



Pràctica: Instal·lació, firma i validació mitjançant un certificat electrònic

L'objectiu d'aquesta pràctica és veure com s'instal·la un certificat electrònic en un ordinador personal, analitzar la informació que conté i realitzar una prova de firma i validació d'un document pdf.

Exercici 1: Instal·lació d'un certificat electrònic a l'ordinador

1.1. Descarrega el certificat `ACTIVO_EIDAS_CERTIFICADO_PRUEBAS___99999999R.p12`.

1.2. Fes doble clic sobre ell i instal·la el certificat a l'ordinador. En un entorn Windows s'engegarà un assistent per la importació de certificats

← Asistente para importar certificados

Este es el Asistente para importar certificados

Este asistente lo ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde su disco a un almacén de certificados.

Un certificado, que lo emite una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.

Ubicación del almacén

☒ Usuario actual

☐ Equipo local

Haga clic en Siguiente para continuar.

Siguiente Cancelar

El password és: 1234

← 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:

12345

☒ 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.

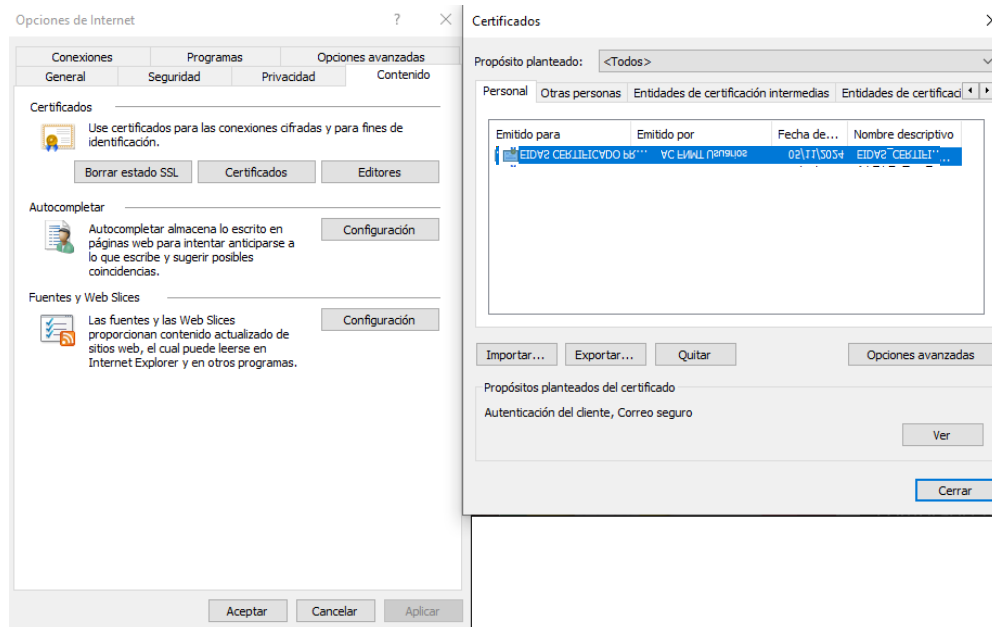
☐ Proteger la clave privada mediante security(Non-exportable) basada en virtualizado

☒ Incluir todas las propiedades extendidas.

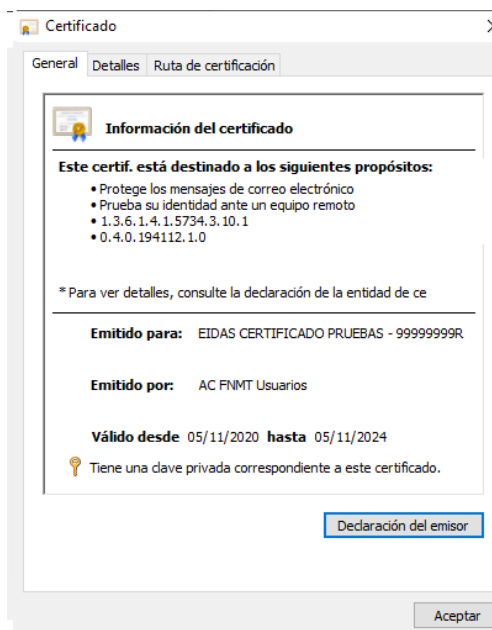
Siguiente Cancelar



1.3. Obre l'explorador Internet Explorer i ves al menú Herramientas → Opciones de internet i selecciona la pipella de Contenidos. Allà veuràs un botó que diu Certificados. Si hi fas clic veuràs els certificats que hi ha instal·lats.



1.4. Localitza el certificat que acabes d'instal·lar i comprova les dades que conté (Nom, DNI, ús del certificat, jerarquia d'autoritats de certificació,...)



Exercici 2: Signar un document pdf utilitzant l'aplicació d'Autofirma

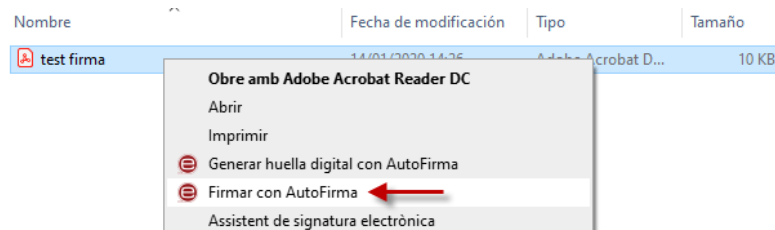


2.1. Autofirma és aplicació gratuïta del Ministeri d'Hisenda i Administracions Públiques que permet a un usuari signar qualsevol tipus de document de manera senzilla. Podeu descarregar-la des del següent enllaç: <https://firmaelectronica.gob.es/Home/Descargas.html>.

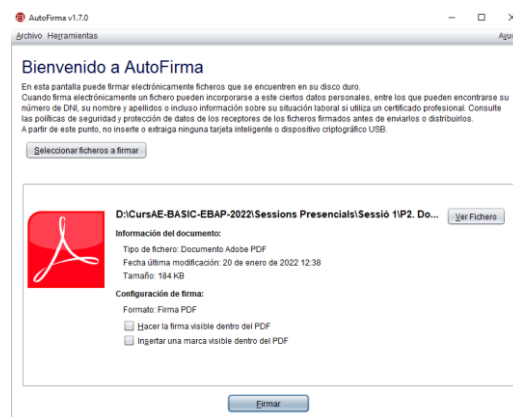
En el nostre cas l'aplicació **ja està instal·lada** a tots els ordinadors de l'EBAP.

2.2. Descarrega el document test_firma.pdf

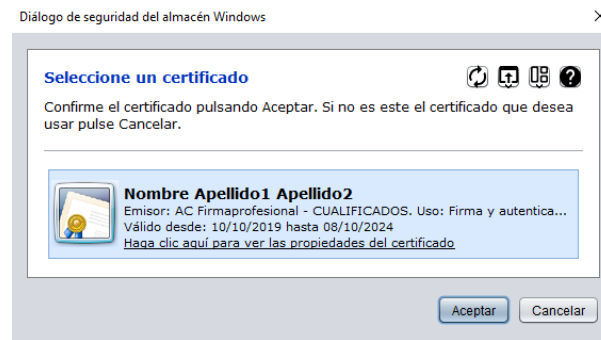
2.3. Clica amb el botó dret del ratolí sobre el document i selecciona "Firmar con AutoFirma"



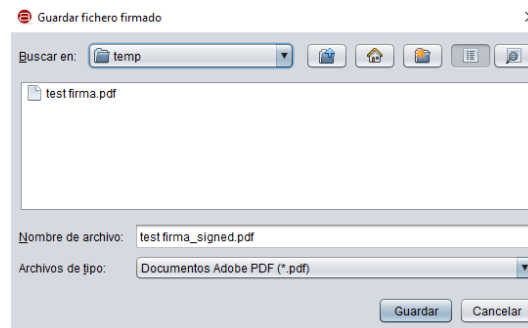
2.4. Això t'obrirà un assistent que et sol·licitarà signar el document. Clica a "Firmar".



2.5. Això t'obrirà un assistent que et sol·licitarà signar el document. Clica a "Firmar" i selecciona el certificat amb el que vols signar el document.



2.6 Selecciona la carpeta on vols guardar el document signat



Exercici 3: Validació de la signatura de documents

3.1 Finalment, comprovarem la validesa de la signatura del document que acabem de firmar. Per això utilitzarem el servei de validació Valide, disponible a <https://valide.redsara.es/valide/>



Pràctica Instal·lació d'un certificat electrònic



The screenshot shows the VALIDe website interface. At the top, there's a header with the 'gob.es' logo, the 'VALIDe' logo, and navigation links: 'Bienvenido | Benvingut | Ongeietorri | Benvido | Welcome'. There's also a 'Contactar' link and a 'GOBIERNO DE ESPAÑA' logo. A 'Selecciona idioma' button is present. The main content area is divided into several sections: 'Validar Certificado' (with a description and a 'Validar Certificado' button), 'Realizar Firma' (with a description and a 'Realizar firma' button), 'Visualizar Firma' (with a description and a 'Visualizar Firma' button), 'Validar Firma' (with a description and a 'Validar Firma' button), and 'Validar Sede Electrónica' (with a description and a 'Validar Sede Electrónica' button). On the right, there's a 'Preguntas Frecuentes' section with several questions and a 'Ver más' link. At the bottom right, there's a 'Portal de Firma electrónica' button. A small disclaimer at the bottom states: 'En cumplimiento con la LOPD LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL y reglamentos de desarrollo posteriores, todos los datos de carácter personal asociados a las firmas y certificados electrónicos que sean enviados por los usuarios, serán usados exclusivamente con fines de validación y serán eliminados de los registros temporales de VALIDe una vez realizadas las operaciones de validación correspondientes. LOPD LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL y reglamentos de desarrollo posteriores, todos los datos de carácter personal asociados a las firmas y certificados electrónicos que sean enviados por los usuarios, serán usados exclusivamente con fines de validación y serán eliminados de los registros temporales de VALIDe una vez realizadas las operaciones de validación correspondientes.'

3.2. Seleccionem l'opció "Validar Firma", triem el document que acabem de signar, introduïm el codi de seguretat proposat i clicam el botó "Validar"



The screenshot shows the 'Validar Firma' page on the VALIDe website. The page has a sidebar with links: 'Validar Certificado', 'Realizar firma', 'Validar Firma', 'Validar Sede Electrónica', 'Visualizar Firma', and 'Faqs'. The main content area is titled 'Validar Firma' and includes the text: 'Puedes comprobar la validez de una firma digital utilizando para ello la plataforma @firma.' Below this, there are two steps: 1. 'Selecciona la firma a validar' with a 'Seleccionar archivo' button and a text input field containing 'test firma_signed.pdf'. A note below says 'Tamaño máximo de fichero admitido (8 MBs)'. 2. 'Introduce el código de seguridad' with a visual security code 'y2xam' and a text input field containing 'y2xam'. A red 'Validar' button is at the bottom. A disclaimer at the bottom states: 'Nota: Las firmas soportadas por el sistema son aquellas que han sido realizadas con los certificados 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 firma no se valida correctamente, porque se indica certificado no soportado, pero tu certificado si se encuentra entre los recogidos en la Página del Ministerio de Industria te rogamos te pongas en contacto con el servicio de soporte.'



3.3. El servei ens proporcionarà el resultat del procés de validació de la firma, que en aquest cas serà vàlida. Fixau-vos en la informació proporcionada per l'opció "Detalle de la validación"

Validar Certificado
Realizar firma
Validar Firma
Validar Sede Electrónica
Visualizar Firma
Faqs

 **Resultado de Validar Firma**

 **Firma válida**

Firmantes:

- Nombre Apellido1 Apellido2

[Descargar Justificante](#)

Detalle de la validación

- Formato de firma detectado:** PAdES B-Level
- Firmantes**
 - Apellidos del responsable:** Apellido1 Apellido2
 - Clasificación:** 0
 - Email:** info@firmaprofesional.com
 - Extensión del uso del certificado:** KeyPurposeId 0: TLS Web client authentication
KeyPurposeId 1: E-mail protection
 - ID Emisor:** CN=AC Firmaprofesional - CUALIFICADOS,serialNumber=A62634068,OU=Certificados Cualificados,O=Firmaprofesional S.A.,C=ES
 - ID Política:** MITyC
 - NIF Responsable:** 99999999R
 - Nombre/Apellid. Responsable:** Nombre Apellido1 Apellido2
 - Nombre del responsable:** Nombre
 - Número de serie:** 160918539356026883184872562364949713765
 - Organización emisora:** Firmaprofesional S.A.
 - País:** ES
 - Política:** 1.3.6.1.4.1.13177.10.1.40.2.0.4.0.194112.1.0
 - Primer apellido del responsable:** Apellido1
 - Segundo apellido del responsable:** Apellido2
 - Asunto:** CN=Nombre Apellido1 Apellido2,serialNumber=IDCES-99999999R,givenName=Nombre,SN=Apellido1 Apellido2,C=ES
 - Tipo de certificado:** FP PF Certificado Personal
 - Uso del certificado:** digitalSignature | nonRepudiation | keyEncipherment
 - Válido desde:** 2019-10-10 jue 13:54:59 +0200
 - Válido hasta:** 2024-10-08 mar 13:54:59 +0200
 - Versión política:** 23
 - Hora de Consulta:** 20-ene-2022 12:54:01 PM GMT+0100