



# Manual usuario

Implantación de sistema de firma digital

**CARLOS ORTEGA MUÑOZ**  
IES RIBERA DE CASTILLA CARTIF

# Índice

1. Conceptos .....	3
1.1 Firma electrónica .....	3
1.2 Firma digital .....	3
1.3 Sello de tiempo .....	3
1.4 eIDAS .....	3
2. Formato de firma .....	4
2.1 Estructura de firma .....	4
2.1.1 CAdES (CMS).....	4
2.1.2 XAdES (XML).....	4
2.1.3 PAdES .....	4
2.1.4 JAdES (JWS) .....	4
2.1.5 Otras estructuras .....	4
2.2 Empaquetado.....	4
2.3 Niveles.....	6
2.3.1 Nivel Baseline-B (B-B).....	6
2.3.2 Nivel Baseline-T (B-T) .....	6
2.3.3 Nivel Baseline-LT (B-LT).....	6
2.3.4 Nivel Baseline-LTA (B-LTA) .....	6
2.4 Contenedores (ASiC) .....	7
2.4.1 ASiC Sencillo (ASiC-S) .....	7
2.4.2 ASiC Extendido (ASiC-E) .....	7
2.5 Algoritmo función hash.....	7
3. Aplicación Web .....	9
3.1 Firma .....	9
3.1.1 Firma de un documento.....	9
3.1.2 Firma de una función hash.....	9
3.1.3 Firma de un PDF .....	10
3.1.4 Firma con JAdES .....	11
3.1.5 Firma de múltiples documentos .....	12
3.1.6 Contrafirma de una firma .....	13
3.2 Validación.....	14
3.2.1 Validación una firma .....	14
3.2.2 Validación un certificado.....	15
3.2.3 Validación certificados SSL.....	15

3.2.4 Reproducción de datos de diagnostico.....	15
3.2.5 Lista de proveedores de confianza .....	16
3.2.6 Certificados de confianza del Diario Oficial .....	16
3.3 Servidor .....	17
3.3.1 Extensión de una firma .....	17
3.3.2 Sellado temporal de documentos.....	17
4.NexU.....	18
4.1 Instalación .....	18
4.2 Certificado.....	20
4.2.1 Carga de certificado .....	20
4.2.2 Cálculo de la función hash .....	21
4.2.3 Firma de la función hash.....	21
4.2.4 Descarga del documento firmado.....	23
4.3 Almacén de certificados de Windows.....	23
4.4 Smartcard.....	26
4.5 Resolución de problemas.....	26
4.5.1 The user has cancelled the operation.....	26
5. Aplicación Independiente .....	28
5.1 Obtención.....	28
5.2 Utilización.....	30

# 1. Conceptos

## 1.1 Firma electrónica

---

**Concepto jurídico** donde una persona acepta y da por validado el contenido de un mensaje electrónico a través de cualquier medio electrónico que sea legítimo y permitido, esto puede ser una tarjeta de coordenadas, una firma con un lápiz electrónico o una firma biométrica.

En el artículo 3.10 de eIDAS, el reglamento para la identificación electrónica aplicado a los países europeos del que hablaremos más adelante define de la siguiente manera la firma electrónica:

“los datos en formato electrónico anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar;” (eIDAS Artículo 3.10)

## 1.2 Firma digital

---

Una firma digital, en cambio, es un tipo de firma electrónica que hace uso de un **algoritmo** o mecanismo criptográfico que proporciona la capacidad de recopilar evidencias electrónicas de **integridad** e **identificación**, ambas proporcionan la posibilidad de dar fe legalmente de la voluntad del firmante.

## 1.3 Sello de tiempo

---

Un sello de tiempo electrónico es un dato en forma electrónica que vincula otros datos en forma electrónica a un tiempo particular, estableciendo evidencia de que estos últimos datos **existían en ese momento**.

Por ejemplo, un signatario puede usar un sello de tiempo electrónico para vincular un documento firmado a una fecha y hora en particular y probar en el futuro que el documento firmado existía en esa fecha y hora en particular.

## 1.4 eIDAS

---

La regulación **Nº910/2014** también llamada **eIDAS Regulation** reemplazo a **eSignature Directive** de 1999 y es un conjunto de normas para la identificación electrónica y de los servicios de confianza para transacciones electrónicas en el mercado único europeo y se aplicó desde el 1 de julio de 2016 a todos los miembros de la unión europea.



## 2. Formato de firma

El formato de firma es la forma de la que se genera el documento de firma, así 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 información en el fichero, las **etiquetas** de los campos, así 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 más conveniente el uso de una estructura u otra. A demás, ciertos organismos trabajan únicamente con determinadas estructuras de firma, por ejemplo, la aplicación [eCoFirma](#) del Ministerio de Industria y Comercio únicamente trabaja con **XAdES**.

#### 2.1.1 CADES (CMS)

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

#### 2.1.2 XAdES (XML)

La salida del documento de firma será un fichero XML, un lenguaje de marcas, los documentos de salida de esta estructura son más 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 fácilmente 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, útil tanto para documentos XML, PDF y ficheros binarios.

#### 2.1.5 Otras estructuras

Existen otras estructuras de firma como **OOXML** y **ODF** utilizados para suites ofimáticas como **Microsoft Office** o **Libre Office** respectivamente.

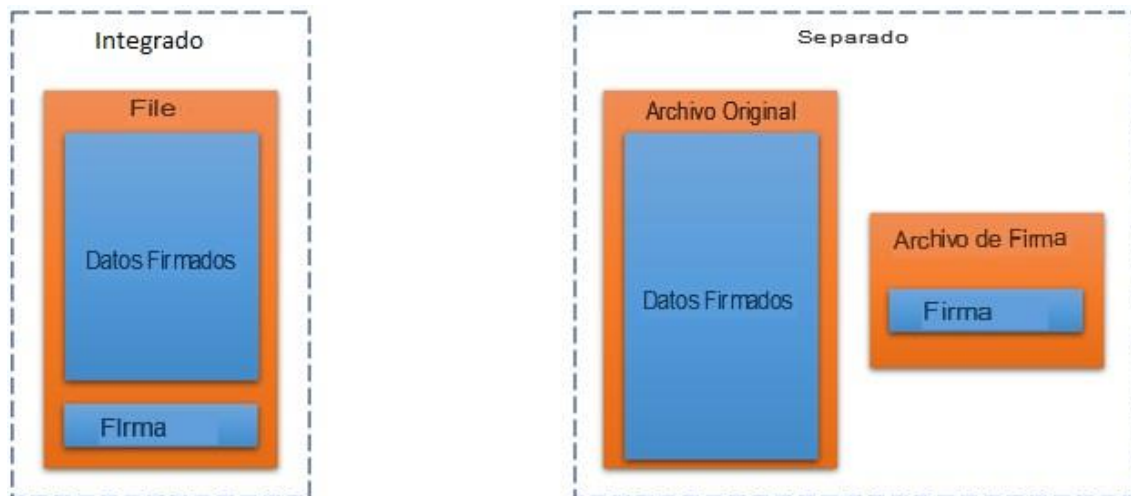
## 2.2 Empaquetado

---

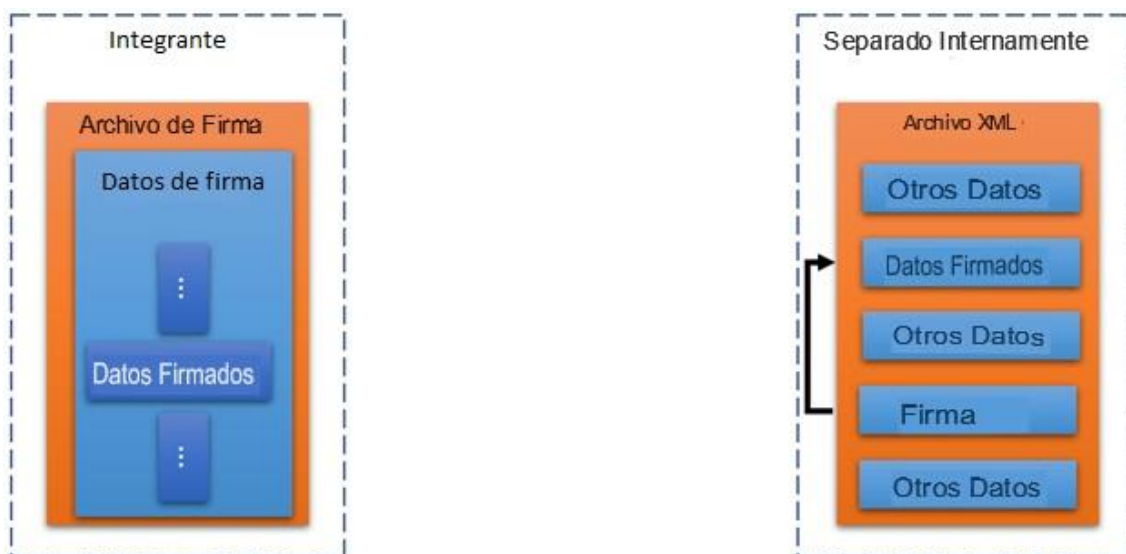
El empaquetado consiste en la **forma en la que se almacenan** tanto los datos de la firma, como los del fichero original, existen cuatro formas de empaquetado:

1. Firma integrada.
2. Firma separada.
3. Firma integrante.
4. Firma internamente separada.

Una firma puede ser **integrada** o **separada**, en función de que se incluya como elemento del archivo que contiene los datos firmados, obteniendo como resultado un solo fichero o se cree un archivo de firma separado, obteniendo dos ficheros, uno para la información firmada y otro para la firma.



También puede ser **integrante** cuando los datos firmados se incluyen como subelemento de la firma, y en casos especiales en los que se desvincula la firma, pero se incluyen tanto los datos firmados como los datos de la firma en otro archivo, se denomina **desvinculación interna**. (Las firmas separadas internamente se usan muy raramente).



No todos los formatos de firma admiten estas diferentes ubicaciones y posicionamientos de una firma y se puede dar una descripción general simplificada de la siguiente manera:

- Las firmas integradas se pueden crear utilizando los formatos XAdES o PAdES.
- Las firmas separadas se pueden crear usando formatos XAdES, CAdES o JAdES.
- Las firmas integrantes se pueden crear usando formatos XAdES, CAdES o JAdES.
- Las firmas separadas internamente solo se pueden crear con el formato XAdES.

## 2.3 Niveles

---

Los estándares ETSI<sup>1</sup> han definido cuatro niveles de firmas de referencia para los formatos CAdES, XAdES, PAdES y JAdES.

El nivel apropiado para usar al crear una firma electrónica depende del uso previsto de la firma:

- Si la firma solo necesita ser **validada a corto plazo** (por ejemplo, al firmar facturas), una firma básica en el nivel **B-B** generalmente sería suficiente;
- Por otro lado, si existe la necesidad de que una firma pueda ser **validada a largo plazo**, se debe considerar un proceso de preservación de aumento periódico del nivel **B-LTA**. Sin embargo, dicho proceso de conservación suele ser mucho más complicado de implementar que la simple generación de una firma electrónica y su aplicación debe estar debidamente justificada.

### 2.3.1 Nivel Baseline-B (B-B)

Nivel de una Firma Básica, es decir, es una firma que se puede validar siempre que el certificado de firma sea válido (no revocado ni caducado).

### 2.3.2 Nivel Baseline-T (B-T)

Nivel de una Firma con Tiempo, es decir, es una firma que prueba que la firma existió en un momento dado. Se construye desde el nivel anterior agregando un token de marca de tiempo en la firma como propiedades sin firmar.

### 2.3.3 Nivel Baseline-LT (B-LT)

Nivel de una Firma con Material de Validación a Largo Plazo, es decir, es una firma que proporciona la disponibilidad a largo plazo al incorporar todo el material o referencias a material necesario para validar la firma. Se construye a partir del nivel anterior añadiendo este material, es decir: el certificado completo y los datos de revocación de la firma y el(los) sello(s) de tiempo como propiedades no firmadas.

### 2.3.4 Nivel Baseline-LTA (B-LTA)

Nivel de una firma que proporciona disponibilidad a largo plazo e integridad del material de validación. Se construye a partir del nivel anterior agregando un token de marca de tiempo en el material de validación como propiedades sin firmar, estableciendo así evidencia de que los datos de validación existían en el momento indicado.

Si se implementan las medidas apropiadas (por ejemplo, sellado de tiempo periódico), una firma en este nivel aún podría validarse mucho después de que los algoritmos criptográficos utilizados para su creación ya no se consideren lo suficientemente seguros, o después de la expiración de los datos de validación.

---

<sup>1</sup> El **Instituto Europeo de Normas de Telecomunicaciones** (*European Telecommunications Standards Institute*; [ETSI]) es una organización de [normalización](#) independiente, sin fines de lucro de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial.

## 2.4 Contenedores (ASiC)

---

**Contenedores de Firma Asociada** o *Associated Signature Containers (ASiC)*, especifica el uso de estructuras contenedoras para unir uno o más objetos firmados con firmas electrónicas avanzadas o tokens de sellos de tiempo en un único contenedor digital. Funcionando de la misma manera que un fichero comprimido.

Existen diferentes tipos de contenedores ASiC, sin embargo, únicamente cubriremos los dos principales tipos de contenedores, ya que son los soportados por la aplicación web: **ASiC Sencillo (ASiC-S)** y **ASiC Extendido (ASiC-E)**.

Ambos contenedores ASiC son capaces de mantener la disponibilidad y la integridad a largo plazo cuando se almacenan firmas XAdES o CAdES mediante el uso de tokens de sello de tiempo o archivos de manifiesto de registro de pruebas que están contenidos en los contenedores. Los contenedores ASiC deben cumplir la especificación ZIP y las limitaciones que se aplican a ZIP.

### 2.4.1 ASiC Sencillo (ASiC-S)

Un único objeto de archivo se asocia a un archivo de firma o de marca temporal.

Este tipo de contenedor permitirá añadir firmas adicionales en el futuro con el fin de utilizarlas para firmar objetos de archivo almacenados. Cuando se utilizan tokens de marca de tiempo, los archivos ASiC Archive Manifest se utilizan para proteger los tokens de marca de tiempo a contra la manipulación.

### 2.4.2 ASiC Extendido (ASiC-E)

Puede contener uno o varios archivos de firma o de marca temporal.

ASiC-E con XAdES se ocupa de los archivos de firma, mientras que ASiC-E con CAdES se ocupa de las marcas de tiempo.

Los archivos dentro de estos contenedores ASiC se aplican a sus propios conjuntos de objetos de archivo. Cada objeto de archivo puede tener metadatos o información adicional asociada que también puede ser protegida por la firma. Un contenedor ASiC-E está diseñado para evitar esta modificación o permitir su inclusión sin causar daños a las firmas anteriores

## 2.5 Algoritmo función hash

---

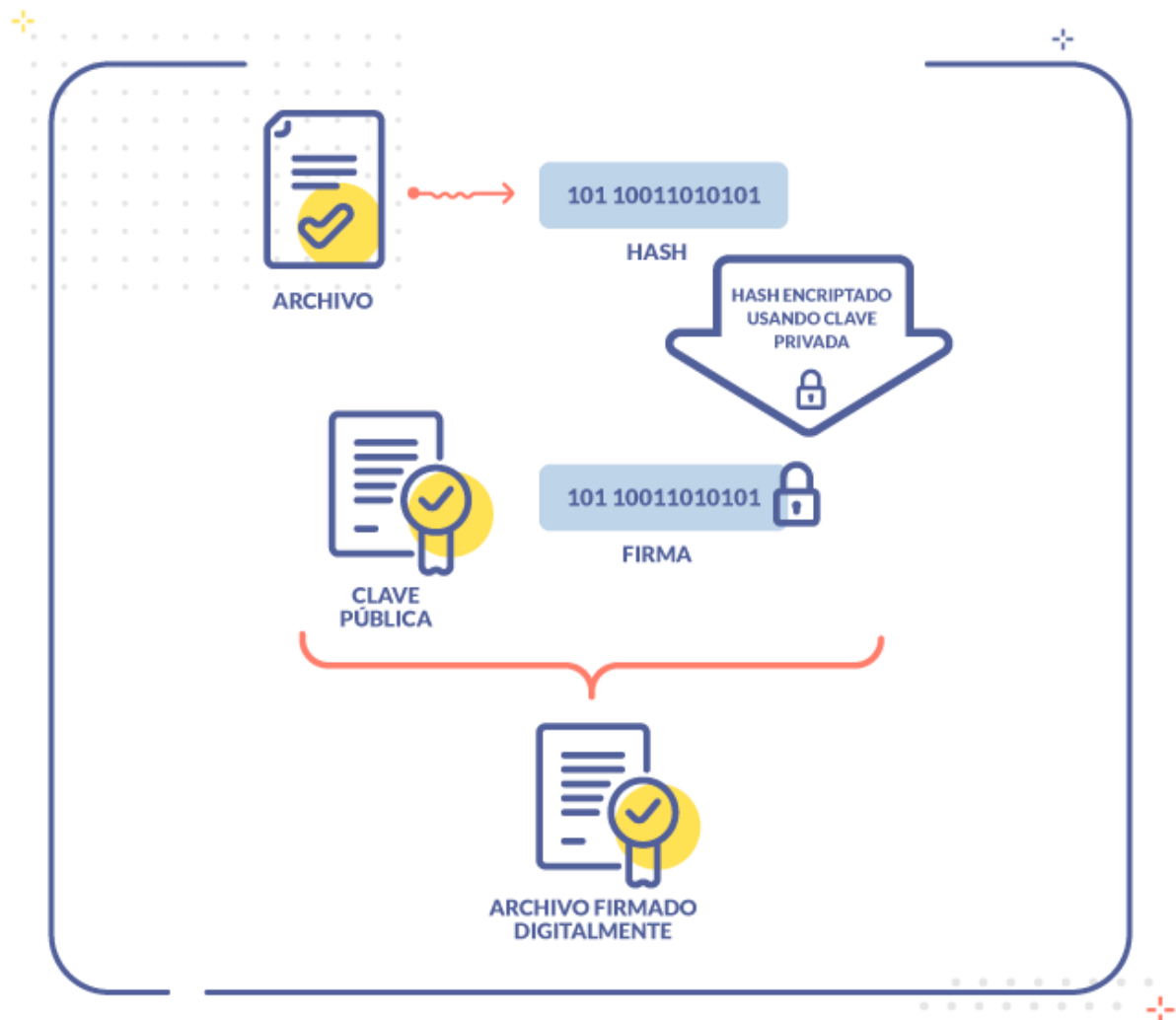
Una función hash consiste en un **algoritmo matemático** que genera una cadena de caracteres alfanuméricos como salida, a partir de cualquier documento que se introduzca como entrada. Es aplicable, en general, a cualquier tipo de archivo digital: documentos, imágenes, audios, vídeos, programas, carpetas, etc.

Son funciones de tipo **unidireccional**. Esto significa que es posible y relativamente sencillo computacionalmente hablando, el calcular dicha cadena resumen. Sin embargo, no es posible generar, mediante un cómputo inverso, el documento o archivo original a partir de la huella digital.

Otra propiedad fundamental de las funciones hash está en la unicidad de la cadena de caracteres que conforma la huella digital. Esta propiedad plantea que cualquier variación en el documento o archivo de entrada, por mínima que esta sea, implica la generación de una **huella totalmente diferente** a la inicial.



La función hash juega un papel muy importante dentro de la firma digital, ya que, durante el proceso de firma, se calcula el valor hash del fichero a firmar, para posteriormente encriptarlo usando la clave privada del certificado firmante.



A la hora de verificar el fichero firmado, se utiliza la clave pública del certificado firmante, la cual ha sido incluido en el fichero firmado para descifrar el valor hash, calcular de nuevo la función hash del fichero y compararlo con el descifrado, en el caso de que este haya variado, significa que el fichero ha sido alterado desde su firma.

El **algoritmo por defecto** establecido en la aplicación web es el **SHA-256**, existen algoritmos que generan hashes de mayor longitud como el SHA-384 o el SHA-512, sin embargo, conllevan el empleo de un mayor ancho de banda para ser transportados, mayor capacidad de memoria y procesamiento para su cálculo, a cambio de una ganancia en seguridad que no es significativa respecto a SHA-256. Por otra parte, existe el riesgo de experimentar problemas de compatibilidad al emplearlos en sistemas que no los entiendan.

## 3. Aplicación Web

### 3.1 Firma

#### 3.1.1 Firma de un documento

En esta primera página podremos firmar cualquier documento configurando cada uno de los parámetros del formato de la firma explicados previamente, pulsamos sobre el botón “**Examinar...**”, seleccionamos el fichero a firmar y ajustamos los parámetros según nuestras necesidades (Contenedor, Formato de firma, Empaquetado, Nivel y Algoritmo función hash).

A su vez, podemos hacer uso de las dos últimas casillas de selección para permitir hacer uso de un certificado caducado y añadir un sellado temporal respectivamente.

[Inicio](#) > [Firmar un documento](#)

Firmas

[Firmar un documento](#)

Firmar una función hash

Firmar un PDF

Firmar con JAdES

Firmar múltiples documentos

Contrafirmar una firma

Aplicación independiente

REST/SOAP APIs

Validación

Validar una firma

Validar un certificado

Validación de certificado SSL

Reproducir datos de

## Firmar un documento

Fichero a firmar

Examinar...

No se ha seleccionado ningún archivo.

Contenedor

☒ Ninguno ☐ ASiC-S ☐ ASiC-E

Formato de firma

☐ XAdES ☐ CAdES ☐ PAdES ☐ JAdES

Empaquetado

☐ Integrada ☐ Integrante ☐ Separada  
☐ Internamente separada

Nivel

Algoritmo función hash

☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512

Permitir certificados caducados

☐

Añadir un sello temporal del contenido

☐

NexU está listo. Por favor, conecte el lector de Smart Cards, inserte su tarjeta y pulse el botón de abajo.

Enviar

Limpiar

#### 3.1.2 Firma de una función hash

Como ya se desarrolló en el apartado de función hash, cuando se firma un fichero, se calcula su valor hash, el cual posteriormente se cifra.

Usando esta página podemos firmar directamente un hash, para que en el caso de que únicamente deseemos generar la firma de un valor hash podamos introducirlo en el cuadro de texto en **base64** o bien arrastrar un fichero del que se desee calcular el valor hash al cuadro rallado para que se **calcule automáticamente** para posteriormente ajustar el resto de parámetros ya vistos.

[Inicio](#) > [Firmar una función hash](#)

Firmas
<a href="#">Firmar un documento</a>
<a href="#">Firmar una función hash</a>
<a href="#">Firmar un PDF</a>
<a href="#">Firmar con JAdES</a>
<a href="#">Firmar múltiples documentos</a>
<a href="#">Contrafirmar una firma</a>
<a href="#">Aplicación independiente</a>
<a href="#">REST/SOAP APIs</a>

Validación
<a href="#">Validar una firma</a>

## Firmar una función hash

Formato de firma	<input type="radio"/> XAdES <input type="radio"/> CAdES <input type="radio"/> JAdES
Algoritmo función hash	<input type="radio"/> SHA1 <input checked="" type="radio"/> SHA256 <input type="radio"/> SHA384 <input type="radio"/> SHA512
Función hash a firmar (Base64)	<input type="text"/>
	<div>Arrastre un fichero aquí para calcular su valor hash</div>
Nivel	<input type="text"/>
Permitir certificados caducados	<input type="checkbox"/>
Añadir un sello temporal del contenido	<input type="checkbox"/>

### 3.1.3 Firma de un PDF

En el caso de que el documento a firmar sea un **PDF**, podemos hacer uso de esta página, aquí únicamente debemos arrastrar el documento PDF al cuadro rallado o pulsar sobre el para seleccionarlo usando el explorador y automáticamente nos llevara al proceso de firma de NexU.

Esta pensado con el fin de agilizar el proceso de firma de documentos PDF, realiza el mismo proceso que si seleccionáramos los siguientes parámetros en la primera página de “Firmar un documento”:

- **Estructura de firma:** PAdES.
- **Empaquetado:** Integrado.
- **Nivel:** Baseline-B.
- **Algoritmo función hash:** SHA-256.

[Inicio](#) > [Firmar un PDF](#)

Firmas
<a href="#">Firmar un documento</a>
<a href="#">Firmar una función hash</a>
<a href="#">Firmar un PDF</a>
<a href="#">Firmar con JAdES</a>
<a href="#">Firmar múltiples documentos</a>

## Firmar un PDF

Arrastra un PDF aquí o pulsa sobre esta área.

### 3.1.4 Firma con JAdES

En esta pagina podremos firmar documentos usando el estándar recientemente publicado de firma digital de formato de firma JAdES, este estándar posee algunas características y parámetros adicionales haciendo necesario una página dedicada para este.

Estos son los elementos a tener en cuenta que varían de los estándares ya vistos:

#### Empaquetado

1. Integrante: Solo permite firmar un documento.
2. Separada: Permite firmar múltiples ficheros mediante 3 posibles mecanismos:
  - a. Encabezados HTTP: Utilizado para firmar solicitudes HTTP, tanto el encabezado como el cuerpo.
  - b. Identificador por URI: Los archivos firmados son des referenciados por URIs.
  - c. Identificador por hash de URI: Se firma la función hash de los documentos originales.

#### Serialización JWS

Esta posee tres formatos:

##### 1. Compacta

```
BASE64URL(UTF8(JWS Protected Header)) || '.' ||
BASE64URL(JWS Payload) || '.' ||
BASE64URL(JWS Signature)
```

##### 2. JSON

```
{
  "protected": BASE64URL(UTF8(JWS Protected Header)),
  "header": "JWS Unprotected Header",
  "payload": BASE64URL(JWS Payload),
  "signature": BASE64URL(JWS Signature)
}
```

##### 3. JSON aplanada

#### Codificación en Base64URL

Función que codifica una cadena de caracteres en base64 usando un conjunto de caracteres seguros para envío por URL, omitiendo los caracteres =, y reemplazando / por \_ y + por -.

Source	Text (ASCII)	M								a								n							
	Octets	77 (0x4d)								97 (0x61)								110 (0x6e)							
Bits		0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Base64 encoded	Sextets	19				22				5				46											
	Character	T				W				F				u											
	Octets	84 (0x54)				87 (0x57)				70 (0x46)				117 (0x75)											

Firmas	
Firmar un documento	
Firmar una función hash	
Firmar un PDF	
<u>Firmar con JAdES</u>	
Firmar múltiples documentos	
Contrafirmar una firma	
Aplicación independiente	
REST/SOAP APIs	

Validación	
Validar una firma	
Validar un certificado	
Validación de certificado SSL	
Reproducir datos de diagnóstico	
Listas de proveedores de confianza	

## Firmar un documento

Fichero(s) a firmar  No se han seleccionado archivos.

Tipo de serialización JWS  
☒ Serialización compacta  
☐ Serialización JSON  
☐ Serialización JSON aplanada

Empaquetado  
☐ Integrante ☐ Separada

Mecanismo de firma separada (SigD)  
☐ Encabezados HTTP  
☐ Identificador de objeto por URI  
☐ Identificador de objeto por función hash de URI

Usar codificación Base64Url ☒

Nivel

Use una EtsiU codificada en Base64Url ☒

Algoritmo función hash  
☒ SHA256 ☐ SHA384 ☐ SHA512

Permitir certificados caducados ☐

Añadir un sello temporal del contenido ☐

### 3.1.5 Firma de múltiples documentos

En el caso de que deseemos firmar múltiples documentos, también hay una página, con la idea de facilitar el proceso de firmado, reduciendo los parámetros a ajustar a los aplicables para contenedores de documentos firmados.

Para la firma de múltiples documentos podemos elegir entre los dos tipos de contenedores existentes y explicados previamente:

- ASiC-S
- ASiC-E

A su vez, únicamente podemos hacer uso de los siguientes formatos de firma:

- XAdES
- CAdES

El resto de parámetros son los comunes al resto de páginas.

Inicio &gt; Firmar múltiples documentos

**Firmas**

Firmar un documento

Firmar una función hash

Firmar un PDF

Firmar con JAdES

Firmar múltiples documentos

Contrafirmar una firma

Aplicación independiente

REST/SOAP APIs

**Validación**

## Firmar múltiples documentos

Fichero(s) a firmar

Examinar...

No se han seleccionado archivos.

Contenedor

☐ ASiC-S ☐ ASiC-E

Formato de firma

☐ XAdES ☐ CAdES

Nivel

Algoritmo función hash

☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512

Permitir certificados caducados

☐

Añadir un sello temporal del contenido

☐

### 3.1.6 Contrafirma de una firma

Una contrafirma es una firma adicional aplicada sobre datos que ya han sido firmados previamente.

Los posibles casos de uso son solicitudes de alquiler e hipoteca, documentos de salud, pasaportes y visas.

Seleccionamos el documento a contrafirmar, seleccionamos el identificador de la firma existente y ajustamos el resto de parámetros según nuestras necesidades.

Inicio &gt; Contrafirmar una firma

**Firmas**

Firmar un documento

Firmar una función hash

Firmar un PDF

Firmar con JAdES

Firmar múltiples documentos

Contrafirmar una firma

Aplicación independiente

REST/SOAP APIs

**Validación**

## Contrafirmar una firma

Fichero a contrafirmar

Examinar...

No se ha seleccionado ningún archivo.

Identificador de firma

Nivel

Algoritmo función hash

☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512

Permitir certificados caducados

☐

NexU está listo. Por favor, conecte el lector de Smart Cards, inserte su tarjeta y pulse el botón de abajo.

Enviar

Limpiar

## 3.2 Validación

### 3.2.1 Validación una firma

A la hora de validar una firma tenemos que introducir el fichero firmado, y el fichero original en el caso de que el tipo de firma sea

#### Nivel de validación

Cambiar la configuración predeterminada solo reducirá el conjunto de firmas a validar teniendo en cuenta que:

- El proceso de validación de Firmas Básicas solo considera atributos de nivel B y realiza una validación básica de sellos de tiempo;
- El proceso de validación de Firma con Datos de Validación a Largo Plazo es un proceso de validación de Firma Básica que también valida los datos de revocación;
- El proceso de validación de Firma con Datos de Archivo (recomendado) se construye desde el nivel anterior al permitir también la validación de la firma en el pasado con todos los datos recopilados.

#### Fichero de validación personalizado

Opcionalmente, elija usar un archivo de restricciones de validación personalizado. El archivo de restricciones de validación predeterminado está disponible en la sección de documentación de la aplicación web y se puede usar para modificar los elementos a validar.

También tenemos la opción de adjuntar certificados para el caso de que no estén embebidos en el fichero de firma/firmado, a demás de poder extraer datos de revocación o marcas de tiempo.

Inicio > Validar una firma

Firmas

Firmar un documento

Firmar una función hash

Firmar un PDF

Firmar con JAdES

Firmar múltiples documentos

Contrafirmar una firma

Aplicación independiente

REST/SOAP APIs

Validación

Validar una firma

Validar un certificado

Validación de certificado SSL

Reproducir datos de diagnóstico

Listas de proveedores de

## Validar una firma

Fichero firmado

Examinar...

No se ha seleccionado ningún archivo.

Fichero(s) original(es)

Examinar...

No se han seleccionado archivos.

Enviar documento(s) original(es) como

☒ Documentos completos

☐ SHA1

☐ SHA256

☐ SHA384

☐ SHA512

Más opciones

Nivel de validación

Proceso de validación para firmas con datos de archivo (recomendado)

☒ Validar firma y lo que sea: AdES, AdES/QC o QES. Todos los certificados y sus cadenas relacionadas son validadas contra la EU MS TSL.

☐ Fichero de restricción de validación personalizado

Examinar...

No se ha seleccionado ningún archivo.

Certificado firmante

Examinar...

No se ha seleccionado ningún archivo. ⓘ

Adjuntar certificados

Examinar...

No se han seleccionado archivos. ⓘ

Certificados

☐ ⓘ

Timestamps

☐ ⓘ

### 3.2.2 Validación un certificado

A la hora de validar un certificado, podemos seleccionarlo directamente usando el explorador de archivos, o bien, podemos introducirlo codificado en Base64, a su vez, podemos introducir opcionalmente una cadena de certificados o un tiempo de validación.

Y, al igual que validando una firma, podemos extraer los certificados o datos de revocación del certificado.

Inicio > Validar un certificado

**Firmas**

- Firmar un documento
- Firmar una función hash
- Firmar un PDF
- Firmar con JAdES
- Firmar múltiples documentos
- Contrafirmar una firma
- Aplicación independiente
- REST/SOAP APIs

## Validar un certificado

Fichero de certificado (DER/PEM)

Examinar...

No se ha seleccionado ningún archivo

Entrada en Base64

Cadena de certificados (opcional)

Examinar...

No se han seleccionado archivos.

Tiempo de validación (opcional)

22 / 05 / 2022

Certificados
☐

Datos de revocación
☐

Identificadores user friendly
☒

### 3.2.3 Validación certificados SSL

La siguiente pagina nos posibilita validar un certificado SSL de una URL, y opcionalmente extraer certificados y datos de revocación del mismo.

Inicio > Validación de certificado SSL

**Firmas**

- Firmar un documento
- Firmar una función hash
- Firmar un PDF

## Validación de certificado SSL

URL

Introduce una URL para validar el certificado SSL

Certificados
☐

Datos de revocación
☐

### 3.2.4 Reproducción de datos de diagnostico

Los datos de diagnóstico son un conjunto de datos construido a partir de la información contenida en la propia firma, pero también de información recuperada dinámicamente como datos de revocación e información extrapolada como la validez matemática de una firma. Los datos de diagnóstico se construyen antes de que se realice la validación completa y se usa para validar la firma y crear un informe de validación.

Los datos de diagnóstico son independientes de la política de validación aplicada. Dos validaciones diferentes las políticas aplicadas a los mismos datos de diagnóstico pueden conducir a resultados diferentes.



Inicio &gt; Reproducir datos de diagnóstico

Firmas	
Firmar un documento	Fichero de diagnóstico <input type="button" value="Examinar..."/> No se ha seleccionado ningún archivo.
Firmar una función hash	Restablecer fecha de validación <input type="checkbox"/>
Firmar un PDF	Nivel de validación <input type="text" value="Proceso de validación para firmas con datos de archivo (recomendado)"/>
Firmar con JAdES	<input checked="" type="radio"/> Validar firma y lo que sea: AdES, AdES/QC o QES. Todos los certificados y sus cadenas relacionadas son validadas contra la EU MS TSL.
Firmar múltiples documentos	<input type="radio"/> Fichero de restricción <input type="button" value="Examinar..."/> No se ha seleccionado ningún archivo.
Contrafirmar una firma	<input type="radio"/> de validación
Aplicación independiente	<input type="radio"/> personalizado

### 3.2.5 Lista de proveedores de confianza

Podemos acceder a una lista actualizada de los proveedores de confianza.

Inicio &gt; Resumen de proveedores de confianza

Firmas																							
Firmar un documento	<h2>Resumen de proveedores de confianza</h2> <p> LOTL Nº1 (<a href="https://ec.europa.eu/tools/lotl/eu-lotl.xml">https://ec.europa.eu/tools/lotl/eu-lotl.xml</a>)</p> <table border="1"> <tbody> <tr> <td>Último intento de descarga</td> <td>22-may-2022 19:15:52</td> </tr> <tr> <td>Última descarga exitosa</td> <td>22-may-2022 19:15:52</td> </tr> <tr> <td>Descargar estado</td> <td>SYNCHRONIZED  22-may-2022 19:15:52</td> </tr> <tr> <td>Estado del análisis</td> <td>SYNCHRONIZED  22-may-2022 19:15:52</td> </tr> <tr> <td>Estado de validación</td> <td>SYNCHRONIZED  22-may-2022 19:15:52</td> </tr> <tr> <td>Número de secuencia</td> <td>306</td> </tr> <tr> <td>Fecha de emisión LOTL</td> <td>15-mar-2022 11:00:29</td> </tr> <tr> <td>Siguiente actualización LOTL</td> <td>14-sep-2022 11:00:29</td> </tr> <tr> <td>Puntos de distribución TL</td> <td><a href="https://ec.europa.eu/tools/lotl/eu-lotl.xml">https://ec.europa.eu/tools/lotl/eu-lotl.xml</a></td> </tr> <tr> <td>Indicación</td> <td><b>TOTAL_PASSED</b></td> </tr> <tr> <td>Fecha de firmado</td> <td>15-mar-2022 12:40:01</td> </tr> </tbody> </table>	Último intento de descarga	22-may-2022 19:15:52	Última descarga exitosa	22-may-2022 19:15:52	Descargar estado	SYNCHRONIZED  22-may-2022 19:15:52	Estado del análisis	SYNCHRONIZED  22-may-2022 19:15:52	Estado de validación	SYNCHRONIZED  22-may-2022 19:15:52	Número de secuencia	306	Fecha de emisión LOTL	15-mar-2022 11:00:29	Siguiente actualización LOTL	14-sep-2022 11:00:29	Puntos de distribución TL	<a href="https://ec.europa.eu/tools/lotl/eu-lotl.xml">https://ec.europa.eu/tools/lotl/eu-lotl.xml</a>	Indicación	<b>TOTAL_PASSED</b>	Fecha de firmado	15-mar-2022 12:40:01
Último intento de descarga		22-may-2022 19:15:52																					
Última descarga exitosa		22-may-2022 19:15:52																					
Descargar estado		SYNCHRONIZED  22-may-2022 19:15:52																					
Estado del análisis		SYNCHRONIZED  22-may-2022 19:15:52																					
Estado de validación		SYNCHRONIZED  22-may-2022 19:15:52																					
Número de secuencia		306																					
Fecha de emisión LOTL		15-mar-2022 11:00:29																					
Siguiente actualización LOTL		14-sep-2022 11:00:29																					
Puntos de distribución TL		<a href="https://ec.europa.eu/tools/lotl/eu-lotl.xml">https://ec.europa.eu/tools/lotl/eu-lotl.xml</a>																					
Indicación	<b>TOTAL_PASSED</b>																						
Fecha de firmado	15-mar-2022 12:40:01																						
Firmar una función hash																							
Firmar un PDF																							
Firmar con JAdES																							
Firmar múltiples documentos																							
Contrafirmar una firma																							
Aplicación independiente																							
REST/SOAP APIs																							
Validación																							

### 3.2.6 Certificados de confianza del Diario Oficial

Así como los certificados de confianza del Diario Oficial de la Unión Europea.

Inicio &gt; Certificados de confianza del Diario Oficial (O) de la Unión Europea

Firmas															
Firmar un documento	<h2>Certificados de confianza del Diario Oficial (O) de la Unión Europea</h2> <p>Certificados de confianza del Diario Oficial (OJ) en el almacén <b>8 Certificados de confianza del Diario Oficial (O) de la Unión Europea</b> de claves DSS</p> <p>El almacén de claves actual está sincronizado con <a href="#">Página del Diario Oficial de la Unión Europea</a></p> <table border="1"> <tbody> <tr> <td><b>Nombre del asunto</b></td> <td>serialNumber=67022330340,givenName=Jean-Marc,surname=Verbergt,commonName=Jean-Marc Verbergt (Signature),countryName=BE</td> </tr> <tr> <td><b>Nombre del emisor</b></td> <td>serialNumber=201508,commonName=Citizen CA,countryName=BE</td> </tr> <tr> <td><b>Inicio</b></td> <td>01-may-2015 20:54:54</td> </tr> <tr> <td><b>Fin</b></td> <td>26-abr-2025 01:59:59</td> </tr> <tr> <td><b>SHA256 (HEX)</b></td> <td>54 00 ab 71 2c 41 aa f0 c4 0b 50 5e 26 4d 54 94 d8 af 41 80 f8 f6 29 55 d1 62 23 b3 29 0f 97 c3</td> </tr> <tr> <td><b>SHA1 (HEX)</b></td> <td>4b 9d d1 8f 1f 2c d8 b0 5f 46 73 5d 4b 5c f8 6f 92 33 61 b4</td> </tr> <tr> <td><b>SHA256 (Base64)</b></td> <td>VACrcSxBqvDEC1BeJk1UINivQYD49iIV0WljsykPI8M=</td> </tr> </tbody> </table>	<b>Nombre del asunto</b>	serialNumber=67022330340,givenName=Jean-Marc,surname=Verbergt,commonName=Jean-Marc Verbergt (Signature),countryName=BE	<b>Nombre del emisor</b>	serialNumber=201508,commonName=Citizen CA,countryName=BE	<b>Inicio</b>	01-may-2015 20:54:54	<b>Fin</b>	26-abr-2025 01:59:59	<b>SHA256 (HEX)</b>	54 00 ab 71 2c 41 aa f0 c4 0b 50 5e 26 4d 54 94 d8 af 41 80 f8 f6 29 55 d1 62 23 b3 29 0f 97 c3	<b>SHA1 (HEX)</b>	4b 9d d1 8f 1f 2c d8 b0 5f 46 73 5d 4b 5c f8 6f 92 33 61 b4	<b>SHA256 (Base64)</b>	VACrcSxBqvDEC1BeJk1UINivQYD49iIV0WljsykPI8M=
<b>Nombre del asunto</b>		serialNumber=67022330340,givenName=Jean-Marc,surname=Verbergt,commonName=Jean-Marc Verbergt (Signature),countryName=BE													
<b>Nombre del emisor</b>		serialNumber=201508,commonName=Citizen CA,countryName=BE													
<b>Inicio</b>		01-may-2015 20:54:54													
<b>Fin</b>		26-abr-2025 01:59:59													
<b>SHA256 (HEX)</b>		54 00 ab 71 2c 41 aa f0 c4 0b 50 5e 26 4d 54 94 d8 af 41 80 f8 f6 29 55 d1 62 23 b3 29 0f 97 c3													
<b>SHA1 (HEX)</b>		4b 9d d1 8f 1f 2c d8 b0 5f 46 73 5d 4b 5c f8 6f 92 33 61 b4													
<b>SHA256 (Base64)</b>		VACrcSxBqvDEC1BeJk1UINivQYD49iIV0WljsykPI8M=													
Firmar una función hash															
Firmar un PDF															
Firmar con JAdES															
Firmar múltiples documentos															
Contrafirmar una firma															
Aplicación independiente															
REST/SOAP APIs															
Validación															

## 3.3 Servidor

En esta sección se encuentran todas las funcionalidades que hacen uso del certificado ubicado en el sistema que aloja la aplicación web de firma digital.

### 3.3.1 Extensión de una firma

La extensión de una firma se utiliza cuando un usuario desea aumentar el nivel de una firma o bien extender el período de tiempo durante el cual la firma puede validarse con éxito.

Por ejemplo, cuando el certificado que admite una firma XAdES-B-B está a punto de caducar (o el certificado está a punto de ser revocado), se puede aumentar la firma a una firma XAdES-B-T, lo que permite que la validación sobreviva a la caducidad del certificado.

Inicio > Extender una firma

Firmas

Firmar un documento

Firmar una función hash

Firmar un PDF

Firmar con JAdES

Firmar múltiples documentos

Contrafirmar una firma

Aplicación independiente

## Extender una firma

Fichero firmado

Examinar...

No se ha seleccionado ningún archivo.

Fichero(s) original(es)

Examinar...

No se han seleccionado archivos.

Contenedor

☒ Ninguno ☐ ASiC-S ☐ ASiC-E

Formato de firma

☐ XAdES ☐ CAdES ☐ PAdES ☐ JAdES

Nivel

Enviar

Limpiar

### 3.3.2 Sellado temporal de documentos

Para sellar temporalmente un documento usando el certificado del servidor debemos usar esta página.

Inicio > Sellar temporalmente documento(s)

Firmas

Firmar un documento

Firmar una función hash

Firmar un PDF

Firmar con JAdES

## Sellar temporalmente documento(s)

Fichero(s) original(es)

Examinar...

No se han seleccionado archivos.

Formato de sello temporal

☐ PDF ☐ ASiC-E ☐ ASiC-S

Enviar

Limpiar

## 4. NexU

NexU es un sencillo software de firma basado en navegador 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

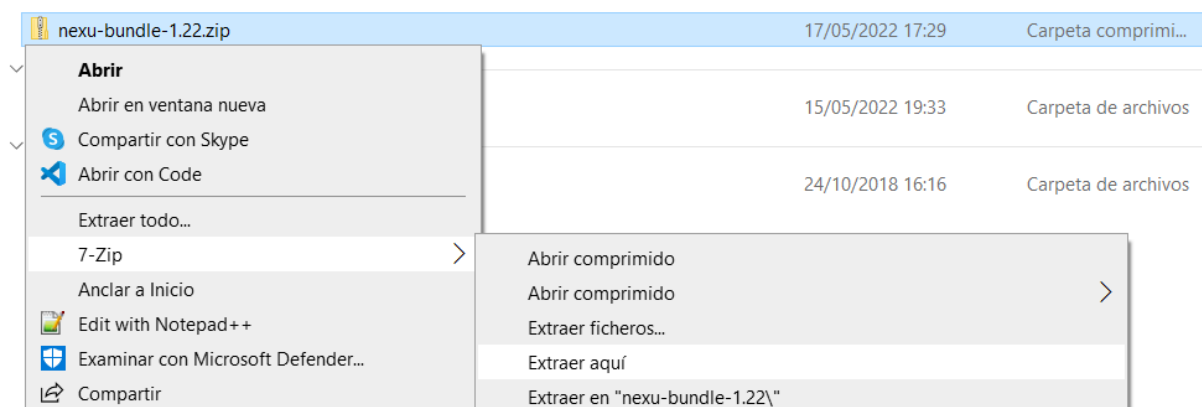
La primer vez que vayamos a utilizar la aplicación de firma digital, en el caso de que no tengamos ya instalado el software, al final de la página nos mostrara el siguiente mensaje, en el, se indica que debemos descargar el software NexU, para ello hacemos **clic sobre el hiperenlace**, esto automáticamente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

¡NexU no detectado! Descarga la versión de código abierto de NexU (más información)

Instale NexU

Limpiar

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"**.

Nombre	Fecha de modificación	Tipo	Tamaño
java	16/06/2017 13:13	Carpeta de archivos	
nexu.jar	24/10/2018 16:16	Executable Jar File	20.652 KB
NexU-Startup.bat	24/10/2018 16:16	Archivo por lotes ...	1 KB

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 acción).



## Resumen

Crear una tarea básica

Desencadenar

Acción

Iniciar un programa

Finalizar

Nombre: NexU

Descripción:

Desencadenador: Al iniciar la sesión; Cuando DESKTOP-NSFJMNU\user inicie sesión

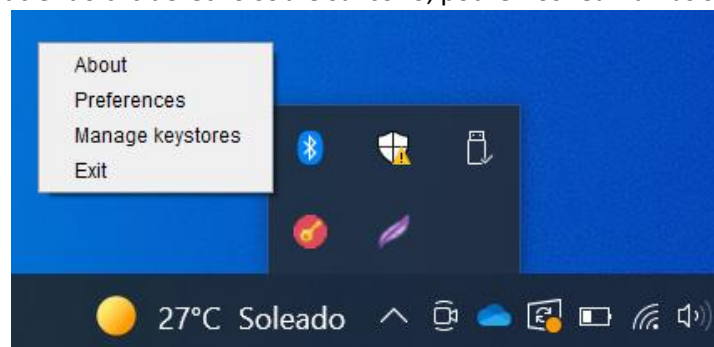
Acción: Iniciar un programa; "C:\Program Files\nexu-bundle-1.22\NexU-Startup.bi

☐ Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar

Al hacer clic en Finalizar, la nueva tarea se creará y se agregará a su programación de Windows.

< Atrás Finalizar Cancelar

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.

NexU está listo. Por favor, conecte el lector de Smart Cards, inserte su tarjeta y pulse el botón de abajo.

Enviar

Limpiar

### 4.2.1 Carga de certificado

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

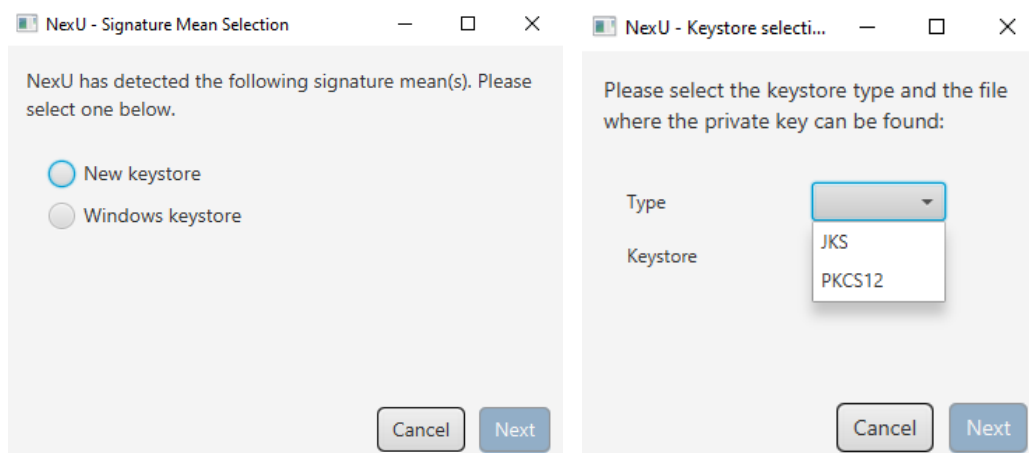
## Proceso de firma de NexU

Cargando certifi

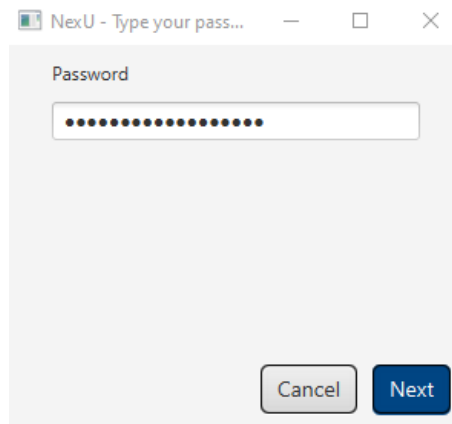
Nos saldrá la siguiente ventana de NexU, en la que, al ser la primera vez que firmamos, no tenemos ningún certificado guardado en el almacén de certificados de NexU, por lo que nos dará la opción de cargar un nuevo certificado usando el explorador o cargarlo directamente del almacén de certificados de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

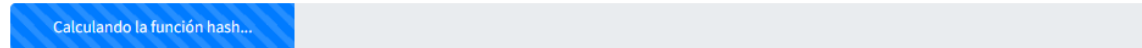


#### 4.2.2 Cálculo de la función hash

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 más](#).

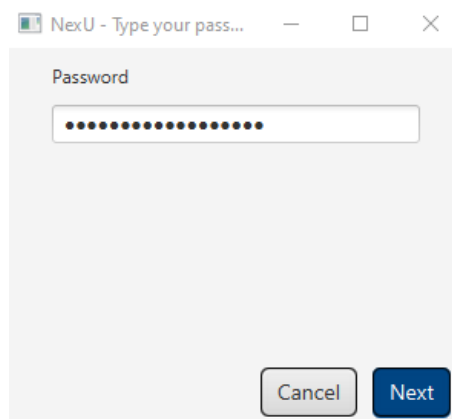
## Proceso de firma de NexU



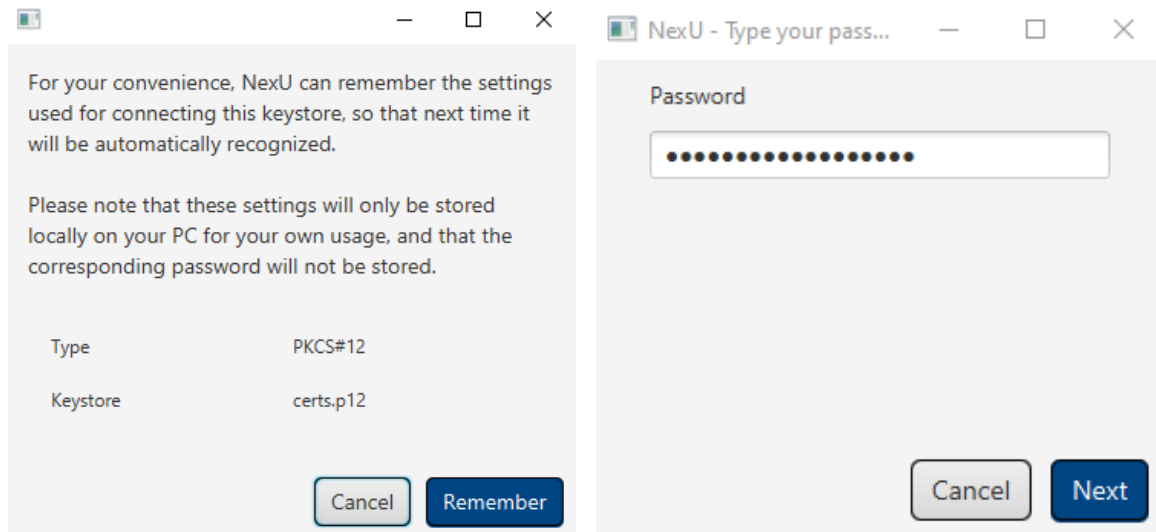
#### 4.2.3 Firma de la función hash.

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.

## Proceso de firma de NexU

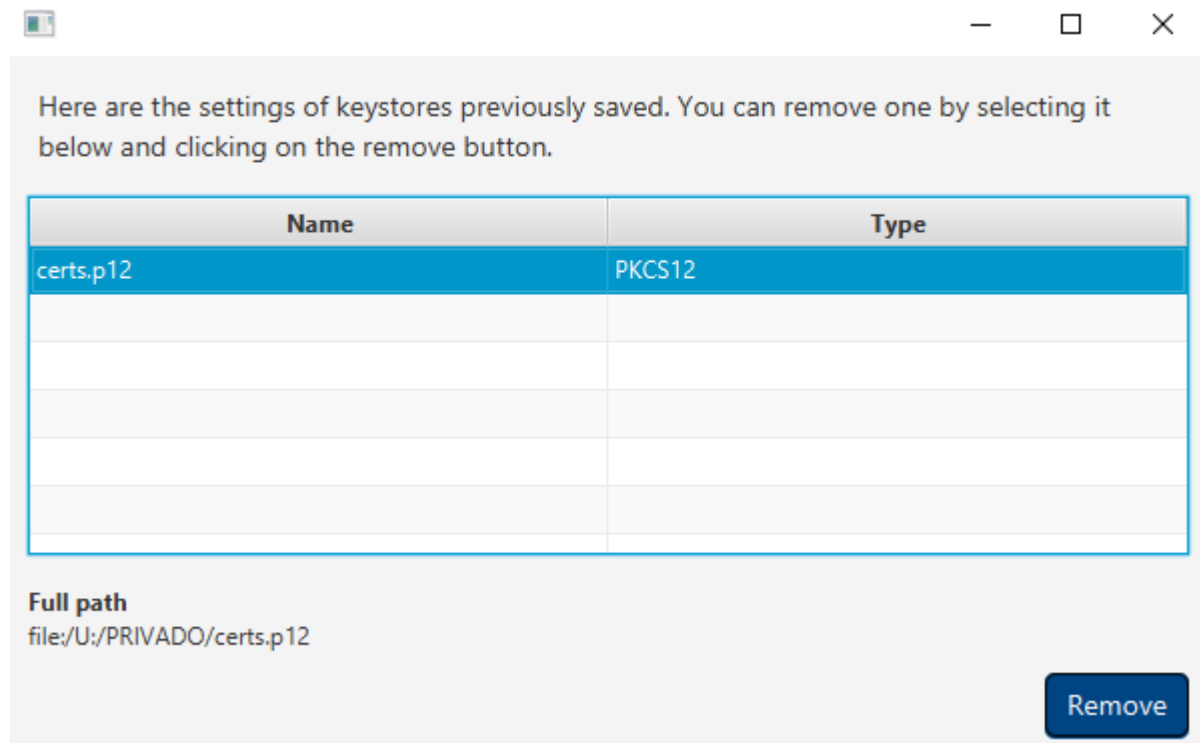


En el caso de que no tengamos el certificado guardado en el almacén de NexU, nos mostrará el siguiente mensaje ofreciéndonos guardarlo para poder usarlo más fácilmente sin tener que introducir la ruta del certificado constantemente, para guardarlo nos pedirá de nuevo la contraseña, sin embargo, esta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



Posteriormente podremos ver el certificado guardado en el almacén 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 descargará automáticamente el documento firmado.

## Proceso de firma de NexU

Hecho!

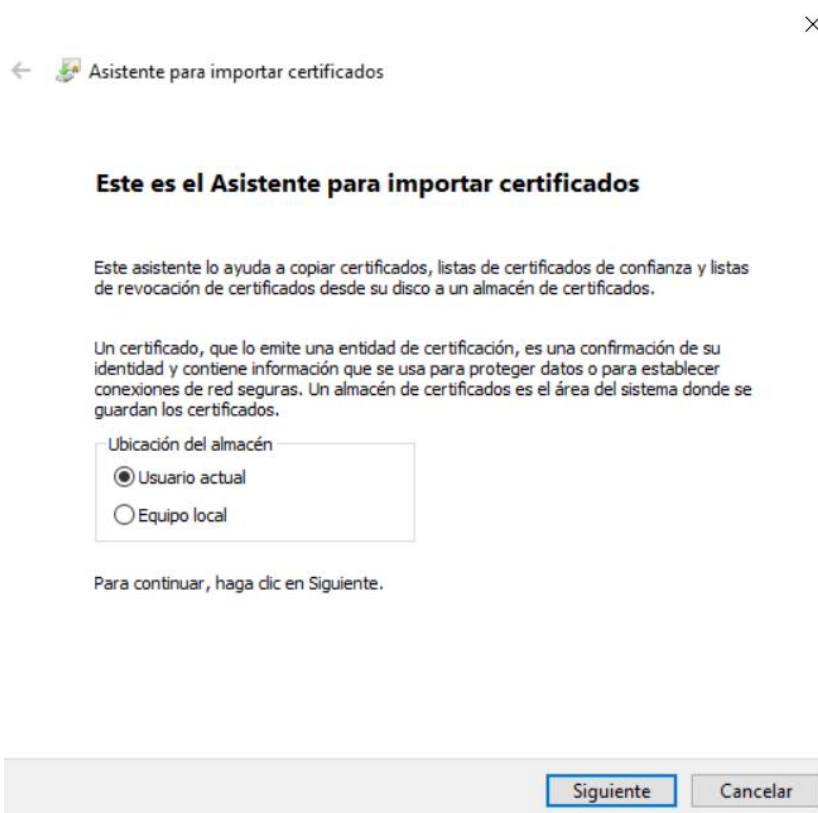
### 4.3 Almacén de certificados de Windows

NexU puede comunicarse con el **almacén de certificados de Windows** con el fin de hacer uso de un certificado del almacén de certificados de Windows para el firmado de un documento a través de la aplicación web de firma digital, para hacerlo primero debemos instalar el certificado en nuestro equipo.

Para ello, empezamos haciendo doble clic sobre el certificado a instalar:




Nos aparecerá el siguiente asistente, en la primera de sus ventanas debemos indicar si deseamos instalar el certificado en el almacén del usuario o del equipo, como se trata de nuestro certificado personal lo guardaremos en el almacén de usuario.





Indicamos la **ruta del certificado** que deseemos importar, este campo debería estar ya rellenado dado que hemos lanzado el asistente directamente desde el certificado.

×

←  Asistente para importar certificados

**Archivo para importar**  
Especifique el archivo que desea importar.

---


Nombre de archivo:

Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:

- Intercambio de información personal: PKCS #12 (.PFX,.P12)
- Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
- Almacén de certificados en serie de Microsoft (.SST)

Introducimos la **contraseña** de la clave privada del certificado y activamos la protección segura de la clave privada (primera casilla de selección) para que nos pida confirmación a la hora de utilizarlo.

×

←  Asistente para importar certificados

**Protección de clave privada**  
Para mantener la seguridad, la clave privada se protege con una contraseña.

---

Escriba la contraseña para la clave privada.

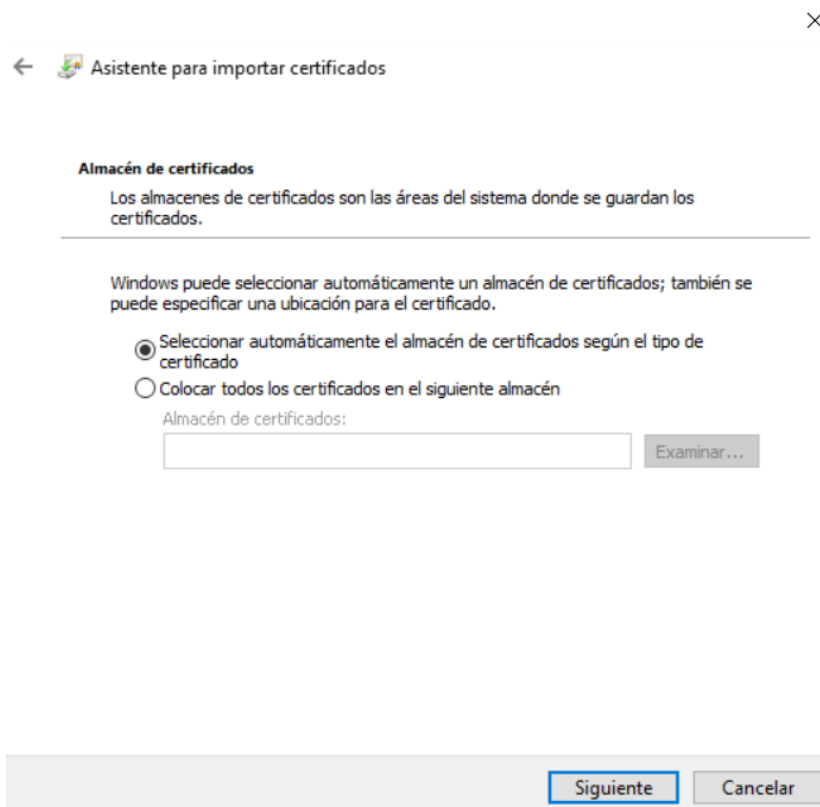
Contraseña:

☐ Mostrar contraseña

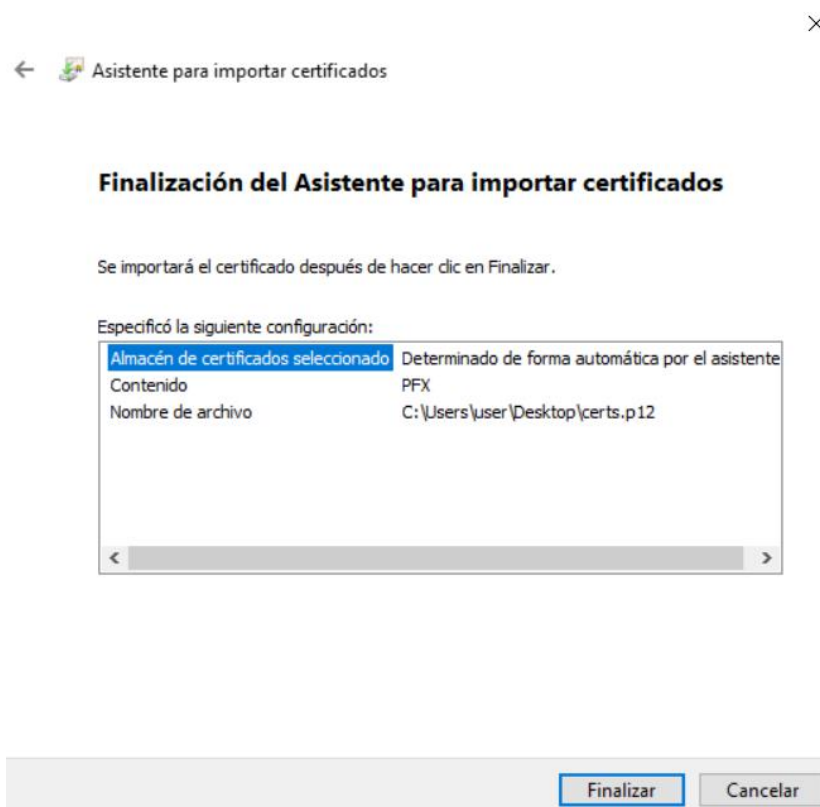
Opciones de importación:

- ☒ Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.
- ☐ Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.
- ☐ Proteger la clave privada mediante security(Non-exportable) basada en virtualizado
- ☒ Incluir todas las propiedades extendidas.

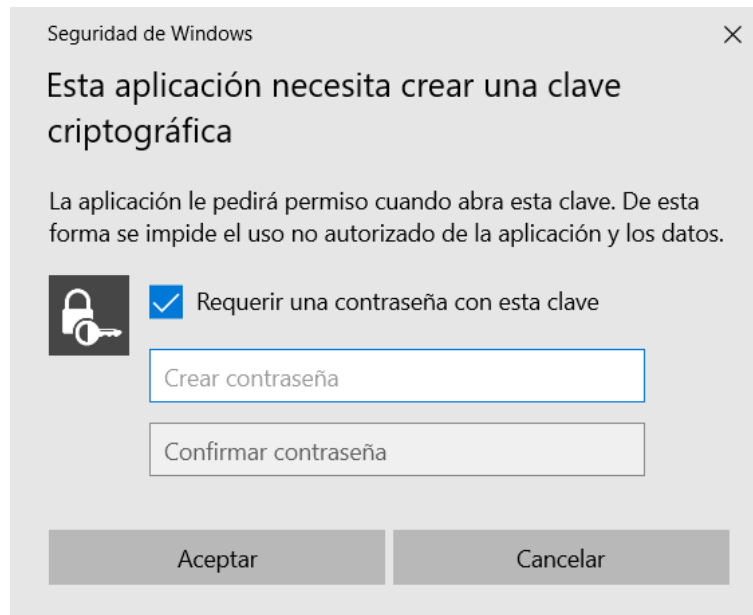
Seleccionamos el directorio del almacén de certificados donde deseemos almacenarlo, en el caso de que dejemos la opción por defecto, este se almacenara en el **almacén "Personal"**.



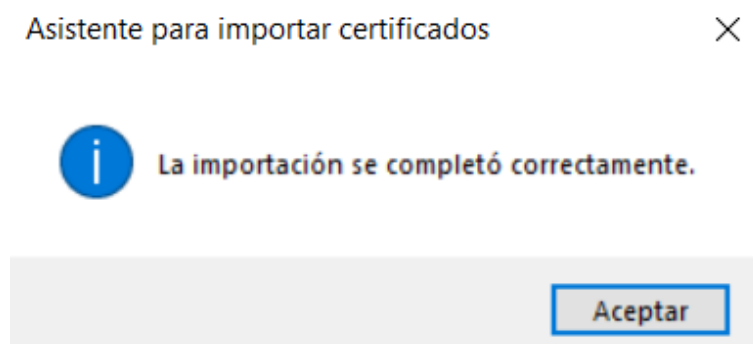
Por último, nos mostrara un resumen del proceso de importación de certificados, revisamos que todo este correctamente y finalizamos el asistente.



Al haber habilitado la protección segura de clave privada, deberemos establecer una contraseña mediante la cual podremos conceder el acceso por parte de las aplicaciones al certificado recientemente importado, esta nos la pedirá cada vez que vayamos a hacer uso del certificado.



Una vez hecho esto, habremos completado el proceso de importación del certificado.



## 4.4 Smartcard

**\*\*Por testear\*\***

## 4.5 Resolución de problemas

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

### 4.5.1 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 botón "Cancel".

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

## Proceso de firma de NexU

Cargando certificado

**¡Se ha producido un error!** The user has cancelled the operation.

## 5. Aplicación Independiente

Esta aplicación nos permitirá firmar documentos digitalmente de forma totalmente independiente a la aplicación web de firma, esta contiene todas las funcionalidades necesarias para el firmado de documentos, de la misma forma que nos lo permite la página de “**Firmar un documento**” de la aplicación web.

### 5.1 Obtención

Desde la página “**Aplicación independiente**” desde la aplicación web de firma digital podremos descargar las dos versiones disponibles de la aplicación de firma digital independiente:

- **ZIP mínimo:** Posee únicamente la aplicación y el lanzador, el siguiente software debe estar previamente instalado en el dispositivo: OpenJDK y JavaFX.
- **ZIP completo:** Incluye todo lo necesario dentro para el correcto funcionamiento de la aplicación.

Inicio > Aplicación independiente

Firmas

Firmar un documento

Firmar una función hash

Firmar un PDF

Firmar con JAdES

Firmar múltiples documentos

Contrafirmar una firma

Aplicación independiente

REST/SOAP APIs

Validación

Validar una firma

Validar un certificado

## Aplicación independiente

Descarga la aplicación independiente (Windows x64)

- ZIP mínimo (aplicación + lanzador (.bat) (dependencias necesarias))
- ZIP completo (aplicación + lanzador (.bat) + OpenJDK + JavaFX SDK)

Mas información...

Esto es una aplicación JavaFX independiente.

La aplicación se conecta directamente a la infraestructura de la CA (Autoridad Certificadora) para recuperar información como CRL, OCSP, certificados de AIA...

Todo las funciones están embebidas en la aplicación, haciendola totalmente independiente de esta aplicación web.

Existen dos versiones disponibles:

- ZIP mínimo: Posee únicamente la aplicación y el lanzador, el siguiente software debe estar previamente instalado en el dispositivo:
  - OpenJDK
  - JavaFX
- ZIP completo: Incluye todo lo necesario dentro para el correcto funcionamiento de la aplicación.

Para descargarla hacemos clic sobre uno de los hiperenlaces situados al inicio de la página, se nos descargará automáticamente la aplicación en formato **ZIP**, usamos un gestor de archivos comprimidos como por ejemplo 7z para descomprimirlo.

hoy (1)

dss-app-complete-windows-x64.zip 114.682 KB

Abrir

Abrir en ventana nueva

Compartir con Skype

Abrir con Code

Extraer todo...

7-Zip

Anclar a Inicio

Edit with Notepad++

Examinar con Microsoft Defender...

Compartir

Abrir con...

Abrir comprimido

Abrir comprimido






Extraer ficheros...

Extraer aquí

Extraer en "dss-app-complete-windows-x64\"

Comprobar archivo

Los ficheros resultantes de la extracción serán los siguientes en el caso del ZIP completo, para lanzar la aplicación usaremos el fichero **dss-run.bat** cuando lo estemos ejecutando desde Windows y **dss-run.sh** cuando lo estemos haciendo desde un sistema Linux.

Nombre	Tipo	Tamaño
▼ hoy (5)		
 dss-app.jar	Executable Jar File	34.967 KB
 dss-run.bat	Archivo por lotes de Windows	1 KB
 dss-run.sh	Shell Script	1 KB
 fx-sdk	Carpeta de archivos	
 java	Carpeta de archivos	


Tras ejecutar dicho fichero se nos abrirá la siguiente ventana, durante este proceso la aplicación establecerá comunicación con los servidores de la unión europea oficiales para la validación de certificados.

```

C:\Windows\system32\cmd.exe
[pool-2-thread-30] INFO eu.europa.esig.dss.validation.CommonCertificateVerifier - + New CommonCertificateVerifier created.
[pool-2-thread-5] INFO eu.europa.esig.dss.xades.validation.XAdESCertificateSource - +XAdESCertificateSource
[pool-2-thread-6] INFO eu.europa.esig.dss.validation.CommonCertificateVerifier - + New CommonCertificateVerifier created
[pool-2-thread-30] INFO eu.europa.esig.dss.xades.validation.XAdESCertificateSource - +XAdESCertificateSource
[pool-2-thread-6] INFO eu.europa.esig.dss.validation.SignedDocumentValidator - Document validation...
[pool-2-thread-14] INFO eu.europa.esig.dss.xades.validation.XAdESCertificateSource - +XAdESCertificateSource
[pool-2-thread-6] INFO eu.europa.esig.dss.validation.CommonCertificateVerifier - + New CommonCertificateVerifier created
[pool-2-thread-10] INFO eu.europa.esig.dss.xades.validation.XAdESCertificateSource - +XAdESCertificateSource
[pool-2-thread-17] INFO eu.europa.esig.dss.xades.validation.XAdESCertificateSource - +XAdESCertificateSource
[pool-2-thread-6] INFO eu.europa.esig.dss.xades.validation.XAdESCertificateSource - +XAdESCertificateSource
[JavaFX Application Thread] INFO eu.europa.esig.dss.tsl.job.TLValidationJob - Analysis is DONE for 31 TLSource(s)
[JavaFX Application Thread] WARN eu.europa.esig.dss.tsl.sync.TrustedListCertificateSourceSynchronizer - No Parsing result for TLInfo with url [https://ssi.gouv.fr/uploads/tl-fr.xml]
[JavaFX Application Thread] WARN eu.europa.esig.dss.tsl.sync.TrustedListCertificateSourceSynchronizer - No Parsing result for TLInfo with url [https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/publicaties/2018/januari/01/digitale-statuslijst-van-vertrouwensdiensten/current-tsl.xml]
[JavaFX Application Thread] INFO eu.europa.esig.dss.tsl.job.TLValidationJob - Running CacheCleaner
[JavaFX Application Thread] INFO eu.europa.esig.dss.tsl.job.TLValidationJob - CacheCleaner process is DONE
[JavaFX Application Thread] INFO eu.europa.esig.dss.tsl.job.TLValidationJob - Offline refresh is DONE.

```

Después de unos instantes se nos abrirá la ventana de la aplicación independiente, esta tiene el siguiente aspecto.

 Firma Digital Cartif

Archivo a firmar

Selecciona un fichero...

Tipo de contenedor

☐ Ninguno
☐ ASiC-S
☐ ASiC-E

Formato de firma

☐ CAdES
☐ PAdES
☐ XAdES
☐ JAdES

Embalaje

☐ Integrada
☐ Integrante
☐ Separada
☐ Internamente separada

Nivel

Algoritmo hash

☐ SHA1
☐ SHA224
☐ SHA256
☐ SHA384
☐ SHA512
☐ SHA3-224
☐ SHA3-256
☐ SHA3-384
☐ SHA3-512

Certificado para firma

☐ PKCS #11
☐ PKCS #12
☐ MS CAPI

Firmar

0%

Actualizar LOTL

Número de certificados fiables: 3261

## 5.2 Utilización

---

Los parámetros de firma son los mismos que en la aplicación web, empezamos seleccionando el fichero que deseamos firmar, indicamos el tipo de contenedor, la estructura de la firma, el empaquetado, el nivel, el algoritmo de la función hash y el tipo de certificado a usar, sin embargo, existen un par de diferencias:

- **Algoritmo hash:** En la aplicación independiente poseemos una mayor variedad de algoritmos a seleccionar, teniendo también como opción la familia SHA3, esta familia de algoritmos implementa mejoras de seguridad y rendimiento frente su familia predecesora SHA2, sin embargo, puede que determinados sitios no puedan interpretarlos, por lo que, en caso de dudar, se recomienda seleccionar el algoritmo SHA-256.
- **Certificado de firma:** Al tratarse de una aplicación independiente ejecutada directamente desde nuestro dispositivo no es necesario hacer uso de aplicaciones como NexU para hacer de intermediario, por lo que poseemos tres formas diferentes de seleccionar el certificado a usar para firmar el documento.
  - **PKCS #11:** Protocolo utilizado para acceder a dispositivos de cifrado de hardware, como tokens USB, tarjetas inteligentes o “Vaults” (como Azure Vault). Ficheros con extensión dll.
  - **PKCS #12:** Formato de archivo para almacenar certificados y claves privadas. Ficheros con extensión: p12, pfx.
  - **MS CAPI:** Interfaz de programación de aplicaciones criptográficas, es una interfaz de programación presente en el sistema operativo Microsoft Windows y permite utilizar las funciones de los sistemas criptográficos implementados en los Proveedores de Servicios Criptográficos, esto nos permite cifrar documentos usando certificados del almacén de certificados de Windows de la misma forma de la que lo hacíamos seleccionando la opción de “Windows keystore” usando NexU.