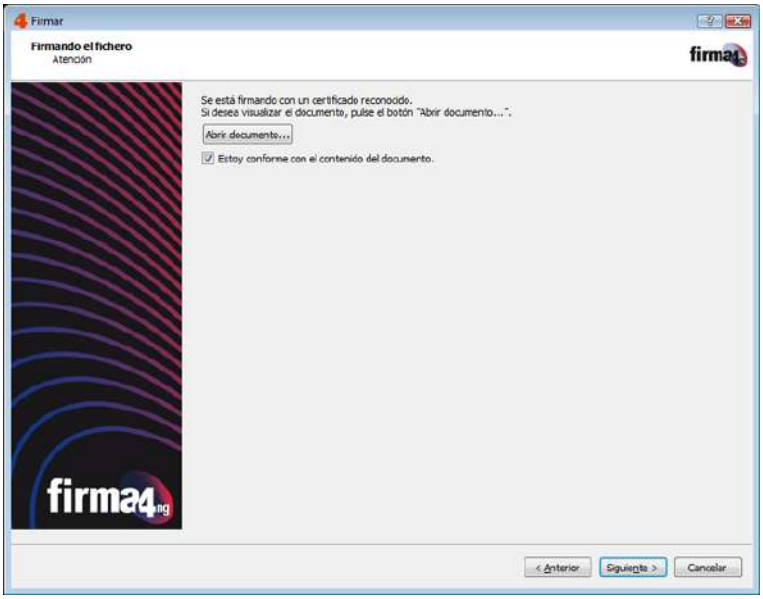
- Algoritmo de hash (resumen): deberá seleccionar SHA1 (algoritmo menos seguro, aunque compatible con la mayoría de validadores) o SHA256 (algoritmo más seguro, aunque no es compatible con validadores antiguos).

Según el tipo de firma seleccionado podrá acceder a diferentes características.

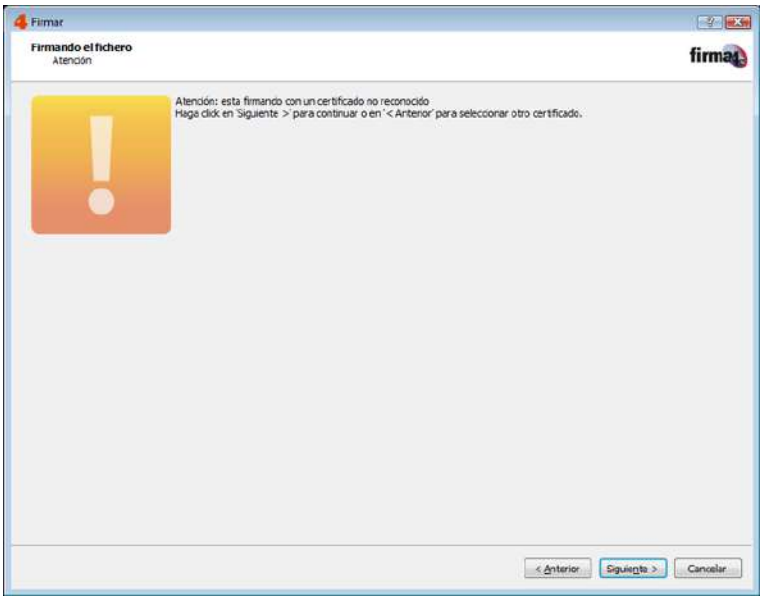


Una vez seleccionado el certificado, introducido el PIN del KeyFour Bit4id y escogido el formato de firma y las opciones, pulse en "Siguiente".

Si el certificado está emitido por una Autoridad de Certificación reconocida, se indica que se va a realizar una firma reconocida con validez legal, y se requiere marcar la casilla que indica la conformidad con el contenido del documento.



Si se utilizase un certificado no reconocido, se muestra un mensaje que indica que la firma puede no ser reconocida.

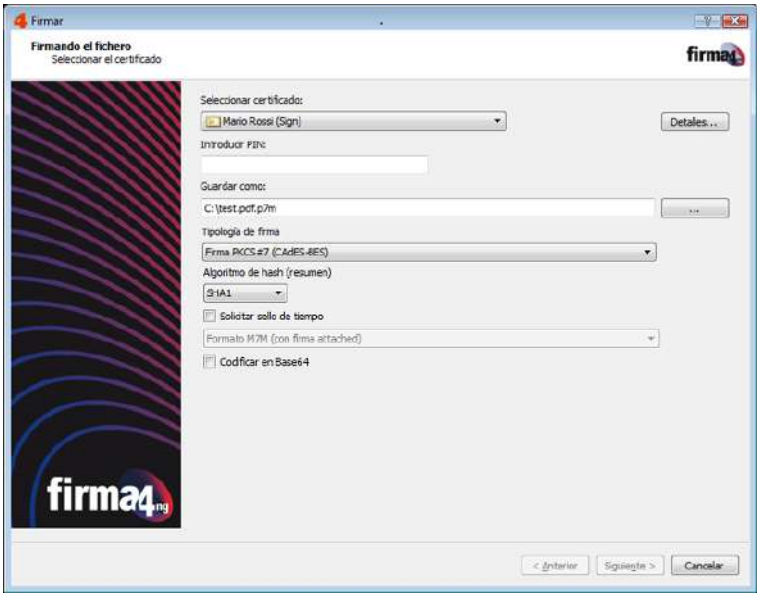


El resto del proceso de firma depende del formato elegido, y se indican a continuación.

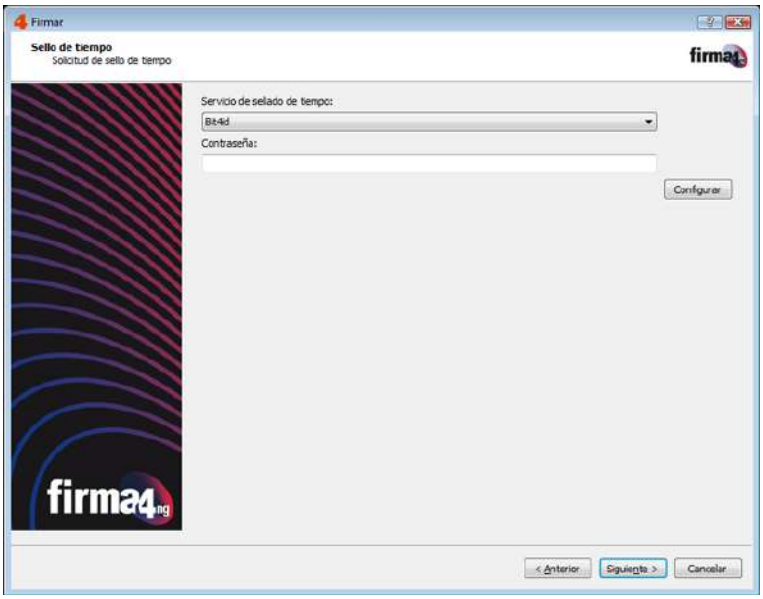
Formatos de firma

Firma CAdES - PKCS#7

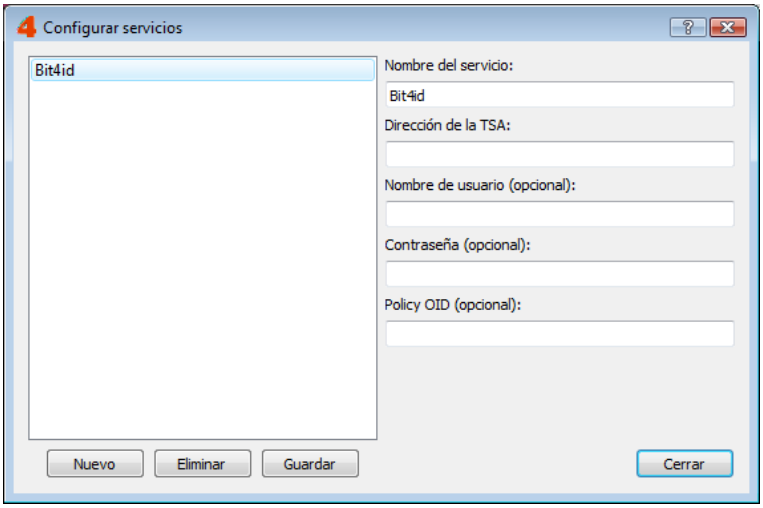
Para el formato CAdES, puede solicitar la incorporación de sello de tiempo, así como elegir el formato del fichero de salida. Además puede solicitar la codificación en Base64 cuando se requiera.



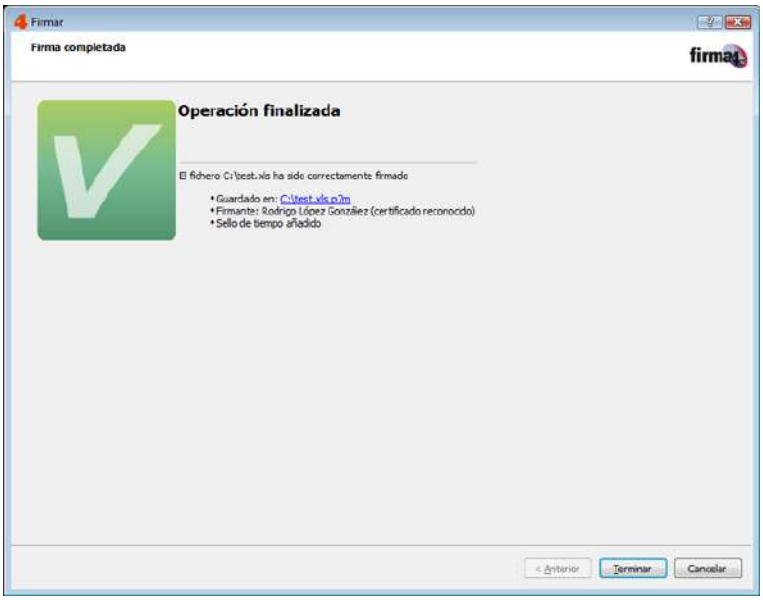
1. El proceso de firma prosigue después de aceptar la conformidad con el contenido del documento, en caso de tratarse de una firma reconocida. En caso de solicitarse sello de tiempo, se le solicita la configuración (datos de acceso al servicio que su proveedor de sellado de tiempo deberá proporcionar) o confirmación del mismo.



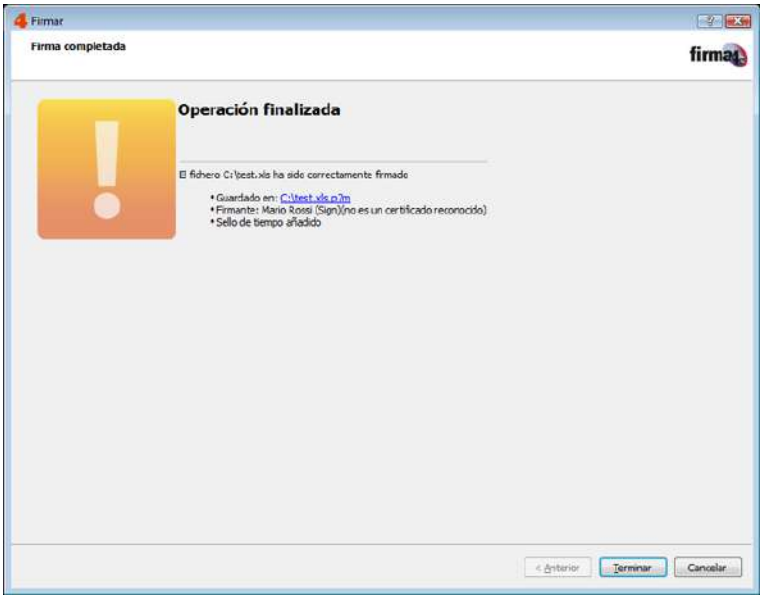
2. La opción de configuración permite añadir diferentes servicios de sellado de tiempo, especificando los campos indicados que le proporcionará su Prestador de Servicios de Certificación.



3. Si todo el proceso se realiza correctamente, la firma se habrá realizado, incluyendo el sello de tiempo si fue solicitado y correctamente configurado.

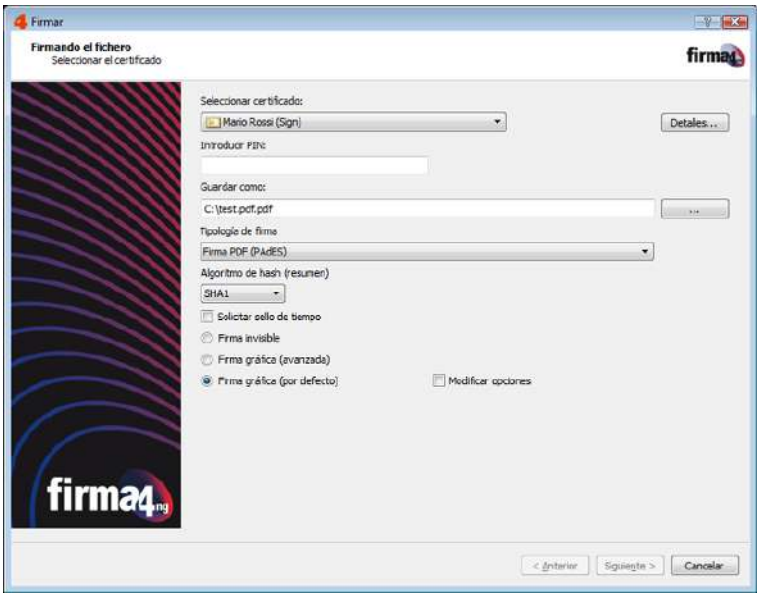


4. Si todo el proceso se realiza correctamente pero se realiza la firma con un certificado no reconocido, la firma se habrá realizado, incluyendo el sello de tiempo si fue solicitado y correctamente configurado, pero se indicará que no se puede garantizar que se trate de una firma reconocida.

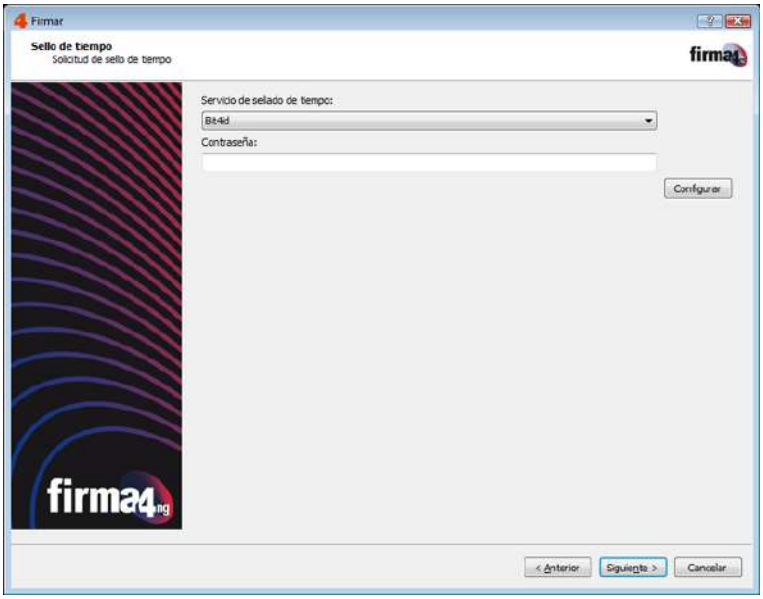


Firma PAdES - PDF

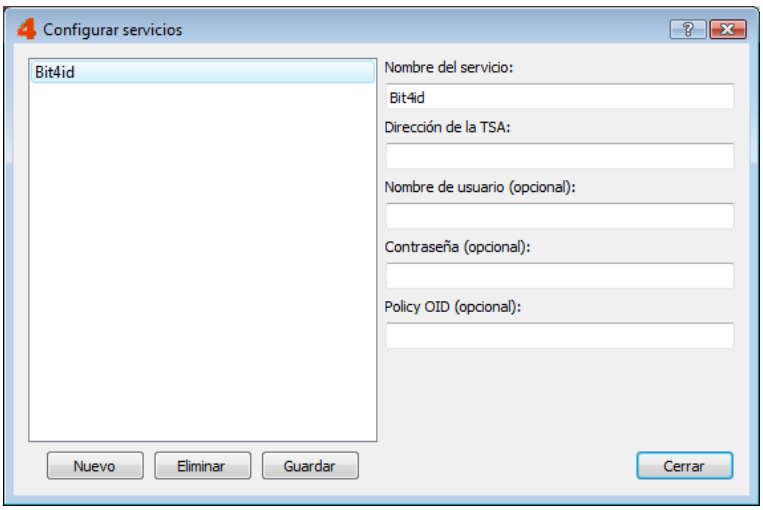
Para el formato PDF PAdES, puede solicitar la incorporación de sello de tiempo, así como elegir si se desea incorporar una marca gráfica en el documento.



1. El proceso de firma prosigue después de aceptar la conformidad con el contenido del documento, en caso de tratarse de una firma reconocida. En caso de solicitarse sello de tiempo, se le solicita la configuración o confirmación del mismo

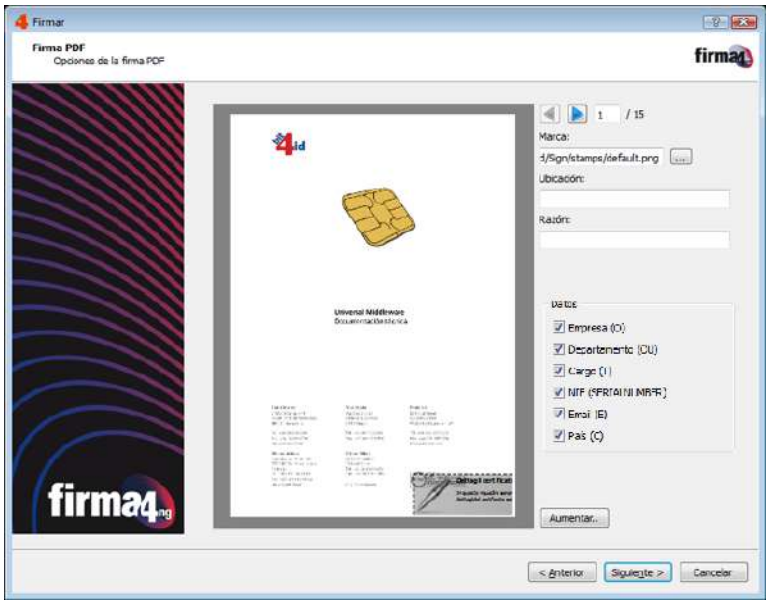


2. La opción de configuración permite añadir diferentes servicios de sellado de tiempo, especificando los campos indicados que le proporcionará su Prestador de Servicios de Certificación.

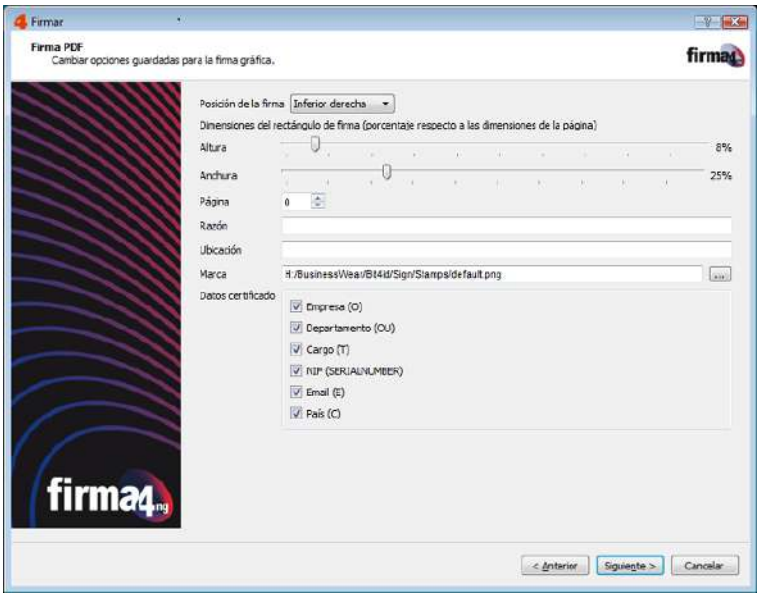


3. A continuación, y si se ha solicitado insertar una firma gráfica avanzada, se permite configurar las opciones de la firma gráfica.
   - Puede ubicar la firma en cualquier página, es suficiente con navegar a la página seleccionada y hacer doble click en cualquier parte de la página. Se trasladará la marca a esa página.
   - Puede cambiar las dimensiones del área de la firma gráfica, arrastrando las esquinas del área seleccionada.
   - Puede escoger una imagen personalizada para incluir en la imagen de la marca gráfica, así como la ubicación desde la que estamos realizando la firma, la razón por la cual firmamos el documento y algunos datos del certificado.

- En caso necesario, puede hacer zoom de la página para afinar la ubicación de la firma haciendo click en el botón "Aumentar".

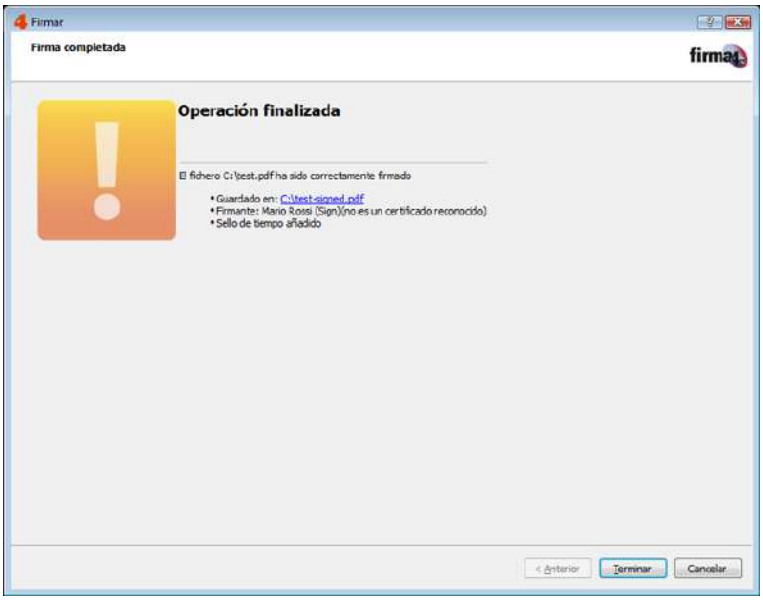


4. Si ha solicitado insertar una firma gráfica con las opciones por defecto, modificando dichas opciones, se permite configurar las opciones de la firma gráfica por defecto.
   - Puede ubicar la firma en cualquiera de las 4 esquinas de cualquier página
   - Puede escoger el tamaño de la marca gráfica en base a las proporciones relativas respecto a la página
   - Puede escoger una imagen personalizada para incluir en la imagen de la marca gráfica, así como la ubicación desde la que se realiza la firma, la razón por la cual firmamos el documento y algunos datos del certificado



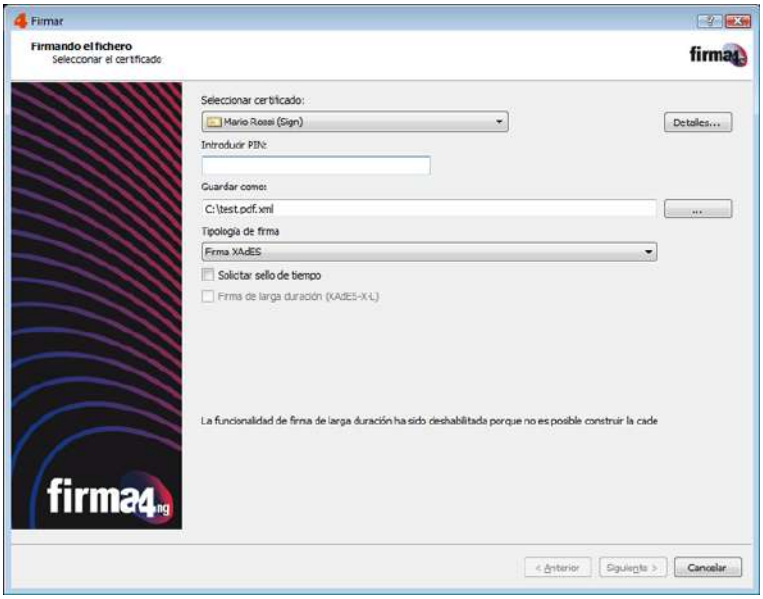
5. Si todo el proceso se realiza correctamente, la firma se habrá realizado, incluyendo el sello de tiempo si fue solicitado y correctamente configurado.

6. Si todo el proceso se realiza correctamente pero se realiza la firma con un certificado no reconocido, la firma se habrá realizado, incluyendo el sello de tiempo si fue solicitado y correctamente configurado, pero se indicará que no se puede garantizar que se trate de una firma reconocida.

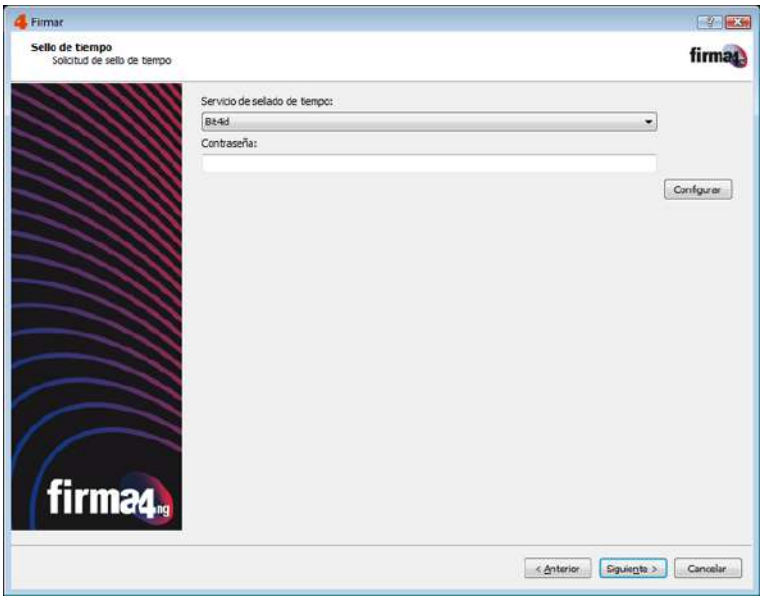


Firma XAdES - XML

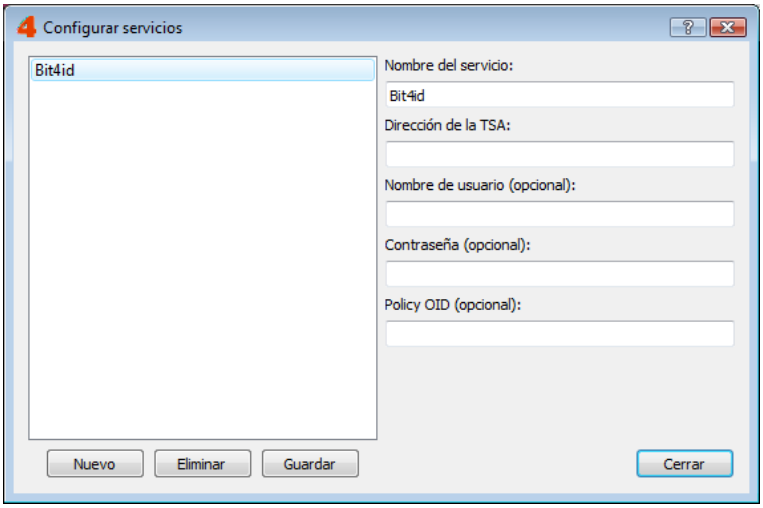
Para el formato XAdES, puede solicitar la incorporación de sello de tiempo, así como elegir si desea realizar una firma de larga duración XAdES-X-L, siempre que la Autoridad de Certificación emisora del certificado lo permita (en caso de no ser posible, dicha opción se encuentra deshabilitada y se muestra un mensaje informativo).



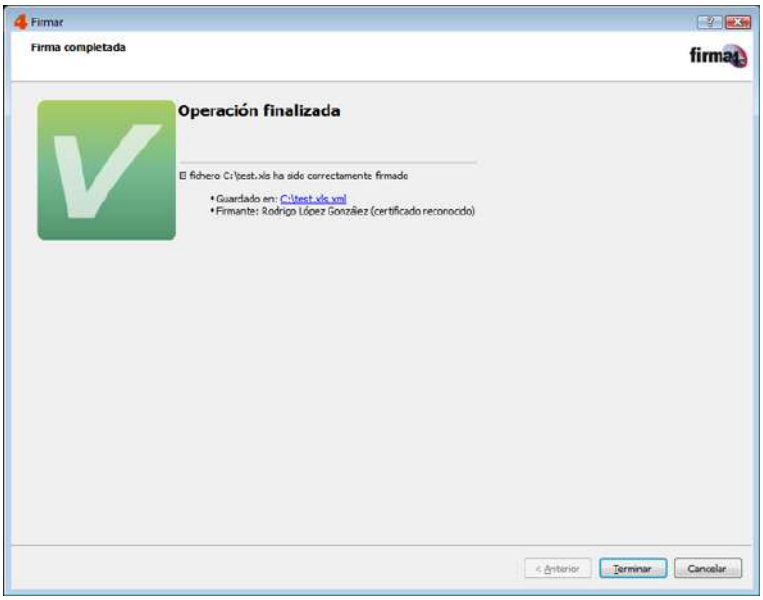
1. El proceso de firma prosigue después de aceptar la conformidad con el contenido del documento, en caso de tratarse de una firma reconocida. En caso de solicitarse sello de tiempo, se solicita la configuración o confirmación del mismo



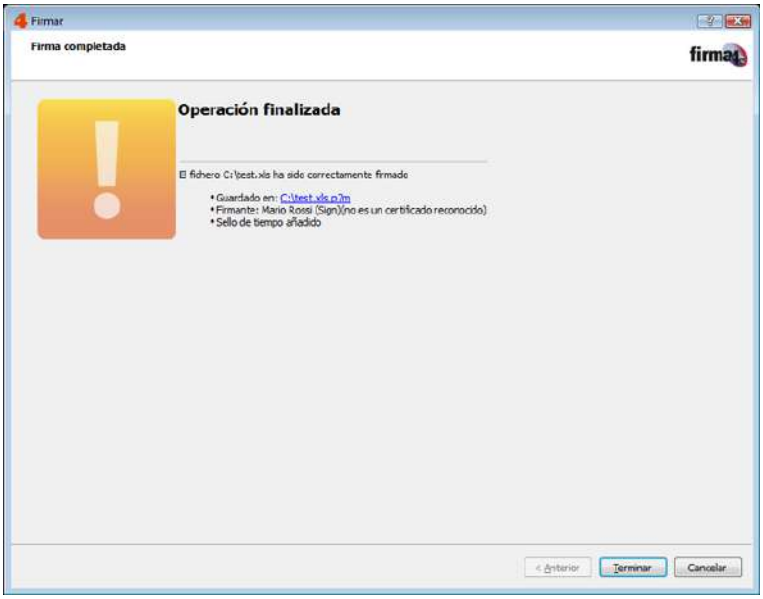
2. La opción de configuración permite añadir diferentes servicios de sellado de tiempo, especificando los campos indicados que le proporcionará su Prestador de Servicios de Certificación.



3. Si todo el proceso se realiza correctamente, la firma se habrá realizado, incluyendo el sello de tiempo si fue solicitado y correctamente configurado.



4. Si todo el proceso se realiza correctamente pero se realiza la firma con un certificado no reconocido, la firma se habrá realizado, incluyendo el sello de tiempo si fue solicitado y correctamente configurado, pero se indicará que no se puede garantizar que se trate de una firma reconocida.



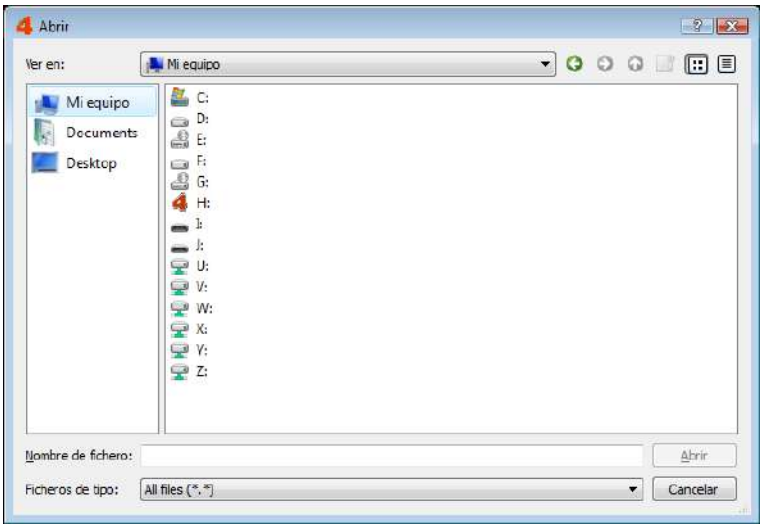
Validar

Iniciar el proceso de validación

Esta aplicación le permitirá validar los documentos firmados electrónicamente, ver su contenido y detalles así como añadir una firma o contrafirma y guardar una copia de su contenido.

Para lanzar el proceso de validación tiene dos opciones:

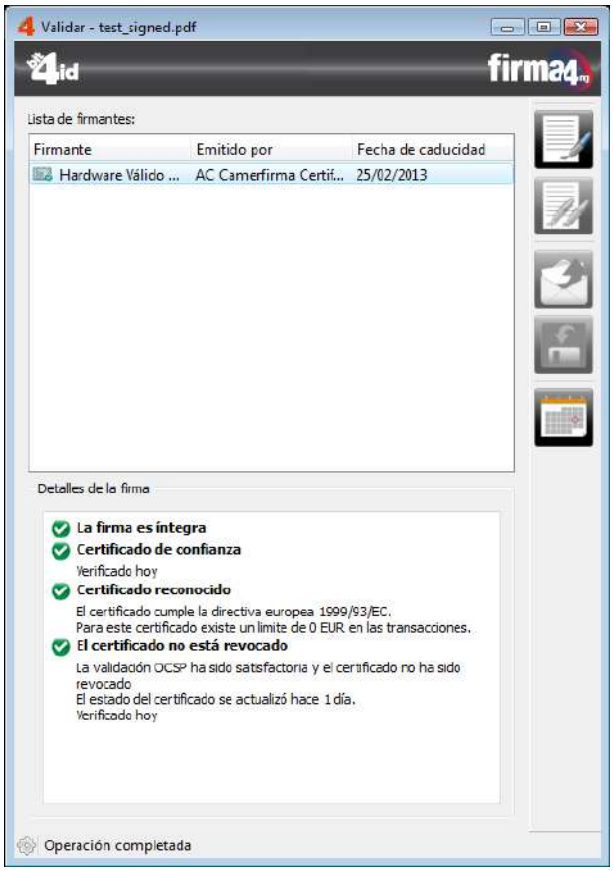
- Puede simplemente pulsar sobre el icono Validar. A continuación abre una ventana donde deberá indicar o buscar la ruta del archivo. Una vez seleccionado el documento o archivo pulse en Abrir.



- Puede seleccionar el archivo que desea de su PC y arrastrarlo encima del icono de Validar, dentro del submenú de Aplicaciones.

Opciones de validación

El programa mostrará una nueva ventana con una lista de firmantes (en caso de encontrarse) y detalles de las firmas. Pulsando una vez sobre el firmante podrá ver los detalles en el recuadro inferior, en cambio si desea ver los detalles del certificado deberá pulsar dos veces sobre el firmante.



En el menú de la derecha se encuentras los iconos que brindan acceso a las funcionalidades de la aplicación de validación:

Puede añadir una firma a un documento PDF o CAdES, siguiendo los pasos indicados en el apartado Firmar. Para añadir otro tipo de firmas es necesario volver a abrir el documento directamente desde el proceso de Firmar

Puede añadir una contrafirma a un documento con firma CAdES. Deberá seleccionar la firma sobre la que desea añadir la contrafirma y seguir los pasos indicados en el apartado firma

Puede abrir el contenido y visualizarlo con el programa por defecto para el formato de archivo que se ha firmado. Por ejemplo, para PDF puede ser Adobe Reader

Puede guardar el contenido que se ha firmado, indicando la ruta donde quiere guardarlo

Puede validar la firma en una fecha determinada pare verificar la validez pasada de la firma del documento

Internet

El dispositivo incorpora una versión personalizada del explorador web Mozilla Firefox, utilizable sin ningún tipo de instalación o modificación de su sistema. Tan solo basta con pulsar en el icono Internet y se iniciara una ventana donde poder comenzar a explorar la Web.

Todo el historial, favoritos y archivo temporales nunca quedaran almacenados en el PC local ya que siempre viajan almacenados en el dispositivo y disponibles en su próximo uso en cualquier otro PC

Tenga en cuenta que si en el PC hay una instancia de Mozilla Firefox en ejecución, la versión portable no se podrá iniciar. Deberá primero cerrar cualquier otra ventana de Mozilla Firefox.

Para más información acceda al menú ayuda en la ventana de esta aplicación (tecla F1) o visite la página de http://www.mozilla.com/es-ES/

Herramientas

Opciones

Pulsando en el botón Opciones, se abre una pantalla que le dará la posibilidad de modificar las opciones configuradas por defecto en su dispositivo.

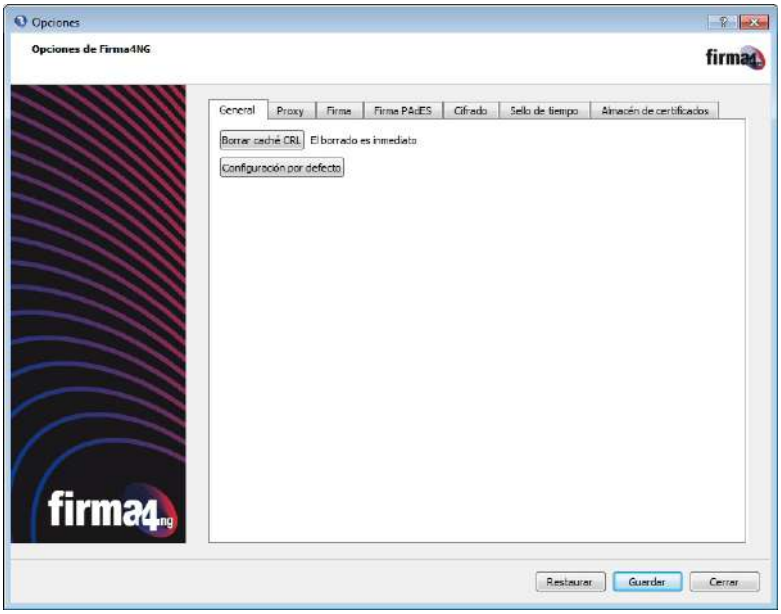
Funcionalidades de la aplicación

Pantalla principal

La siguiente ventana será mostrada:

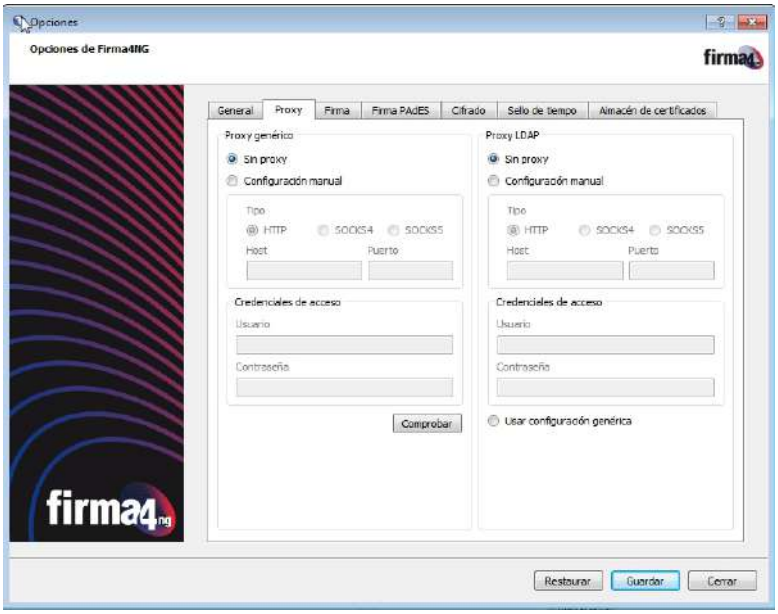
General

Borrar la memoria cache de la CRL (Lista de Certificados Revocados).



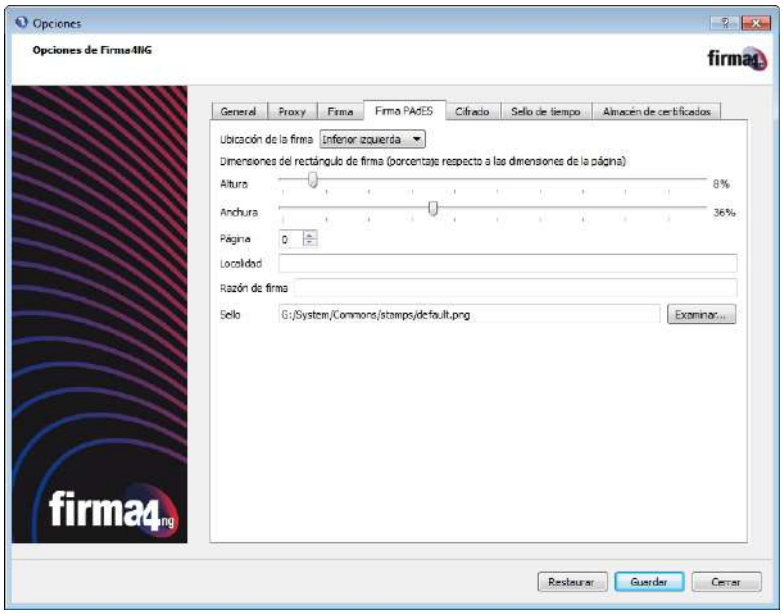
Proxy

Configurar los parámetros para el server proxy (en caso de existir).



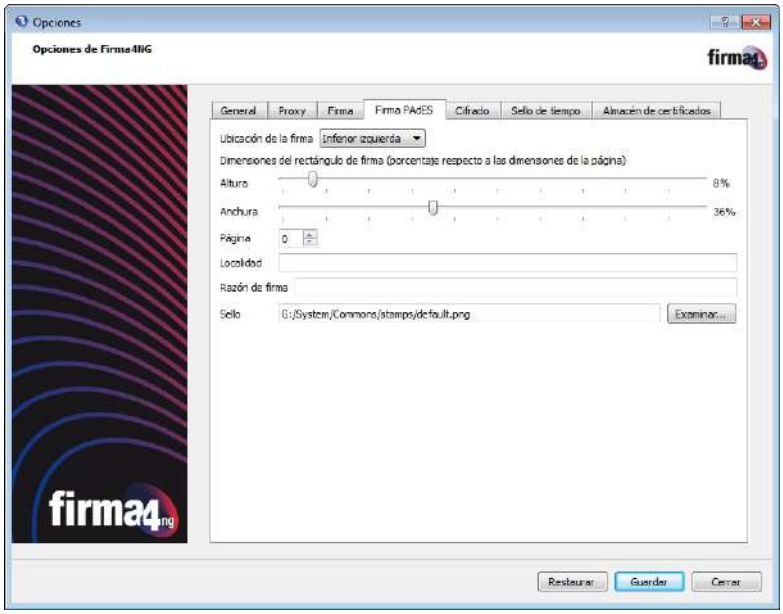
Firma

En esta pestaña se puede configurar la firma por defecto que aparece en la aplicación de firma. la carpeta para el guardado de firmas múltiples y la librería PKCS#11 a utilizar.



Firma PAdES

En esta pestaña se puede configurar la firma en formato PAdES con todas sus características.

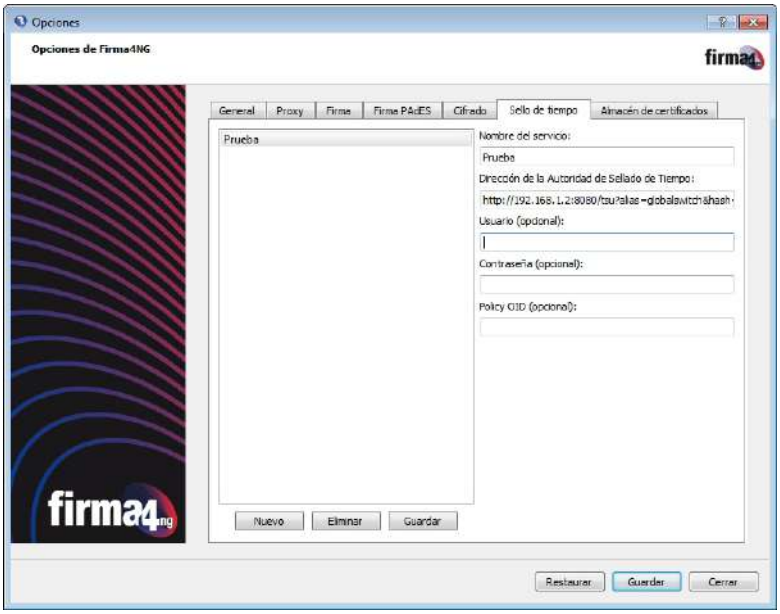


Cifrado

Algoritmo de cifrado

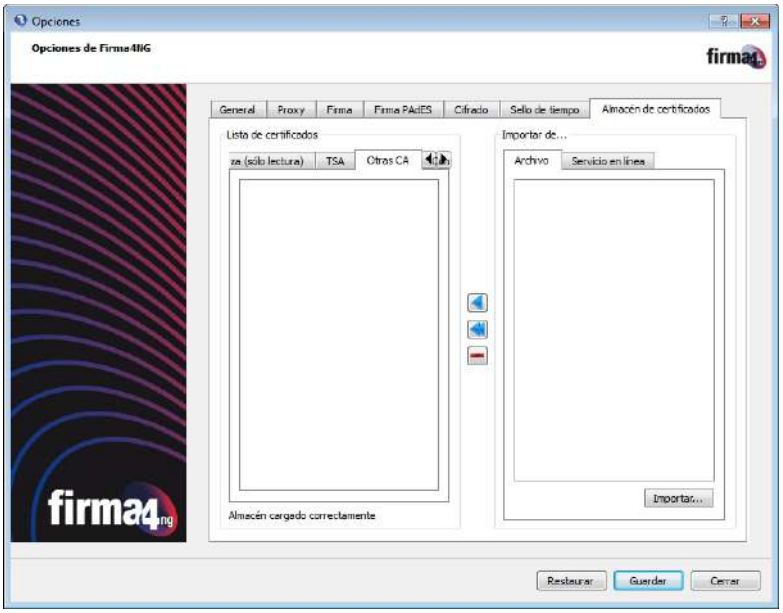
Sello de tiempo

Configurar los parámetros para la solicitud de sellos de tiempo.



Almacén de certificados

Visualizar y añadir los certificados de CA para utilizar durante el proceso de validación.



Token manager

Token manager es una herramienta para usuarios avanzados que permite gestionar y administrar sus certificados.

Funcionalidades de la aplicación

Pantalla principal

Imagen 1

Función	Descripción
Cambiar PIN	Función para cambiar el PIN de la tarjeta (*ver imagen 2*)
Cambiar PUK	Función para cambiar el PUK de la tarjeta (*ver imagen 3*)
Desbloquear PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma (*ver imagen 4*)
Importando…	Función para importar certificados a la tarjeta *(ver imagen 5)*
Ver…	Función para ver el listado de certificados que se encuentra en la tarjeta *(ver imagen 6)*
Información de tarjeta	Ventana que muestra las funciones correspondientes
Acerca de…	Función que muestra las versión instalada *(ver imagen 8)*
Seleccionar Lector	Función para seleccionar el lector con el que se quiere interactuar en el caso de que haya más de uno

Cambiar PIN

Introducir el PIN antiguo de la tarjeta y el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.

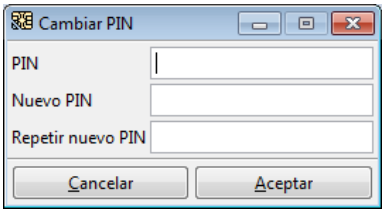


Imagen 2

Cambiar PUK

Introducir el PUK antiguo de la tarjeta y el nuevo PUK. El nuevo PUK tiene que tener entre 6 y 8 dígitos alfanuméricos.

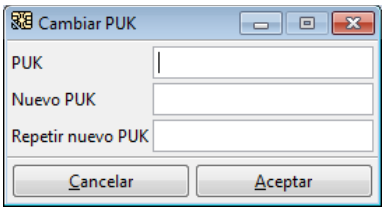


Imagen 3

Desbloquear PIN

Para desbloquear el PIN, introducir el PUK de la tarjeta e introducir el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.

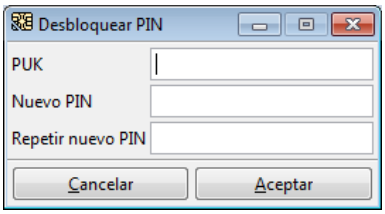


Imagen 4

Importando…

Para importar un certificado a la tarjeta en formato .p12 o .pfx, seleccionar el certificado desde su ubicación y presionar “Open”.

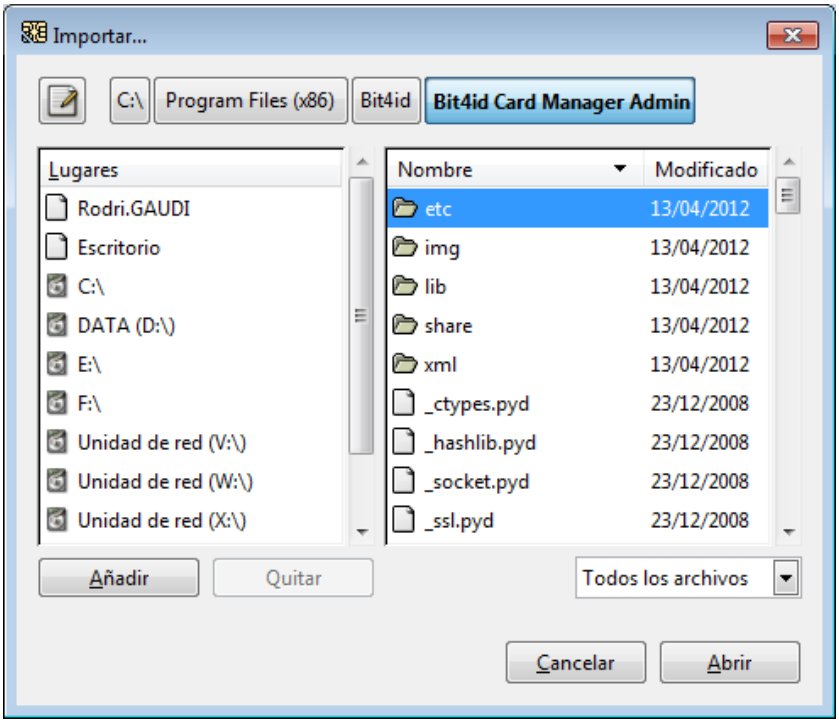


Imagen 5

Ver…

Para ver los certificados que se encuentran en la tarjeta, introducir el PIN de la tarjeta cuando sea solicitado. NO ELIMINAR LOS CERTIFICADOS DE LA TARJETA a no ser que disponga de una copia de los certificados (clave privada y clave pública).

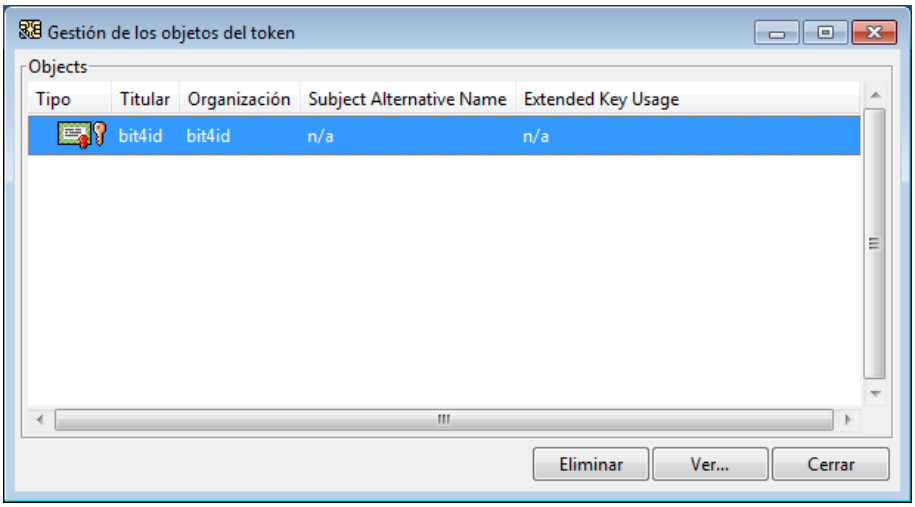


Imagen 6

Información de la tarjeta

Visualiza las características de la tarjeta.

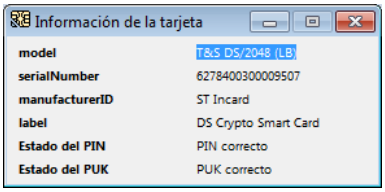


Imagen 7

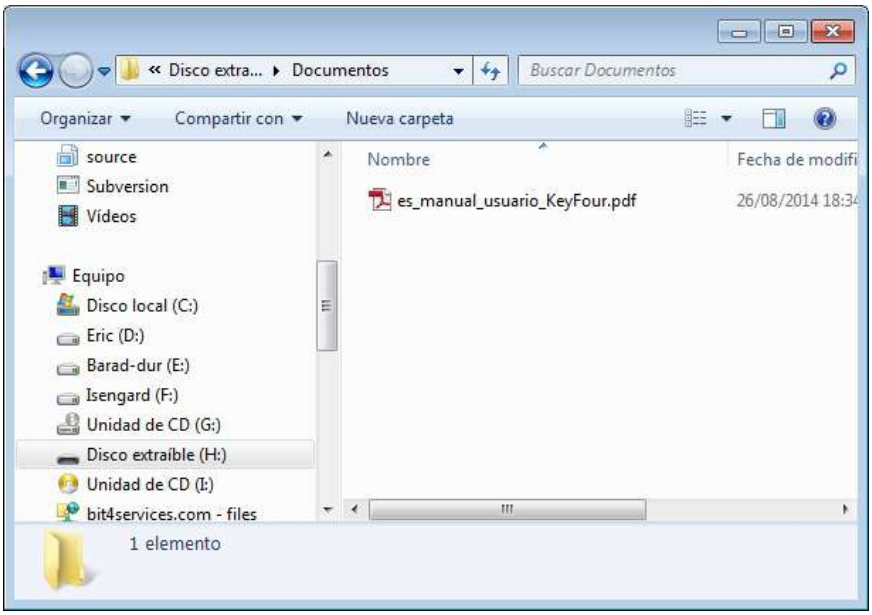
Acerca de…

Ventana que muestra las versiones del Card Manager Admin, importador automático de certificados al store de Windows, PKCS#11 y CSP instalados en el sistema.

Imagen 8

Documentos

Si hace clic en el icono *Documentos* accederá directamente a una carpeta de su dispositivo donde podrá guardar o acceder a los documentos que requiera que hayan sido previamente salvados en esta ubicación.



Modo compatibilidad

Modo compatibilidad es una opción para usuarios avanzados para habilitar el dispositivo como token criptográfico convencional (CCID), reconocido por el sistema operativo. Automáticamente se instalan los drivers y librerías necesarias para poder utilizar el dispositivo con cualquier aplicación instalada en su PC.

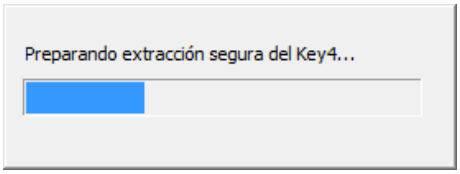
Una vez haya pulsado en el botón Modo compatibilidad, se configurará un servicio en el PC para que siempre que se conecte, lo pase automáticamente a este modo.

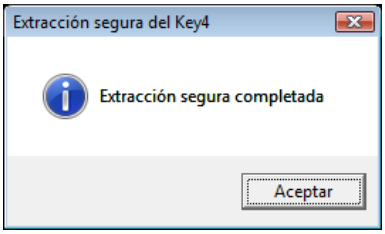
Expulsar

Para evitar problemas de coherencia de los datos en el dispositivo, siempre es conveniente realizar una extracción segura, que garantiza que no haya problemas con los ficheros abiertos.

Una vez pulse en el icono extracción segura le aparecerá una barra de progreso que en completarse le indicará que ya puede desconectar el dispositivo del puerto USB.

Recuerde que si desea reemprender su uso deberá desconectarlo y conectarlo nuevamente al puerto.





Ayuda

Le mostrará una guía interactiva rápida de uso del dispositivo.

Preguntas frecuentes

¿Por qué en Validar no puedo ver el contenido de un documento?

Seguramente usted no tendrá ningún programa asociado para visualizar ese tipo de archivo.

Vea la extensión del archivo y concrete que programa necesita instalar o contacte con su administrador del sistema.

He insertado el dispositivo pero no me muestra nada por pantalla.

Si las luces del dispositivo no parpadean asegúrese de haberlo conectado correctamente o pruebe de conectarlo en otro puerto.

Si las luces ya parpadean consulte el apartado puesta en marcha, en caso contrario consulte con su administrador del sistema.

No puedo acceder a la ayuda

Busque cualquier ventana de Internet abierta y ciérrelas todas ya que si tiene una instancia en ejecución en su PC del Mozilla Firefox no podrá acceder al archivo de ayuda.

No puedo iniciar Internet

Busque cualquier ventana de Internet abierta y ciérrelas todas

Si tiene una instancia en ejecución en su PC local del Mozilla Firefox no podrá acceder al archivo de ayuda.

No veo correctamente el documento PDF firmado

Para la correcta visualización en adobe Acrobat Reader de documentos PDF firmados se recomienda tener instalada la versión como mínimo Acrobat Reader XI

Configuración de Acrobat Reader para el correcto funcionamiento con certificados digitales en Windows: Ir a "Edición" --> "Preferencias" --> en Categorías, seleccionar "Firmas" y en la pantalla de derecha pulsar en "Más..." correspondiente a Verificación. En la pantalla nueva, marcar la casilla “Validando documentos certificados” en la sección “Integración con Windows”. Aceptar todos los cambios.

No puedo firmar un documento PDF

Vaya a las propiedades del documento PDF y compruebe si se permite la firma. Abra el documento PDF, “Archivo” --> “Propiedades” --> “Seguridad”.

No puedo sellar en el tiempo un documento

Compruebe que las credenciales de acceso al sistema son correctas, sino póngase en contacto con su proveedor de servicios de sellado de tiempo o TSA.

Modo compatibilidad bajo Linux me muestra un mensaje "El servicio PCSD no está instalado: Instalar y después es recomendado reiniciar el equipo"

Linux por defecto no tiene el servicio de tarjeta inteligente (PCSCD) instalado, así que hay que tomar un paso adicional para cada sistema operativo, ejecutar el siguiente comando en el terminal de Linux:

Fedora (con permisos de administrador): yum install pcsc-lite.

Ubuntu: sudo apt-get install pcscd.

Debian (con permisos de administrador): apt-get install pcscd.

Glosario

Algoritmo: Secuencia de reglas e instrucciones que indican el procedimiento a partir del cual se resuelve un problema. La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

Autenticación: La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. Otra manera de definirlo seria, la capacidad de determinar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje.

Autoridad de Certificación: Es la entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica. La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Autoridad de Registro: Es la entidad encargada de identificar, de registrar y de entregar certificados electrónicos a los usuarios y ofrece sus servicios a otras entidades.

Autoridad de sellado del tiempo: Actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

CAdES (PKCS#7): formato de firma electrónica. Fue uno de los primeros estándares internacionales de firma, muy implantado en países avanzados en firma electrónica.

Caducidad del certificado digital: El certificado digital tiene un período de vigencia que consta en el mismo certificado. Generalmente es de 2 años, aunque por ley se permite una vigencia de hasta 5 años. Una vez el certificado haya caducado, no se podrán utilizar los servicios ofrecidos por la Administración que requieran firma electrónica, y cualquier firma electrónica que se haga a partir de ese momento no tendrá validez.

Certificado digital: Documento en soporte informático emitido y firmado por la Autoridad de Certificación, que garantiza la identidad de su propietario.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Codificación en Base64: Estructura de información requerida por algunos servicios o programas.

Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que este autorizado. De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada.

Contrafirma: Firma electrónica realizada sobre una firma anterior, y no sobre todo el documento anterior.

CRL: Lista de Certificados Revocados de las autoridades de certificación, donde figuran exclusivamente la relación de certificados revocados o suspendidos.

Dispositivo seguro de creación de Firma: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Certificación common criteria certification EAL4+ based on CWA 14169.

Drivers: Componente informático que permite al sistema operativo interactuar con un periférico, como un ratón, teclado, impresora, etc.

ETSI: European Telecommunications Standards Institute (ETSI) o Instituto Europeo de Normas de Telecomunicaciones, es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial. Principal abanderado del estándar XMLDSig o XAdES como formato estandarizado para la firma electrónica avanzada.

Firma de larga duración XAdES-X-L: Formato de firma electrónica basado en lenguaje XML que permite la validación de la firma durante un largo período de tiempo, ya que incluye una "instantánea" de la situación en que se realiza la firma, permitiendo su validación posterior.

Firma electrónica: Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Existen 3 tipos de firma electrónica: firma electrónica simple, avanzada y reconocida.

Firma electrónica simple: Conjunto de datos, en forma electrónica, anejos a otros datos.

Firma electrónica avanzada: Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Listas de Revocación de Certificados o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

No repudio: El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de la clave privada que únicamente conoce él y que está obligado a custodiar. El no repudio permite, además, comprobar quién participó en una transacción.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero

P7M: archivo SMIME de tipo SignedData.

PAdES (PDF): Formato de firma electrónica avanzada basado en el estándar Adobe PDF

Prestador de Servicios de Certificación o PSC: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Ver Autoridad de Certificación.

PIN: Secuencia de caracteres que permiten el acceso a los certificados. Clave Personal de Acceso.

Puerto USB: Es la interfaz más común de conexión de periféricos al PC.

Renovación: La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, antes de la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación: Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las claves. La revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Estas listas son públicas y deben estar siempre disponibles.

Suspensión: Invalidación temporal de un certificado digital como consecuencia de la petición del suscriptor, o por propia iniciativa de la autoridad de certificación, en caso de duda sobre la seguridad de las claves.

Sello de tiempo: Mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 de la ETSI y está en el registro de estándares de Internet.

Una Autoridad de Sellado de Tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos. Las normas europeas TS 101 733 y TS 101 903 establecen dos modalidades de firma que incluyen sellado de tiempo. La variante ES-T añade el sellado a una firma básica (BES) y la variante ES-C añade, además del sellado de tiempo, información sobre la ruta en la que se puede verificar la validez del certificado obtenido de una consulta OCSP o de CRL. Además estas normas prevén la modalidad ES-XL que incluye información sobre el estado de revocación del certificado. De esta forma se obtiene una firma completa que libera al receptor de la firma del problema de deducir de la firma o del certificado la forma de comprobar la validez del certificado que puede variar de PSC en PSC.

Tarjeta inteligente (smartcard): Cualquier tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.

TSA: Contracción del vocablo inglés "Time-Stamping Authority". Correspondiente al término Autoridad de Sellado de Tiempo.

TSQ: Contracción del vocablo inglés "Time Stamp Request". Corresponde a la solicitud de sello de tiempo a una Autoridad de Sellado de tiempo.

TSR: Contracción del vocablo inglés "Time Stamp Response". Es la respuesta que la TSA da a una mensaje time stamp request.

TSS: Contracción del vocablo inglés "time-stamp service". Corresponde al término servicio de sellado de tiempo, que emite TST.

TST: Contracción del vocablo inglés "time-stamp token". Corresponde al sello digital de tiempo emitido por un servicio de sellado de tiempo desde un TSU.

TSU: Contracción del vocablo inglés "time-stamp unit". Corresponde a una Unidad específica de sellado de tiempo, perteneciente a los TSS de la TSA. Es la unidad desde la que se crean y firman en nombre de la TSA los sellos digitales de tiempo.

Validar documento: Mecanismo que permite verificar si un documento o fichero ha sido alterado, además de identificar con seguridad a la persona que lo ha firmado, y opcionalmente, garantizar el momento exacto (fecha y hora) en que se produjo la firma.

XAdES (XML): XAdES sigla en inglés de XML Advanced Electronic Signatures (Firma electrónica avanzada XML) es un conjunto de extensiones a las recomendaciones XML-DSig haciéndolas adecuadas para la fima electrónica avanzada. Mientras que XML-DSig es un entorno general para firmar digitalmente documentos XML, XAdES especifica perfiles precisos de XML-DSig para ser usados con firma electrónica reconocida con el sentido de la directiva 1999/93/EC de la Unión Europea. Un beneficio importante de XAdES es que los documentos firmados electrónicamente pueden seguir siendo válidos durante largos periodos de tiempo, incluso aunque los algoritmos criptográficos de firma hayan sido reventados. XAdES define seis perfiles, cada perfil incluye y extiende al previo:

XAdES, forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada,

XAdES-T (timestamp), añade un campo de timestamp (firma de tiempo) para proteger contra el repudio,

XAdES-X-L (extended long-term), añade certificados reales y listas de revocación a los documentos firmados para permitir la verificación en el futuro incluso si el código original no está disponible.