MANUAL DE INSTALACIÓN DE CERTIFICADOS EN DISPOSITIVOS ANDROID

1. Requisitos

Tener instalado un navegador Chrome en el dispositivo. Si no es el caso se puede instalar accediendo a la tienda Google Play desde el dispositivo.

Desde la tienda de Google Play podrá efectuar la instalación de Google Chrome:

https://play.google.com/store/apps/details?id=com.android.chrome

2. Importación de certificados

A continuación, se detallan dos formas de instalar los certificados en un dispositivo Android. Dependiendo de la versión de Android funcionará una u otra.

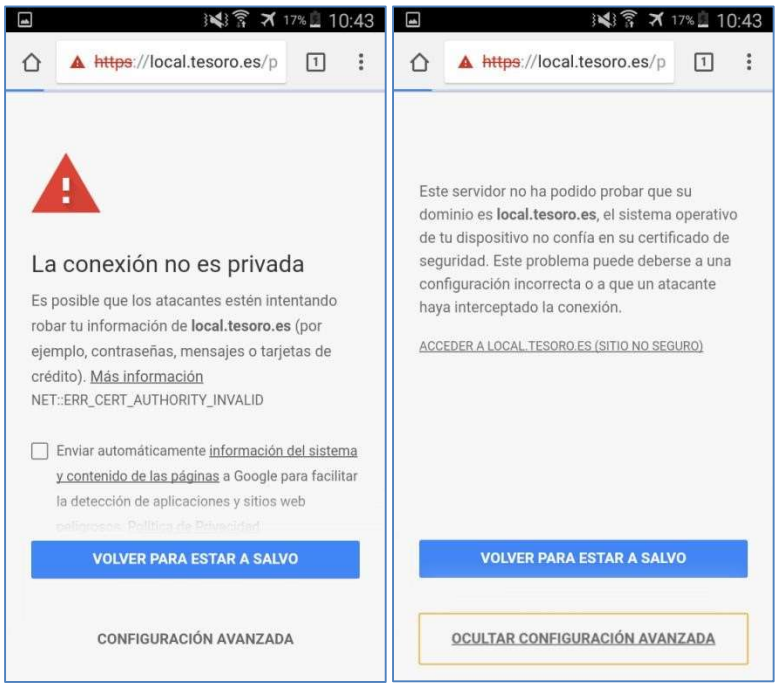
a Forma 1 (versiones de Android más antiguas)

1) Acceder a la página del Servicio de Compra y Venta de Valores (en adelante SCVV) con un navegador Chrome. Si no tiene Chrome instalado deberá instalarse (Firefox no funciona con certificados en dispositivos móviles y no se puede asegurar la compatibilidad del navegador por defecto incluido en el dispositivo, depende de cada versión).

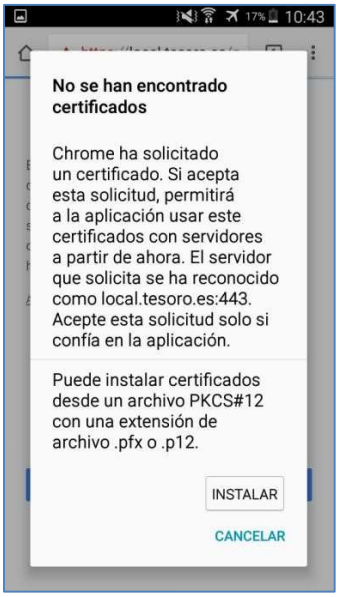
2) Acceder al SCVV desde la URL siguiente:

https://wwws.tesoro.es

Al acceder por primera vez el navegador dirá que **La conexión no es privada** al no ser reconocido el certificado del SCVV. Deberá pulsarse en **Configuración Avanzada** y en el segundo aviso pulsar sobre **Acceder a wwws.tesoro.es (sitio no seguro)**. En el punto siguiente se instalarán los certificados del SCVV para que este aviso no vuelva a aparecer.



Al no tener certificado de usuario instalado se mostrará un aviso para su instalación. De momento pulsar **Cancelar**, se instalará el certificado de usuario más adelante.



3) Se muestra la página de descarga de certificados del SCVV.

Al no tener todavía el certificado de usuario se dirigirá a la página de descargas:

Miércoles 7 de Marzo de 2018, 16:24

GOBIERNO DE ESPAÑA | MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD | TesoroPúblico SEDE ELECTRÓNICA | 902 155 050

Certificados para dispositivos móviles

En los dispositivos móviles Apple iOS y Google Android es necesario instalar los certificados del Tesoro Público, consulte el manual asocociado según su tipo de dispositivo para su instalación.

- Certificado *.tesoro.es para Apple iOS y Android
- Certificado AC RAIZ FNMT-RCM para Apple iOS y Google Android
- Certificado AC Componentes Informáticos para Apple iOS y Google Android

- Manual de instalación de certificados en Apple iOS y Cliente móvil @firma
- Manual de instalación de certificados en Google Android y Cliente móvil @firma

AutoFirma y Cliente móvil @firma

AutoFirma es una aplicación de escritorio que el usuario debe instalar en su ordenador y que permite la ejecución de operaciones de firma locales en los sistemas Operativos Windows, Mac OS, Linux y dispositivos móviles iOS o Android. Es invocada por el Servicio de Compra y Venta de Valores para la ejecución de operaciones de firma electrónica. En particular permite efectuar operaciones de firma desde navegadores de última generación sin requerir el Runtime de Java.

Los navegadores actualmente soportados son los siguientes:

- Google Chrome v64 o superior (ordenador y dispositivos móviles con sistema Android 7 o superior)
- Mozilla Firefox v59 o superior
- Microsoft Edge v40 o superior
- Apple Safari v10 o superior (dispositivos móviles con sistema iOS 10 o superior)
- Internet Explorer v11 (las versiones 9 y 10 siguen requiriendo la utilización de Java)

Elija la opción adecuada a su Sistema Operativo para descargar AutoFirma y después proceda a su instalación tras descomprimir el archivo zip:

- AutoFirma para Sistemas Windows 32 bits
- AutoFirma para Sistemas Windows 64 bits
- AutoFirma para Sistemas MacOS
- AutoFirma para Sistemas Linux

- Cliente movil @firma para Sistemas Apple iOS
- Cliente movil @firma para Sistemas Google Android

- Manual de instalación de AutoFirma
- Ayuda AutoFirma para los usuarios

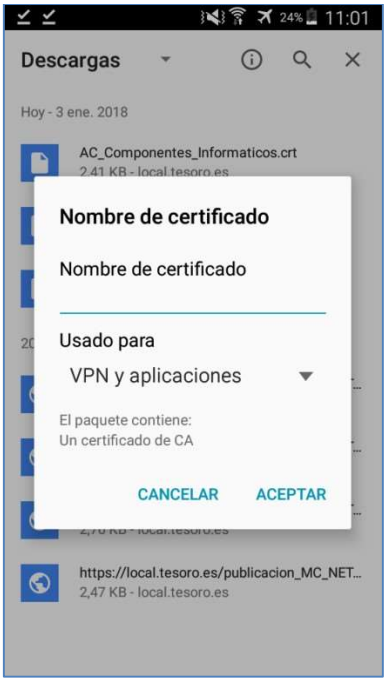
4) Descargar los tres certificados del SCVV del apartado superior de la página de descargas.

- Certificado *.tesoro.es para Apple iOS y Android
- Certificado AC RAIZ FNMT-RCM para Apple iOS y Google Android
- Certificado AC Componentes Informáticos para Apple iOS y Google Android

5) Ir a las descargas del navegador Chrome.

Desde las notificaciones de descargas o desde el propio Chrome se puede acceder a los archivos descargados.

6) Pulsar sobre cada uno de los certificados anteriores descargados y se mostrará una ventana de importación: en caso de no aparecer el nombre por defecto del certificado introducir un nombre descriptivo para cada uno (por ejemplo: tesoro1, tesoro2, tesoro3) y pulsar Aceptar para cada uno.

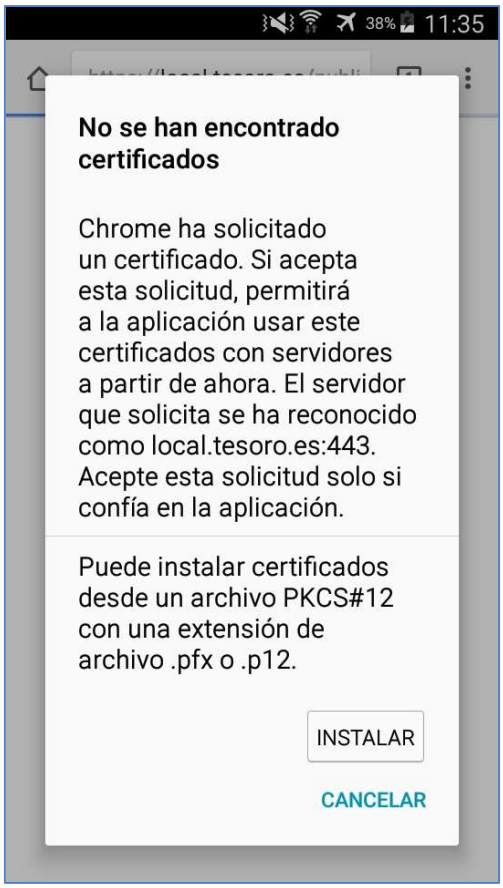


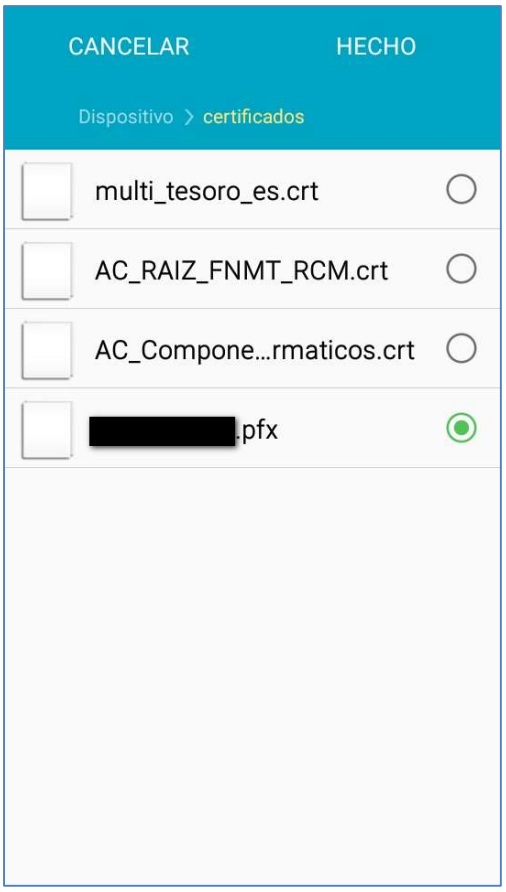
7) Para instalar el certificado de usuario en el dispositivo, **el usuario deberá enviarse un correo adjuntando su certificado digital** (fichero con extensión ".pfx") y desde su dispositivo deberá **guardarlo en un directorio del propio dispositivo**.

Nota: si se usa un DNIe el dispositivo Android deberá disponer de NFC (tecnología de comunicación inalámbrica, de corto alcance que permite el intercambio de datos entre dispositivos) para usar el DNIe v3 o de un lector de DNIe compatible con el dispositivo (todas versiones del DNIe). En caso contrario se deberá utilizar un certificado digital.

8) Cerrar completamente el navegador Chrome (no es suficiente cerrar la pestaña actual) en el dispositivo.

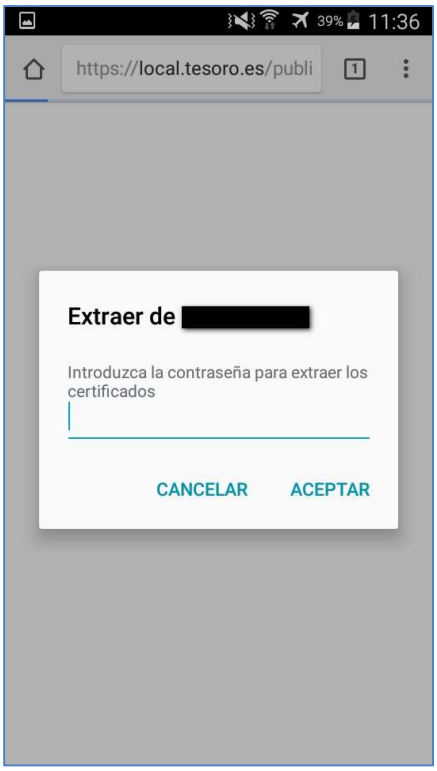
9) Al volver a acceder a la página del SCVV, cuando se solicite un certificado de usuario, se deberá pulsar **Instalar** y seleccionar el certificado guardado previamente en el dispositivo, **introducir su contraseña** y pulsar **Aceptar** para realizar su instalación en el dispositivo.

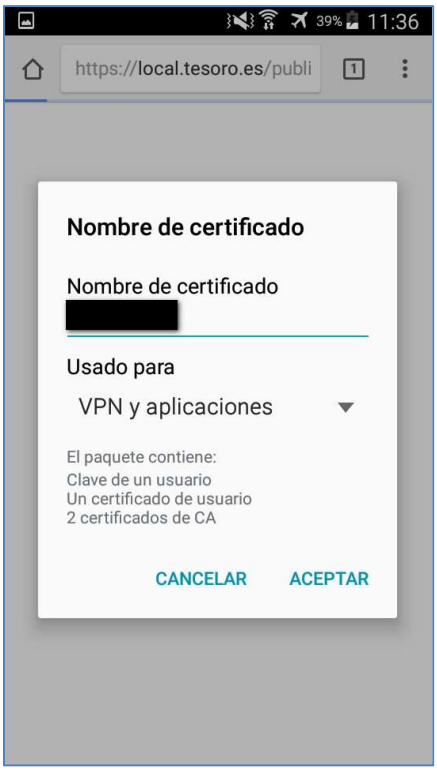




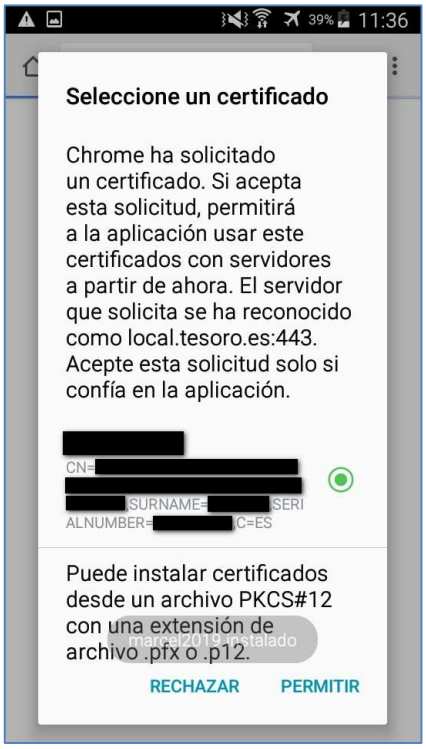
Tras seleccionarlo pulsar en **Hecho** en la parte superior, se pedirá la contraseña del certificado para importarlo en el dispositivo. Tras esto se solicitará el nombre de certificado que se mostrará al usuario, si no se muestra el nombre por defecto deberá introducir uno y pulsar **Aceptar**.

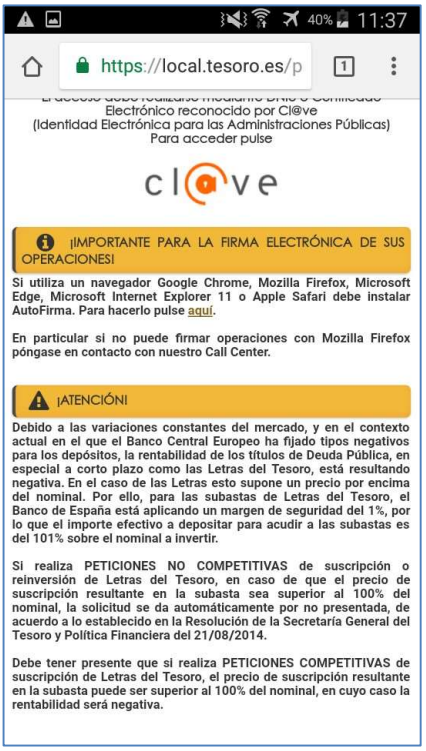
Nota: cada vez que acceda al SCVV se mostrará el certificado instalado, y se deberá permitir su uso para acceder a la página principal del SCVV. No es necesario volver a instalar el certificado, aunque el aviso indique que se puede instalar un certificado.





10) Cada vez que acceda al SCVV se mostrará un aviso al usuario para avisarle que se va a utilizar su certificado de usuario y si desea permitirlo pulsando sobre **Permitir**. Es necesario que se permita su utilización para acceder al SCVV.





Nota: es importante que la URL muestre el candado seguro de color verde confirmando la validez de los certificados.

b Forma 2 (dispositivos Android más actuales)

En los dispositivos Android, debido a la configuración de Seguridad, se puede pedir una contraseña para instalar los certificados disponibles en la URL https://wwws.tesoro.es/Descarga_AutoFirma.aspx cuando se pulsa sobre el enlace del certificado para su descarga e instalación.

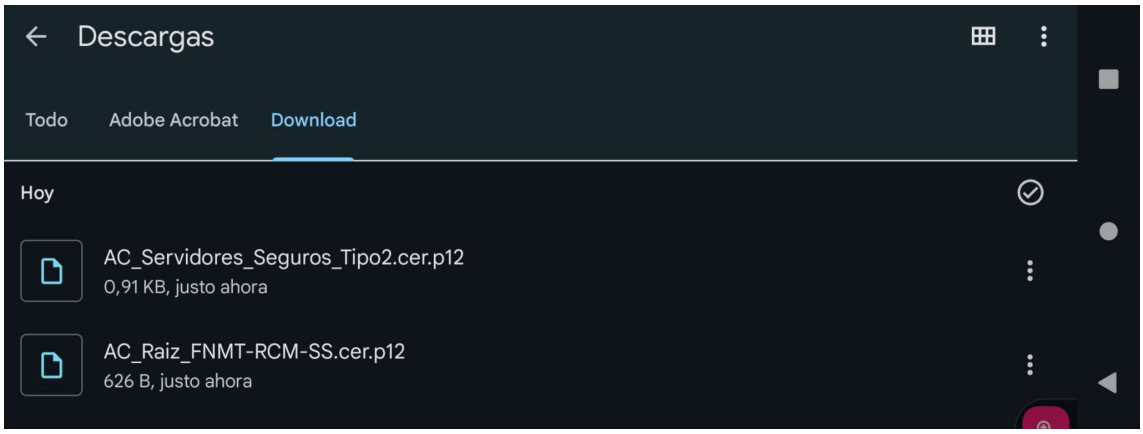
Sin embargo, hay que indicar que los certificados disponibles en esta URL no tienen contraseña, y la solicitud de contraseña viene, como se ha comentado, de la configuración de seguridad del dispositivo Android.

De los disponibles en el enlace anterior, los certificados a descargar e instalar en el dispositivo Android son los siguientes:

- 1. Certificado AC RAIZ FNMT-RCM-SS.
- 2. Certificado AC Servidores Seguros Tipo 2.

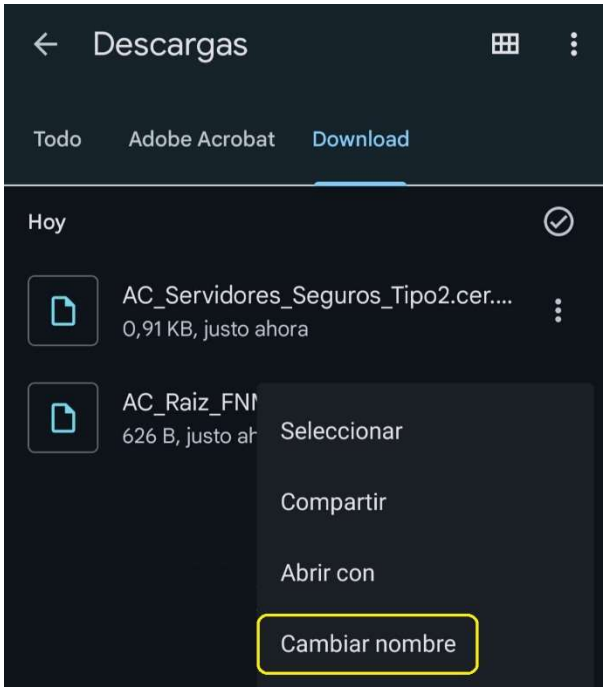
Cuando se pulsa sobre el enlace de un certificado, automáticamente este se descarga en la carpeta "Descargas" del dispositivo Android. Si en este paso solicitara el password del certificado se debe pulsar "Cancelar".

Al descargar los certificados, debe comprobarse la extensión del fichero descargado.



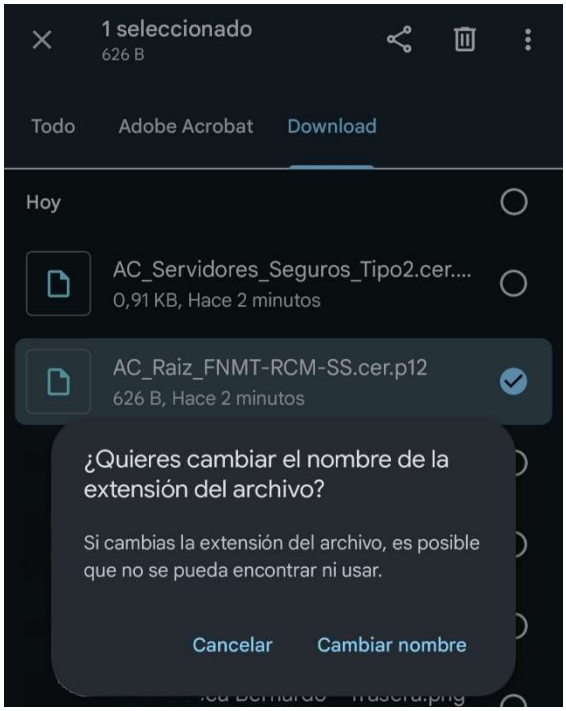
En caso de haberse descargado los certificados con extensión ".cer.p12" ó ".cer.pfx", hay que renombrar el fichero para que solo tenga extensión ".cer".

Para ello, en el menú contextual que aparece al pulsar los 3 puntos verticales en cada fichero, se elige la opción "Cambiar nombre".

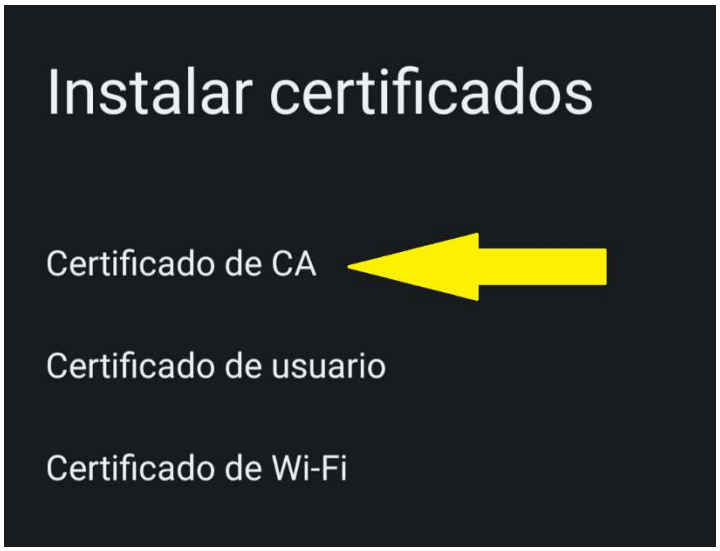


Al editar el nombre, se elimina la extensión hasta que solo quede ".cer", y pulsar "Aceptar".

Entonces se solicitará la confirmación del cambio de nombre, y debe aceptarse pulsando "Cambiar nombre".



Una vez los certificados están descargados y renombrados si hubiera sido necesario, hay que acceder a “Ajustes”, “Seguridad”, “Cifrado y credenciales”, “Instalar certificados”, y seleccionar “Certificado de CA”.



Elegir entonces “Certificado de CA”, “Instalar (No seguro)”, y mostrará la carpeta “Descargas”, o “Reciente” pero en el menú contextual se podrá seleccionar “Descargas”.

Ahí seleccionar el certificado a instalar y debería hacerlo sin solicitar contraseña.

Una vez hecho esto, se debería ver en “Credenciales de confianza” apartado “Usuario” los dos certificados de entidades CA instalados.

Para instalar el certificado de usuario en el dispositivo, **el usuario deberá enviarse un correo adjuntando su certificado digital** (fichero con extensión ".pfx") y desde su dispositivo deberá **guardarlo en un directorio del propio dispositivo**, y seguir los mismos pasos de instalación que para los certificados anteriores. Este certificado aparecerá en el apartado "Credenciales de usuario".

3. Instalación cliente móvil @firma y configuración

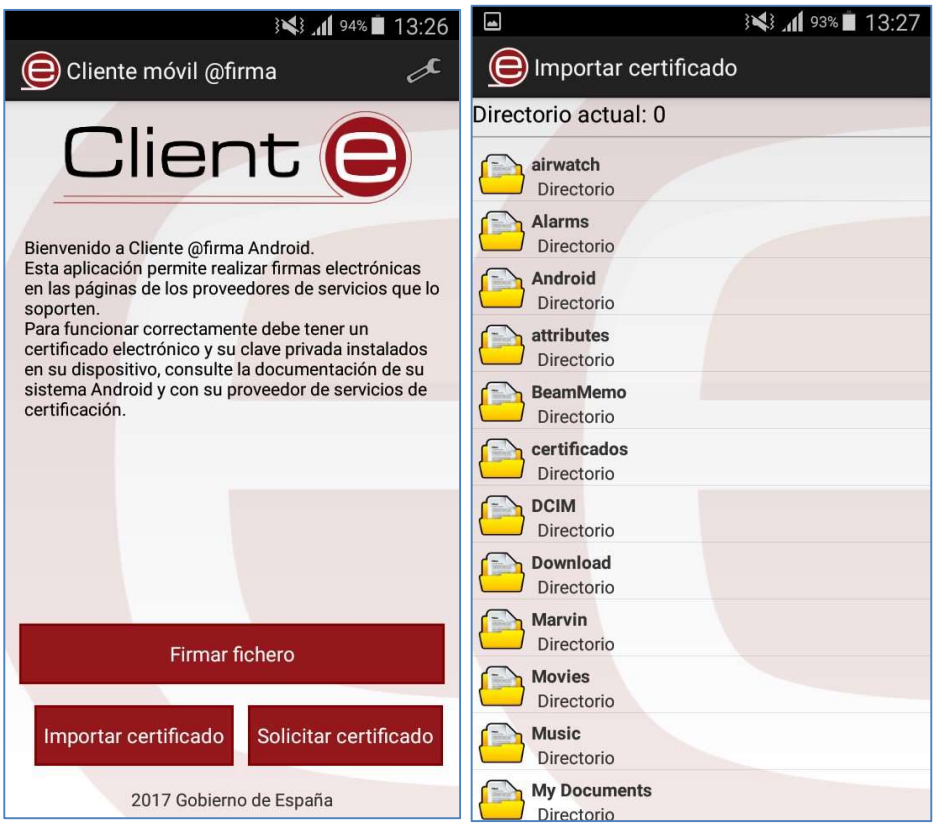
Desde la página de descarga se debe seleccionar la opción Cliente móvil @firma (aplicación gratuita) para sistemas Google Android. Desde este enlace se accederá a la tienda de Google Play para proceder a la instalación de la aplicación en el dispositivo.

o desde la siguiente URL:

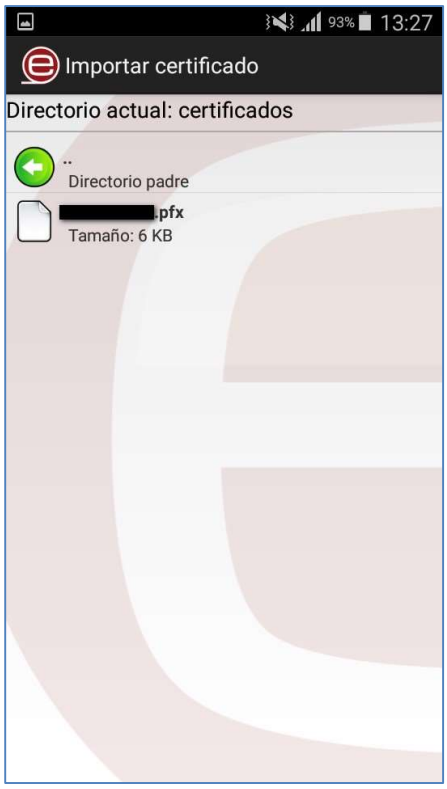
https://play.google.com/store/apps/details?id=es.gob.afirma

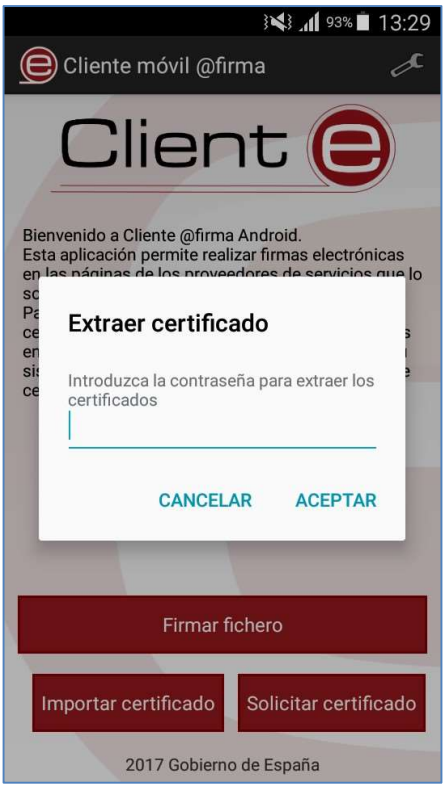
- No debería ser necesario importar el certificado de usuario en el Cliente móvil de @firma para poder firmar operaciones. Al haberse realizado previamente esta importación en el dispositivo, tal como se ha indicado en los puntos anteriores, la aplicación lo utilizará automáticamente avisando para confirmar su utilización.

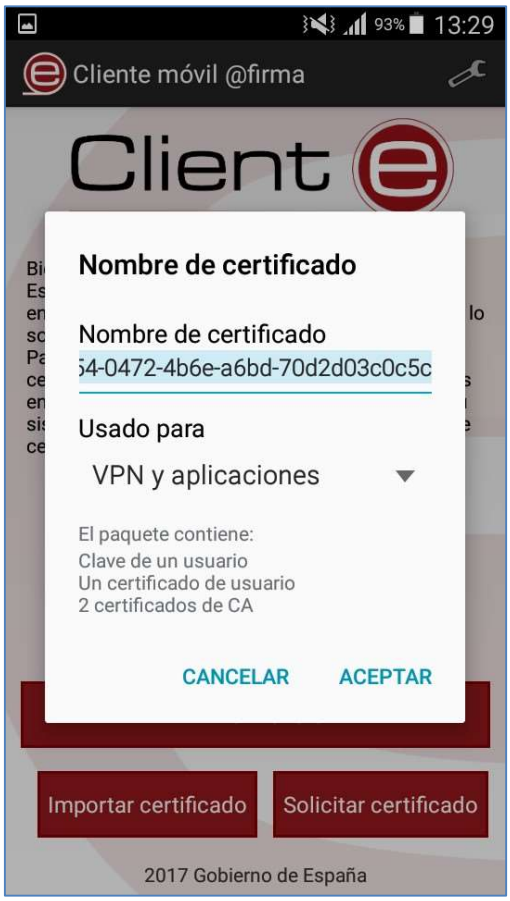
- En caso de que el certificado de usuario no sea detectado por el Cliente móvil @firma deberá proceder a su instalación pulsando sobre la opción de **Importar certificado** del propio Cliente móvil @firma.



Seleccionar el directorio de su certificado de usuario para importarlo, se pedirá introducir la contraseña y un nombre para su utilización.

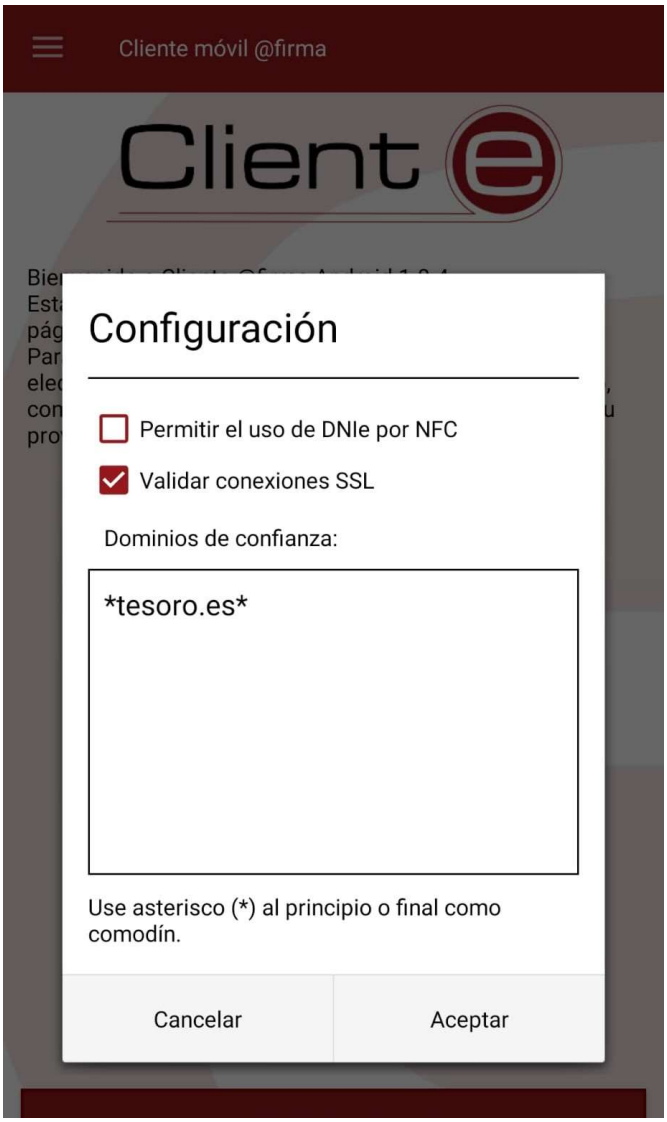






Este será el certificado que se usará en todas las operaciones de firma del SCVV.

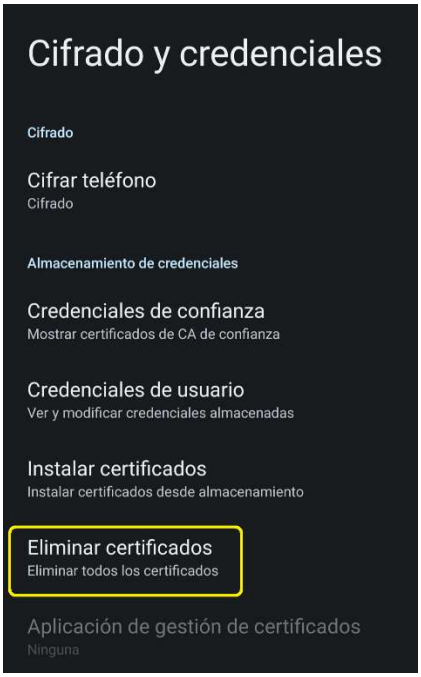
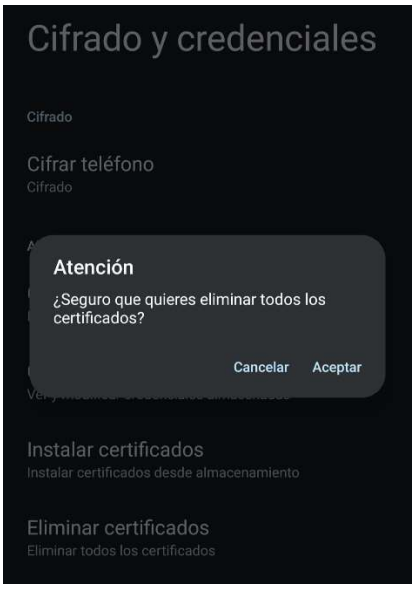
También hay que acceder a la configuración de la aplicación, y comprobar que está marcado el apartado “Validar conexiones SSL”, e introducir el valor “*tesoro.es*” como dominio de confianza.



El paso siguiente es solo para indicar cómo eliminar los certificados instalados anteriormente.

4. Borrar/Eliminar certificados de usuario y del SCVV

Si se desea eliminar todos los certificados del dispositivo, se deberá acceder a los Ajustes del dispositivo, ir a las opciones de **Seguridad, Cifrado y Credenciales** y pulsar en **Borrar Credenciales**. Se eliminará el certificado de usuario y todos los certificados que se importaron manualmente en los pasos anteriores.



Se pedirá confirmación para eliminar todo el contenido, pulsar en **Aceptar**.