

# MANUAL DE INSTALACIÓN DE CERTIFICADOS EN DISPOSITIVOS ANDROID

## 1. Requisitos

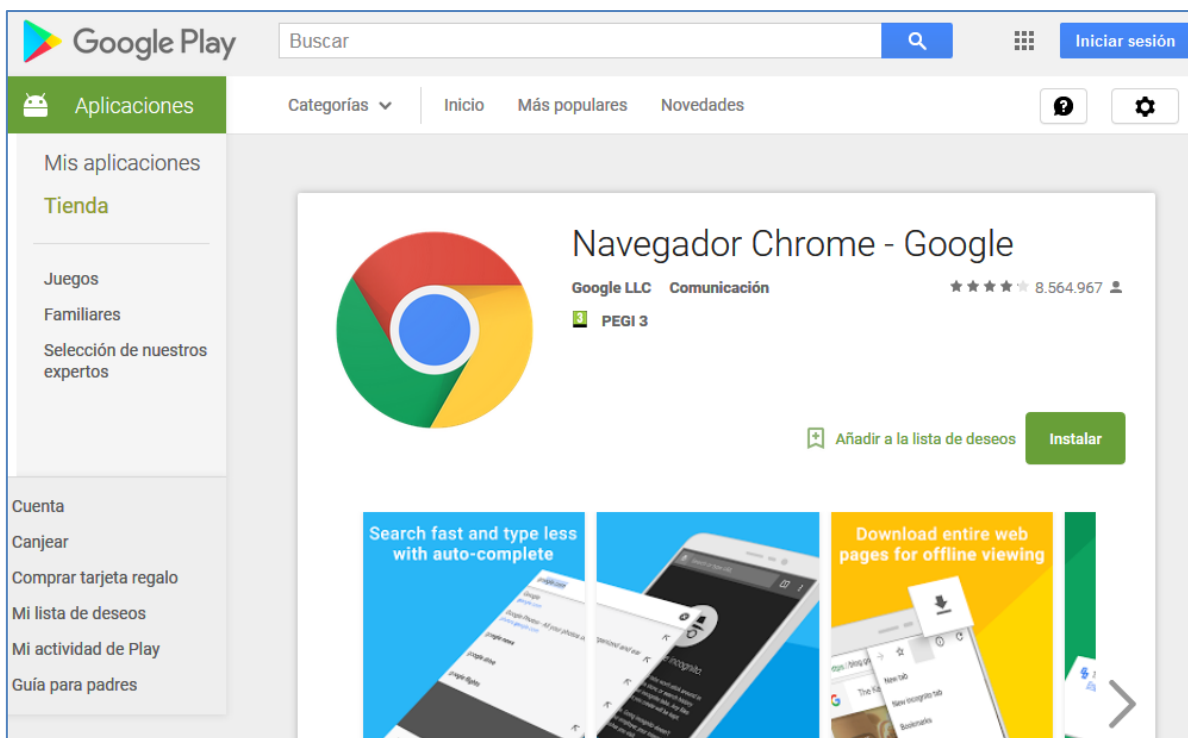
Tener instalado un navegador Chrome en el dispositivo. Si no es el caso lo puede instalar accediendo a la tienda Google Play desde su dispositivo.

## 2. Importación de certificados

- 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 instalarlo (Firefox no funciona con certificados en dispositivos móviles y no podemos asegurar la compatibilidad del navegador por defecto incluido en el dispositivo, depende de cada versión).

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

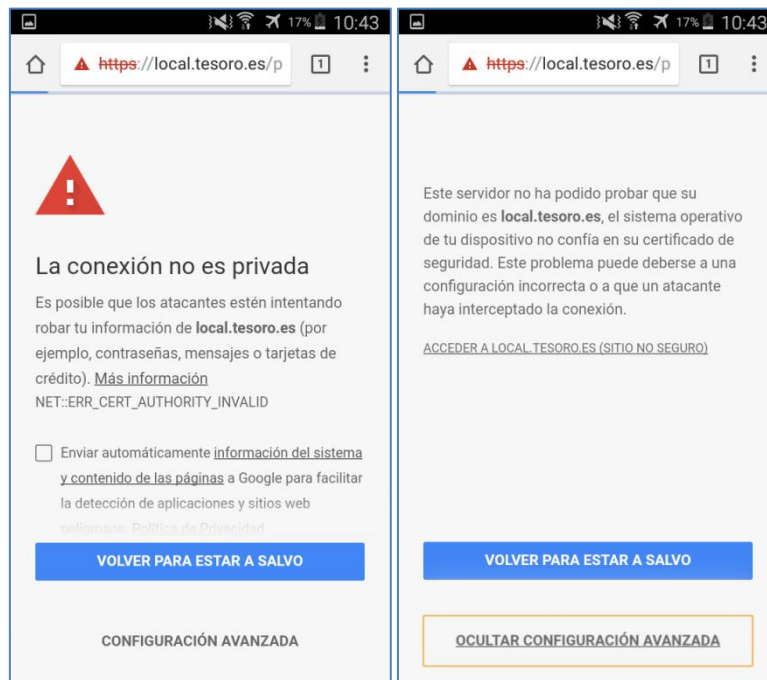
<https://play.google.com/store/apps/details?id=com.android.chrome>



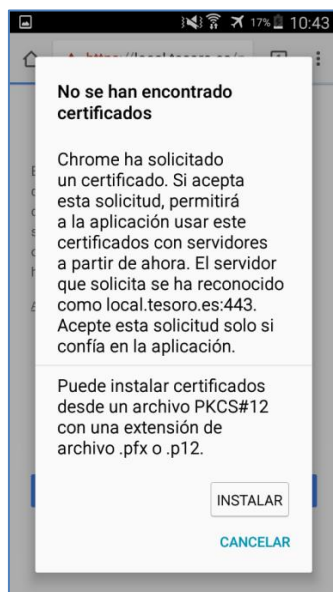
2) Acceder al SCVV desde la URL siguiente:

<https://wwws.tesoro.es>

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



Al no tener certificado de usuario instalado le mostrará un aviso para su instalación. De momento pulsar **Cancelar**, instalaremos 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 le dirigirá a la página de descargas:

Miércoles 7 de Marzo de 2018, 16:24



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 asociado 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:

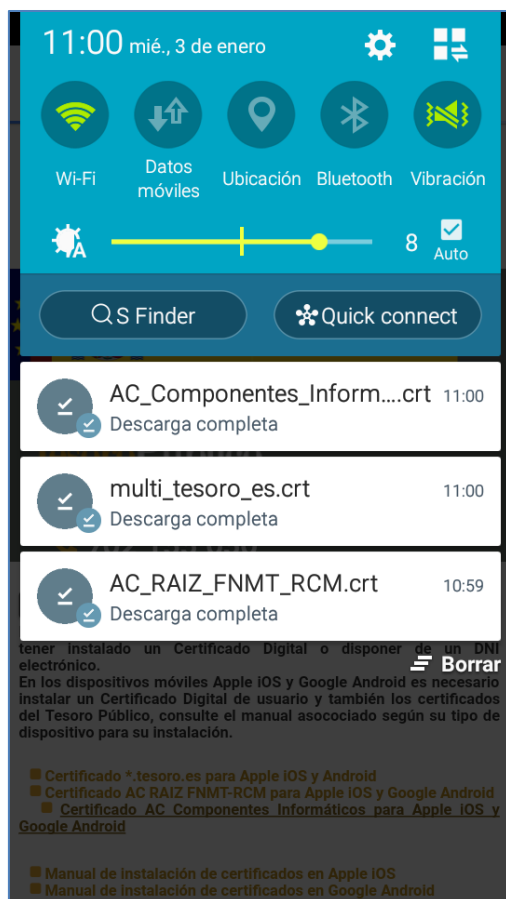
- AutoFirma para Sistemas Windows 32 bits
- AutoFirma para Sistemas Windows 64 bits
- AutoFirma para Sistemas MacOS
- AutoFirma para Sistemas Linux
- Cliente móvil @firma para Sistemas Apple iOS
- Cliente móvil @firma para Sistemas Google Android
- Manual de instalación de AutoFirma
- Ayuda AutoFirma para los usuarios

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

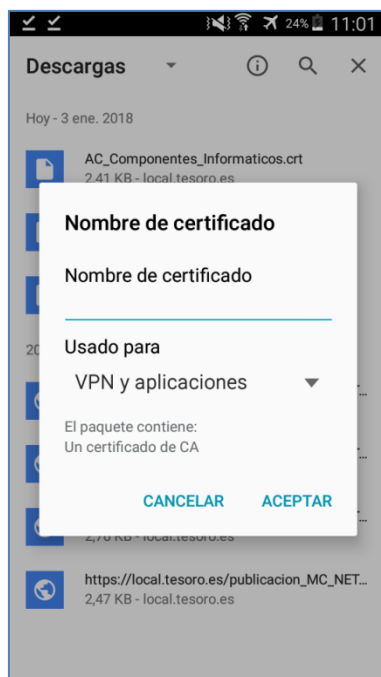
- Certificado \*.tesoro.es para Apple iOS y Android
- Certificado AC RAIZ FNMT-RCM para Apple iOS y Google Android
- Certificado AC Componentes Informáticos para Apple iOS y Google Android

5) Ir a las descargas del navegador Chrome.

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



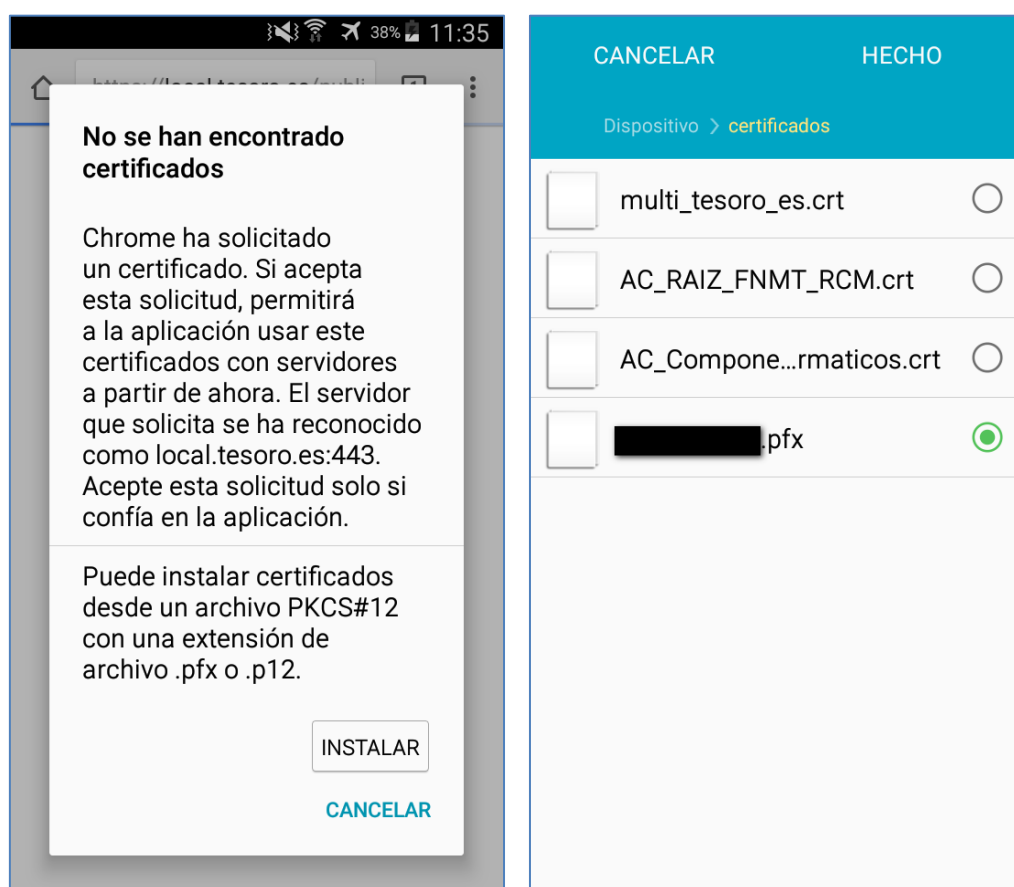
- 6) Pulsar sobre cada uno de los certificados anteriores descargados y se mostrara una ventana de importación: en caso de no aparecer el nombre por defecto del certificado introducir un nombre descriptivo para cada uno (por ejemplo tesoro1, tesoro2, tesoro3) y pulsar Aceptar para cada uno.



- 7) Para instalar su 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 usa un DNle su dispositivo deberá disponer de NFC (tecnología de comunicación inalámbrica, de corto alcance que permite el intercambio de datos entre dispositivos) para usar el DNle v3 o de un lector de DNle compatible con su dispositivo (todas versiones del DNle). En caso contrario deberá utilizar un certificado digital.

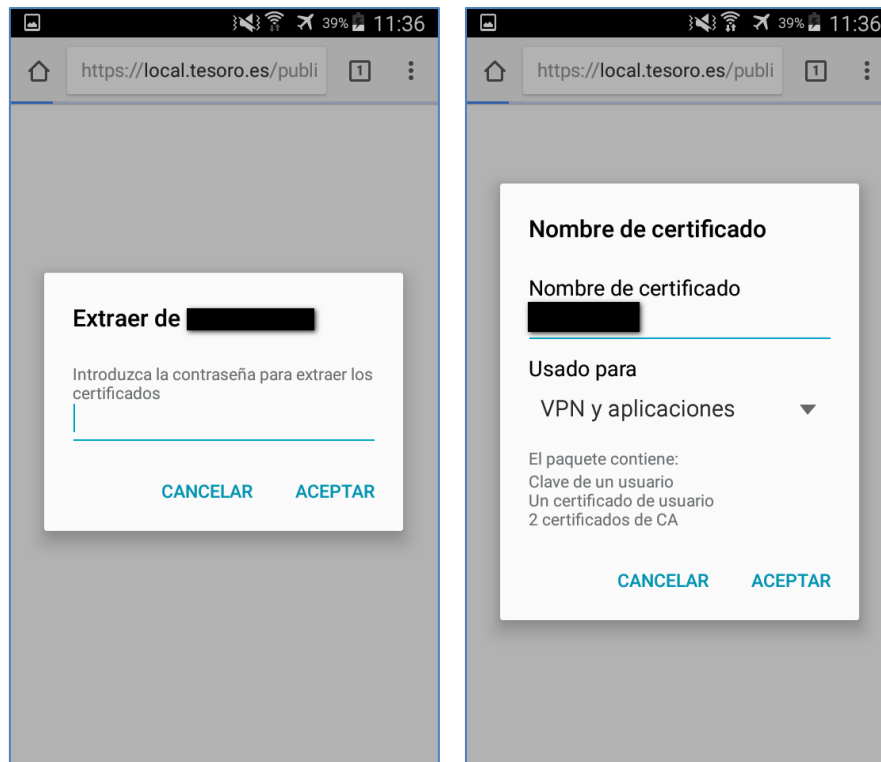
- 8) Cierre completamente su navegador Chrome (no es suficiente cerrar la pestaña actual) en su dispositivo.
- 9) Al volver a acceder a la página del SCVV, cuando se le solicite un certificado de usuario, deberá pulsar **Instalar** y seleccionar su certificado guardado previamente en el dispositivo, **introducir su contraseña** y pulsar **Aceptar** para realizar su instalación en el dispositivo.



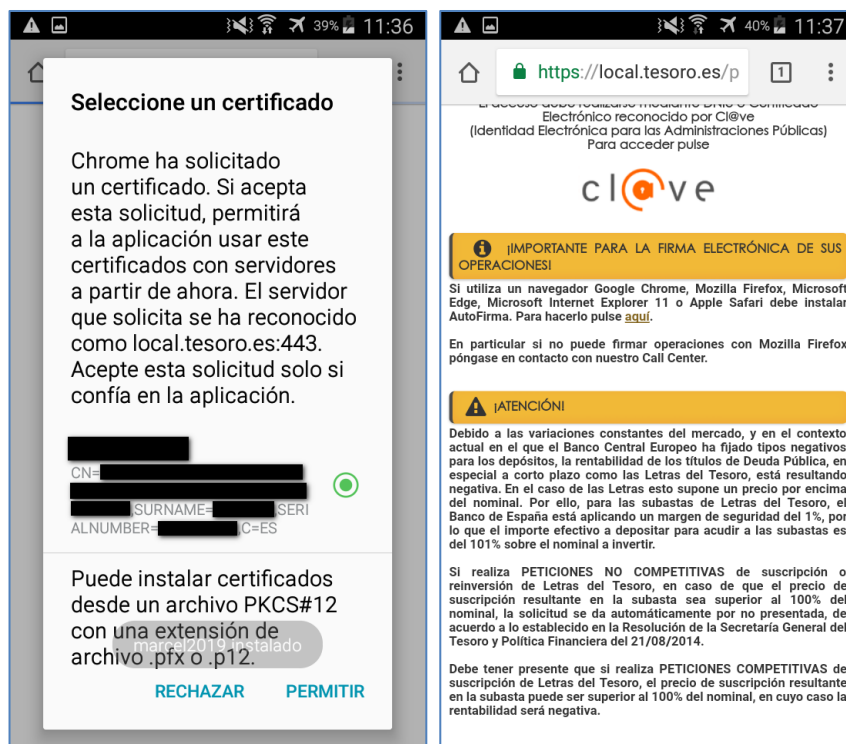
Tras seleccionarlo pulsar en **Hecho** en la parte superior, se le pedirá la contraseña de su certificado para importarlo en el dispositivo. Tras esto se solicitará el nombre de

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 le mostrara el certificado instalado, 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 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 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.

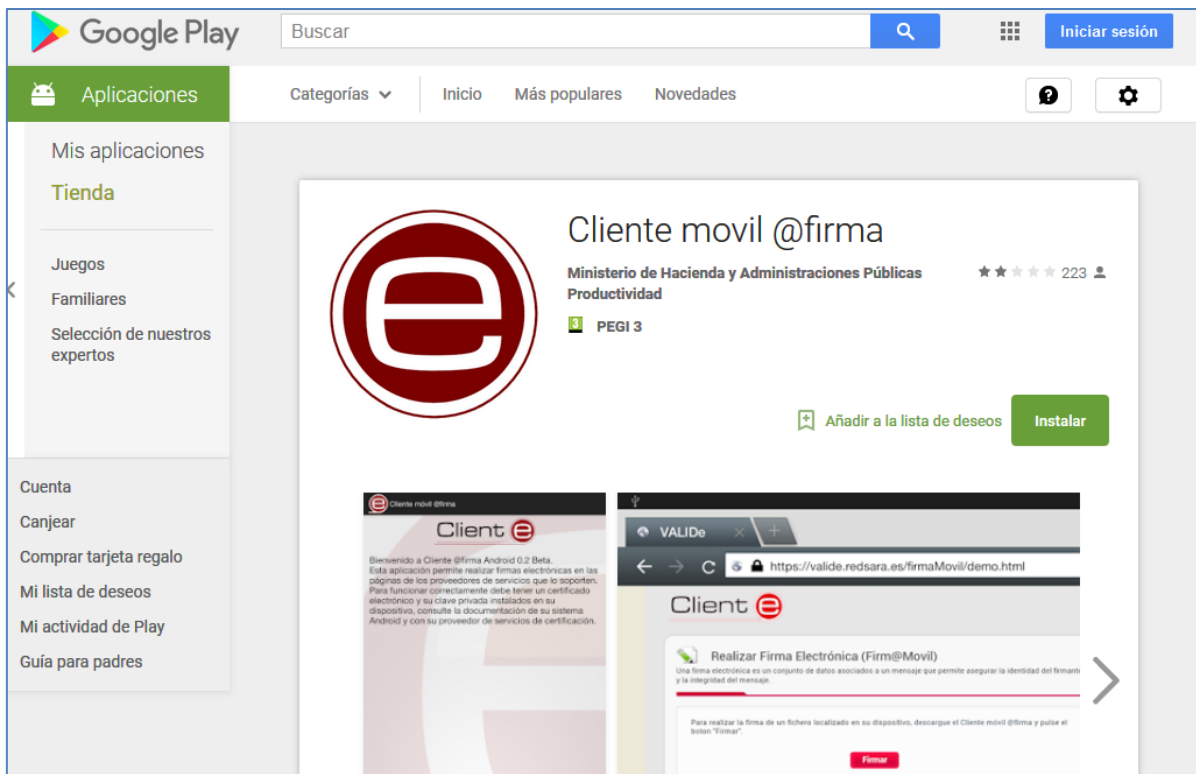
### 3. Instalación cliente móvil @firma y configuración

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

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

o desde la siguiente URL:

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

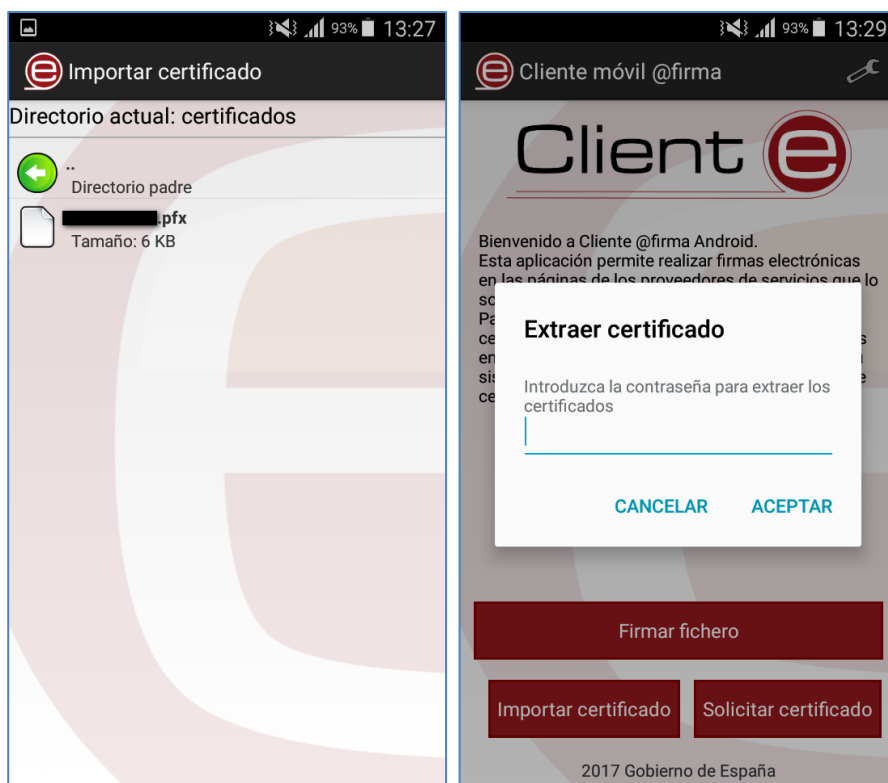


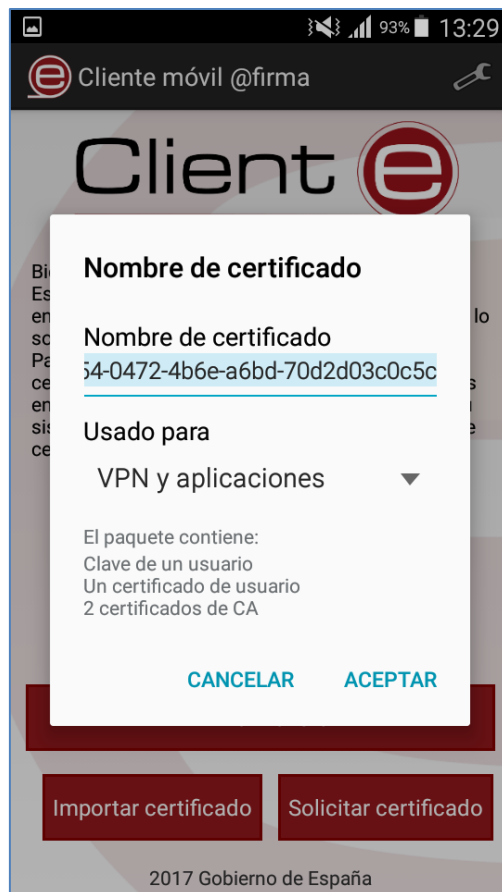
- No debería ser necesario importar su certificado de usuario en el Cliente móvil de @firma para poder firmar operaciones. Al haberse realizado previamente esta importación en su dispositivo, tal como se ha indicado en los puntos anteriores, la aplicación lo utilizara automáticamente avisándole para que confirme su utilización.
- En caso de que su 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 le pedirá introducir la contraseña y un nombre para su utilización.



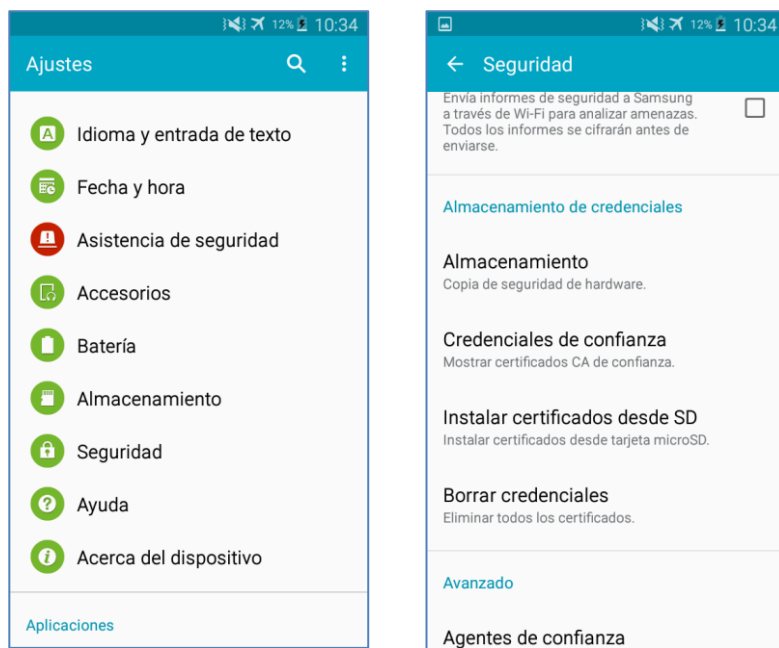


Este será el certificado que se usará en todas las operaciones de firma del SCVV.

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

#### 4. Borrar/Eliminar certificados de usuario y del SCVV

Si desea eliminar todos sus certificados del dispositivo, deberá acceder a las Ajustes de su dispositivo, ir a las opciones de **Seguridad** y pulsar en **Borrar Credenciales**. Se eliminara su certificado de usuario y todos los certificados que importó manualmente en los pasos anteriores.



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

