



Manual de Instalación del Certificado Digital



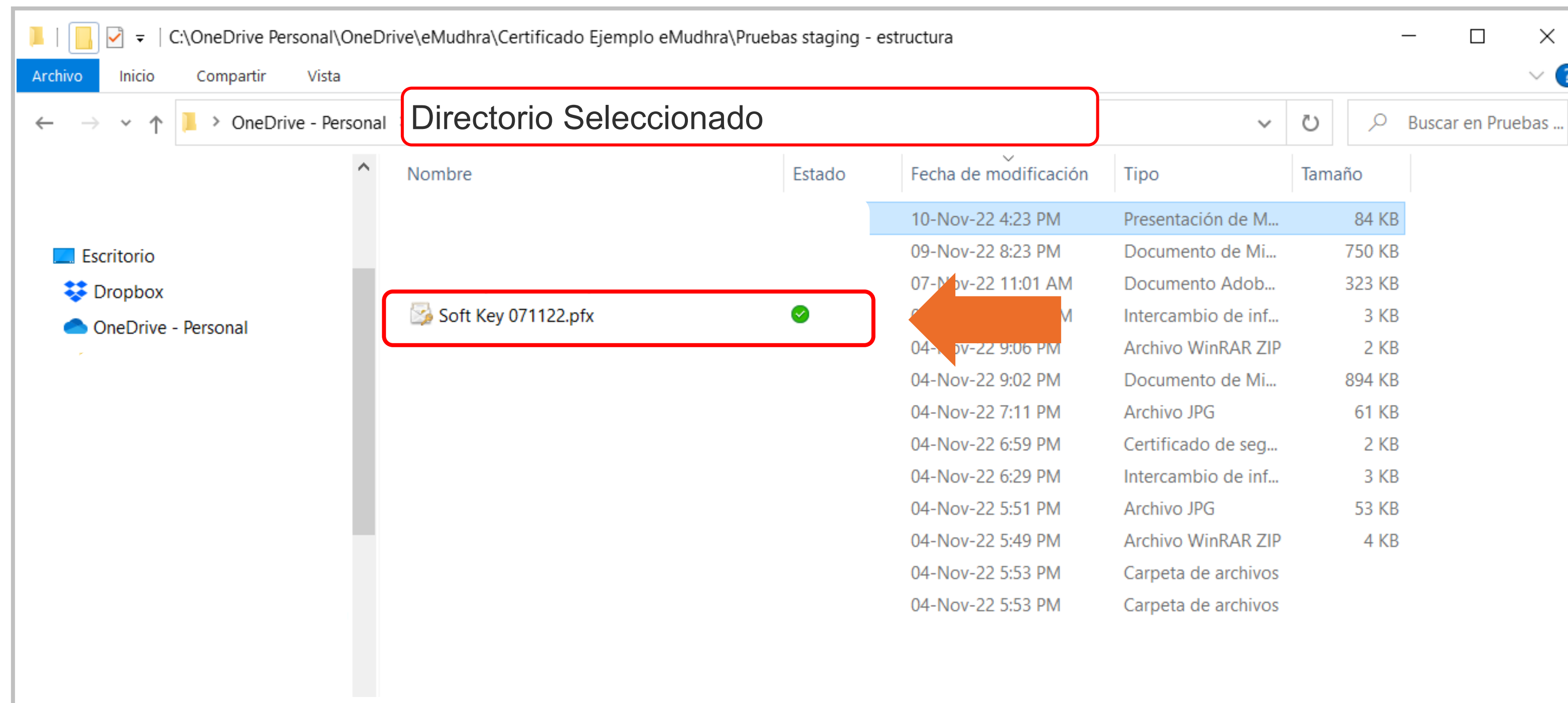
Escoja su Sistema Operativo

Windows

Mac

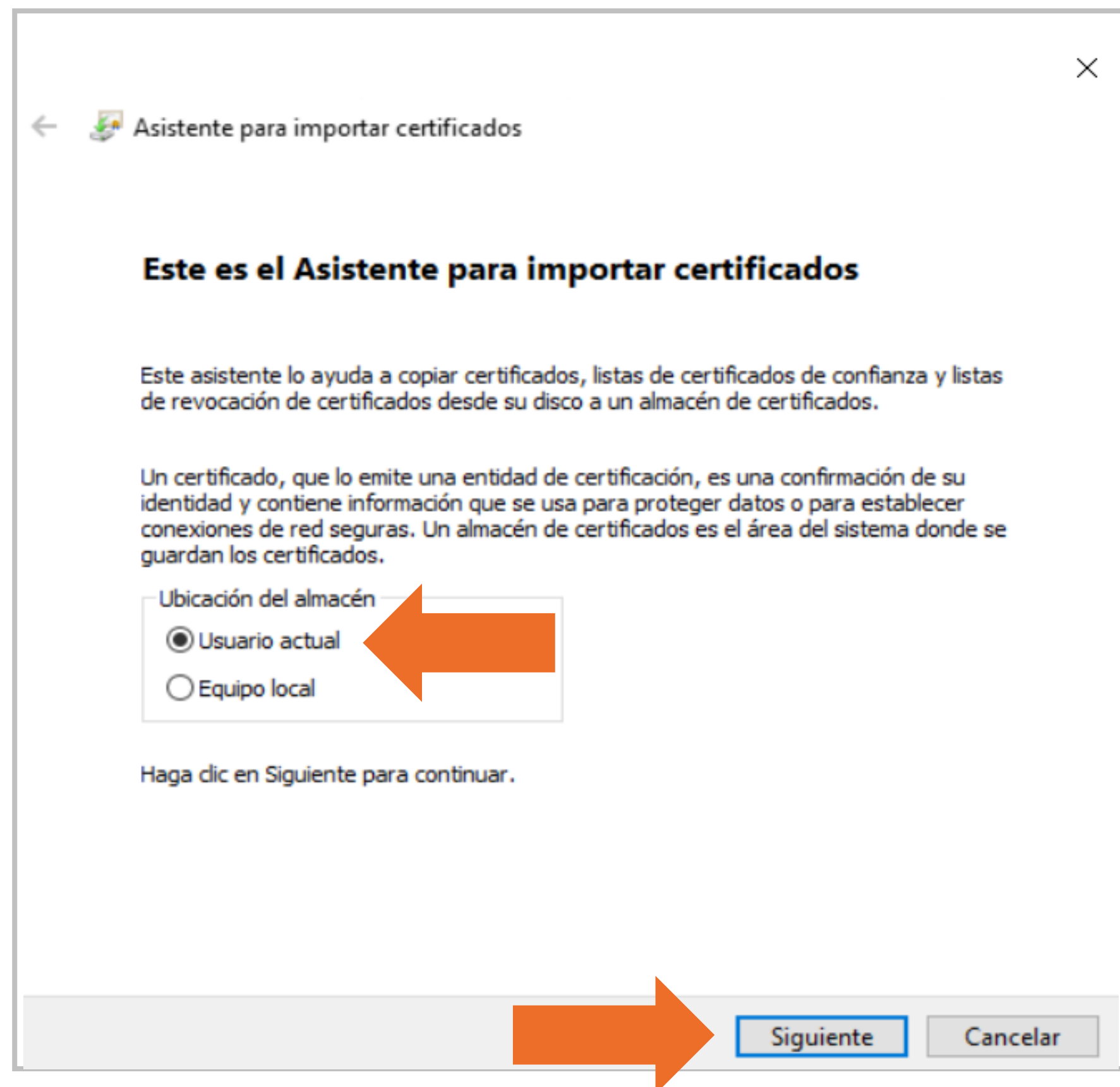
Instalación de Certificado Digital en Windows

1. El primer paso para instalar un certificado electrónico es ubicar el archivo “.pfx” que descargó en el directorio seleccionado al momento de la descarga:

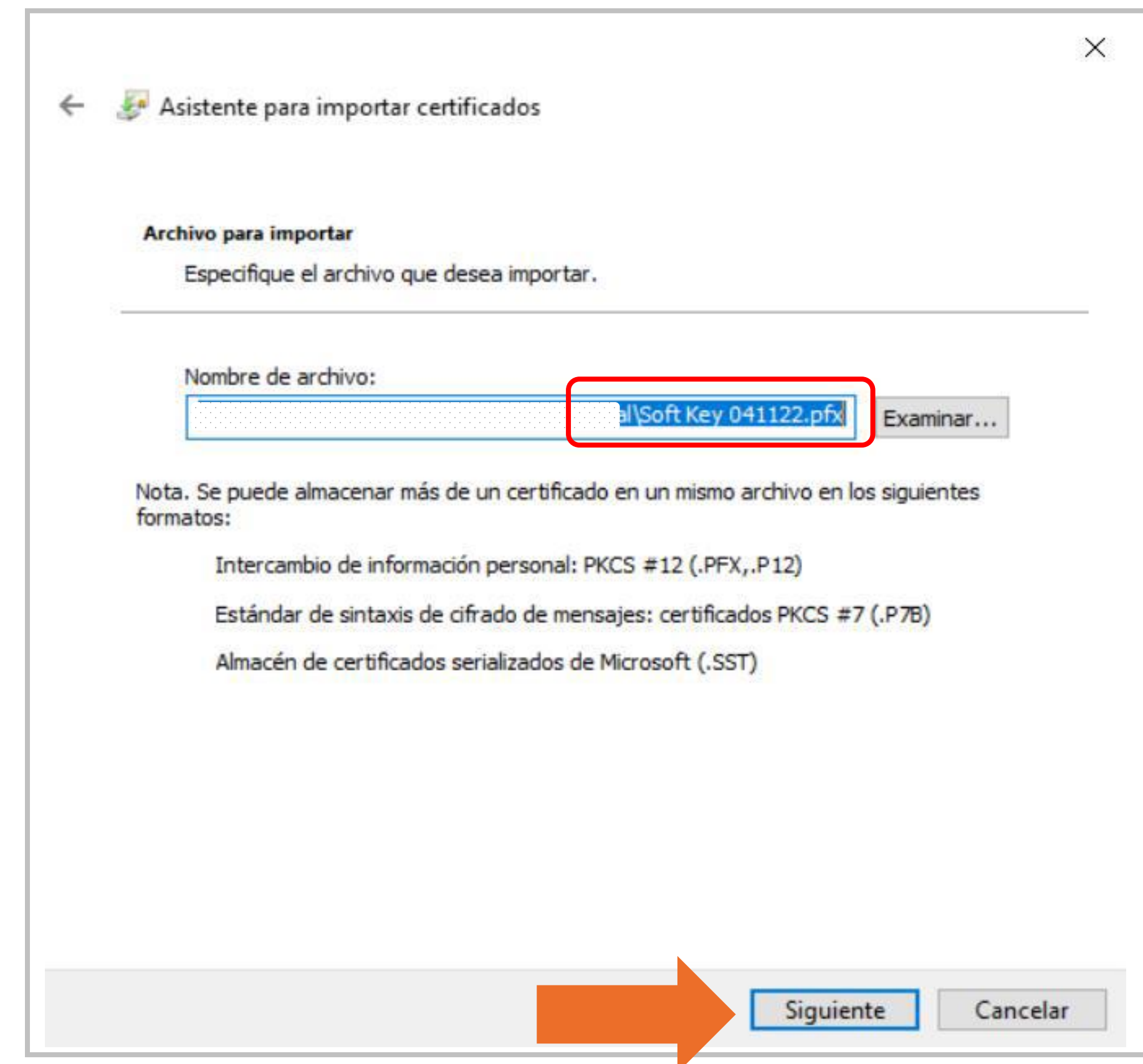


Instalación de Certificado Digital en Windows

2. Haga doble click sobre el archivo del certificado y espere que aparezca la siguiente pantalla:



3. Haga click en Siguiete y espere que aparezca la siguiente ventana:



Instalación de Certificado Digital en Windows

4. Ahora introduzca la contraseña que creó al descargar el certificado y asegúrese que estén marcados los casilleros como se indica en la figura y haga click en Siguiente.

← Asistente para importar certificados

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

Escribe la contraseña para la clave privada.

Contraseña:

☐ Mostrar contraseña

Opciones de importación:

- ☒ Habilitar protección segura de clave privada. Si habilitas esta opción, se te avisará cada vez que una aplicación use la clave privada.
- ☒ Marcar esta clave como exportable. Esto te permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.
- ☐ Proteger la clave privada mediante seguridad basada en virtualización (no exportable)
- ☒ Incluir todas las propiedades extendidas.

Siguiente Cancelar

5. Haga click en Siguiente y espere que aparezca la próxima pantalla:

← Asistente para importar certificados

Almacén de certificados
Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.

Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.

☒ Seleccionar automáticamente el almacén de certificados según el tipo de certificado

☐ Colocar todos los certificados en el siguiente almacén

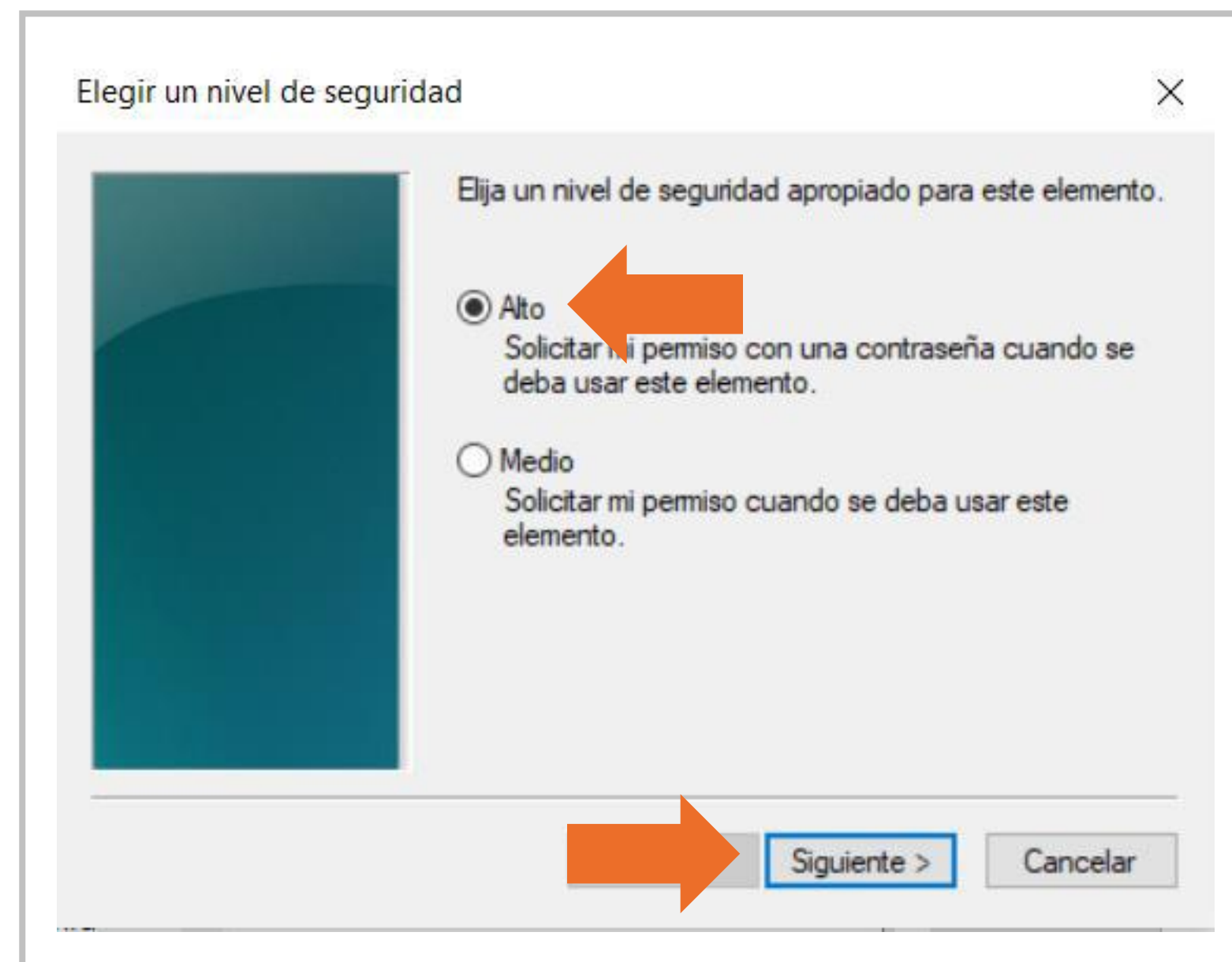
Almacén de certificados: Examinar...

Siguiente Cancelar

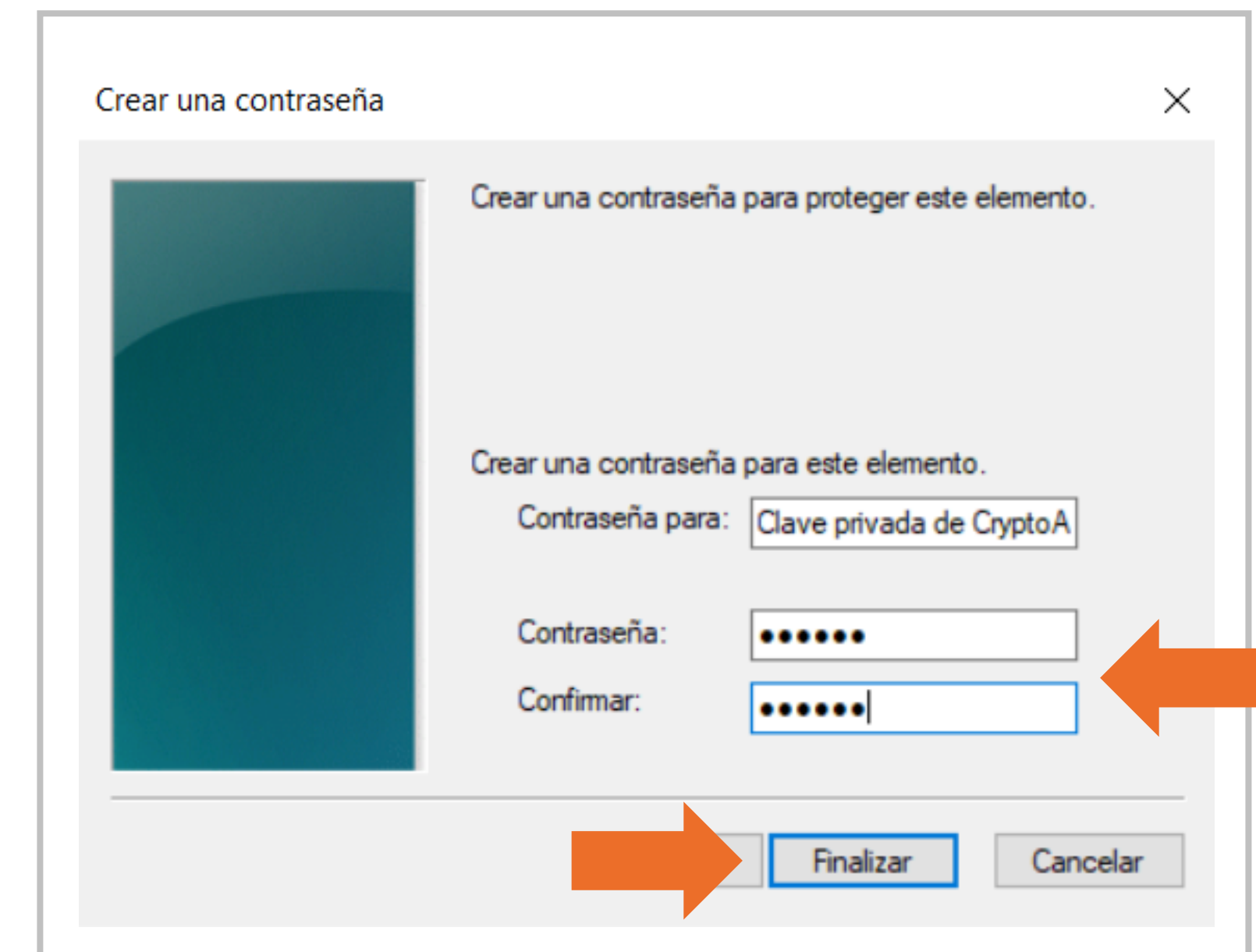


Instalación de Certificado Digital en Windows

8. Asegúrese de marcar el botón Alto, haga click en Siguiente y espere que aparezca la siguiente:



9. Introduzca una clave de seguridad alfanumérica de al menos seis caracteres. Esta clave le será solicitada cada vez que utilice el certificado ya instalado, para firmar (esta clave puede ser la misma del certificado o una distinta especial para firmar documentos). Haga click en Finalizar para terminar la instalación del certificado en su equipo:



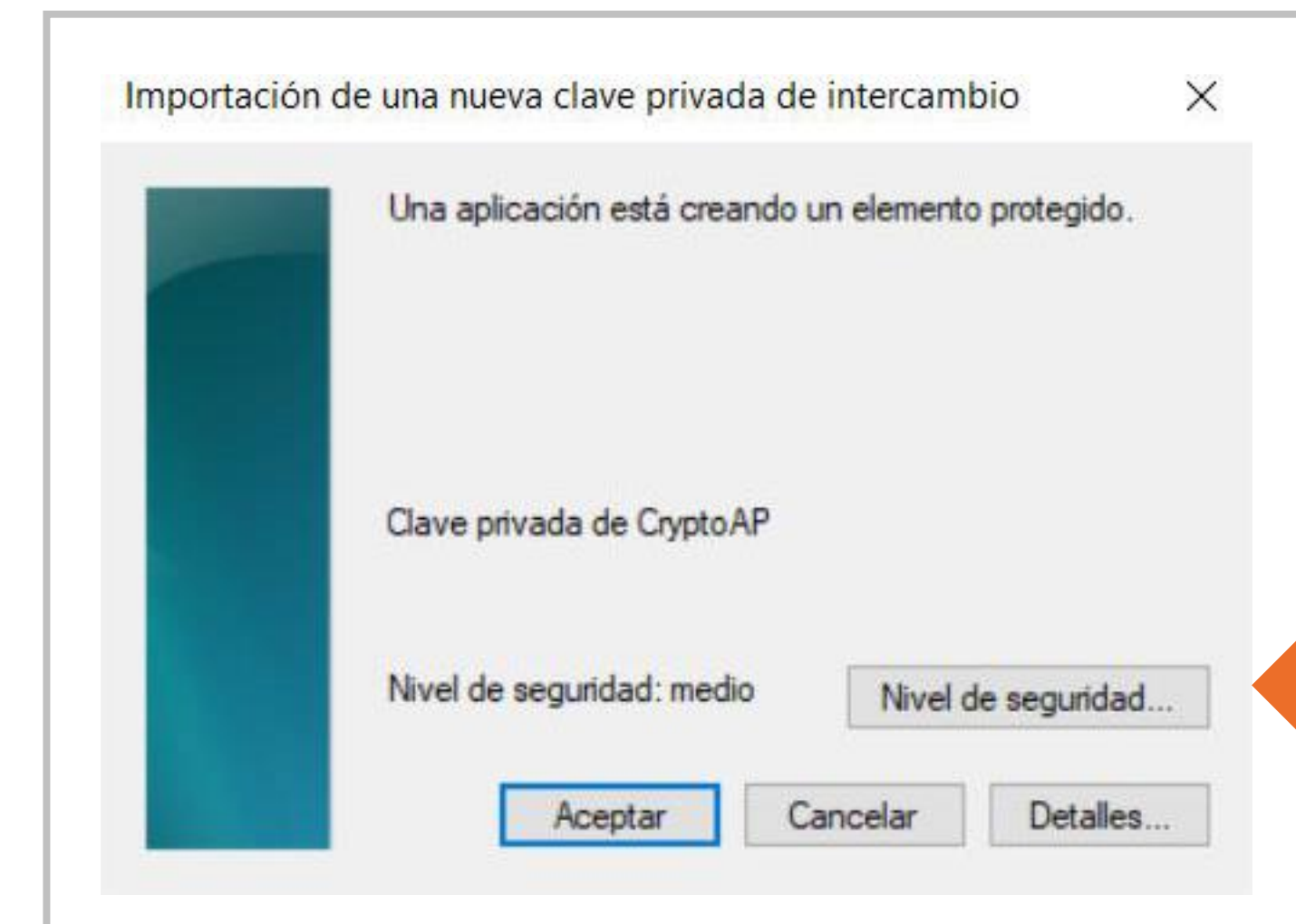
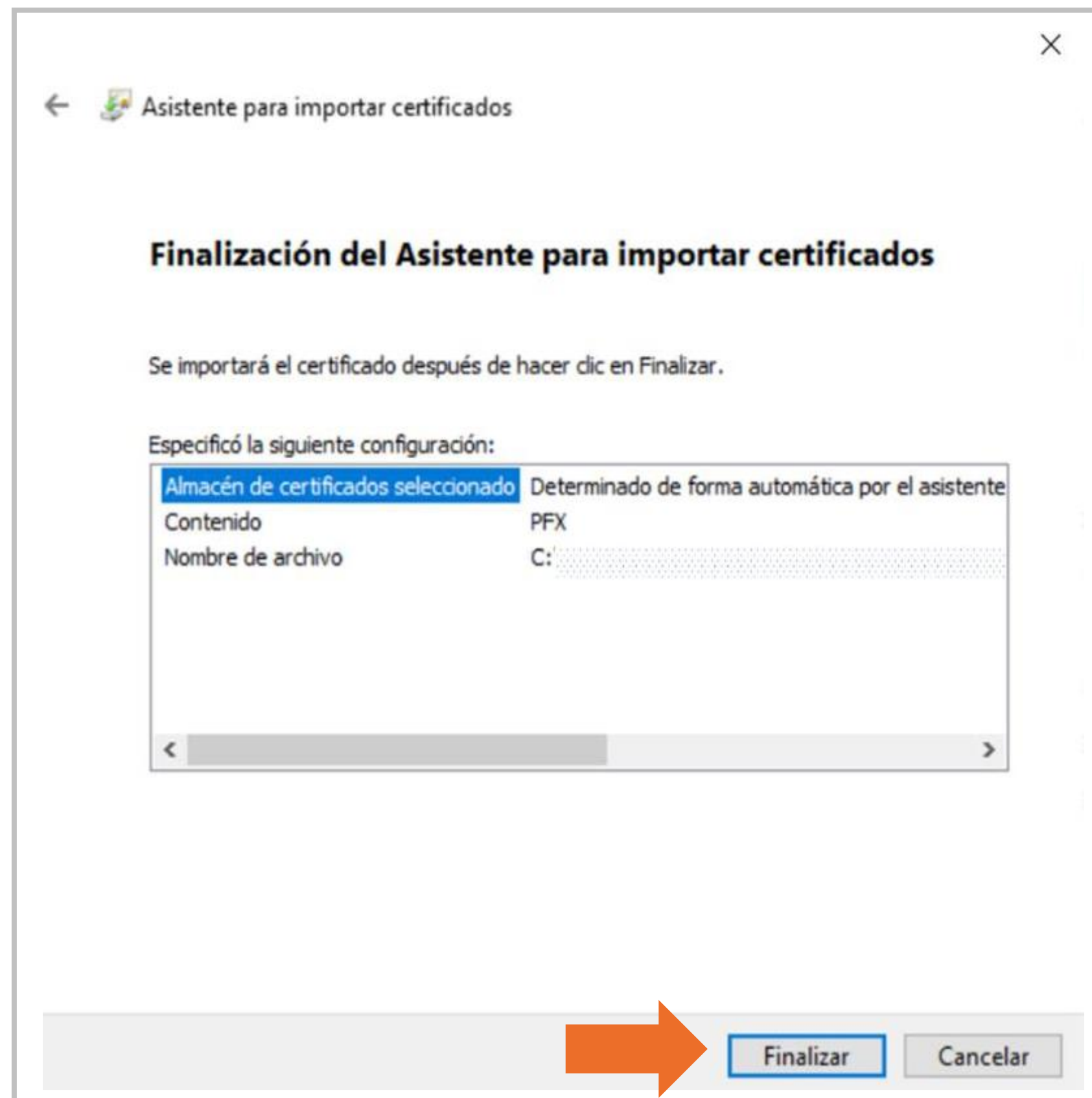
- **Importante:** Sugerimos guardar en un lugar seguro está clave y que sea de fácil recordación para cuando sea solicitada al momento de firmar sus documentos.



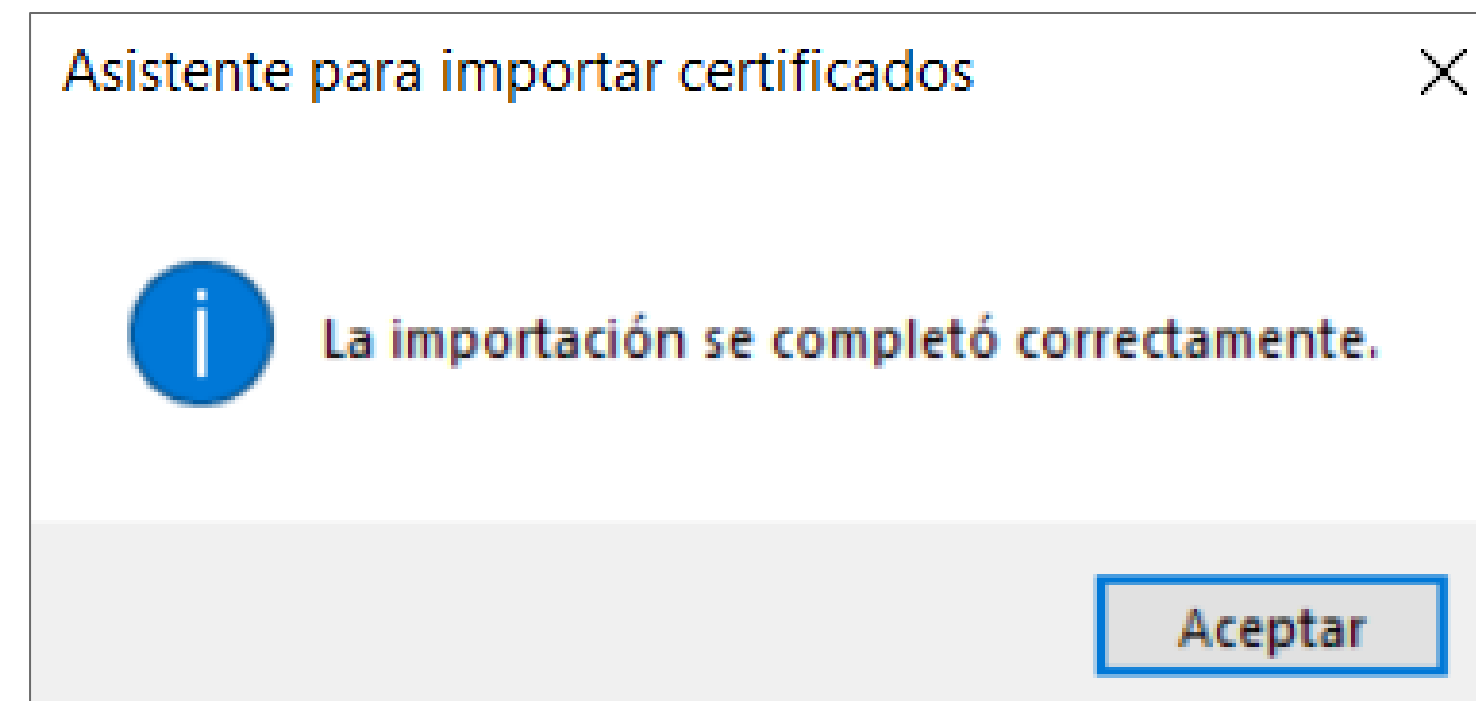
Instalación de Certificado Digital en Windows

6. Haga click en Finalizar y espere que aparezca la próxima pantalla:

7. Haga click en Nivel de Seguridad y espere que aparezca la siguiente pantalla:



Instalación de Certificado Digital en Windows



Cadena de Confianza en Windows

Si su sistema no reconoce de forma automática la cadena de confianza del certificado instalado, siga el siguiente procedimiento:

1. Firme un documento en formato PDF utilizando Adobe Acrobat Reader (ver como firmar un documento PDF). Una vez firmado haga click en la firma y aparecerá el siguiente recuadro debe hacer click en el botón Propiedades de la Firma:

Estado de validación de la firma



La validez de la firma es DESCONOCIDA.

- No ha habido modificaciones en: documento desde que se firmó.
- La identidad del firmante es desconocida porque no se incluyó en su lista de certificados de confianza y ninguno de sus certificados principales son certificados de confianza



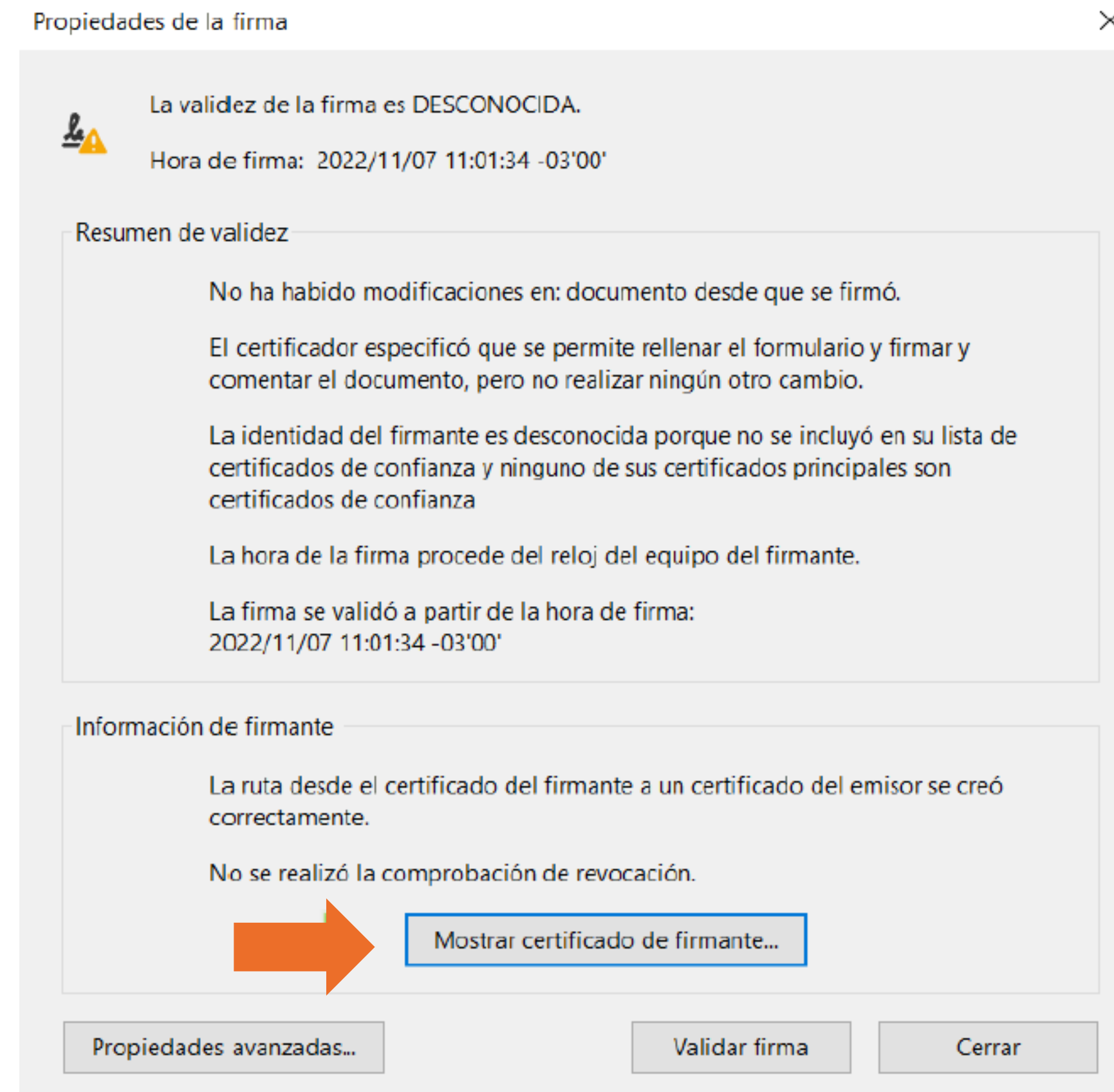
Propiedades de la firma...

Cerrar



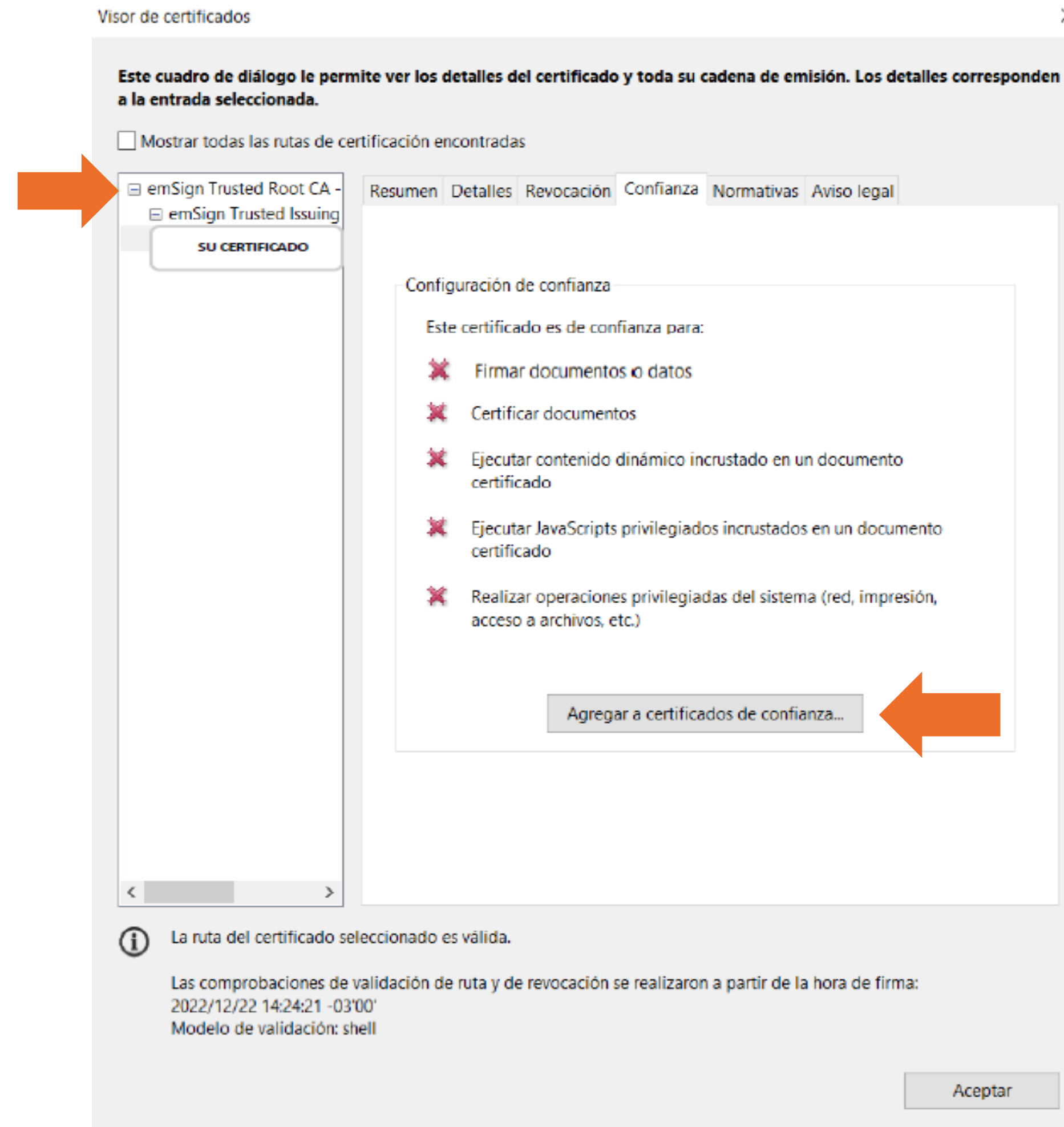
Cadena de Confianza en Windows

2. En el recuadro siguiente haga click en **Mostrar certificado de firmante:**



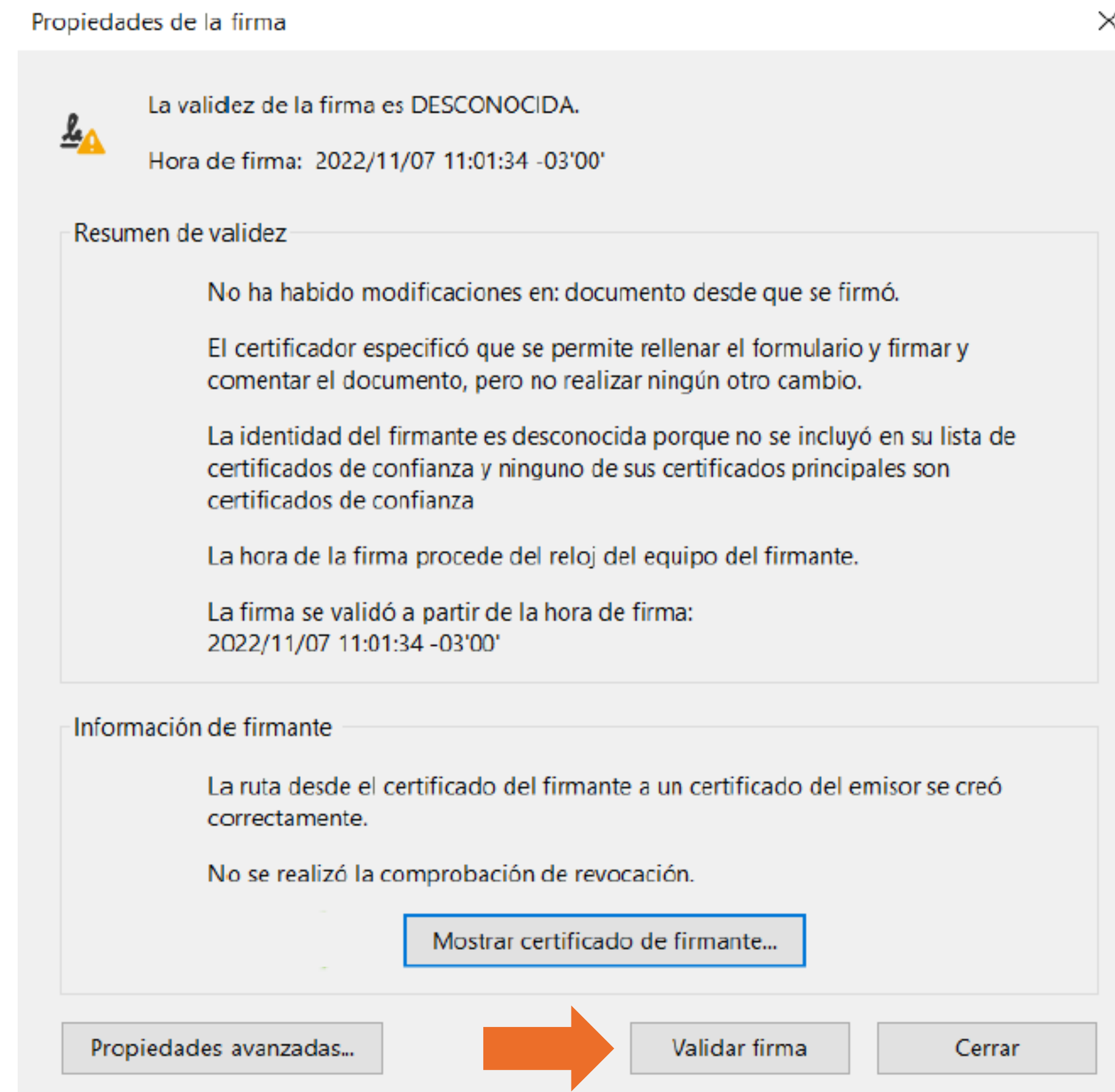
Cadena de Confianza en Windows

3. Haga click en la pestaña Confianza y en el botón **“Agregar a Certificados de Confianza”**. Haga click en Aceptar



Cadena de Confianza en Windows

4. Salga del cuadro de diálogo marcando **Validar Firma** y luego **Cerrar**.
5. Salga del documento Pdf. Con este proceso que se realiza sólo una vez, su firma quedará agregada a los Almacenes de Confianza de Adobe, siendo reconocida en cualquier parte del mundo como válida.



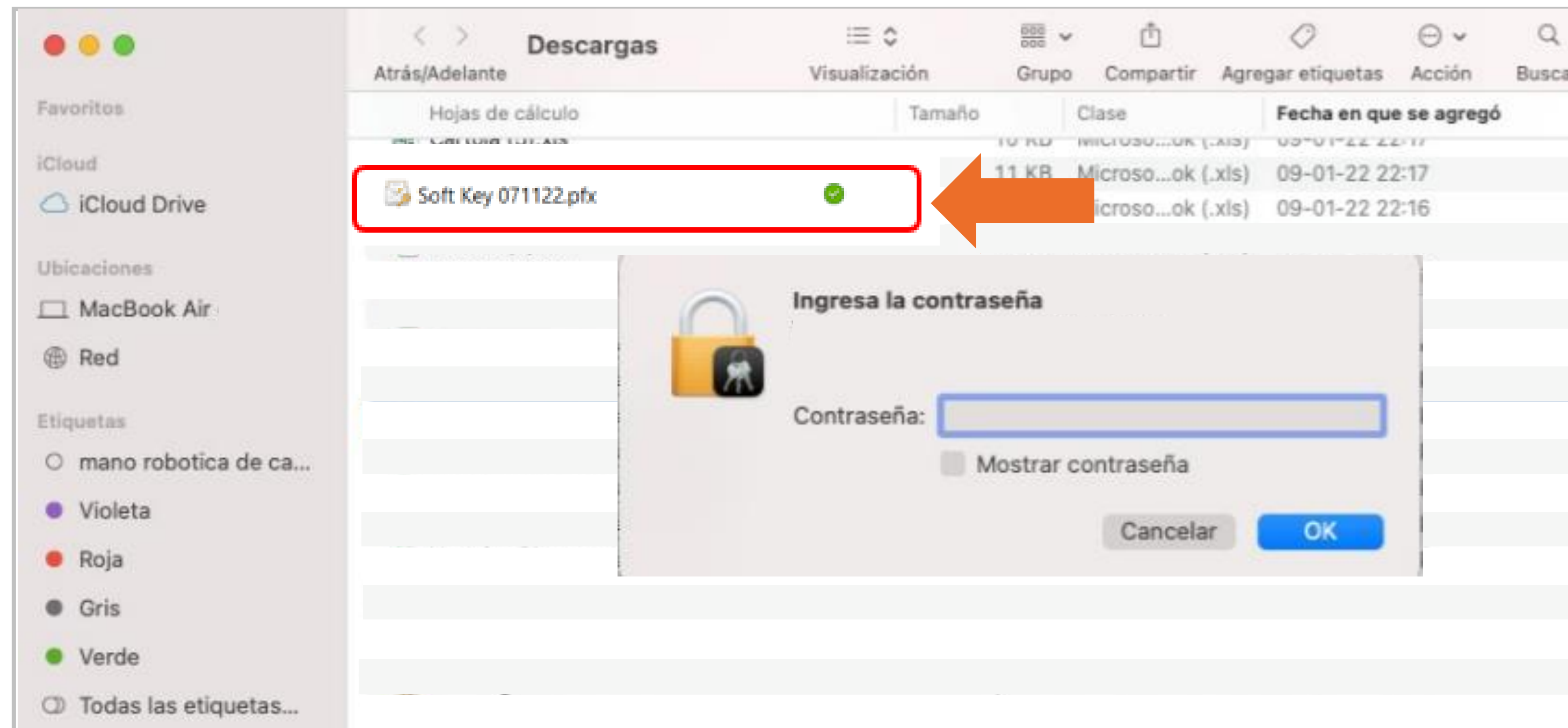
¡Felicitaciones, la instalación se ha realizado exitosamente!

AXERA

El socio regional de  **emudhra**
Trust Delivered

Instalación de Certificado Digital en Mac

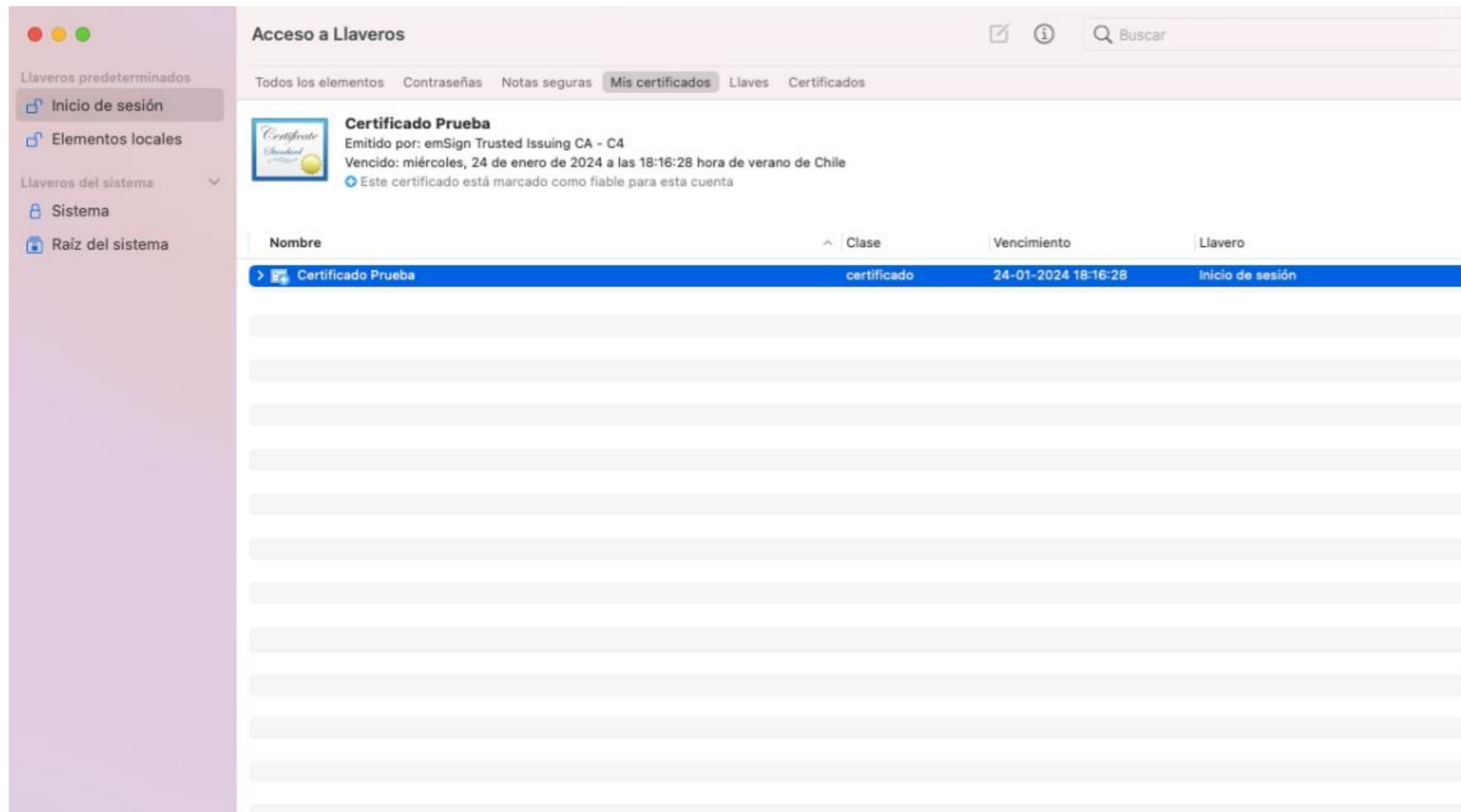
1. El primer paso para instalar un certificado electrónico es ubicar el archivo “.pfx” que descargó en el directorio seleccionado al momento de la descarga. Luego debe dar doble click sobre el archivo, le solicitará la clave del certificado.



Instalación de Certificado Digital en Mac



2. El certificado se agrega a Acceso a Llaveros en Inicio de Sesión – Mis Certificados.



Cadena de Confianza en Mac

1. Por motivos de seguridad inherentes a Equipos Mac toda descarga de certificados se gestiona mediante el **Acceso a Llaveros** y quedan en el estado **“Este certificado raíz no es fiable”**, para su correcta utilización debemos cambiar habilitar la cadena de confianza. Haga click en Confiar.

Llaveros predeterminados

Inicio de sesión

Elementos locales

Llaveros del sistema

Sistema

Raíz del sistema

Acceso a Llaveros

Todos los elementosContraseñasNotas segurasMis certificadosLlavesCertificados

Certificado Prueba

Emitido por: emSign Trusted Issuing CA - C4

Vencido: miércoles, 24 de enero de 2024 a las 18:16:28 hora de verano de Chile

Este certificado raíz no es fiable

Nombre

> Certifi

Nombre

8

Llavero

Inicio de sesión

Karin Torres

Certificado Prueba

Emitido por: emSign Staging Trusted Issuing CA - C4

Vencimiento: viernes, 7 de junio de 2024 a las 13:46:28 hora estándar de Chile

Este certificado raíz no es fiable

> Confiar

> Detalles

Sujeto

País o región

CL

Estado/Provincia

Region Metropolitana de Santiago

Localidad

Providencia

Dirección de correo

karin.torres@bmcpro.net

Empresa

Karin Torres

Nombre común

Karin Torres

Emisor

País o región

US

Empresa

emSign PKI

Nombre común

emSign Staging Trusted Issuing CA - C4

Número de serie

00 CF D0 A3 86 E8 84 B1 8A

Versión

3

Algoritmo de firma

SHA-256 con encriptación RSA (1.2.840.113549.1.1.11)

Parámetros

Ninguno

No válido antes de

miércoles, 7 de junio de 2023 a las 13:46:28 hora estándar de Chile

No válido después de

viernes, 7 de junio de 2024 a las 13:46:28 hora estándar de Chile

Información de la clave pública

Algoritmo

Encriptación RSA (1.2.840.113549.1.1.1)

Parámetros

Ninguno

Clave pública

256 bytes: B0 F6 4A 83 C1 5E 1E 17 ...



Cadena de Confianza en Mac

2. Para cambiar el estado y habilitar la confianza en el certificado debemos escoger la opción **Confiar siempre** al utilizar este certificado, luego se debe presionar en la **X** para cerrar y se solicitará la Contraseña de Inicio de Sesión para autorizar el cambio. Con esto queda habilitada la cadena de confianza del certificado para Mac.

Llaveros predeterminados

Inicio de sesión

Elementos locales

Llaveros del sistema

Sistema

Raíz del sistema

Acceso a Llaveros

Todos los elementosContraseñasNotas segurasMis certificadosLlavesCertificados

Certificado Prueba

Emitido por: emSign Trusted Issuing CA - C4

Vencido: miércoles, 24 de enero de 2024 a las 18:16:28 hora de verano de Chile

Este certificado raíz no es fiable

Nombre

Karin Torres

Certificado Prueba

Emitido por: emSign Staging Trusted Issuing CA - C4

Vencimiento: viernes, 7 de junio de 2024 a las 13:46:28 hora estándar

Este certificado raíz no es fiable

Confiar

Al utilizar este certificado: Confiar siempre

SSL (Secure Sockets Layer) Confiar siempre

Correo seguro (S/MIME) Confiar siempre

Autenticación ampliada (EAP) Confiar siempre

Seguridad IP (IPsec) Confiar siempre

Firma de código Confiar siempre

Impresión de fecha Confiar siempre

Política básica X.509 Confiar siempre

Detalles

Sujeto

País o región

US

Unidad organizativa

emSign PKI

Empresa

eMudhra Inc

Nombre común

emSign Trusted Root CA - C4

Emisor

País o región

US

Unidad organizativa

emSign PKI

Empresa

eMudhra Inc

Nombre común

emSign Trusted Root CA - C4

Número de serie

79 ED 61 33 73 02 CB DB 6A 52

Versión

3

Clave pública

256 bytes: B0 F6 4A 83 C1 5E 1E 17 ...

Estás realizando cambios en tu configuración de confianza para certificados.

Ingresa tu contraseña para permitir esta acción.

Usuario:

Contraseña:

Cancelar

Actualizar configuración

Debes seleccionar la opción de Confiar siempre para poder habilitar el certificado

¡Felicitaciones, la instalación se ha realizado exitosamente!

AXERA

El socio regional de  **emudhra**
Trust Delivered