SSI

Práctica 4: Firma electrónica

Realizado por:

- Marcos RIvas Kyoguro (70962760D)
- Pablo Moreno Barrios (70908442V)

70962760D Firmado digitalmente por 70962760D Fecha: 2024.11.02 18:04:04 +01'00'

70908442V Firmado digitalmente por 70908442V Fecha: 2024.11.02 18:06:38 +01'00'

Objetivos

- Ser capaz de firmar documentos con validez legal
- Ser capaz de comprobar la firma de documentos

Entorno de realización

- XolidoSign
- Autofirma
- VALIDe
- Adobe Acrobat

MARCOS| RIVAS| KYOGURO Firmado digitalmente por MARCOS|RIVAS| KYOGURO Fecha: 2024.11.02 18:10:47 +01'00'

1. Introducción y marco legal de la firma electrónica en España:

La firma electrónica en España está regulada por varias leyes, las más destacadas son:

- **Ley 59/2003**, de 19 de diciembre: Regula la firma electrónica y define su marco legal, aunque ha sido derogada por la Ley 6/2020.
- **Ley 6/2020**, de 11 de noviembre: Regula ciertos aspectos de los servicios electrónicos de confianza.
- **Ley 11/2007**, de 22 de junio: Reconoce el derecho de los ciudadanos a interactuar con la Administración Pública a través de medios electrónicos.

El Portal de la Administración Electrónica proporciona recursos y normativa para que los ciudadanos y las empresas puedan interactuar de forma segura y efectiva con las entidades públicas mediante herramientas de firma electrónica.

2. Tipos Principales de Firma Electrónica

La **firma electrónica simple** representa la forma más básica de firma electrónica. No garantiza la identificación del firmante ni la integridad del documento. Suele consistir en un conjunto de datos electrónicos, como una imagen de la firma. Debido a su naturaleza básica, las firmas simples son más vulnerables a fraudes y manipulaciones.

La **firma electrónica avanzada**, conocida como AdES (Advanced Electronic Signature), ofrece un nivel de seguridad superior en comparación al anterior. Este tipo de firma garantiza la identidad del firmante y la integridad del documento firmado. Para cumplir con los requisitos legales y de seguridad, la firma electrónica avanzada debe cumplir los siguientes requisitos:

- Ser exclusiva del firmante.
- Permitir la identificación del firmante de manera clara y verificable.
- Asociarse con los datos firmados de tal manera que cualquier modificación al documento sea fácilmente detectable.
- Utilizar medios que el firmante puede controlar, como certificados digitales y claves criptográficas.

Gracias a estas características, las firmas electrónicas avanzadas son ampliamente aceptadas en procesos legales y administrativos.

La **firma electrónica cualificada** representa el nivel más alto de seguridad en el ámbito de las firmas electrónicas. Este tipo de firma debe ser emitida por una entidad certificadora reconocida y acreditada.

La firma cualificada es equivalente a una firma manuscrita. Esto significa que los documentos firmados con este tipo de firma cuentan con la misma validez jurídica que aquellos firmados de forma tradicional, lo que la convierte en una herramienta esencial para trámites legales, contratos y documentos oficiales.

3. Tipos de firma electrónica avanzada (AdES)

La firma electrónica avanzada (AdES), como ya vimos antes, es un tipo de firma que cumple con ciertos requisitos para garantizar la integridad y autenticidad del documento firmado.

Entre los formatos más utilizados se encuentran:

- **AdES-BES (Basic Electronic Signature)**: Es la versión básica de la firma electrónica avanzada. Ésta, garantiza que el documento no se ha modificado desde que fue firmado.

- **AdES-T (Timestamped Signature)**: Añade una marca de tiempo a la firma, lo que garantiza que el documento existía y fue firmado en un momento específico. La marca de tiempo ayuda a verificar la validez de la firma, incluso después de la caducidad del certificado del firmante.

- **AdES-C (Complete Signature)**: Incluye certificados y otra información adicional necesaria para verificar la firma a largo plazo. Este tipo de firma permite una validación completa, incluso si los certificados ya han caducado o no están disponibles.

- **AdES-X (Extended Signature)**: Es una extensión de AdES-C que añade múltiples marcas de tiempo. Además de la marca de tiempo inicial, incluye marcas de tiempo adicionales para fortalecer la validez de la firma a lo largo del tiempo. Esto asegura que, aunque se produzcan cambios en la infraestructura de certificación, la firma mantenga su validez.

A continuación, se presenta una tabla comparativa que detalla los tipos de firma electrónica, sus características, y sus casos de uso.

Tipo de Firma	Características	Caso de uso
Firma simple	Básica, sin verificación de identidad ni integridad	Correo electrónico con nombre del remitente
Firma Avanzada (AdES)	Identificación del firmante y detección de cambios en el documento.	Firma de contratos y documentos oficiales.
Firma Cualificada	Uso de certificado cualificado, equivalente a la firma manuscrita.	Contratos legales, trámites administrativos.
AdES-BES	Firma avanzada básica, sin marca de tiempo ni certificados adicionales.	Documentos oficiales de corta duración.
AdES-T	Incluye marca de tiempo que registra el momento de la firma.	Facturas electrónicas, contratos con vencimiento.
AdES-C	Incluye certificados y cadena de validación para verificación a largo plazo.	Contratos y documentos con validez indefinida.
AdES-X	Variante extendida con múltiples marcas de tiempo para verificación robusta a largo plazo.	Documentos de gran importancia legal y duradera.

3. Registro de marcas de tiempo

Las marcas de tiempo son un elemento clave en la validación de firmas electrónicas a largo plazo, ya que permiten certificar que un documento existía en un momento específico.

Estos registros de tiempo son emitidos por Autoridades de Sellado de Tiempo, que aseguran la integridad temporal del documento.

Cumplen funciones clave como:

1. **Autenticidad Temporal**: Proporcionan prueba de cuándo se creó o firmó un documento.
2. **Validación de la Firma Electrónica**: Aseguran que una firma fue realizada mientras el certificado del firmante era válido.
3. **Prevención de Fraudes**: Detectan cualquier modificación posterior a la firma.

Las marcas de tiempo son vitales para la validación a largo plazo de documentos firmados electrónicamente, garantizando que sigan siendo válidos incluso después de la caducidad del certificado. Éstos, se aplican en contratos electrónicos, facturación, y registros de auditoría, asegurando que las acciones se registraron en un momento determinado.

4. Herramientas para la generación y verificación de firmas electrónicas

El enunciado propone un estudio comparativo de dos herramientas para la firma electrónica; **Xolido** y **Autofirma.:**

4.1 Xolido

Aplicación que permite realizar acciones como: la firma, validación y verificación de documentos electrónicos y correos. Soporta múltiples formatos de firma y opciones de marcado de tiempo.

Posee una interfaz intuitiva y soporte para firmas XAdES, CAdES y PAdES. Tiene un enfoque en la usabilidad para usuarios individuales y corporativos.

4.2 Autofirma

Aplicación desarrollada por el Gobierno de España para su uso en la Administración Pública. Al igual que Xolido, facilita la firma electrónica de documentos para procesos administrativos.

Es compatible con los estándares de firma electrónica AdES y sus subtipos. Además, posee una integración con certificados de entidades públicas reconocidas y autoridades de certificación.

XolidoSign

XolidoSign es una aplicación de escritorio que permite a los usuarios verificar y firmar documentos electrónicamente. Sus funcionalidades principales son:

- Verificación de firmas electrónicas sin importar el certificado usado.
- Compatibilidad con múltiples formatos de firma, permitiendo la interoperabilidad entre certificados de diferentes entidades.
- Firma electrónica y sellado de tiempo para autenticar documentos y asegurarse de su integridad a lo largo del tiempo.

XolidoSign destaca por ser una herramienta de escritorio intuitiva, diseñada tanto para usuarios particulares como para empresas, permitiendo gestionar grandes volúmenes de documentos y contratos.

VALIDe

Por otro lado, VALIDe es un servicio en línea proporcionado por el Gobierno de España. Esta herramienta facilita la validación de:

- Certificados electrónicos: confirma la validez de los certificados empleados.
- Sedes electrónicas: asegura la autenticidad de los sitios web de entidades gubernamentales.
- Firmas electrónicas: valida la autenticidad y la integridad de los documentos firmados.

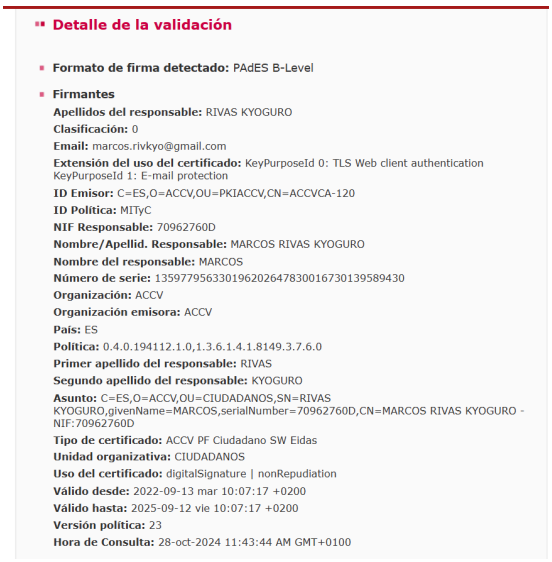
Está enfocado en asegurar que los documentos digitales cumplan con la normativa española y europea sobre firma electrónica. No solo permite la validación de certificados, sino que también incluye un validador de documentos firmados, incrementando la confianza en la autenticidad de los documentos.

Vamos a utilizar una de sus funcionalidades (**Validación de Firma Electrónica en PDF**)

A continuación, vamos a verificar la validez de la firma electrónica en un documento PDF, asegurando que cumple con los requisitos de autenticidad e integridad establecidos en la normativa europea eIDAS.

Para ello ingresamos al portal web de VALIDe y seleccionamos la opción “Validación de Firma”. Hecho esto, cargamos el PDF Firmado.

VALIDe analiza el documento, detectando cualquier firma electrónica y los certificados aplicados. Verifica si el documento ha mantenido su integridad desde que fue firmado. Comprueba la validez y cualificación del certificado de la firma. Revisa la fecha y hora de la firma y, si aplica, la presencia de un sello de tiempo.



El documento PDF firmado por nosotros, **Marcos Rivas Kyoguro**, ha sido validado correctamente y presenta un certificado que cumple con los estándares europeos de autenticidad. La firma es válida, y el certificado emitido por **ACCV** sigue vigente hasta la fecha de caducidad especificada, **12 de septiembre de 2025**.

Este documento, utiliza una firma electrónica de tipo PAdES B-Level, es decir, posee validez legal y puede ser utilizado en procedimientos administrativos y legales en la Unión Europea.

Acrobat de Adobe Systems

Algunas aplicaciones permiten generar documentos firmados electrónicamente y verificar dichas firmas, asegurando la integridad y autenticidad del contenido. Entre estas aplicaciones se encuentra Adobe Acrobat.

A continuación, se detallan las funciones de Acrobat en relación con la generación y verificación de firmas electrónicas, así como la metodología para determinar y comentar la validez de un documento PDF firmado.

1. Funciones de Firma Electrónica en Adobe Acrobat

Adobe Acrobat permite añadir firmas digitales de diferentes tipos en documentos PDF. Estas firmas pueden ser visibles o invisibles y están respaldadas por un certificado digital que permite autenticar al firmante y garantizar la integridad del documento.

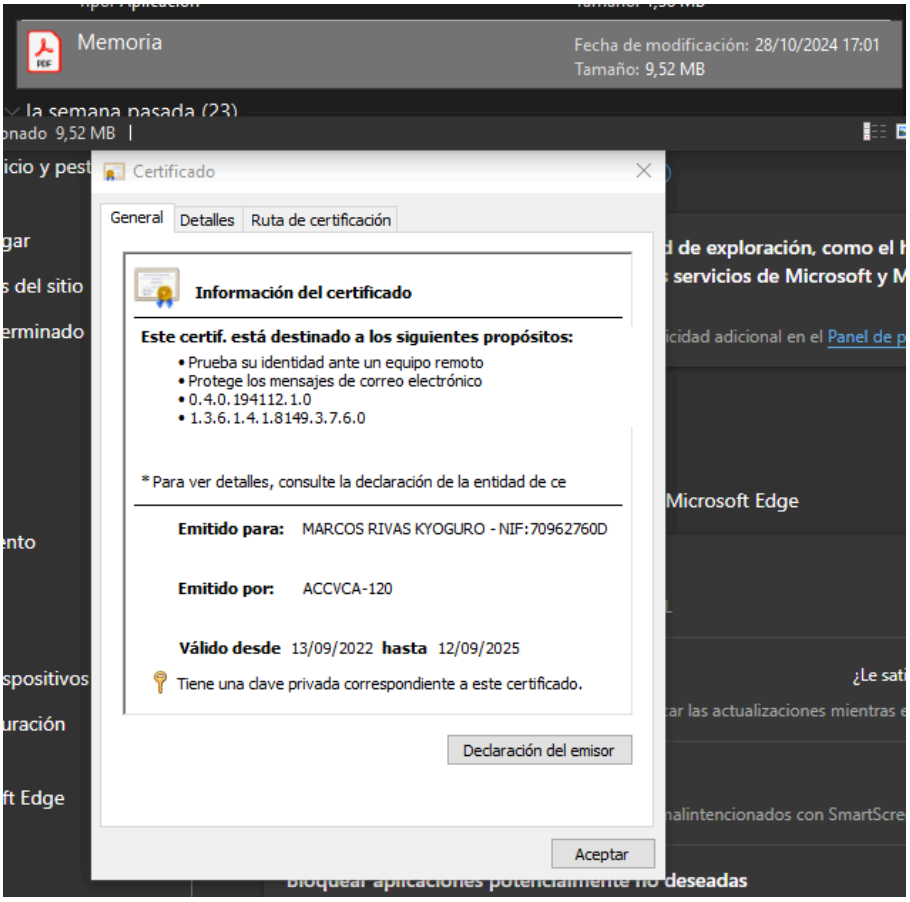
Acrobat permite utilizar un certificado digital emitido por una autoridad de certificación para firmar el documento, cumpliendo así con estándares avanzados de firma como AdES. Esto asegura que la firma tiene validez jurídica y proporciona evidencia en caso de que sea necesario verificarla a largo plazo.

2. Verificación de Firmas en Documentos PDF

Al abrir un documento PDF firmado, Adobe Acrobat ofrece herramientas para verificar la autenticidad de la firma y la integridad del documento, lo que asegura que el archivo no ha sido alterado desde la firma.

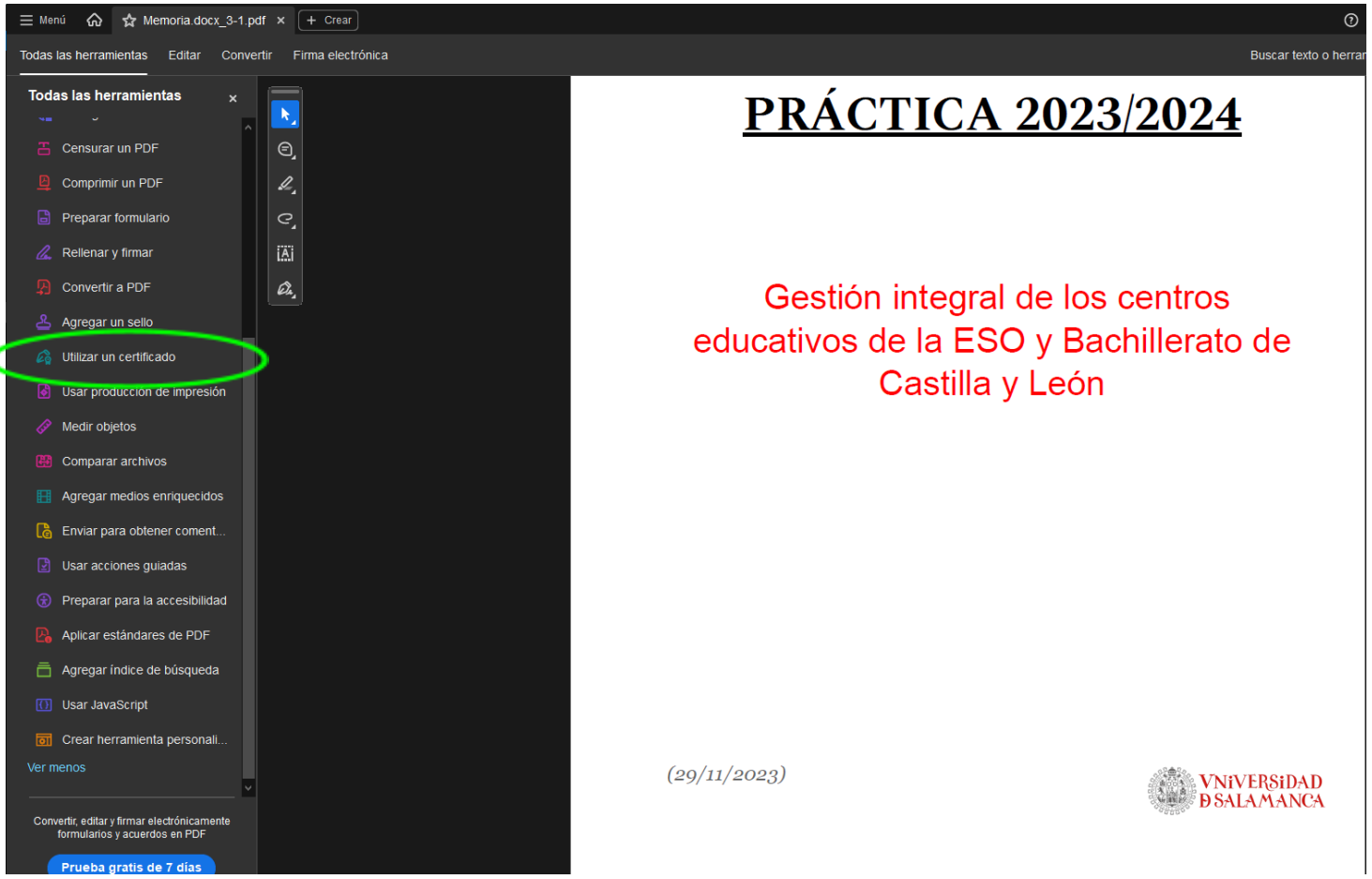
A continuación se presenta cómo firmar un documento PDF utilizando un certificado digital y cómo verificar la validez de la firma con Adobe Acrobat Reader.

Para este estudio, firmaremos el documento "Memoria.pdf" con mi certificado digital, emitido por la ACCV.

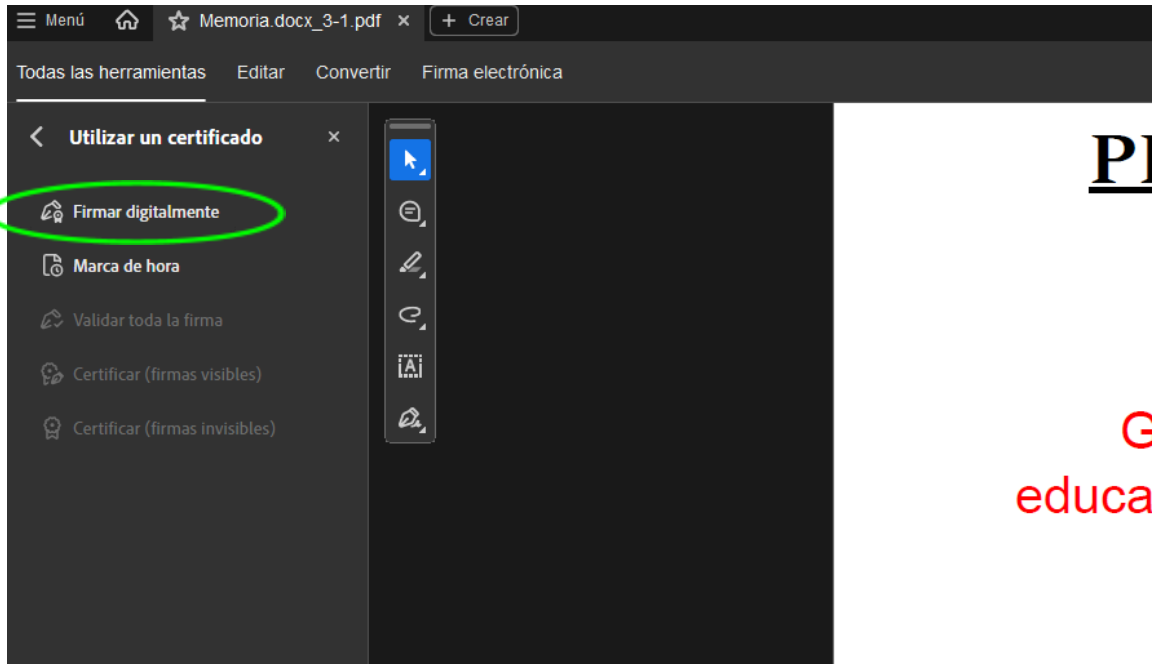


FIRMAR DOCUMENTO PDF

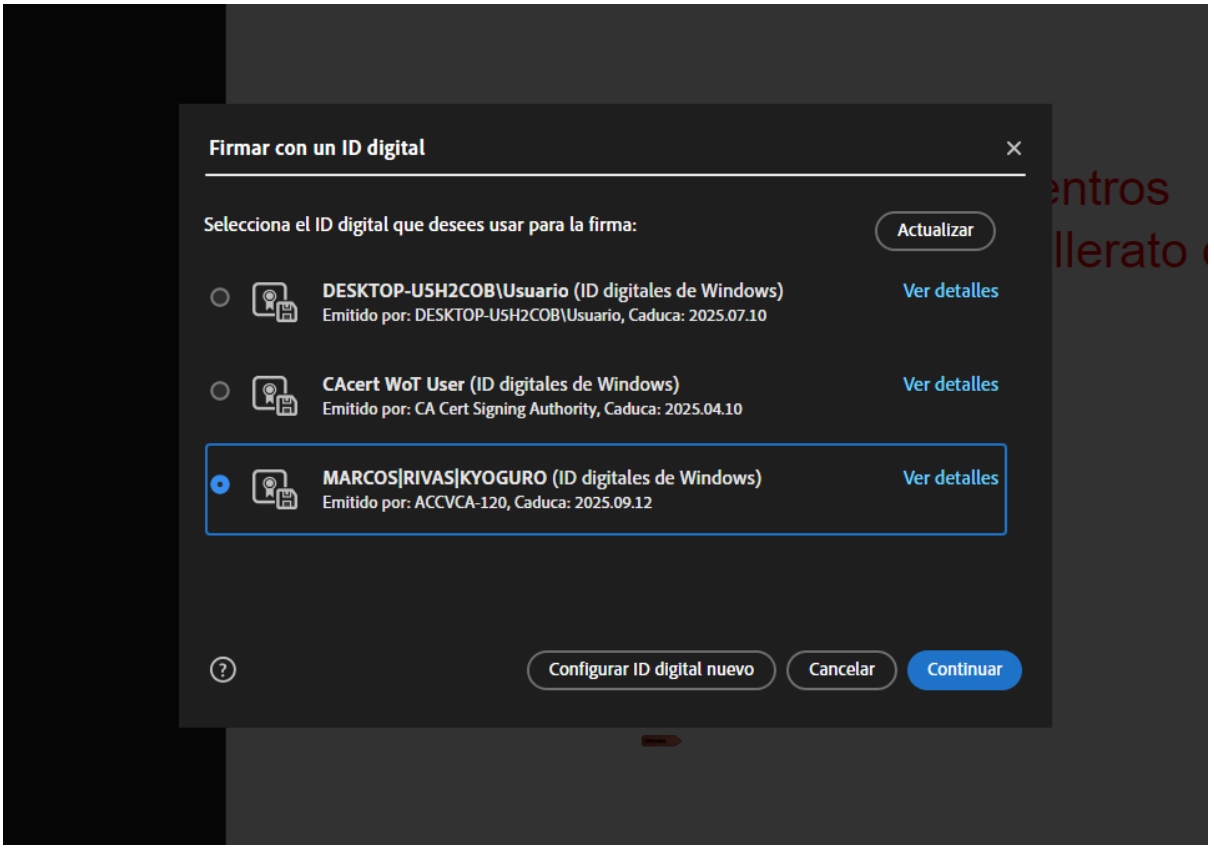
Abrimos el documento que vamos a firmar con Adobe Acrobat Reader, “Memoria.pdf”. Y pulsamos: Herramientas – Utilizar un Certificado.



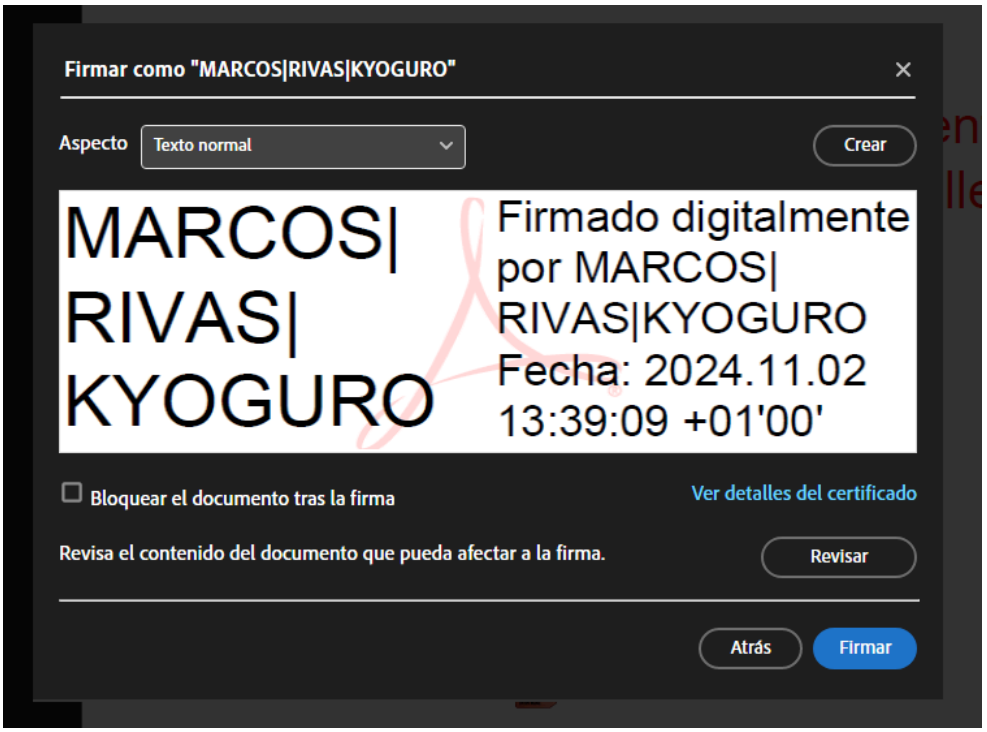
A continuación, pulsamos en “Firmar digitalmente”.



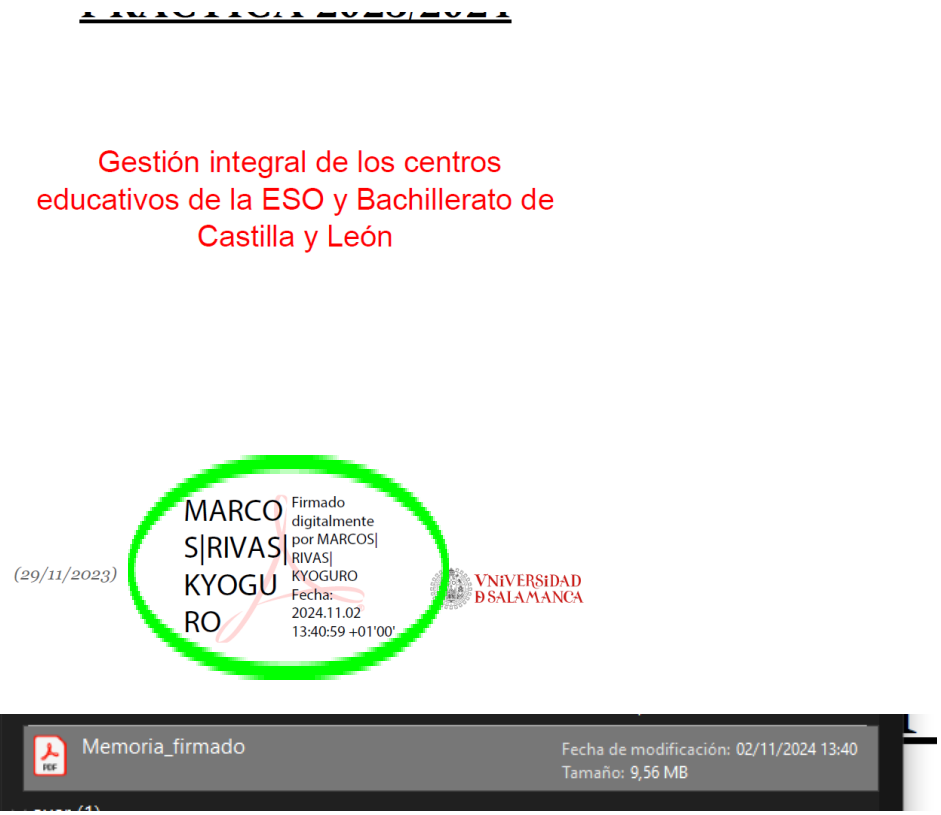
Con el puntero del ratón seleccionamos el área del documento donde queremos insertar la firma. Al soltar el botón del ratón nos aparece la ventana con el listado de certificados digitales disponibles para seleccionar. Elegimos el certificado deseado y pulsamos continuar.



En la siguiente ventana pulsamos el botón “Firmar”.

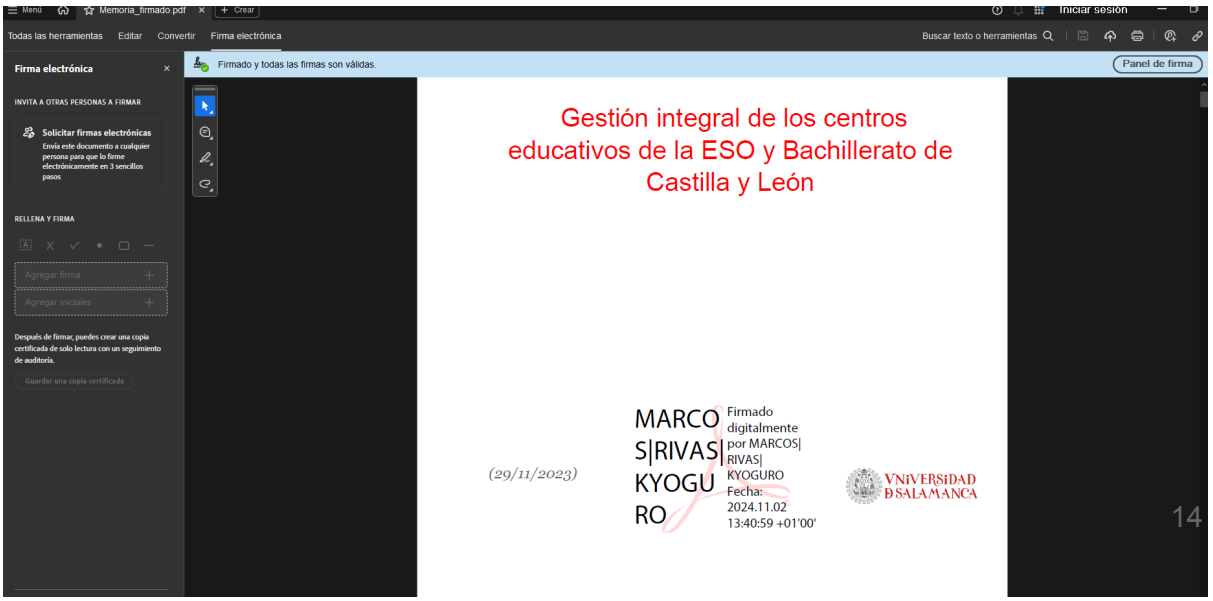


A continuación, nos pedirá la contraseña del certificado, para establecer la firma al documento. La introducimos, y si todo es correcto el documento mostrará la firma digital insertada:

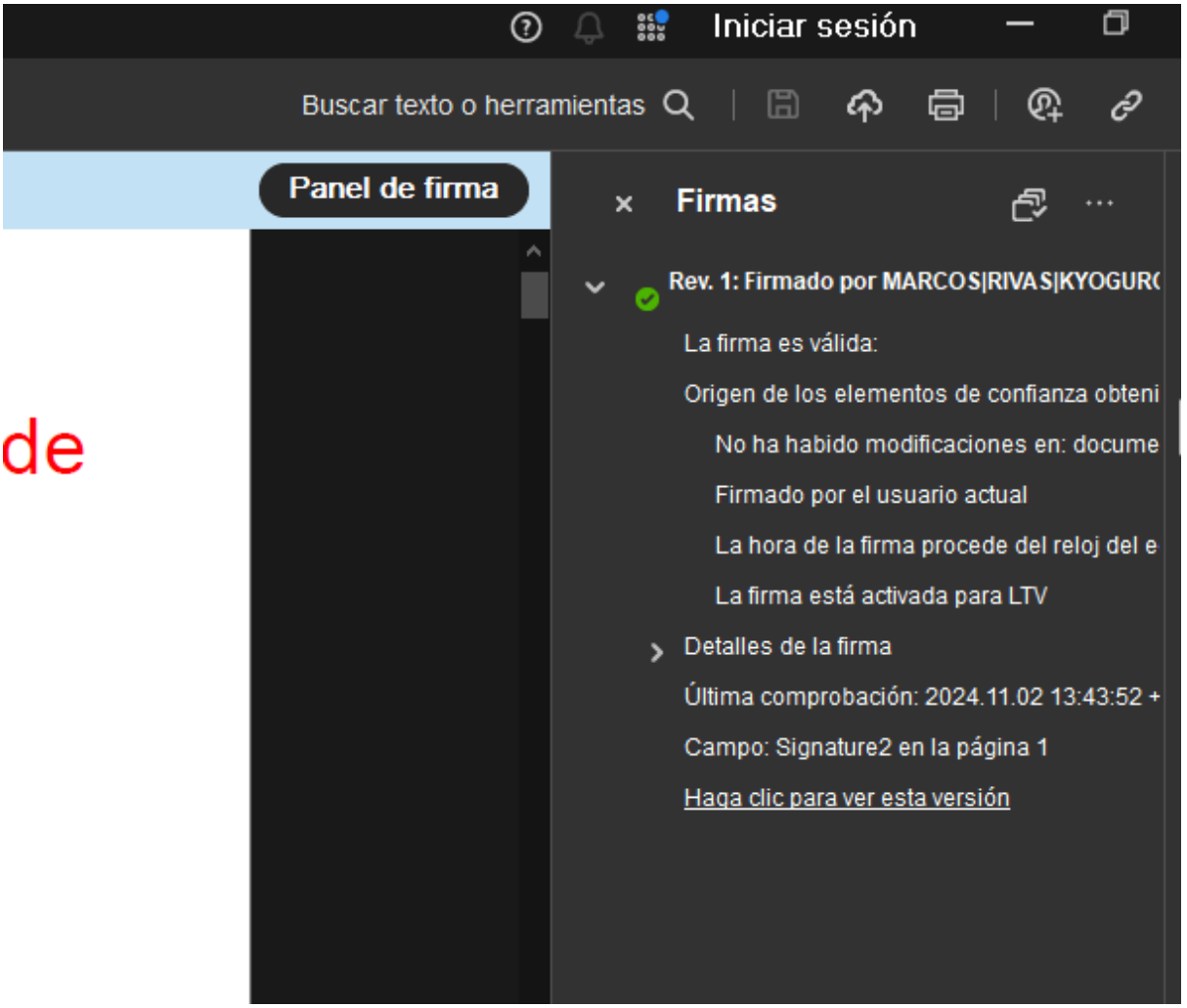


VALIDAR LA FIRMA DE UN DOCUMENTO FIRMADO DIGITALMENTE CON ADOBE ACROBAT READER DC

Abrimos el documento firmado.



Pulsamos sobre el texto con la firma o sobre el botón “Panel de firma”.



Ahí encontramos campos clave como:

- **Rev. 1: Firmado por MARCOS|RIVA|KYOGURO <marcos.rivkyo@gmail.com>:** Es el nombre y correo electrónico del firmante del documento.

- **La firma es válida**: Indica que la firma digital es válida, es decir, cumple con los requisitos de autenticidad y seguridad.

- **No ha habido modificaciones en documento desde que se firmó**: Confirma que el documento no ha sido alterado desde que fue firmado. Esto asegura que el contenido del documento se mantiene íntegro y sin cambios desde su firma.

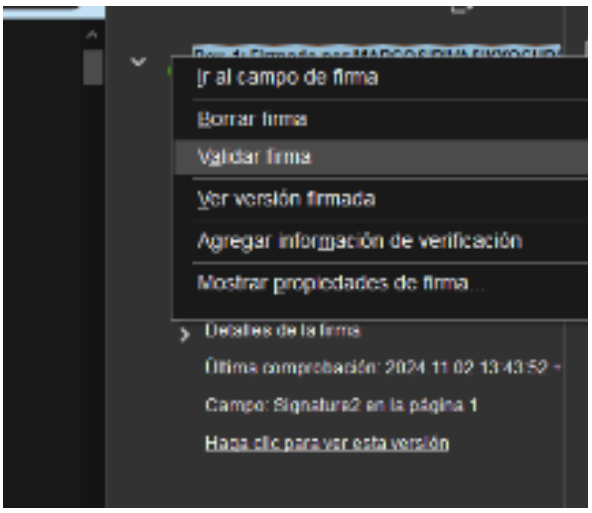
- **La hora de la firma procede del reloj del equipo del firmante**: La hora registrada en la firma proviene del reloj del equipo en el que se hizo la firma, en lugar de un servidor de tiempo externo.

- **La firma está activada para LTV (Long-Term Validation)**: LTV, o Validación a Largo Plazo, significa que la firma ha sido configurada para que pueda ser verificada en el futuro, incluso si el certificado original ya no está disponible o expira.

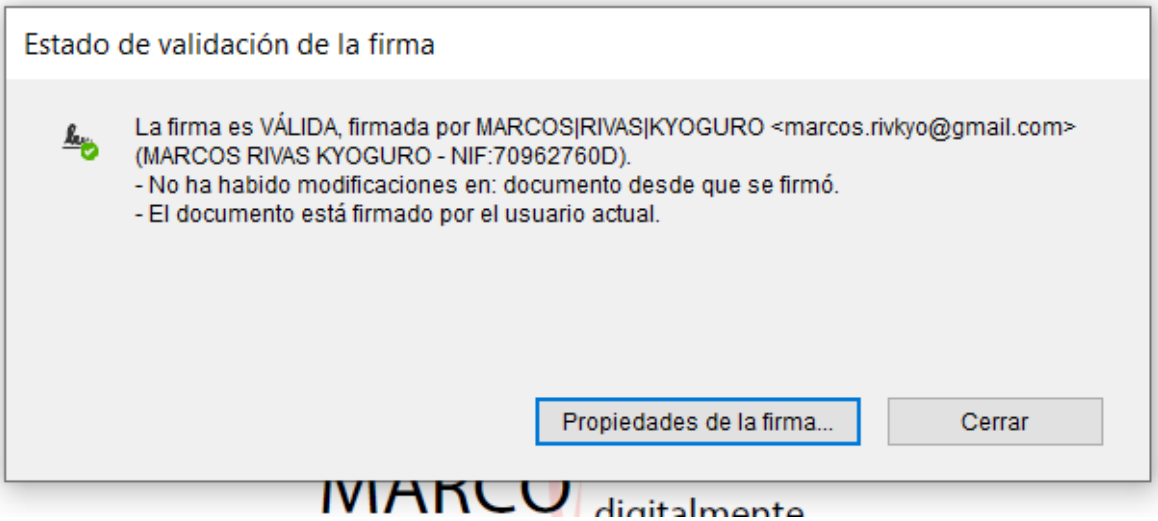
- **Última comprobación: 2024.11.02 13:52:53 +01:00**: Fecha y hora de la última verificación de la firma. Esto muestra cuándo fue verificada por última vez, en este caso, el 2 de noviembre de 2024, a las 13:52:53 (zona horaria GMT+1).

Estos detalles permiten verificar tanto la autenticidad de la firma como la integridad del documento.

Finalmente, pulsamos con el botón derecho del ratón sobre “Rev. 1: Firmado por …” y seleccionamos “Validar firma”.

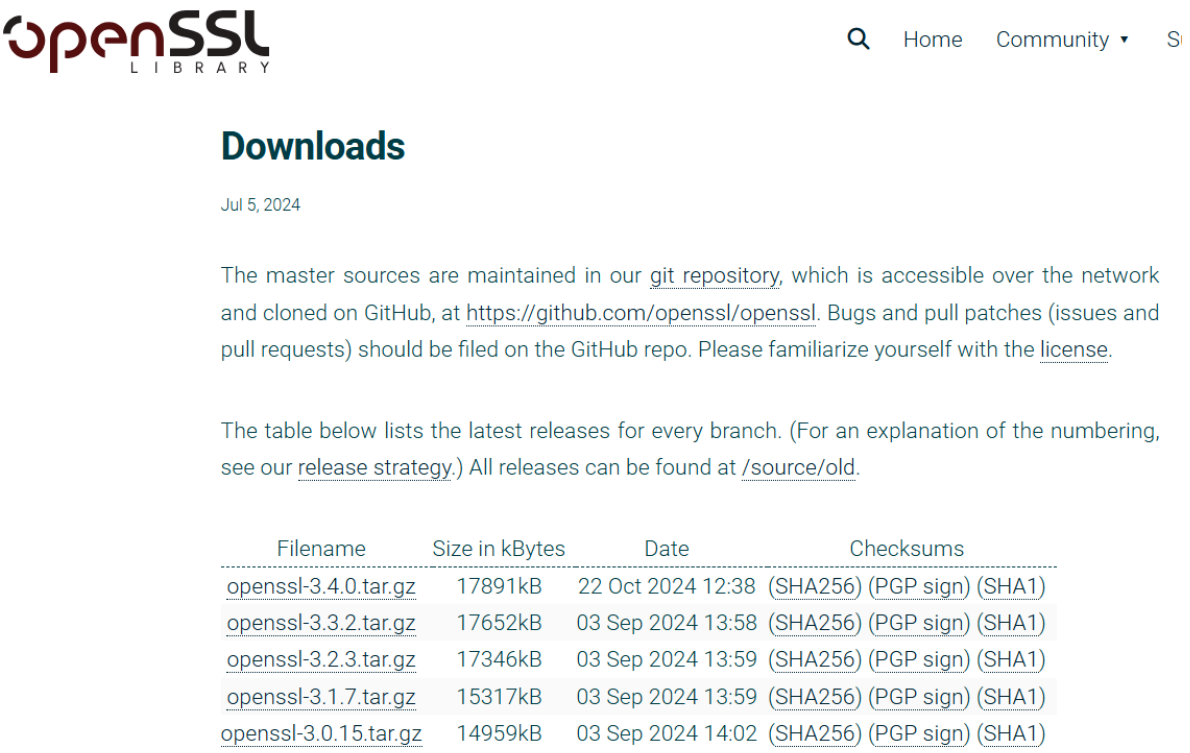


Si la firma se ha validado correctamente aparecerá con una v verde o similar.



Generar y comprobar una firma PGP

También podemos generar y validar firmas digitales con aplicaciones netamente criptográficas como GnuPG. Se trata de verificar la firma del paquete "openssl-3.3.2.tar.gz" que contiene el código fuente y se encuentra en https://www.openssl.org/source/.



OpenSSL LIBRARY

Home Community

Downloads

Jul 5, 2024

The master sources are maintained in our git repository, which is accessible over the network and cloned on GitHub, at https://github.com/openssl/openssl. Bugs and pull patches (issues and pull requests) should be filed on the GitHub repo. Please familiarize yourself with the license.

The table below lists the latest releases for every branch. (For an explanation of the numbering, see our release strategy.) All releases can be found at /source/old.

Filename	Size in kBytes	Date	Checksums
openssl-3.4.0.tar.gz	17891kB	22 Oct 2024 12:38	(SHA256) (PGP sign) (SHA1)
openssl-3.3.2.tar.gz	17652kB	03 Sep 2024 13:58	(SHA256) (PGP sign) (SHA1)
openssl-3.2.3.tar.gz	17346kB	03 Sep 2024 13:59	(SHA256) (PGP sign) (SHA1)
openssl-3.1.7.tar.gz	15317kB	03 Sep 2024 13:59	(SHA256) (PGP sign) (SHA1)
openssl-3.0.15.tar.gz	14959kB	03 Sep 2024 14:02	(SHA256) (PGP sign) (SHA1)

Para garantizar la autenticidad e integridad del código fuente del paquete openssl-3.3.2.tar.gz, se lleva a cabo un proceso de verificación de su firma digital utilizando GnuPG. A continuación, se detallan los pasos realizados:

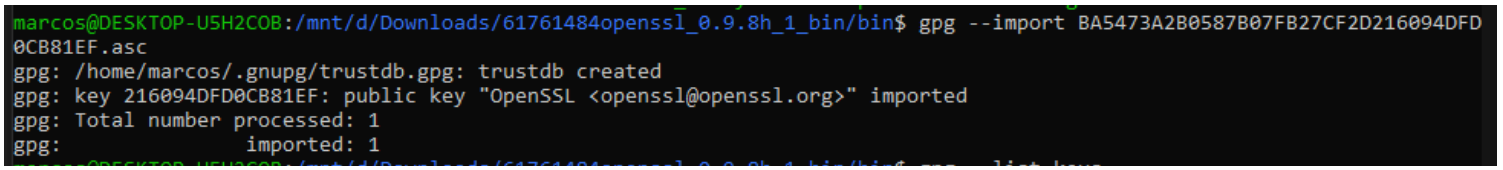
1. **Descarga de Archivos**: Primero, descargamos los siguientes archivos desde el sitio oficial de OpenSSL:
    - openssl-3.3.2.tar.gz: Este archivo contiene el código fuente de OpenSSL.
    - openssl-3.3.2.tar.gz.sig: Este archivo es la firma correspondiente al paquete de código fuente.

Las descargas se realizaron desde el enlace oficial: https://www.openssl.org/source/.

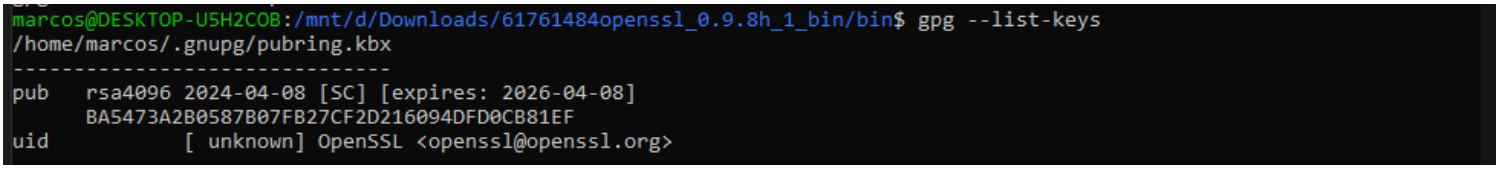
También obtenemos el archivo que contiene la clave pública de OpenSSL, en el siguiente enace: https://keys.openpgp.org/search?q=openssl%40openssl.org

2. **Importación de la Clave Pública**: Se importó la clave pública del proyecto OpenSSL:

```
Unset
gpg --import BA5473A2B0587B07FB27CF2D216094DFD0CB81EF.asc
```

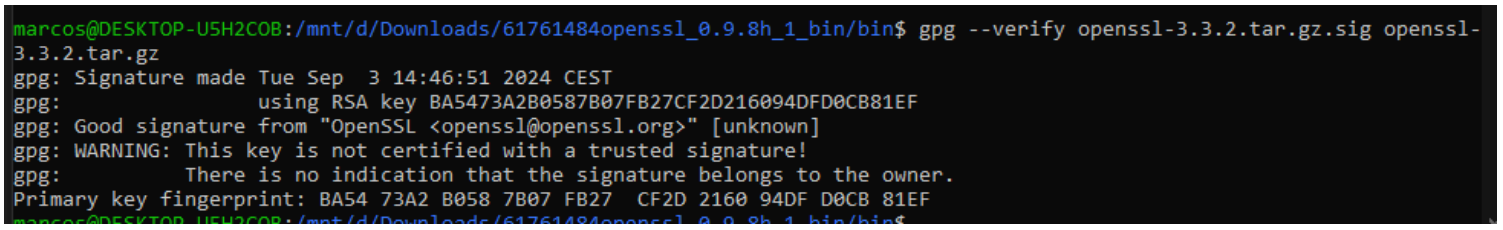


La salida confirma que se creó una base de datos de confianza y se importó correctamente la clave pública asociada a OpenSSL:



3. **Verificación de la Firma**: Finalmente, se procedió a verificar la firma del archivo openssl-3.3.2.tar.gz:

```
Unset
gpg --verify openssl-3.3.2.tar.gz.sig openssl-3.3.2.tar.gz
```



La firma fue validada como "buena", lo que indica que el archivo no ha sido alterado desde que fue firmado por OpenSSL. Sin embargo, se observó una advertencia indicando que la clave no está certificada con una firma de confianza.