

PAI-2 DIGISalud: DIGITALIZACIÓN DE LA AUTENTICACIÓN Y EL CONTROL DE ACCESO PARA SERVICIO DE SALUD DE COMUNIDAD AUTÓNOMA



Araceli María Benítez Díaz

Paula Poley Ceballos

SCG, 3º ISA 2022

Índice

Resumen ejecutivo.....	3
Workpackage 1. Certificados Digitales en Clientes/Servidores para la transmisión segura a través de la Web en el Servicio de Salud	4
1. Realizar la solicitud a las Autoridades de Certificación cualificadas de los certificados digitales para las partes interesadas del Servicio de Salud.....	4
2. Realizar la instalación/desinstalación de los certificados digitales en los browser de las partes interesadas tanto en un dispositivo de escritorio como en un dispositivo móvil.....	9
3. Verificar los certificados digitales de los servidores Web de un Servicio de Salud.....	19
4. Revocación los certificados digitales personales de las partes interesadas	22
Workpackage 2. Verificación Automática de la Política de Control de Acceso teniendo en cuenta conflictos de intereses, separación/segregación de deberes dinámica y binding de deberes.....	23
Workpackage 3 Firmado digital y verificación de firmas en documentos del Servicio de Salud	25
□ Verificación de certificados.....	25
a) Realizar firma.....	26
b) Visualizar firma	35
c) Validar Certificado.....	36
d) Validar firma.....	37
e) Validar Sede Electrónica.....	38
□ Verificación de documentos con CSV.....	39
□ Verificación de documentos firmados digitalmente	41



Resumen ejecutivo

En primer lugar hoy en día los certificados digitales son muy útiles ya que nos permiten identificarnos en distintas páginas web ahorrándonos tiempo y dinero al poder hacer trámites administrativos a la hora que sea y en el sitio que sea a través de Internet. Para ello debemos saber como solicitarlo además de instalarlo en nuestros dispositivos. A continuación se encuentra un pequeño tutorial paso a paso para realizar este proceso.

Es importante saber buscar las propiedades de los certificados y cómo administrar los certificados de otras entidades permitiéndonos confiar o no en distintas páginas web.

En segundo lugar con la herramienta CSP Applet Version 4.6.1 podemos encontrar las distintas soluciones para la gestión de tareas y restricción de usuario de manera más sencilla y rápida.

Por último, es importante conocer la posibilidad de firmar documentos con nuestro certificado ya que nos permite corroborar que somos nosotros y verificar la firma con los datos de esta en un documento.



Workpackage 1. Certificados Digitales en Clientes/Servidores para la transmisión segura a través de la Web en el Servicio de Salud

1. Realizar la solicitud a las Autoridades de Certificación cualificadas de los certificados digitales para las partes interesadas del Servicio de Salud.

Modelo de proceso

Para realizar la solicitud para el Certificado de persona física tenemos que introducir la siguiente ruta: <https://www.sede.fnmt.gob.es/certificados/persona-fisica>

1. En primer lugar, es necesaria la instalación de dos softwares:
 1. **CONFIGURADOR FNMT-RCM:** esta aplicación permite solicitar las claves necesarias en la obtención de un certificado digital.
 2. **AutoFirma:** Aplicación de firma electrónica.
2. A continuación, es necesario introducir los siguientes datos y aceptar las condiciones de expedición.

Nº DEL DOCUMENTO DE IDENTIFICACIÓN	<input type="text"/>
PRIMER APELLIDO(tal y como aparece en su documento de identificación)	<input type="text"/>
CORREO ELECTRÓNICO	<input type="text"/>
Confirme aquí su CORREO ELECTRÓNICO	<input type="text"/>

3. Al enviar los datos en la solicitud anterior, es necesario acreditar los datos en una oficina de acreditación. Para ello, se puede pedir cita previa en nuestra oficina más cercana.

Por favor verifique que los datos que introdujo en la fase de solicitud:

1. Nº de NIF/NIE.
2. Primer apellido.

se corresponden exactamente con los que figuran en el documento que necesita presentar para identificarse en una de nuestras Oficinas de Acreditación. Si detecta cualquier error en los mismos, deberá generar una nueva solicitud.

Con este código de solicitud y la documentación requerida de su identidad, el solicitante y futuro titular del certificado deberá acudir personalmente a una Oficina de Acreditación de Identidad para acreditar sus datos con el **documento de identidad válido, vigente** y en formato **original** o en su defecto, una **fotocopia compulsada** oficialmente. Si por cualquier circunstancia no pudiera hacerlo personalmente, podrá ir una tercera persona en su nombre, pero se le exigirá la previa legitimación de su firma del contrato de la FNMT-RCM ante notario.

- Ciudadano de nacionalidad española: Documento Nacional de Identidad (DNI), pasaporte o carné de conducir.
- Ciudadano de la Unión Europea: Documento oficial donde conste el NIE junto con Pasaporte o documento de identidad de país de origen.
- Ciudadano extranjero: Documento oficial de concesión del NIF/NIE junto con el pasaporte.

Para su comodidad, puede usted hacer uso de nuestro servicio de localización de las Oficinas más cercanas, que encontrará en nuestra Sede Electrónica en [ACREDITAR SU IDENTIDAD](#). (NOTA: En las oficinas de la AEAT y algunas oficinas de la Seguridad Social se requiere de cita previa.)

Allí, será necesario dar el DNI y el código de solicitud. A continuación, la fábrica nacional de moneda y timbre le enviará un correo electrónico con el certificado.

4. Por último, al descargar el certificado, solo hará falta introducir la contraseña que hizo falta poner cuando se realizó la solicitud, y ya estará instalado.
- 5.

**Notificaciones FNMT AC usuarios <ac.usuarios@fnmt.es>**

para mí ▾

Estimado/a Sr/a

En relación al Certificado FNMT de Persona Física que ha solicitado, le informamos que ya puede proceder a descargarlo e instalarlo.

Para ello deberá introducir su Código de Solicitud

, primer apellido y nº de DNI - NIF

- NIE en el siguiente enlace:

[Descarga de su certificado de Persona Física](#)

Recuerde que:

- La descarga e instalación de su certificado deberá llevarla a cabo en el mismo equipo en el que realizó la solicitud.
- Si usted realizó la solicitud del certificado haciendo uso de su aplicación móvil, la descarga deberá realizarla desde el apartado "Solicitudes pendientes" de dicha app.
- Si generó su petición en tarjeta criptográfica, antes de realizar la descarga, confirme que dicha tarjeta está lista para ser usada.

Así mismo le recordamos que con la emisión de su nuevo certificado FNMT de Persona Física, el solicitante autoriza a la FNMT-RCM a revocar y dejar sin efecto cualquier certificado de este mismo tipo que la FNMT-RCM le haya emitido con carácter previo e idénticos nombre, apellidos y NIF/NIE.

Agradecemos sinceramente su interés por nuestros certificados.

Autenticación en Blackboard con el certificado de persona física. Entramos en dicha página: https://ev.us.es/webapps/portal/execute/tabs/tabAction?tab_tab_group_id=29_1 y al pulsar sobre la imagen para acceder nos identificados con otros medios de autentificación.

OTROS MEDIOS DE AUTENTICACIÓNCertificado
digital



Seleccionar un certificado

X

Selecciona un certificado para autenticar tu identidad en sso.us.es:443.

Asunto	Emisor	Número de serie
BENITEZ DIAZ ARACELI MARI...	AC FNMT Usuarios	[REDACTED]

Datos del certificado

Aceptar

Cancelar

Caso de test

Vamos a llevar a cabo dicha implementación utilizando la herramienta OpenSSL. Aunque hay muchas páginas para generar el CSR de manera online por ejemplo esta:
<https://www.dondominio.com/products/ssl/tools/csr-create/>

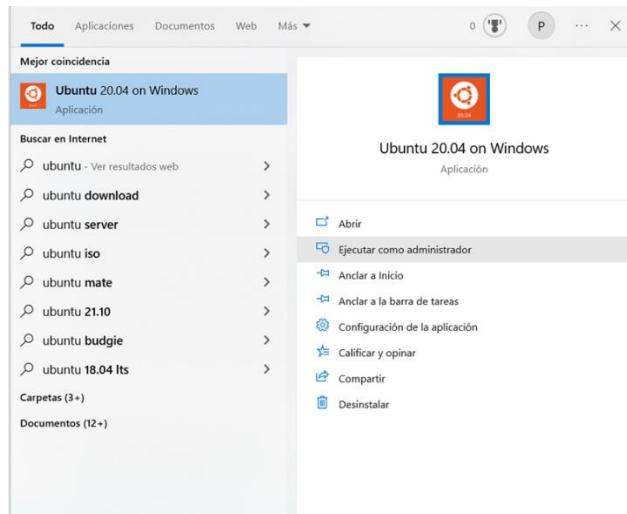
The screenshot shows the 'Generador de CSR online' interface. On the left, there's a sidebar with categories: 'CERTIFICADOS SSL', 'TIPOS DE VALIDACIÓN' (with options for Validation by domain, Validation by company, and Validation extended (EV)), 'NÚMERO DE DOMINIOS' (with options for Single domain, Multi-domain (UCC/SAN), and WildCard), and 'MARCAS' (listing DonDominio, Comodo, GeoTrust, RapidSSL, Symantec, Thawte, and Trustwave). The main area is titled 'Generador de CSR online' and contains fields for generating a CSR: 'Common Name/Subdominio' (with placeholder 'www.dondominio.com' and note about Wildcard), 'Empresa/Organización', 'Sección/Departamento', 'Correo electrónico', 'País' (Spain selected), 'Provincia' (Autonomous Community selected), and 'Localidad' (Municipality selected). A 'Crear' (Create) button is at the bottom right. The browser address bar shows the URL: https://www.dondominio.com/products/ssl/tools/csr-create/.

En la que simplemente rellenas los datos y lo creas. No es conveniente usarlas porque estas metiendo información en la web y es mucho más seguro hacerlo desde tu ordenador por eso utilizaremos OpenSSL.

Por lo tanto, para empezar a crear un certificado, primero es necesario crear la Solicitud de Firma de Certificado o también llamado CSR . Podemos enviar una CSR a una autoridad de certificación o usarla para crear un certificado autofirmado.

Pasos a seguir:

- Abrimos el terminal Ubuntu y lo ejecutamos como administrador.



- b) Escribimos en la terminal de Ubuntu el siguiente comando: openssl genrsa -out privkey.pem 2048 el cual lo que hace es generar un archivo de clave privada llamado privkey.pem (o como quieras llamarlo) en el directorio actual .

```
paulapoley@LAPTOP-NI304GOQ:~$ openssl genrsa -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
paulapoley@LAPTOP-NI304GOQ:~$
```

- c) Para generar una CSR en formato PEM en el directorio lo que hay que poner es el comando: openssl req -new -key privkey.pem -out Request.csr y ya lo habríamos creado.

```
paulapoley@LAPTOP-NI304GOQ:~$ openssl genrsa -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
paulapoley@LAPTOP-NI304GOQ:~$ openssl req -new -key privkey.pem -out request.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

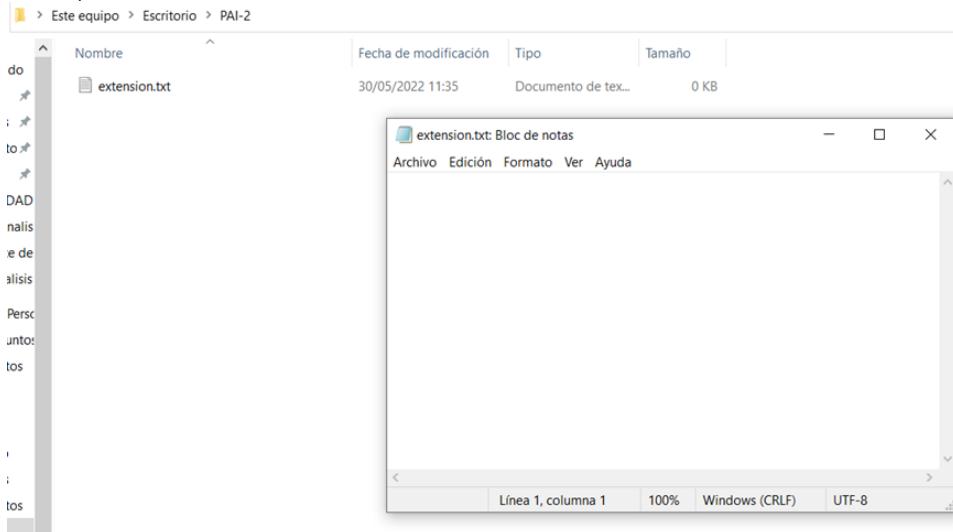
Una vez tecleado el comando nos pregunta una serie de preguntas como podemos ver a continuación.

```
paulapoley@LAPTOP-NI304GOQ:~$ openssl genrsa -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
paulapoley@LAPTOP-NI304GOQ:~$ openssl req -new -key privkey.pem -out request.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Sevilla
Locality Name (eg, city) []:Sevilla
Organization Name (eg, company) [Internet Widgits Pty Ltd]:INSEGUS
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:US
Email Address []:paupolceb@alum.us.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
paulapoley@LAPTOP-NI304GOQ:~$
```

Para crear un certificado temporal y autofirmado hasta que la CA emita su certificado firmado seguimos los siguiente pasos:

- Con el comando extensiones.txt creamos un archivo de texto sin formato



- Agregamos el siguiente texto en el archivo vacío de antes.

```
basicConstraints=CA:TRUE,pathlen:0
keyUsage=digitalSignature,keyEncipherment,keyCertSign,cRLSign
extendedKeyUsage=serverAuth
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
```

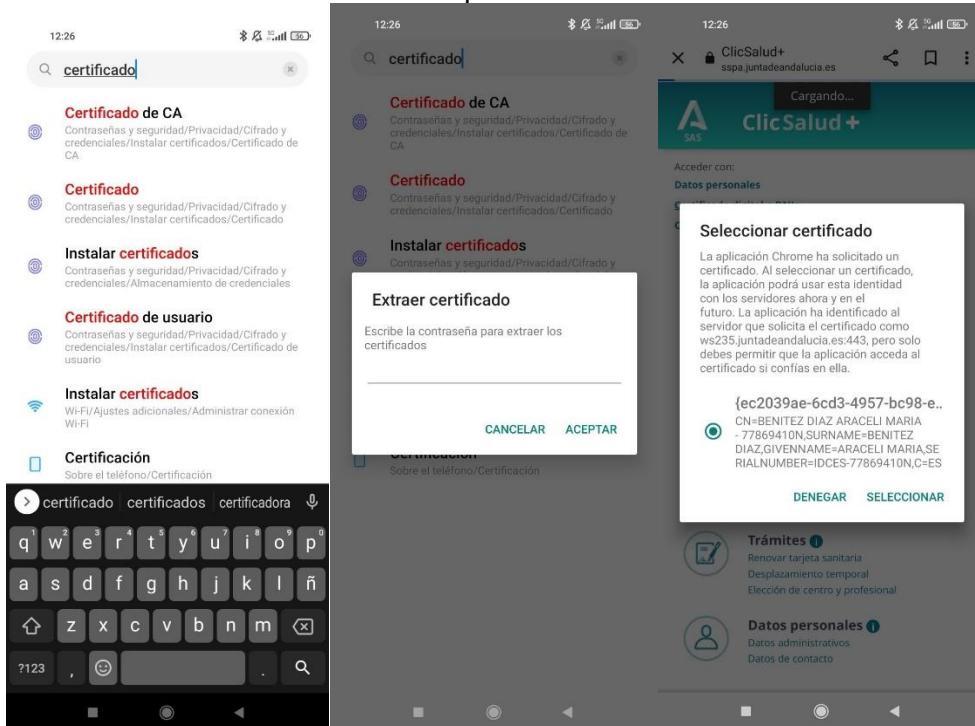
```
extension.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
basicConstraints=CA:TRUE,pathlen:0
keyUsage=digitalSignature,keyEncipherment,keyCertSign,cRLSign
extendedKeyUsage=serverAuth
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
```

Línea 1, columna 1 | 100% | Windows (CRLF) | UTF-8

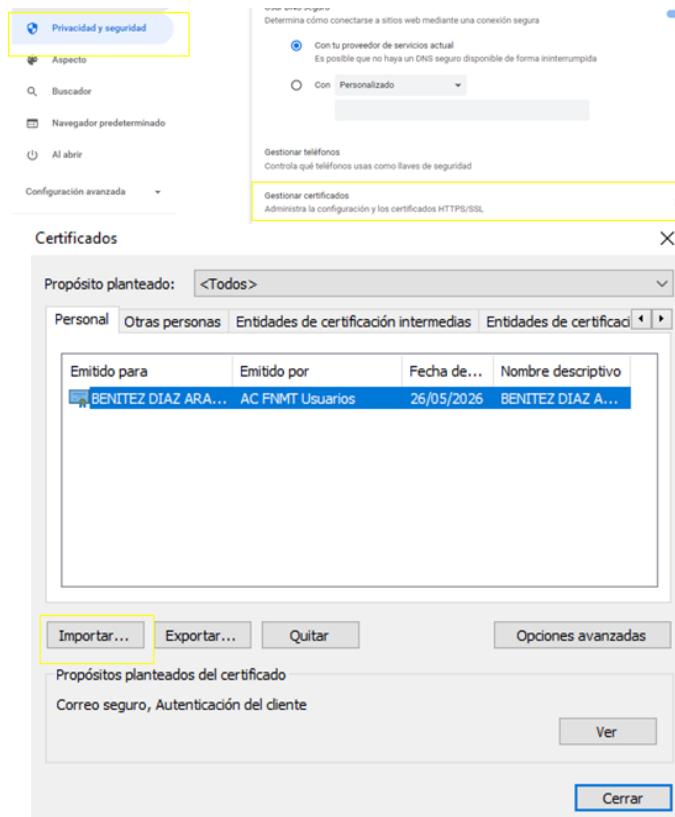
- c) Y para acabar simplemente habría que poner el siguiente comando en la terminal de Command Line Interface :
- ```
openssl x509 -req -days 30 -in request.csr -signkey privkey.pem -extfile extensiones.txt -out sscert.cert.
```
- Al ingresarla se crea un certificado dentro de nuestro directorio actual en el cual hemos puesto que caduca a los 30 días con la clave privada y la CSR creada.

## 2. Realizar la instalación/desinstalación de los certificados digitales en los browser de las partes interesadas tanto en un dispositivo de escritorio como en un dispositivo móvil.

- Instalación del certificado en un dispositivo móvil:



- Configurar el browser para que confíe en el certificado digital del Servicio de Salud.
  1. Ir a configuración de Chrome.
  2. En la parte izquierda, haz clic en **Privacidad y seguridad**.
  3. Haz clic en **Seguridad**.
  4. Desplázate hasta **Configuración avanzada**.
  5. Hacer clic en **Gestionar certificados**.



Para realizar la instalación de un certificado seguimos los pasos anteriores y pinchamos en la opción “Importar”.

← Asistente para importar certificados

Archivo para importar  
Especifique el archivo que desea importar.

Nombre de archivo:  Examinar...

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

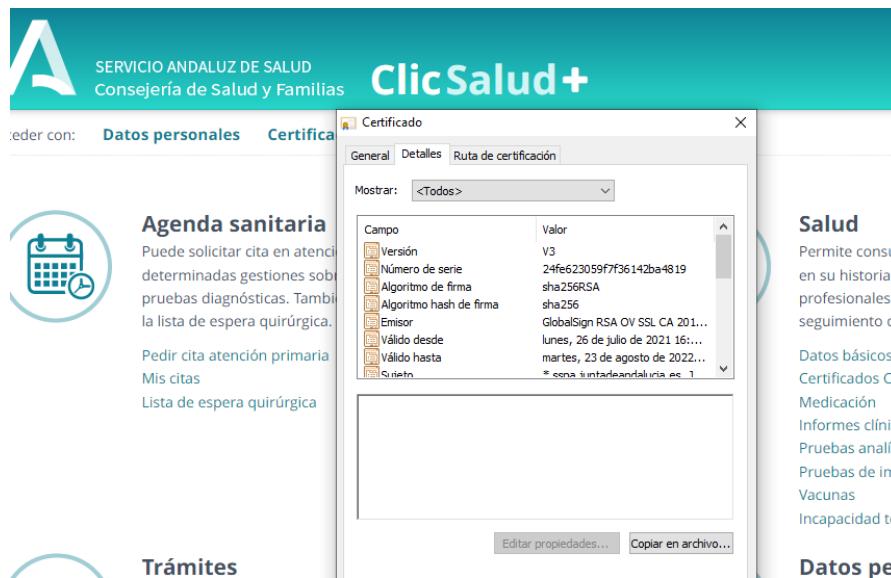
Intercambio de información personal: PKCS #12 (.PFX,.P12)  
Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)  
Almacén de certificados en serie de Microsoft (.SST)

Siguiente Cancelar

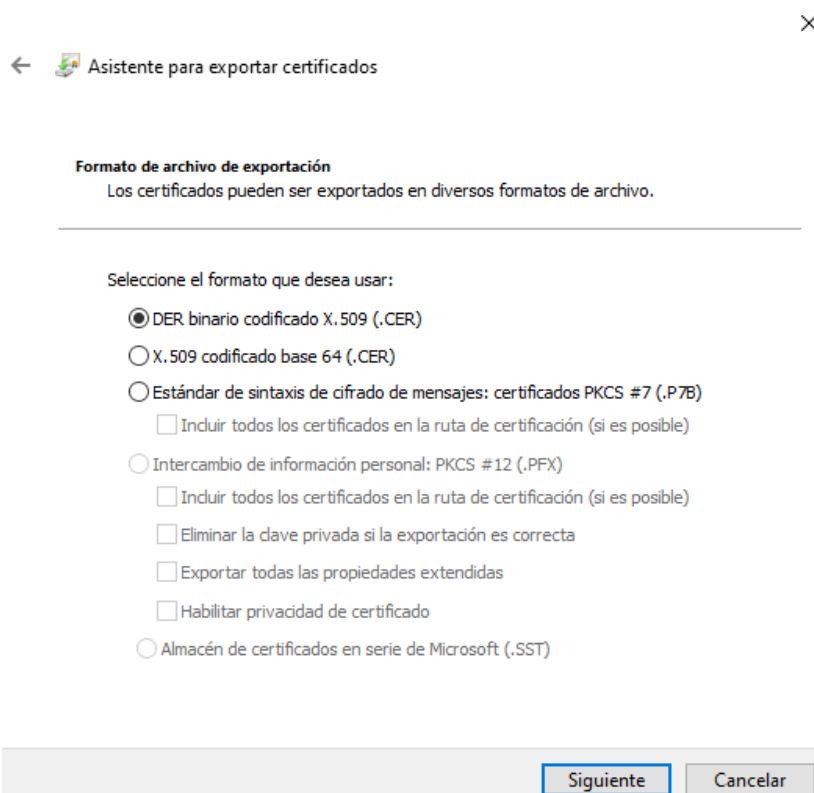
Para ello le indicamos la ruta en la que queremos guardar el certificado, y clicamos en “Siguiente”.

**a) Configurar el browser para que confíe en el certificado digital del Servicio de Salud.**

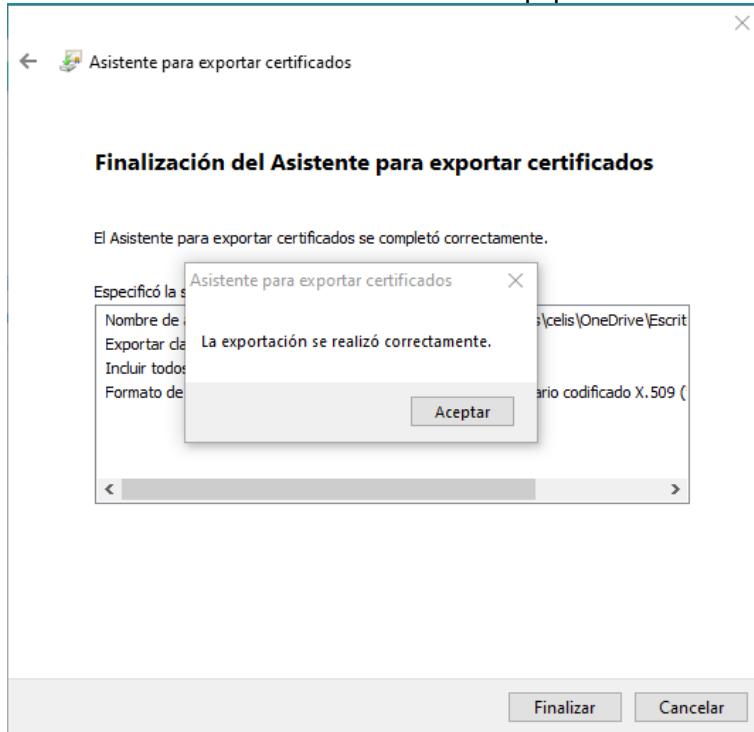
En primer lugar, necesitamos exportar el certificado digital del Servicio de Salud para poder instalarlo en nuestro equipo.



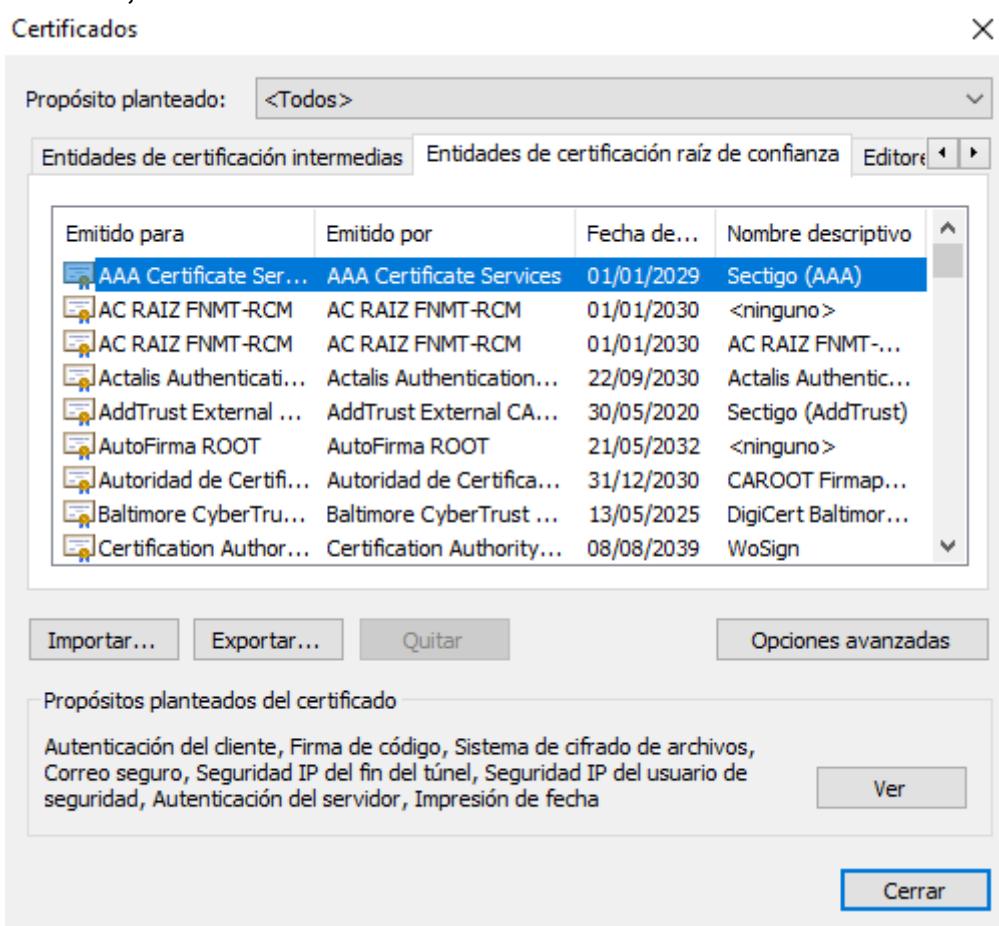
Para poder exportar el certificado, vamos a la pestaña de “Detalles” y ahí pinchamos en el botón de “Copiar archivo”.



Lo guardamos y ya tendríamos el certificado en nuestro equipo.



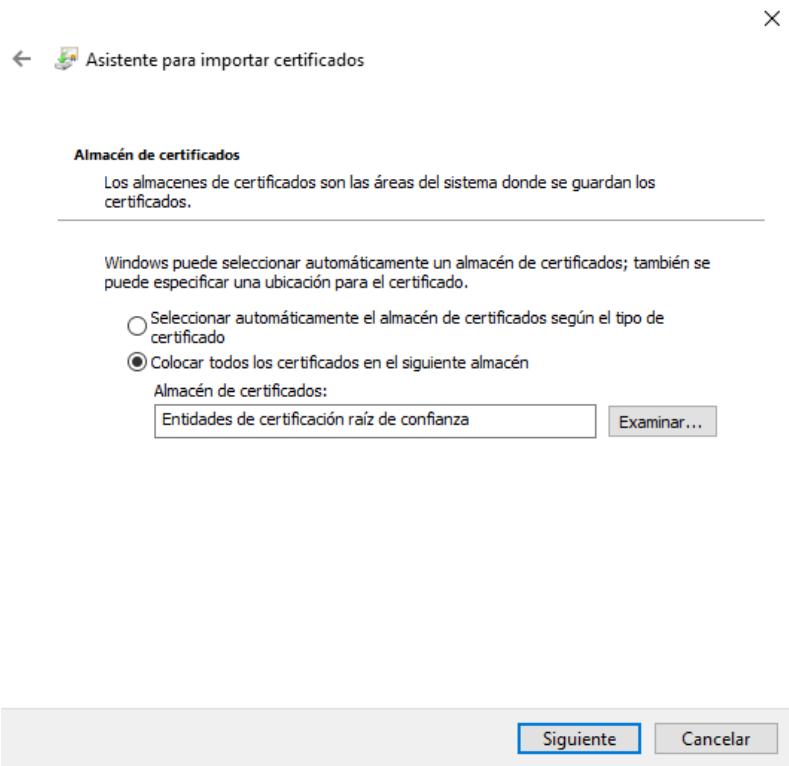
Y a continuación, lo instalamos en Chrome:



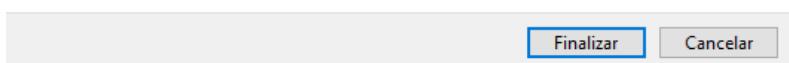
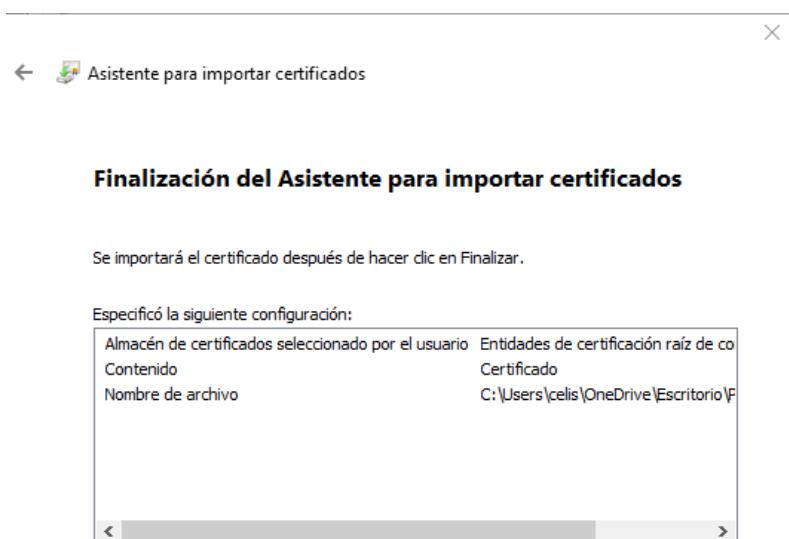
The screenshot shows the 'Certificados' (Certificates) dialog box in Google Chrome. It lists various certificates installed on the system, categorized by purpose: 'Entidades de certificación intermedias' (Intermediate Certificate Authorities), 'Entidades de certificación raíz de confianza' (Root Certificate Authorities), and 'Editores' (Editors). The 'AAA Certificate Ser...' certificate is selected. At the bottom, there are buttons for 'Importar...', 'Exportar...', 'Quitar', 'Opciones avanzadas', and 'Cerrar'.

| Emitido para            | Emitido por                | Fecha de... | Nombre descriptivo   |
|-------------------------|----------------------------|-------------|----------------------|
| AAA Certificate Ser...  | AAA Certificate Services   | 01/01/2029  | Sectigo (AAA)        |
| AC RAIZ FNMT-RCM        | AC RAIZ FNMT-RCM           | 01/01/2030  | <ninguno>            |
| AC RAIZ FNMT-RCM        | AC RAIZ FNMT-RCM           | 01/01/2030  | AC RAIZ FNMT-...     |
| Actalis Authenticati... | Actalis Authentication...  | 22/09/2030  | Actalis Authentic... |
| AddTrust External ...   | AddTrust External CA...    | 30/05/2020  | Sectigo (AddTrust)   |
| AutoFirma ROOT          | AutoFirma ROOT             | 21/05/2032  | <ninguno>            |
| Autoridad de Certifi... | Autoridad de Certifica...  | 31/12/2030  | CAROOT Firma...      |
| Baltimore CyberTru...   | Baltimore CyberTrust ...   | 13/05/2025  | DigiCert Baltimor... |
| Certification Author... | Certification Authority... | 08/08/2039  | WoSign               |

Para instalar el certificado, vamos a la página de certificados del navegador, en ella pinchamos sobre la pestaña de “Entidades de certificación raíz de confianza” y le damos a importar.



El siguiente paso sería seleccionar donde se guardará el certificado y le damos a “Siguiente”. Por último, le damos a finalizar y aceptamos el riesgo de la instalación.



## Advertencia de seguridad



Está a punto de instalar un certificado desde una entidad de certificación (CA) que afirma representar a:

\*.sspa.juntadeandalucia.es

Windows no puede validar que el certificado procede realmente de \*.sspa.juntadeandalucia.es". Póngase en contacto con \*.sspa.juntadeandalucia.es" para confirmar su origen. El siguiente número le ayudará en este proceso:

Huella digital (sha1): 92E84014 725746B0 12E519BF 4681160D  
8ECF60F8

Advertencia:

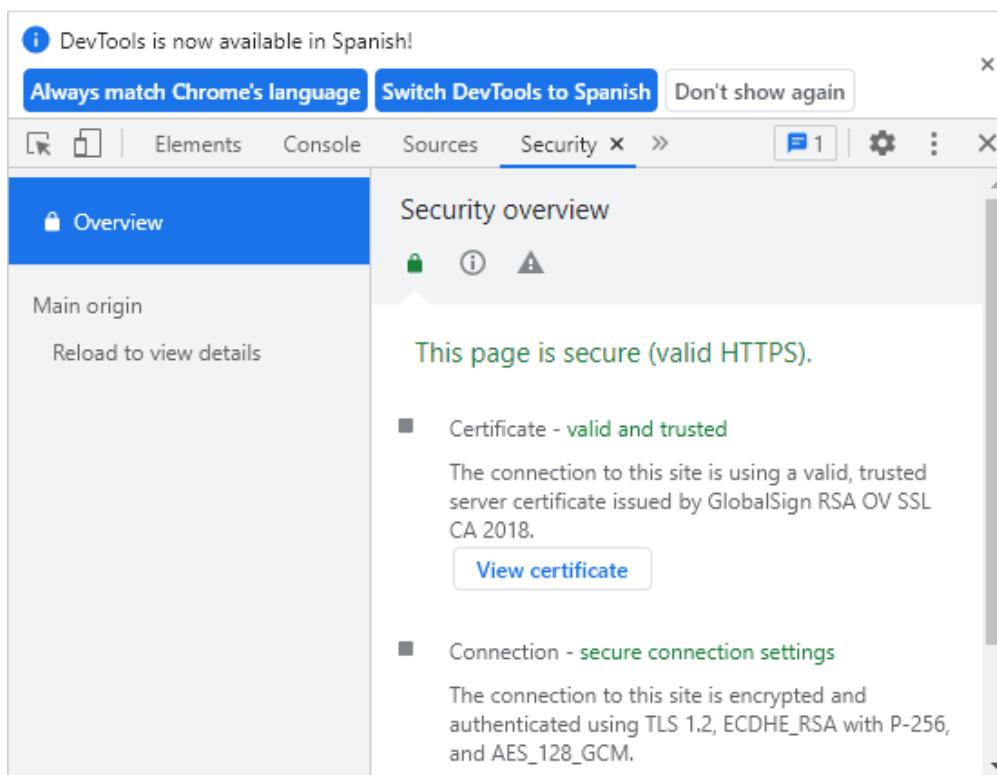
Si instala este certificado de raíz, Windows confiará automáticamente en cualquier certificado emitido por esta CA. La instalación de un certificado con una huella digital sin confirmar supone un riesgo para la seguridad. Al hacer clic en "Sí", asume este riesgo.

¿Desea instalar este certificado?

Sí

No

Y como podemos observar, confiamos en el certificado de seguridad:



The screenshot shows the Chrome DevTools Security tab. A message at the top says "DevTools is now available in Spanish!". There are buttons to "Always match Chrome's language", "Switch DevTools to Spanish", and "Don't show again". The main area is titled "Security overview" and shows a green lock icon, an information icon, and a warning icon. It states "This page is secure (valid HTTPS)". Below this, two sections are listed: "Certificate - valid and trusted" and "Connection - secure connection settings". Under "Certificate", it says the connection uses a valid, trusted server certificate issued by GlobalSign RSA OV SSL CA 2018, and there is a "View certificate" button. Under "Connection", it says the connection is encrypted and authenticated using TLS 1.2, ECDHE\_RSA with P-256, and AES\_128\_GCM.

**b) Configurar el browser para que utilice solamente el protocolo TLS 1.3 y solamente los cipher-suite más robustos para comunicarnos con el Servicio Público**

En primer lugar, introducimos: “chrome://flags/” en la barra de nuestro navegador. Nos debería salir una opción llamada “Maximum TLS version enabled”, en el desplegable seleccionaríamos TLS 1.3.

Omit **TLS** client certificates if credential mode disallows  
Strictly conform the Fetch spec to omit TLS client certificates if credential mode disallows.  
Without this flag enabled, Chrome will always try sending client certificates regardless of the credential mode. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros  
[#omit-cors-client-cert](#)

**c) Configurar el browser para que solamente confíe en certificados válidos de acuerdo a la fecha actual y que no estén revocados.**

El navegador no confiará en un certificado que esté revocado o en el que la fecha actual no esté dentro del rango válido.

### FIREFOX:

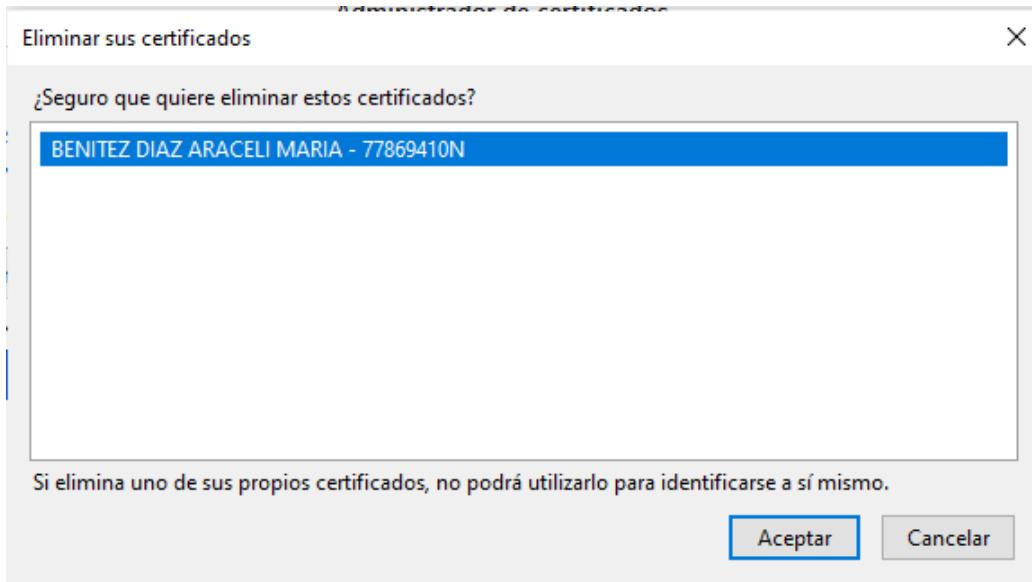
**a) Configurar el browser para que confíe en el certificado digital del Servicio de Salud**

En la pantalla del navegador, clicamos en los tres puntitos de la derecha, Ajustes y Privacidad y Seguridad.

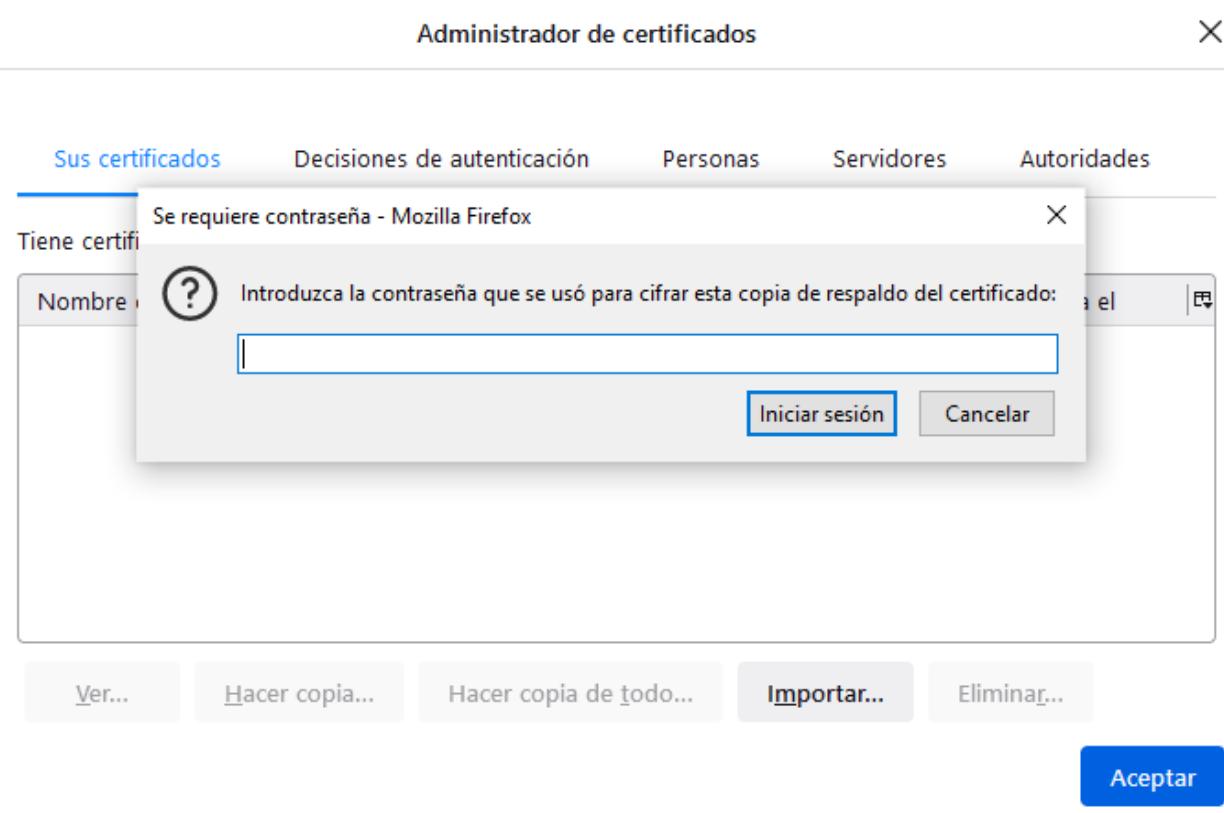
Para comprobar la instalación y desinstalación de los certificados, primero lo desinstalamos:

| Nombre del certificado | Dispositivo de seguridad                               | Número de serie           | Caduca el         |
|------------------------|--------------------------------------------------------|---------------------------|-------------------|
| FNMT-RCM               | BENITEZ DIAZ ARACELI ... OS Client Cert Token (Modern) | 65:6D:40:2D:E8:4B:A5:D... | martes, 26 de ... |

Ver... Hacer copia... Hacer copia de todo... Importar... Eliminar... Aceptar



Una vez desinstalamos, pinchamos en “Importar” y volvemos a instalar el certificado en nuestro navegador:





## Administrador de certificados X

### Sus certificados

### Decisiones de autenticación

### Personas

### Servidores

### Autoridades

Tiene certificados de estas organizaciones que le identifican

| Nombre del certificado                                 | Dispositivo de seguridad  | Número de serie   | Caduca el |
|--------------------------------------------------------|---------------------------|-------------------|-----------|
| ▼ FNMT-RCM                                             |                           |                   |           |
| BENITEZ DIAZ ARACELI ... OS Client Cert Token (Modern) | 65:6D:40:2D:E8:4B:A5:D... | martes, 26 de ... |           |

[Ver...](#)[Hacer copia...](#)[Hacer copia de todo...](#)[Importar...](#)[Eliminar...](#)[Aceptar](#)

Para ello importamos el certificado de “ClicSalud”

Administrador de certificados X

Descargando certificado

Se le ha pedido que confíe en una nueva Autoridad Certificadora (CA).

¿Quiere confiar en "GlobalSign RSA OV SSL CA 2018" para los siguientes propósitos?

Confiar en esta CA para identificar sitios web.

Confiar en esta CA para identificar usuarios de correo.

Antes de confiar en esta CA para cualquier propósito, debe examinar el certificado, política y procedimientos de la CA (si están disponibles).

[Ver](#) [Examinar certificado de CA](#)

[Aceptar](#) [Cancelar](#)

Camerfirma Global Chambersign Root      Builtin Object Token

[Ver...](#) [Editar confianza...](#) [Importar...](#) [Exportar...](#) [Eliminar o dejar de confiar...](#)

[Aceptar](#)

ⓘ DevTools is now available in Spanish!

[Always match Chrome's language](#) [Switch DevTools to Spanish](#) [Don't show again](#)

Elements Console Sources Security > 1 |

Overview

Main origin  
[Reload to view details](#)

Security overview

This page is secure (valid HTTPS).

- Certificate - [valid and trusted](#)  
The connection to this site is using a valid, trusted server certificate issued by GlobalSign RSA OV SSL CA 2018.  
[View certificate](#)
- Connection - [secure connection settings](#)  
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE\_RSA with P-256, and AES\_128\_GCM.

Y como podemos observar, nuestro navegador confía en este certificado.

**b) Configurar el browser para que utilice solamente el protocolo TLS 1.3 y solamente los cipher-suite más robustos para comunicarnos con el Servicio Público**

En la barra de nuestro navegador introducimos “about:config” y buscamos “tls:version” y cómo podemos observar como mínimo usa TLS 1.3.

Firefox about:config

Mostrar solo las preferencias modificadas

|                                        |       |  |
|----------------------------------------|-------|--|
| media.peerconnection.dtls.version.max  | 771   |  |
| media.peerconnection.dtls.version.min  | 771   |  |
| security.tls.version.enable-deprecated | false |  |
| security.tls.version.fallback-limit    | 4     |  |
| security.tls.version.max               | 4     |  |
| security.tls.version.min               | 3     |  |

Booleano  Número  Cadena

- c) Configurar el browser para que solamente confíe en certificados válidos de acuerdo a la fecha actual y que no estén revocados.

El navegador no confiará en un certificado que esté revocado o en el que la fecha actual no esté dentro del rango válido.

### 3. Verificar los certificados digitales de los servidores Web de un Servicio de Salud

Para realizar las siguientes preguntas, observamos los detalles del certificado de "ClicSalud".

**1. El certificado digital del Servicio es extendido o no, ¿cómo se ha determinado?.**

Un certificado con Validación Extendida (EV) es el "tope de línea" de los certificados. La obtención de uno requiere que una empresa pase por un proceso de investigación exhaustivo, todos los detalles de la empresa deben ser verificados como auténticos y legítimos antes de la emisión del certificado.

**Certificado**

General Detalles Ruta de certificación

Mostrar: <Todos>

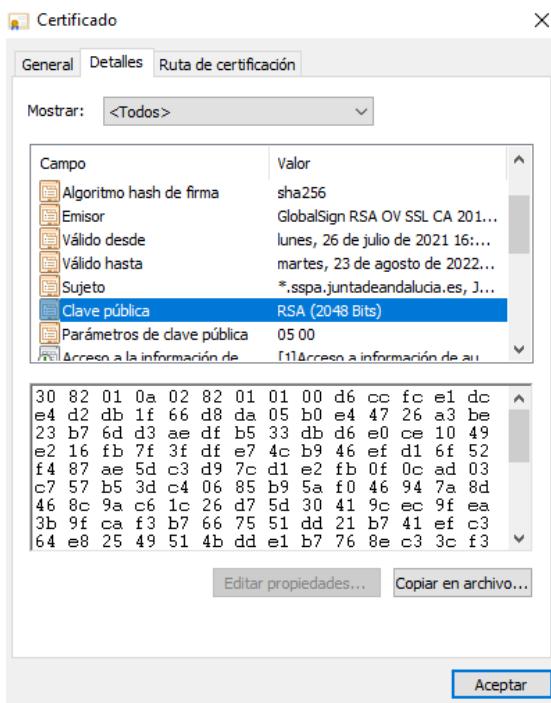
| Campo                   | Valor                             |
|-------------------------|-----------------------------------|
| Número de serie         | 24fe623059f7f36142ba4819          |
| Algoritmo de firma      | sha256RSA                         |
| Algoritmo hash de firma | sha256                            |
| Emisor                  | GlobalSign RSA OV SSL CA 201...   |
| Válido desde            | lunes, 26 de julio de 2021 16:... |
| Válido hasta            | martes, 23 de agosto de 2022..    |
| Sujeto                  | *.sspa.juntadeandalucia.es, J...  |
| Clave pública           | RSA (2048 Bits)                   |

CN = \*.sspa.juntadeandalucia.es  
O = Junta de Andalucía  
OU = Sistema Sanitario Público de Andalucía  
L = Sevilla  
S = Sevilla  
C = ES

Editar propiedades... Copiar en archivo... Aceptar

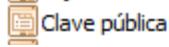
Por tanto, como podemos observar, no es un certificado extendido, sino una validación de la organización.

## 2. ¿Cuál es la clave pública del servidor?



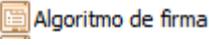
30 82 01 0a 02 82 01 01 00 d6 cc fc e1 dc e4 d2 db 1f 66 d8 da 05 b0 e4 47 26 a3 be 23 b7 6d d3 ae df b5 33 db d6 e0 ce 10 49 e2 16 fb 7f 3f df e7 4c b9 46 ef d1 6f 52 f4 87 ae 5d c3 d9 7c d1 e2 fb 0f 0c ad 03 c7 57 b5 3d c4 06 85 b9 5a f0 46 94 7a 8d 46 8c 9a c6 1c 26 d7 5d 30 41 9c ec 9f ea 3b 9f ca f3 b7 66 75 51 dd 21 b7 41 ef c3 f3 15 a4 36 c4 b7 5f 81 5a 46 b4 49 b3 56 41 84 af 2d 51 86 9b 0f 8a 9c 2f 06 43 0b 78 64 84 89 98 9a 56 8c b3 1b a5 2b 75 fd 28 e8 c9 f1 8b 63 28 02 48 3a dd 81 cf 77 64 58 92 00 9e 7c 3a 51 38 97 cc 81 21 bd 17 45 5d 91 b3 a8 24 f3 86 f5 03 46 95 59 82 75 da ac 3c 03 a9 b7 91 04 c9 89 37 57 0f 6a 44 b6 5c d0 85 c0 b0 c2 86 5d fe ec fb 76 3c 8e 88 ff a8 fa 23 cc 8b 48 47 be 87 80 1b 8f 26 b9 20 97 7c 65 6a 2a 36 dd 02 03 01 00 01

## 3. ¿Cuál es el tamaño de la clave pública del servidor?



RSA (2048 Bits)

## 4. ¿Cuál es el algoritmo usado para firmar el certificado?



sha256RSA

## 5. ¿Cuál la huella digital del certificado? ¿qué representa?



92e84014725746b012e519bf...

92e84014725746b012e519bf4681160d8ecf60f8

Es un conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado.

**6. ¿Durante qué fechas es válido dicho certificado?**

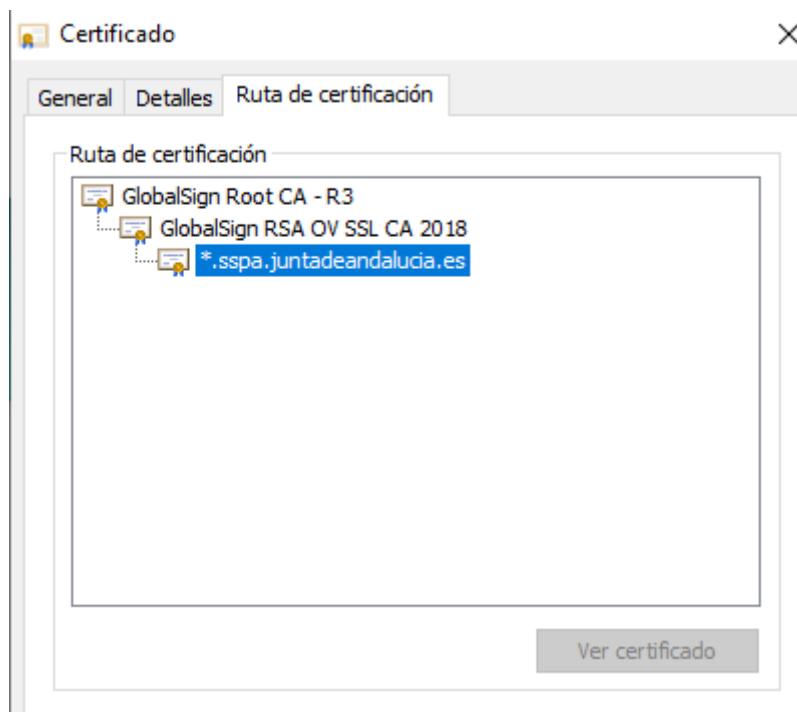
|                                                                                                |                                   |
|------------------------------------------------------------------------------------------------|-----------------------------------|
|  Válido desde | lunes, 26 de julio de 2021 16:... |
|  Válido hasta | martes, 23 de agosto de 2022...   |

**7. ¿Cuáles son los permisos que tiene de uso dicho certificado?**

 **Usos de la clave**

Propósitos      Digital Signature, Key Encipherment

**8. ¿Cuál es la cadena de certificados que entrega dicho Servicio de Salud? Muestre dicha cadena en formato textual**



**9. ¿Dónde se encuentra ubicado el servidor OCSP? ¿Se encuentra soportado el OCSP must staple por el servidor del Servicio de Salud? Nos indica el cliente que le expliquemos qué ventajas le podría reportar tenerlo activado.**

La validación de OCSP en un dispositivo Citrix ADC comienza cuando el dispositivo recibe un certificado de cliente durante un protocolo de enlace SSL. Para validar el certificado, el dispositivo crea una solicitud OCSP y la reenvía al respondedor OCSP.

Los dispositivos Citrix ADC admiten OCSP tal como se define en RFC 2560. OCSP ofrece ventajas significativas sobre las listas de revocación de certificados (CRL) en términos de información oportuna. El estado actualizado de revocación de un certificado de cliente es especialmente útil en transacciones que implican grandes sumas de dinero y operaciones bursátiles de alto valor. También utiliza menos recursos del sistema y de la red. La implementación de Citrix ADC de OCSP incluye el procesamiento por lotes de solicitudes y el almacenamiento en caché de respuestas.



#### 4. Revocación los certificados digitales personales de las partes interesadas

En primer lugar, buscamos la página de la Fábrica Nacional de Moneda y Timbre, clicamos en “Obtener Certificados Electrónicos” - “Persona Física”. Y pinchamos en el botón de “Anular”.

[Inicio](#) > [Obtener Certificados Electrónicos](#) > [Persona Física](#)

| Persona Física                                  |
|-------------------------------------------------|
| <a href="#">Obtener Certificado Software</a>    |
| <a href="#">Obtener Certificado con DNIE</a>    |
| <a href="#">Obtener Certificado con Android</a> |
| <a href="#">Verificar estado</a>                |
| <a href="#">Renovar</a>                         |
| <a href="#">Anular</a>                          |
| Certificado de Representante                    |
| <a href="#">Sector Público</a>                  |
| <a href="#">Certificados de componente</a>      |
| <a href="#">Soporte Técnico</a>                 |

#### Persona Física

El Certificado digital FNMT de Persona Física es la certificación electrónica expedida por la FNMT-RCM que vincula a su suscriptor con unos Datos de verificación de Firma y confirma su identidad.

Este certificado, también conocido como Certificado de Ciudadano o de Usuario, es un documento digital que contiene sus datos identificativos. Le permitirá identificarse en Internet e intercambiar información con otras personas y organismos con la garantía de que sólo Ud. y su interlocutor pueden acceder a ella.

#### ¿Quién puede obtener un Certificado digital de Persona Física?

Cualquier ciudadano español o extranjero, mayor de edad o menor emancipado que esté en posesión de su DNI o NIE, podrá solicitar y obtener su certificado digital de forma gratuita para firmar y acreditar su identidad de forma segura en Internet.

#### ¿Cómo puedo obtener el Certificado?

Existen 2 formas distintas para obtener su Certificado digital de Persona Física como archivo descargable en su ordenador:

- Con acreditación presencial en una oficina. [Obtener Certificado software](#).
- Utilizando su DNIE. [Obtener Certificado con DNIE](#).

#### ¿Para qué sirve?

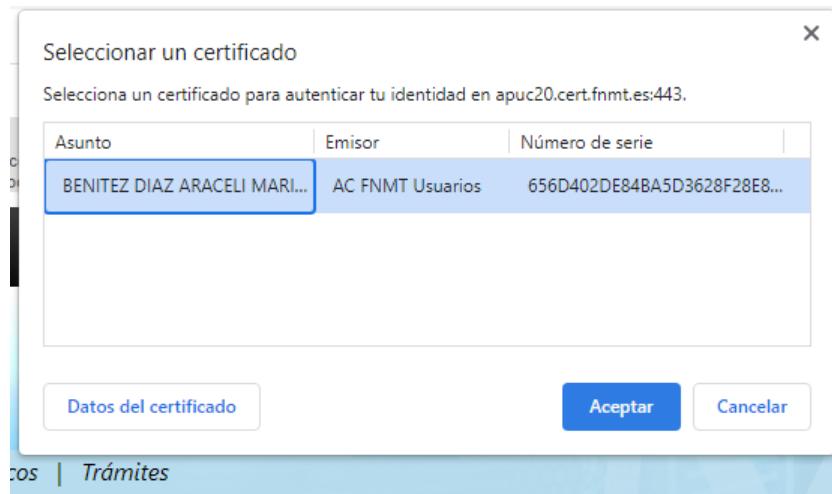
Buscamos el link “Anulación online”.

#### Procedimiento

Para solicitar la anulación del Certificado de Persona Física expedido por la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda puede proceder de la siguiente manera:

- Si el titular del certificado está en posesión del mismo, la revocación puede efectuarse en la aplicación de [anulación online](#).
- Si el titular del certificado no dispone del mismo por extravío, pérdida o robo, deberá personarse en una Oficina de Acreditación.
- En cualquier caso, podrá utilizar el Servicio de revocación telefónica 24x7 de certificados de persona física a través de los siguientes números de teléfono: 902200616 / 917406848 / 913878337

Seleccionamos el certificado que deseamos revocar y le damos a “Aceptar”.

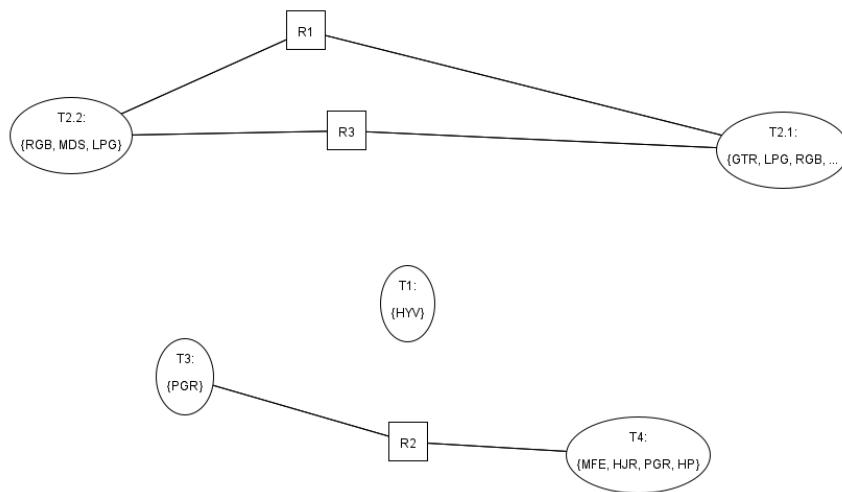


; > Persona Física > Anular > Solicitar anulación

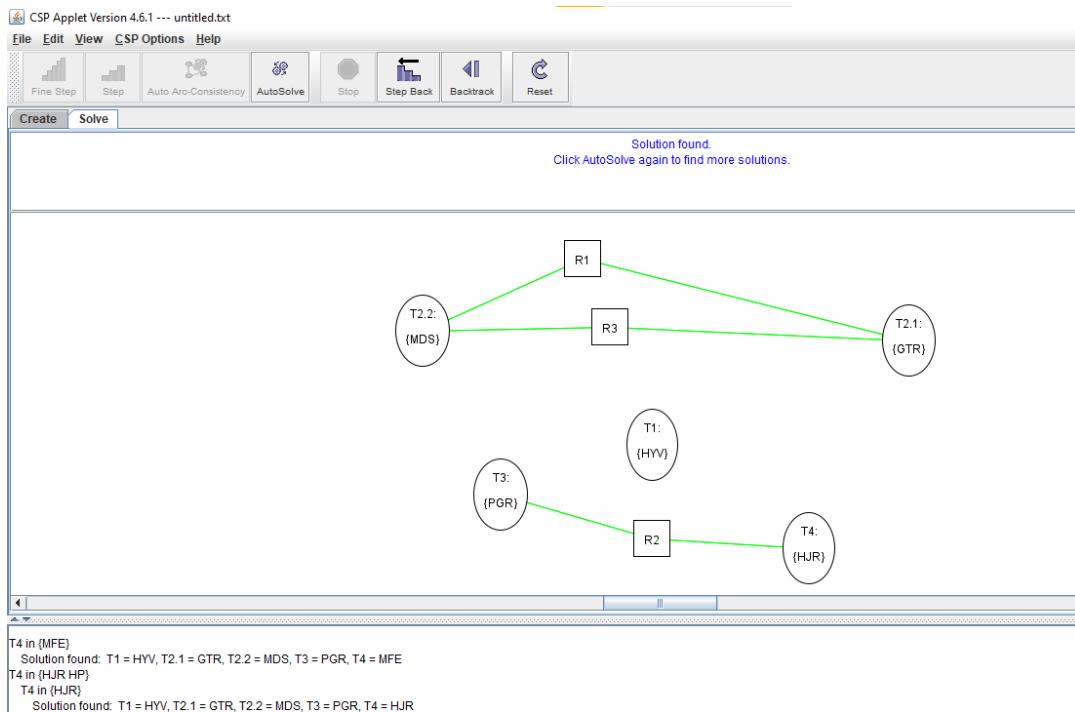
Revocación

## Workpackage 2. Verificación Automática de la Política de Control de Acceso teniendo en cuenta conflictos de intereses, separación/segregación de deberes dinámica y binding de deberes

Entramos en la página web: <http://www.aispace.org/mainApplets.shtml> y nos descargamos “CSP Applet” y creamos nuestro diagrama con las tareas y restricciones que tenemos:



Una vez creado, pulsamos “Solve” para obtener las distintas soluciones para nuestro diagrama:



En la siguiente tabla están generadas las 20 instancias de dicho proceso con las personas que pueden tener acceso a ejecutar las tareas que se han detallado en el enunciado.

| Instancias | T1  | T2.1 | T2.2 | T3  | T4  |
|------------|-----|------|------|-----|-----|
| 1          | HYV | GTR  | MDS  | PGR | MFE |
| 2          | HYV | GTR  | MDS  | PGR | HJR |
| 3          | HYV | GTR  | MDS  | PGR | HP  |
| 4          | HYV | LPG  | RGB  | PGR | MFE |
| 5          | HYV | LPG  | RGB  | PGR | HJR |
| 6          | HYV | LPG  | RGB  | PGR | HP  |
| 7          | HYV | HYV  | RGB  | PGR | MFE |
| 8          | HYV | HYV  | RGB  | PGR | HJR |
| 9          | HYV | HYV  | RGB  | PGR | HP  |
| 10         | HYV | BJC  | RGB  | PGR | MFE |
| 11         | HYV | BJC  | RGB  | PGR | HJR |
| 12         | HYV | BJC  | RGB  | PGR | HP  |
| 13         | HYV | GTR  | MDS  | PGR | MFE |
| 14         | HYV | LPG  | MDS  | PGR | MFE |
| 15         | HYV | RGB  | MDS  | PGR | MFE |
| 16         | HYV | HYV  | MDS  | PGR | MFE |
| 17         | HYV | BJC  | MDS  | PGR | MFE |
| 18         | HYV | GTR  | MDS  | PGR | HJR |
| 19         | HYV | LPG  | MDS  | PGR | HJR |
| 20         | HYV | RGB  | MDS  | PGR | HJR |

## Workpackage 3 Firmado digital y verificación de firmas en documentos del Servicio de Salud

Para realizar el Workpackage 3 y hacer firmado digital y verificación de firmas en documentos entraremos en la Sede Electrónica del Ministerio de Sanidad, Consumo y Bienestar Social y desde ahí responderemos a los modelos de procesos y casos de test de las preguntas 1 y 2 .

Entramos en la Sede Electrónica del Ministerio de Sanidad, Consumo y Bienestar Social. (<https://sede.mscbs.gob.es/home.htm>). Una vez dentro en su página de inicio podemos ver que nos permite hacer diversas verificaciones como podemos ver en la captura siguiente.

The screenshot shows the official website of the Ministry of Health, Consumer Affairs and Social Welfare's electronic service (Sede Electrónica). The top navigation bar includes links for 'Sobre la Sede', 'Trámites', 'Estado de mi solicitud', 'Registro electrónico', 'Notificaciones electrónicas', 'Tasas', 'Servicios', 'Solicita el Certificado COVID Digital de la UE', 'datos abiertos', 'Información' (with links to 'Canal de acceso', 'Protección de Datos Personales', 'Calendario de días hábiles', 'Formulación de sugerencias y quejas', and 'Ayúdenos a mejorar esta página'), and 'Utilidades' (with links to 'Verificación de certificados', 'Verificación de documentos con CSV', and 'Verificación de documentos firmados digitalmente'). Below the main menu, there are sections for 'Sede Electrónica del Ministerio de Sanidad, Consumo y Bienestar Social' (with links to 'Certificado digital' and 'Documentos firmados'), 'CONSULTE SI SU COMUNIDAD AUTÓNOMA EXPIDE EL CERTIFICADO COVID DIGITAL DE LA UE', 'SOLICITUD DE CERTIFICADO COVID DIGITAL DE LA UE', and '¿Tienes dudas? Consulta las preguntas frecuentes'. At the bottom, there are links to other ministry services like 'Sede Electrónica AEMPS', 'Sede Electrónica IMSSERSO', 'Sede Electrónica AESAN', and logos for 'ASENCIA', 'FACTURA', 'dni', 'gob.es', 'BOE', 'CONSEJERÍA DE COMUNICACIÓN SOCIAL', 'ens', and 'WEC'. The footer also features links for 'WEC MÁS', 'WEC RIFAS', and 'WEC CSES'.

Vamos a ver uno por uno y paso por paso la verificación de firmas digitales, verificación de la firma de los documentos firmados.

### • Verificación de certificados.

1. En la barra de utilidades le damos a “Verificación de certificados”

This screenshot shows the 'Utilidades' (Utilities) section of the website. It contains three options: 'Verificación de certificados' (with a key icon), 'Verificación de documentos con CSV' (with a CSV icon), and 'Verificación de documentos firmados digitalmente' (with a document and lock icon). The first option, 'Verificación de certificados', is highlighted with a red circle.



- Al seleccionarlo, nos muestra la siguiente captura y le damos a “Acceso a los servicios de verificación”. Puesto que ofrece la plataforma VALIDE, que verifica la validez del certificado de la Sede Electrónica Central del Ministerio de Sanidad, Consumo y Bienestar Social.

The screenshot shows the official website of the Ministry of Health, Consumer Affairs and Social Welfare ('Sede Electrónica'). The main menu includes links for 'Sobre la Sede', 'Trámites', 'Estado de mi solicitud', 'Registro electrónico', 'Notificaciones electrónicas', 'Tasas', and 'Servicios'. A prominent button labeled 'Solicita el Certificado COVID Digital de la UE' is visible. The 'Utilidades' section contains a link to 'Verificación de certificados'. The right sidebar displays the date and time (07/06/2022 18:51:29), a 'Asesoramiento electrónico' button, and a note about the last update (10/11/2016).

- Al darle nos redirige a otra página en la cual se podría Validar Certificado, firma y sede electrónica a parte de realizar y visualizar firma. Veamos uno a uno.

The screenshot shows the VALIDe platform interface. It features several sections: 'Validar Certificado' (with a link to 'Validar Certificado'), 'Preguntas Frecuentes' (FAQ), 'Realizar Firma' (with a sub-section for 'Firma un documento'), 'Visualizar Firma' (with a sub-section for 'Podrás generar informes'), 'Validar Firma' (with a sub-section for 'Consulta la validez de un documento firmado'), 'Validar Sede Electrónica' (with a sub-section for 'Podrás comprobar las URLs de sede electrónica'), and a 'Portal de Firma electrónica' button. The footer contains a legal notice regarding data protection.

#### a) Realizar firma.

Vamos a firmar el documento con el DNI electrónico o con cualquier certificado reconocido con las máximas garantías de integridad y autenticidad. Le damos a “Realizar firma”



# INGENIERÍA DE SEGURIDAD US

Avda Reina Mercedes s/n. 41012 Sevilla

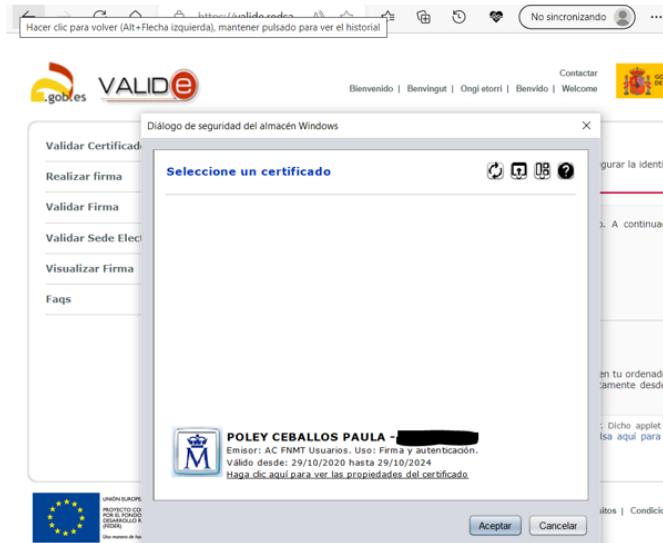


Le damos a firmar y se me abre una aplicación descargada llamada AutoFirma@. Es una aplicación de firma que instalas en tu ordenador y que te permite elegir el tipo de firma que quieras realizar para firmar directamente desde tu ordenador sin necesidad de estar conectado a internet.

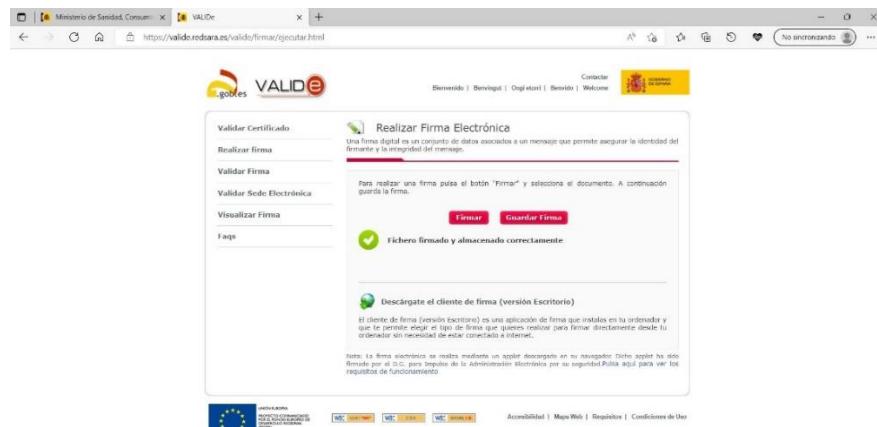
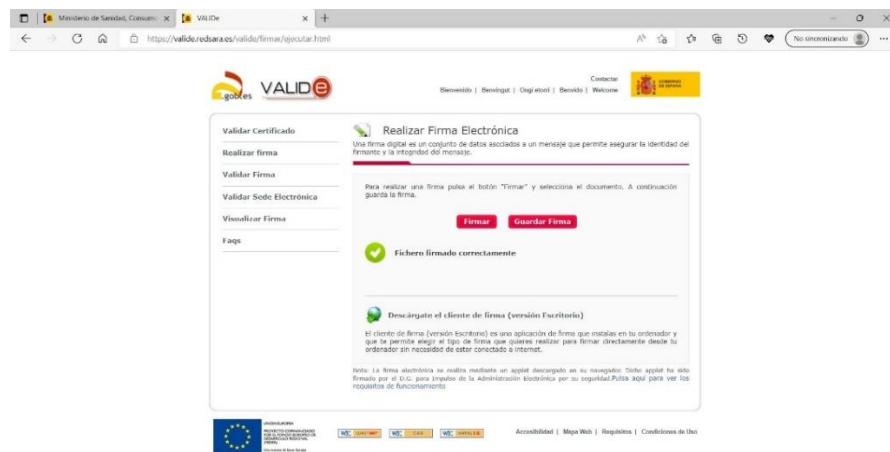
Seleccionamos el lugar y el documento que queremos firmar.



Seleccionamos el certificado con el que queremos firmar el documento.



Le damos a “Aceptar” y si todo ha ido bien nos sale en la página “Fichero firmado correctamente”. Ahora el siguiente paso es guardar el documento firmado y para ello le damos a “guardar firma”. Este nos pregunta dónde queremos guardarlo y el nombre que le queremos poner.



Pero de una forma más fácil esto que hemos hecho lo hacemos directamente con la aplicación de escritorio AutoFirma@. Para descargarla le damos a “Descárgate el cliente de firma (versión Escritorio). Nos sale la página que podemos ver en la captura de abajo y le damos a descargar según el sistema operativo que el ordenador tenga.

**Descargas**

Desde aquí puedes descargar aquellas aplicaciones que necesites para firmar electrónicamente y otras utilidades o documentos.

**Aviso importante sobre la actualización de autofirma**

Respecto a los problemas con AutoFirma resultado de las nuevas actualizaciones de los navegadores Firefox v97, Chrome v98 y Edge v98, son necesarias dos actuaciones: 1. Actualizar AutoFirma en los equipos cliente a la última versión. 2. Actualizar las aplicaciones web, que invocan AutoFirma, tanto en el lado cliente (en su navegador), como en servidor, en nuestros sistemas de actualizaciones, cliente y servidor, para el correcto funcionamiento. Sólo con la actualización del Cliente no se puede completar el proceso de firma.

**AutoFirma (04/02/2022)**

AutoFirma (04/02/2022)

AutoFirma (04/02/2022)

Notas para usuarios de Mac

Una vez que ya tenemos descargada la aplicación . Nos sale la siguiente ventana para que seleccionemos el fichero que queremos firmar y seleccionamos “Firmar”.

**Bienvenido a AutoFirma**

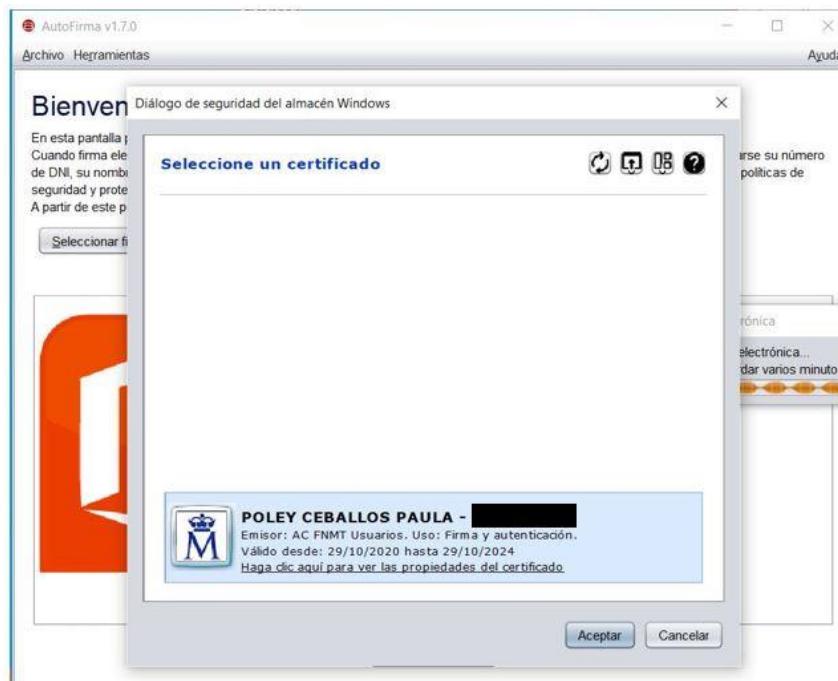
En esta pantalla puede firmar electrónicamente ficheros que se encuentren en su disco duro. Cuando firma electrónicamente un fichero pueden incorporarse a este ciertos datos personales, entre los que pueden encontrarse su número de DNI, su nombre y apellidos o incluso información sobre su situación laboral si utiliza un certificado profesional. Consulte las políticas de seguridad y protección de datos de los receptores de los ficheros firmados antes de enviarlos o distribuirlos. A partir de este punto, no inserte o extraiga ninguna tarjeta inteligente o dispositivo criptográfico USB.

Seleccionar ficheros a firmar

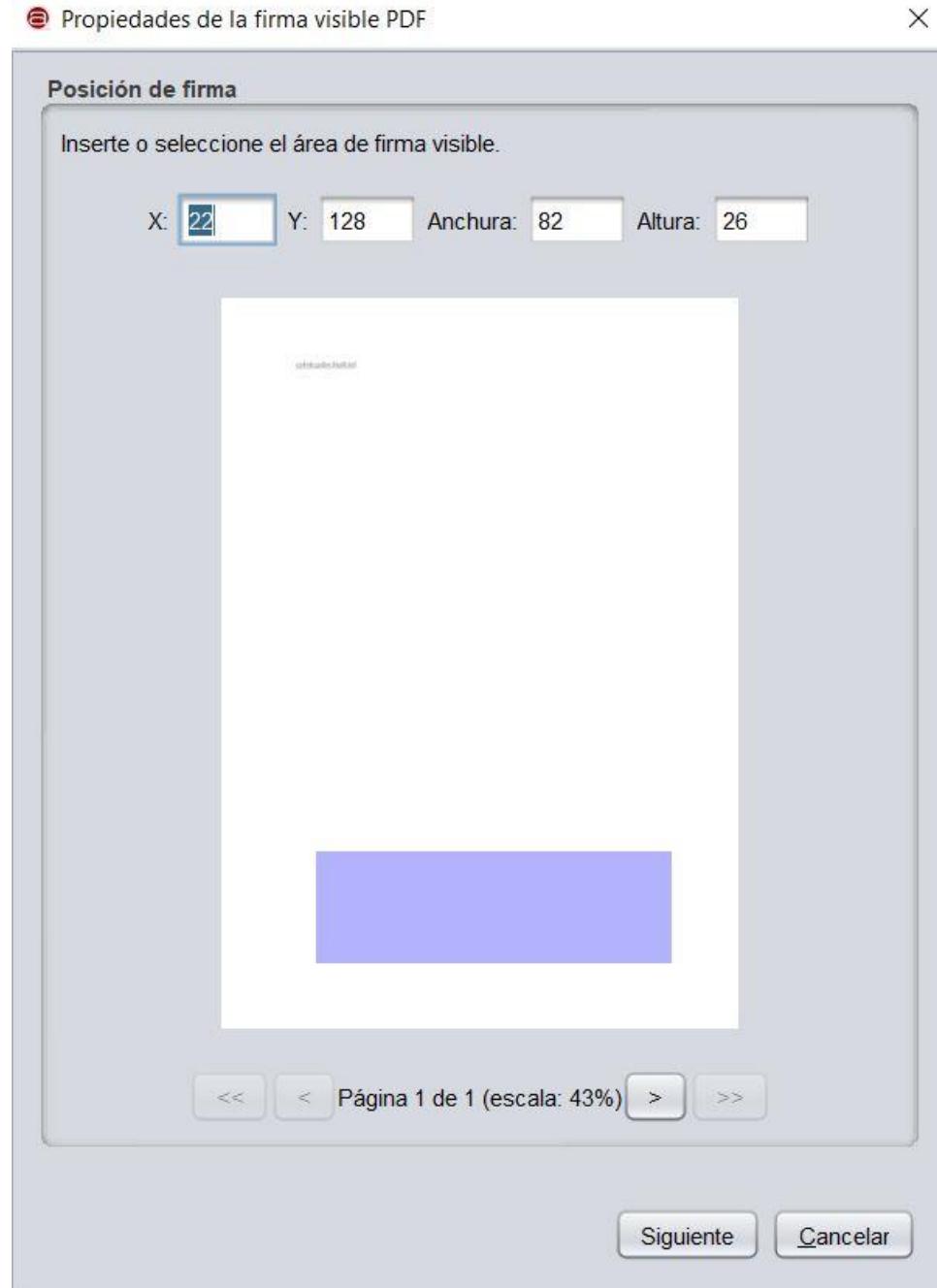
Pulse el botón o arrastre ficheros o directorios a este área

Firmar

Seleccionamos el certificado con el cual queremos firmar el documento. Y le damos a "aceptar".



Al darle a “Hacer la firma visible dentro del PDF” y a “Firmar” nos pregunta donde queremos, es decir, la posición o el área donde queremos que quede la firma. (recuadro lila)



Al darle a “siguiente” podemos editar la firma (cambiar de color, el tipo de letra, el tamaño....) y ver la vista previa de cómo se vería esta.

Propiedades de la firma visible PDF X

**Vista Previa**

Firmado por \$\$SUBJECTCN\$\$ el día \$\$SIGNDATE=dd/MM/yyyy\$\$ con un certificado emitido por \$\$ISSUERCN\$\$.

La previsualización puede diferir del resultado final. Consulte la [página de ayuda](#) para conocer las palabras clave para introducir información del certificado.

**Configuración de firma**

Imagen de firma:

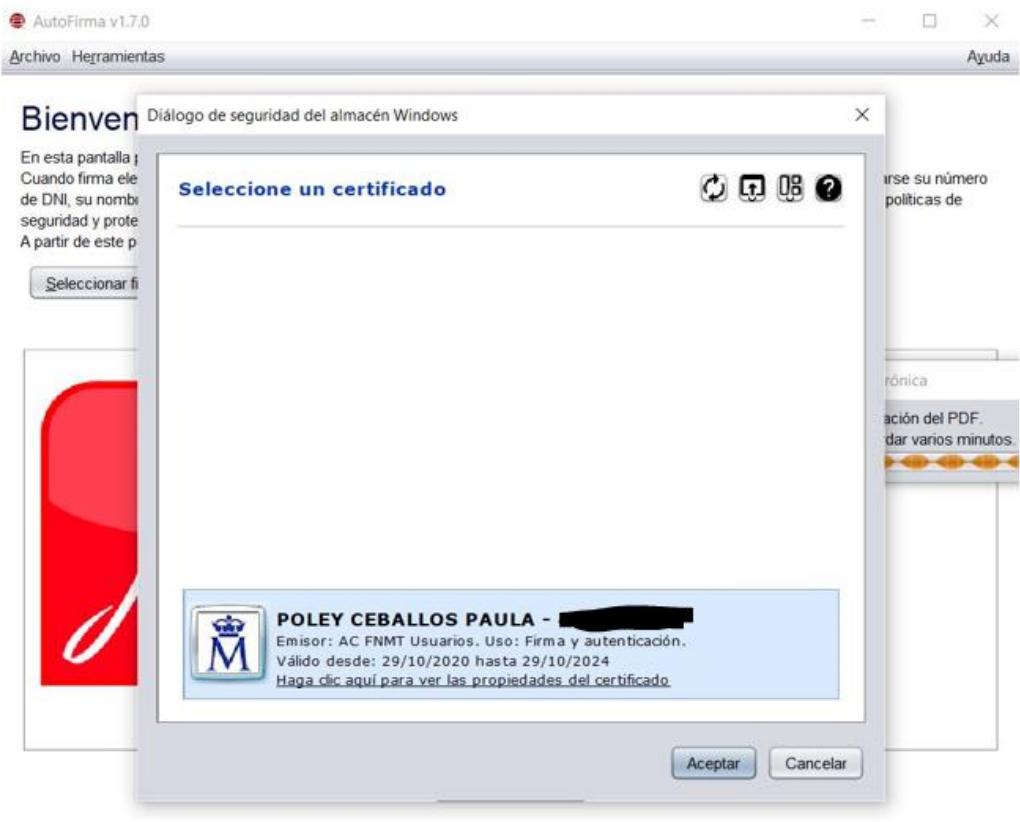
Texto de la firma:

Firmado por \$\$SUBJECTCN\$\$ el día \$\$SIGNDATE=dd/MM/yyyy\$\$ con un certificado emitido por \$\$ISSUERCN\$\$.

Courier 12 No rotar

Recordar configuración

Una vez le demos a “Aceptar” nos obliga a elegir el certificado con el que queremos firmar el documento. Y lo guardamos.



AutoFirma v1.7.0 - PAI-2-Seguridad\_signed.pdf

Archivo Herramientas Ayuda

## Proceso de firma completado satisfactoriamente

La firma es correcta en cuanto a estructura, pero para determinar su completa validez legal debe comprobar además la validez de los certificados usados. Para ello, puede validar esta u otras firmas electrónicas en: <https://valide.redsara.es/>.

Fichero firmado:  
 D:\Users\paula\Downloads\PAI-2-Seguridad\_signed.pdf [Ver fichero](#)

Certificado de firma utilizado:  
 Titular del certificado: POLEY CEBALLOS PAULA - [REDACTED]. Emisor del certificado: **AC FNMT Usuarios**

Datos de la firma:  
▼ Formato de firma  
Adobe PDF  
▼ Datos firmados  
[Ver datos firmados](#)  
▼ Árbol de firmas del documento  
POLEY CEBALLOS PAULA - [REDACTED]

[Firmar más ficheros](#)

Se ha guardado correctamente, y podemos ver como se ha firmado en la siguiente captura.



### b) Visualizar firma

Al darle a “Visualizar firma” podemos generar informes en los que se mostrará información de la firma o firmas asociadas al documento . Nos muestra la siguiente captura, en la cual elegiremos el archivo e introduciremos el código de seguridad.

Al darle a “Visualizar” nos muestra la siguiente página. En la parte izquierda inferior del documento firmado podemos ver que pone por quien está firmado y firma válida.

### c) Validar Certificado

Le damos a “Validar Certificado” y podemos comprobar en línea la validez de este el cual ha podido ser emitido por cualquier entidad de servicio de certificación reconocida. Seleccionamos el certificado que queremos comprobar (subrayado en amarillo) y el código de seguridad.

The screenshot shows the VALIDe website interface. On the left, there's a sidebar with links: 'Validar Certificado' (selected), 'Realizar firma', 'Validar Firma', 'Validar Sede Electrónica', 'Visualizar Firma', and 'FAQs'. The main content area has a title 'Validar Certificado' with a sub-instruction: 'Puedes comprobar la validez de un certificado digital emitido por un prestador de servicios de certificación reconocida.' Below this is a step-by-step process:

1. Selección tu certificado: A red box highlights the text 'Ha seleccionado un certificado del almacén de claves del navegador'.
2. Introduce el código de seguridad: A red box highlights the input field containing '6m6g?'. A red arrow points to this field from the left.

At the bottom, there's a note about supported certificates and a 'Nota' section. The footer includes logos for the European Union and various Spanish government entities, along with links for accessibility, map, requirements, and usage conditions.

Al darle a “Validar” vemos que nos sale que el certificado es válido. Si le damos a “Ver información ampliada” podemos ver que sale ID emisor, ID política, país, asunto, tipo de certificado.....

The screenshot shows the 'Resultado de Validar Certificado' page. It displays a green checkmark icon and the text 'Certificado válido'. Below this, it shows the responsible person's information: 'Nombre/Apellid. Responsable: PAULA [REDACTED]' and 'NIF Responsable: [REDACTED]'. A red box highlights the 'Ver información ampliada' button. The footer is identical to the previous screenshot, featuring EU and Spanish government logos and links for accessibility, map, requirements, and usage conditions.



Ministerio de Sanidad, Consumo VALIDe https://valide.redsara.es/valide/verDetalleCertificado/ejecutar.html

Resultado de Validar Certificado

Certificado válido

Nombre / Apellido. Responsable: PAULA [REDACTED]

\*\* Información del certificado

Apellidos del responsable: [REDACTED]  
Clasificación: 0  
Extensión del uso del certificado: KeyPurposeId 0: E-mail protection KeyPurposeId 1: TLS Web client authentication  
ID Emisor: CN=AC FNMT Usuarios,OU=Ceres,O=FNMT-RCM,C=ES  
ID Política: MITC  
NIF Responsable: [REDACTED]  
Nombre/Apellido. Responsable: PAULA [REDACTED]  
Nombre del responsable: PAULA  
Número de serie: [REDACTED]  
Organización emisora: FNRT-RCM  
País: ES  
Política: 1.3.6.1.4.1.5734.3.10.1.0-4.0.194112.1.0  
Primer apellido del responsable: [REDACTED]  
Segundo apellido del responsable: [REDACTED]  
Asunto: CN=[REDACTED] PAULA - [REDACTED] SN=[REDACTED] givenName=PAULA serialNumber=IDCES-[REDACTED] C=ES  
Tipo de certificado: FNMT PF SW EIDAS - SHA256  
Uso del certificado: digitalSignature | nonRepudiation | keyEncipherment  
Válido desde: 2020-10-29 jue 12:24:56 +0100  
Válido hasta: 2024-10-29 mar 12:24:56 +0100  
Versión política: 23

Observaciones: El certificado es válido, incluyendo su estado de revocación  
Hora de Consulta: 08-jun-2022 10:55:28 AM GMT+0200

Nota: Los certificados soportados por el sistema son aquellos admitidos por el Ministerio de Industria, Energía y Turismo. Se pueden consultar los certificados admitidos revisando el documento Certificados admitidos por la plataforma @firma. Si tu certificado no se valida correctamente, pero sí se encuentra entre los recogidos en la Plataforma del Ministerio de Industria, puedes ponerte en contacto con el servicio de soporte.

#### d) Validar firma

Para ver la validez de un documento firmado electrónicamente con múltiples formatos y tipos de certificados, como facturas electrónicas, contratos....etc le damos a “Validar firma”.

Ministerio de Sanidad, Consumo VALIDe https://valide.redsara.es/valide/ejecutarValidarFirma/ejecutar.html

Bienvenido | Bienvegit | Ongi etorri | Benvido | Welcome | Contactar | GOBIERNO DE ESPAÑA

Validar Certificado

Realizar firma

Validar Firma

Validar Sede Electrónica

Visualizar Firma

Faqs

Validar Firma

Puedes comprobar la validez de una firma digital utilizando para ello la plataforma @firma.

1. Selecciona la firma a validar

Elegir archivo: PAI-2-Seguridad\_signed.pdf

Tamaño máximo de fichero admitido (8 MBs)

2. Introduce el código de seguridad

Escribe el código de seguridad: 41389

Validar

AVANT EUROPA PROYECTO FINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL. Un futuro de Europa

W3C XHTML 1.0 WCAG 2.0 ARIA 1.0

Accesibilidad | Mapa Web | Requisitos | Condiciones de Uso

Cuando le damos a “Validar” vemos como nos sale que la firma es válida y te dice quienes han sido los firmantes del documento. Se puede descargar el justificante además de ver más detalles.



The screenshot shows the VALIDe website interface. On the left, there's a sidebar with links: 'Validar Certificado', 'Realizar firma', 'Validar Firma', 'Validar Sede Electrónica', 'Visualizar Firma', and 'FAQs'. The main content area has a title 'Resultado de Validar Firma' with a green checkmark icon and the text 'Firma válida'. Below it, it says 'Firmantes:' followed by a list with 'PAULA'. A red button labeled 'Descargar Justificante' is present. At the bottom, there's a note about supported signatures and links to 'Nota', 'Ver el detalle de la validación', and 'Descargar justificante'. The footer includes the European Union flag, W3C compliance icons (WAI-ARIA, CSS, XHTML), and links to 'Accesibilidad', 'Mapa Web', 'Requisitos', and 'Condiciones de Uso'.

## e) Validar Sede Electrónica

Por último podemos comprobar las URLs de sede electrónicas, verificando la validez del certificado que contienen. Le damos a “Validar Sede Electrónica”. Por ejemplo vamos a comprobar la URL de la universidad.

The screenshot shows the 'Validar Sede Electrónica' section of the VALIDe website. The sidebar on the left remains the same. The main area has a title 'Validar Sede Electrónica' with a note: 'Puedes comprobar la validez de una sede electrónica (web pública segura) introduciendo la dirección de la página.' It contains two steps: '1. Escribe la URL a validar' with a text input containing 'https://www.informatica.us.es/' and '2. Introduce el código de seguridad' with a CAPTCHA box showing 'n6bfm' and a text input also containing 'n6bfm'. There are buttons for 'Escribir el código de seguridad', a speaker icon for audio verification, and a refresh/circular arrow icon. A red 'Validar' button is at the bottom. A note at the bottom of the form says: 'NOTA: En el siguiente enlace puedes encontrar una lista de las sedes correspondientes a la Lista de Certificados de Sede.' The footer includes the European Union flag, W3C compliance icons, and links to 'Accesibilidad', 'Mapa Web', 'Requisitos', and 'Condiciones de Uso'.



Ministerio de Sanidad, Consumo | VALIDe | Página inicial | Servicio Andaluz | No sincronizando



VALIDe

Contactar  
Bienvenido | Benvingut | Ongi etori | Benvido | Welcome



Validar Certificado

Realizar firma

Validar Firma

Validar Sede Electrónica

Visualizar Firma

Faqs

**Validar Sede Electrónica**

Puedes comprobar la validez de una sede electrónica (web pública segura) introduciendo la dirección de la página.

1. Escribe la URL a validar

2. Introduce el código de seguridad

Escribe el código de seguridad

**Validar**



UNIÓN EUROPEA  
PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE  
DESARROLLO REGIONAL (FEDER)  
Una manera de hacer Europa

W3C URI HTML

W3C CSS

W3C XHTML 1.0

Accesibilidad | Mapa Web | Requisitos | Condiciones de Uso

- Verificación de documentos con CSV

Si le damos a “Verificación de documentos con CSV” podemos consultar la verificación de la integridad y autenticidad de documentos electrónicos a través de su código seguro de verificación (CSV).





# INGENIERÍA DE SEGURIDAD US

Avda Reina Mercedes s/n. 41012 Sevilla



The screenshot shows the 'Sede Electrónica' website with a sidebar containing links like 'Sobre la Sede', 'Trámite', 'Estado de mi solicitud', 'Registro electrónico', 'Notificaciones electrónicas', 'Tasas', 'Servicios', and a button for 'Solicita el Certificado COVID Digital de la UE'. The main content area is titled 'Verificación de documentos con CSV' and includes instructions about CSV verification. A form field is shown with the placeholder 'CSV: NC82X-X3KX2-PQF5S-WFFWJ' and a note 'Campo obligatorio'. A 'Consultar' button is at the bottom right.

Al introducir el código seguro de verificación que aparece en el margen izquierdo del documento (subrayado de amarillo) y dándole a "Consultar" nos muestra la siguiente pantalla en la cual podemos descargarnos el documento original y el documento firmado .

The screenshot shows the same 'Sede Electrónica' website after a successful CSV verification. The main content area displays a summary of the document: 'Documento firmado por SELLO ELECTRONICO MINISTERIO DE SANIDAD SERV SOCIALES E IGUALDAD', 'Este documento se ha almacenado en el MSSSI (https://sede.msssi.gob.es'). Código Seguro de Verificación: NC82X-X3KX2-PQF5S-WFFWJ. INTERNO. Fecha de firma [REDACTED]', and 'El documento consta de un total de 1 folios.' Below this, a table shows a single file entry: 'Nombre: lorem\_ipsum.pdf' with 'Acciones' showing 'Descargar original' and 'Descargar firmado'.

- **Verificación de documentos firmados digitalmente**
- Por último le daremos a “Verificación de documentos firmados digitalmente”.



Con esto consultamos la verificación de la firma digital del documento que haya sido firmado digitalmente usando el documento original (PAI-2-Seguridad.pdf) y/o el documento resultante de la firma digital (PAI-2-Seguridad\_signed.pdf). También simplemente podría seleccionar el fichero resultante de la firma digital (este es de obligatorio cumplimiento) y dejar en blanco el Documento original antes de la firma que nos saldría lo mismo que veremos a continuación.

Le damos a “Validar” y vemos como la firma es válida del documento firmado digitalmente. En la siguiente captura podemos ver más detalles de la verificación.



Ministerio de Sanidad, Consumo

https://sede.mscbs.gob.es/verificacionFirma/home.do?metodo=consultar

Sobre la Sede  
Trámite  
Estado de mi solicitud  
Registro electrónico  
Notificaciones electrónicas  
Tasas  
Servicios

Solicita el Certificado COVID Digital de la UE

datos abiertos

Utilidades  
Verificación de certificados  
Verificación de documentos con CSV  
Verificación de documentos firmados digitalmente

Inicio > Verificación de documentos firmados digitalmente

Verificación de documentos firmados digitalmente

La firma es válida

Firmante:

PAULA [REDACTED]  Ocultar Detalle de la validación

Información básica de la firma  Nivel de firma: PAdES\_B

NIF: [REDACTED]

Fecha de la firma: 08/06/2022 10:36:46

Fecha de la validación: 08/06/2022 11:35:13

Información del certificado  Apellidos del responsable: PAULA [REDACTED]  
 Nombre del responsable: PAULA

Email:  
 Emisor: CN=AC FNMT Usuarios, OU=Ceres, O=FNMT-RCM, C=ES  
 Asunto: CN=PAULA-[REDACTED] SURNAM=[REDACTED] GIVENNAME=PAULA, SERIALNUMBER=IDCES-[REDACTED], C=ES  
 Válido desde: 29/10/2020 12:24:56  
 Válido hasta: 29/10/2024 12:24:56

Enviar

Por último firmaremos el informe del PAI-2 (este mismo documento) siguiendo los pasos descritos en el apartado a) de este Workpackage . Realizamos la firma con la aplicación de escritorio llamada AutoFirma.