Manual usuario

Implantación de sistema de firma digital

CARLOS ORTEGA MUÑOZ
IES RIBERA DE CASTILLA CARTIF

Índice

1. Requisitos mínimos....2
2. Conceptos....2
2.1 Firma electrónica....2
2.2 Firma digital....2
2.3 Sello de tiempo....2
2.4 eIDAS....2
3. DSS....2
3.1 Firma de un documento....2
3.2 Firma de múltiples documentos....2
3.3 Validación certificados SSL....2
3.4 Lista de confianza....7
3.5 Certificados oficiales....12
4.NEXU....14
4.1 Certificado digital....14
4.2 Smartcard....18
5. Referencias....19

1. Conceptos

1.1 Firma electrónica

1.2 Firma digital

1.3 Sello de tiempo

1.4 eIDAS

2. Formato de firma

El formato de firma es la forma de la que se genera el documento de firma, asi como la estructuración del documento generado.

EL formato viene determinado por varios factores:

2.1 Estructura de firma

La estructura condiciona el orden de la informacion en el fichero, las etiquetas de los campos, asi como su opcionalidad.

Se puede usar cualquiera de estas estructuras de datos para firmar cualquier tipo de fichero, pero existen ciertas condiciones de un documento que puede hacer mas conveniente el uso de una estructura u otra. A demas, ciertos organismos trabajan unicamente con determinadas estrucuras de firma, por ejemplo, la aplicación eCoFirma del Ministerio de Industria y Comercio unicamente trabaja con XAdES.

2.1.1 CAdES (CMS)

Esta estructura de firma optimiza el espacio de la información lo que lo hace el mas optimo para firmar archivos grandes, especialmente si la firma contiene el documento original.

2.1.2 XAdES (XML)

La salida del documento de firma sera un fichero XML, un lenguaje de marcas, los documentos de salida de esta estructura son mas grandes que en CAdES, por lo que conviene usarlo con ficheros de menor tamaño.

2.1.3 PAdES

Conviene usar esta estructura cuando el documento a firmar es un fichero PDF, ya que el destinatario puede comprobar facilmente la firma y el documento firmado sin necesidad de utilizar software adicional.

2.1.4 JAdES (JWS)

Presentada en 2021, basada en JSON Web Signature

Otras estructuras

Existen otras estructuras de firma como OOXML y ODF utilizados for suites ofimaticas como Microsoft Office o Libre Office.

2.2 Empaquetado

Nivel

2.3 Contenedor

ASiC-S

ASiC-E

3. Aplicación Web

3.1 Firma de un documento

3.2 Firma de múltiples documentos

3.3 Validación certificados SSL

3.4 Lista de confianza

3.5 Certificados oficiales

4.NexU

NexU es un sencillo software de firma basado en navegador sin Java desarrollado por Nowina, una solución libre que aporta seguridad, privacidad y confiabilidad a la hora de utilizar nuestras claves con el fin de firmar un documento.

Esta herramienta de firma permite que las aplicaciones web interactúen con los lectores de tarjetas con chip locales. También permite el uso de claves de firma almacenadas localmente en un ordenador.

NexU es completamente necesario para el uso de la aplicación web de firma digital.

4.1 Instalación

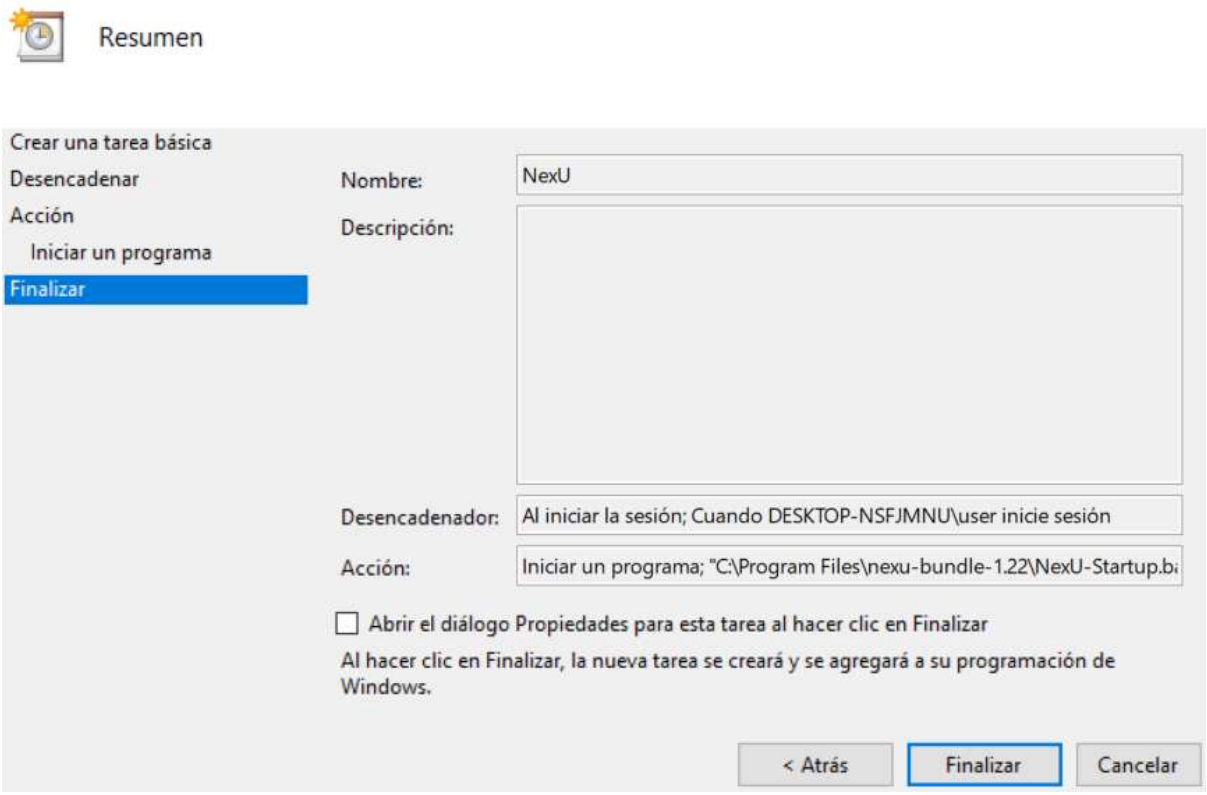
La primer vez que vayamos a utilizar la aplicación de firma digital, en el caso de que no tengamos ya instalado el software, al final de la pagina nos mostrara el siguiente mensaje, en el, se indica que debemos descargar el software NexU, para ello hacemos clic sobre el hiperenlace, esto automáticamente iniciara la descarga del software directamente desde el repositorio oficial de GitHub: https://github.com/nowina-solutions/nexu/releases/

El resultado de la descarga será un fichero comprimido .zip, lo descomprimimos usando un gestor de ficheros comprimidos a elección, por ejemplo, 7z.

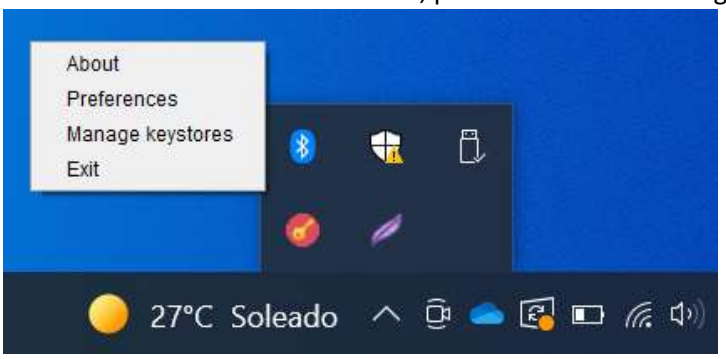
Tras descomprimirlo obtendremos el siguiente directorio, el fichero que debemos ejecutar para iniciar NexU es “NexU-Startup.bat”.

Es recomendable moverlo a un directorio como Archivos de programa para después programar una tarea que lo inicie automáticamente al iniciar sesión en el equipo, de forma que no tengamos que iniciarlo manualmente después de cada reinicio.

Para ello pulsamos la combinación de teclas Ctrl+R y escribimos lo siguiente: taskschd.msc, pulsamos sobre “Crear tarea básica…” e introducimos los datos básicos de la tarea en el asistente (Nombre y descripción, desencadenador y accion).



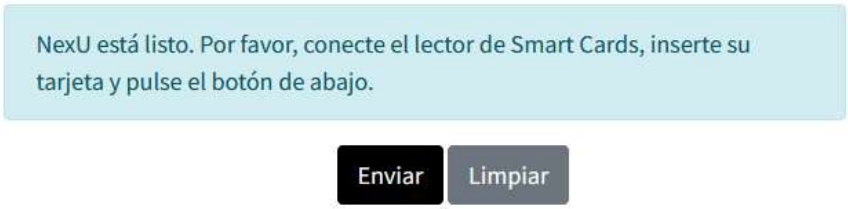
Tras ejecutarlo, haciendo clic derecho sobre su icono, podremos realizar las siguientes acciones.



- About: Visualizar la versión en ejecución de NexU.
- Preferences: Configuración de proxy (opcional).
- Manage keystores: Almacén de claves, NexU posee un almacén de claves para facilitar el proceso de firma, almacenando la ruta de los ficheros de clave, esto en ningún caso almacenara ninguna credencial.
- Exit: Cerrar NexU.

4.2 Certificado

A la hora de firmar un documento, una vez tengamos instalado el software NexU, nos mostrara el siguiente mensaje, pulsamos sobre “Enviar” para iniciar el proceso de firma.



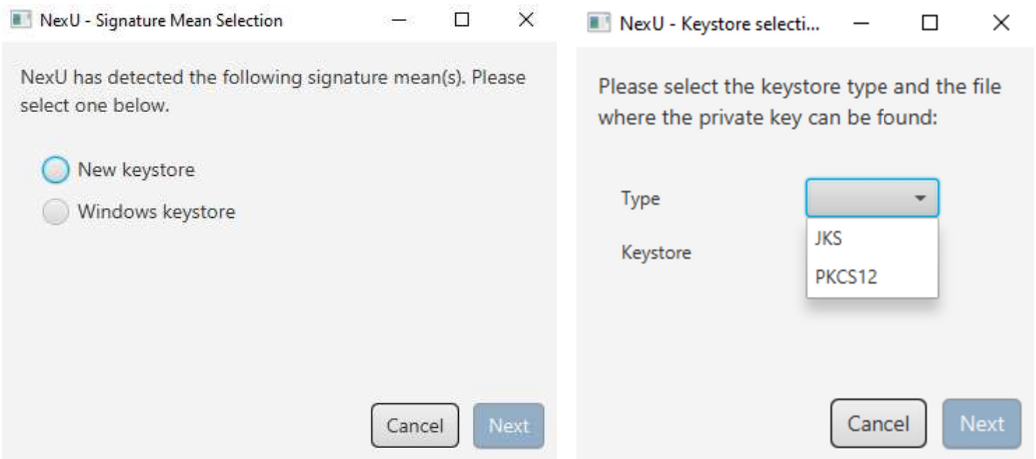
4.2.1 Carga de certificado

En este primer paso tendremos que indicar el certificado que deseamos usar para firmar el documento.

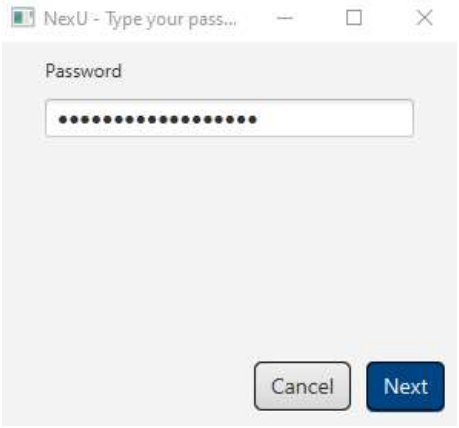
Nos saldrá la siguiente ventana de NexU, en la que, al ser la primera vez que firmamos, no tenemos ningún certificado guardado en el almacen de certificados de NexU, por lo que nos dará la opción de cargar un nuevo certificado usando el explorador o cargarlo directamente del almacen de certificados de Windows.

En el caso de que ya hayamos firmado previamente y hayamos marcado la opción de guardar el certificado en el almacén aparecerá dicho certificado como opción extra.

Si deseamos cargar el fichero del certificado deberemos seleccionar el tipo de certificado que poseamos Java Keystore (JKS) o PKCS12 (P12, PFX) y seleccionamos el fichero del certificado.



Nos pedirá la contraseña del certificado.



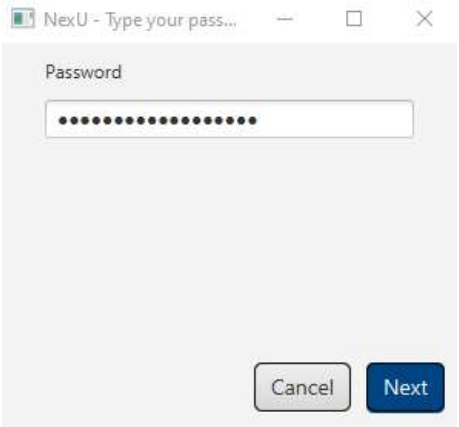
4.2.2 Cálculo de la función hash

El siguiente paso es el cálculo del valor hash del documento a firmar, esto lo realiza automáticamente la aplicación, ya que es la información que se firma, de forma que si el documento se modifica pueda ser detectado.

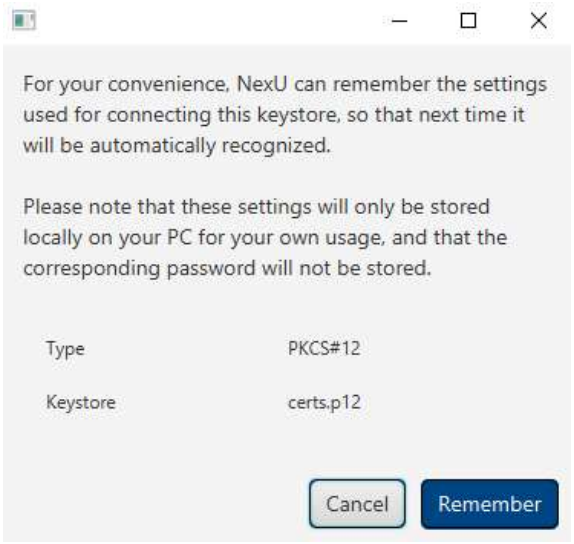
La función hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija y, en el caso de que esta varíe en cualquier medida, el valor hash cambiara por completo, ver mas.

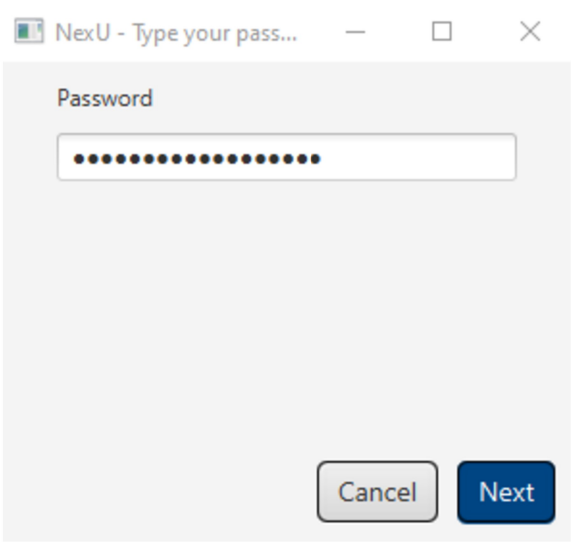
4.2.3 Firma de la función hash.

El tercer paso es el firmado de la función hash generada en el paso anterior, para esto será necesario introducir de nuevo la contraseña del certificado.



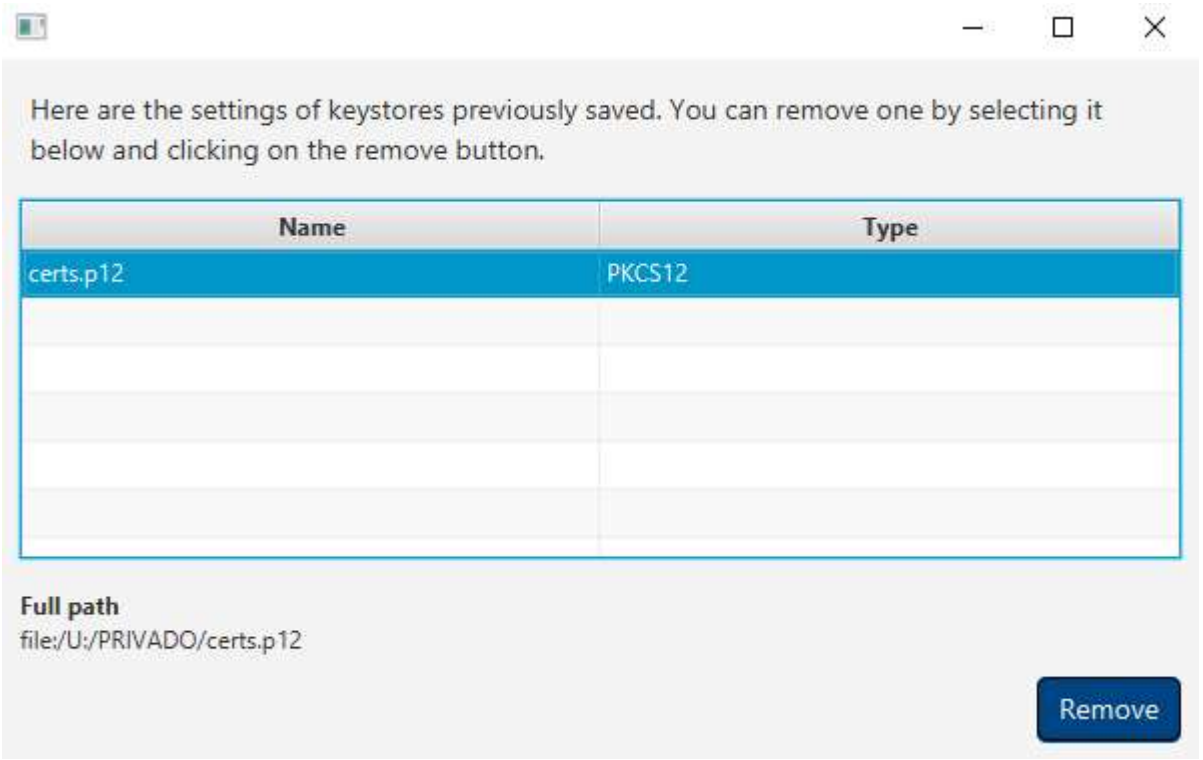
En el caso de que no tengamos el certificado guardado en el almacen de NexU, nos mostrará el siguiente mensaje ofreciéndonos guardarlo para poder usarlo mas fácilmente sin tener que introducir la ruta del certificado constantemente, para guardarlo nos pedirá de nuevo la contraseña, sin embargo, esta NO se almacenara, únicamente se almacena la ruta donde esta ubicado el certificado.





Posteriormente podremos ver el certificado guardado en el almacen de certificados, haciendo clic derecho sobre el icono de NexU.

Ahí nos mostrara el nombre del fichero del certificado, el tipo de certificado y su ruta, a su vez, podemos eliminarlo seleccionando el certificado y pulsando sobre “Remove”.



4.2.4 Descarga del documento firmado

Una vez hayamos finalizado, se nos descargara automáticamente el documento firmado.

4.3 Smartcard

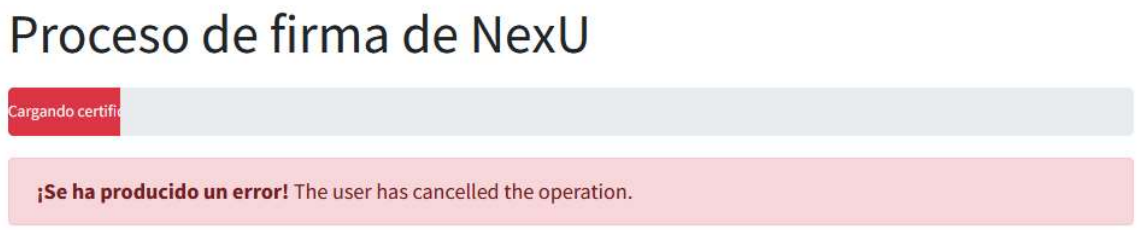
4.4 Resolución de problemas

Existen una serie de errores que nos puede devolver durante el proceso de firma, aquí se recogerán algunos de ellos, asi como su causa y/o solución.

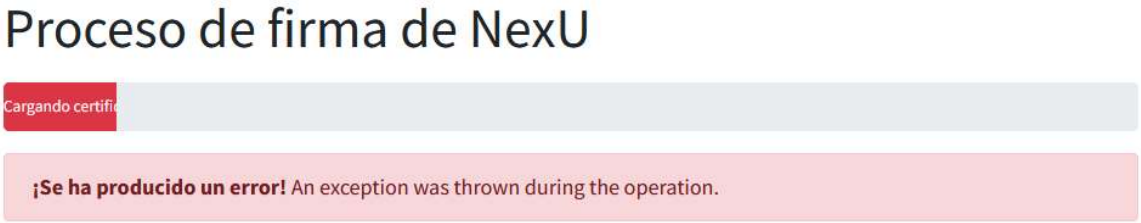
4.4.1 The user has cancelled the operation

Este error aparece en la aplicación web cuando desde NexU, se cierra la ventana o se hace clic sobre el boton “Cancel”.

Para solucionarlo, simplemente actualizamos la página y repetimos el proceso de firma.



4.4.2 An exception was thrown during the operation



5. Aplicación Independiente

6. Referencias