Contenido

1. Cliente de firma iOS

Portafirmas integra mecanismos de autenticación y firma móvil para dispositivos basados en iOS como iPhone, iPad o iPod. A continuación, se detallan uno a uno los pasos para descargar e instalar el cliente de firma así como la instalación de certificados digitales en el mismo.

Para autenticar en la aplicación pulsaremos el botón Acceder mediante certificado para iniciar el proceso de autenticación, en el que arrancará el cliente de firma iOS y se nos mostrará una ventana con los certificados que tengamos instalados. Seleccionando nuestro certificado y pulsando sobre Firmar accederemos al sistema.

Selección de certificados en cliente iOS de Portafirmas

1.1. Descarga e instalación del cliente iOS

Para poder autenticar y firmar peticiones en el sistema desde un dispositivo que funcione bajo iOS es necesario descargar el cliente ligero de firma de Portafirmas desde la App Store de Apple.

Tras pulsar sobre el botón instalar la aplicación quedará instalada en el dispositivo y podremos pasar al siguiente punto, la instalación del certificado en el dispositivo. Una vez instalada no es necesario ejecutar la aplicación, de hecho, si se intenta ejecutar la aplicación no ofrece ninguna funcionalidad, únicamente muestra un mensaje describiendo la misma.

Pantalla de información de cliente Portafirmas iOS

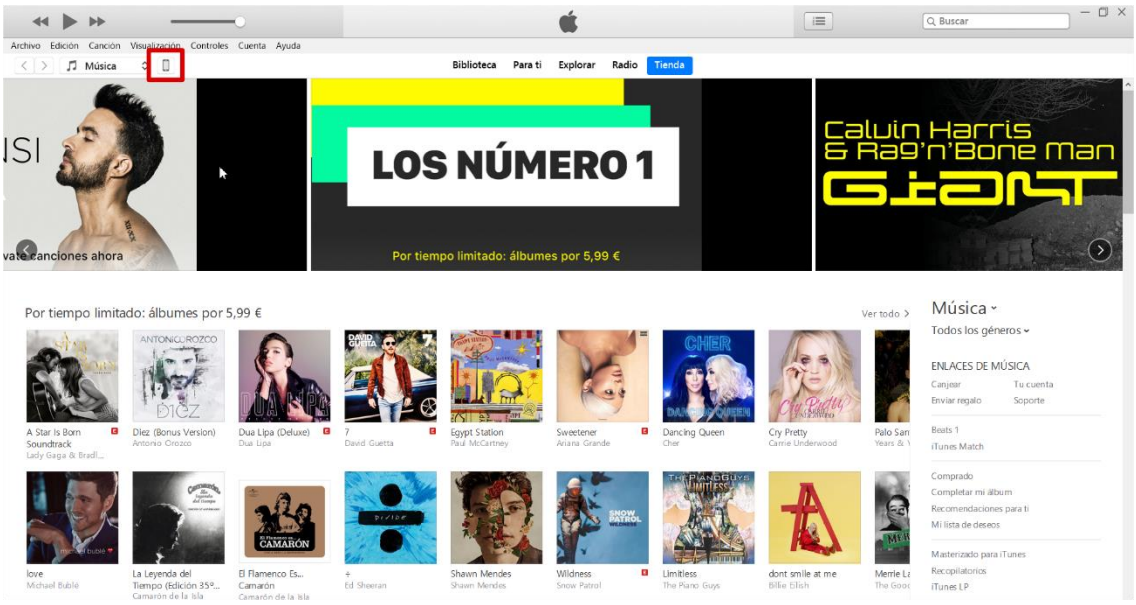
El cliente se ejecutará automáticamente cuando se vaya a realizar una autenticación o una firma desde Portafirmas.

1.2. Instalación de certificado iOS

Al igual que con el cliente de firma de escritorio, es necesario poseer un certificado personal de usuario o usuaria admitido por la plataforma @firma para poder realizar autenticación y firmas en Portafirmas.

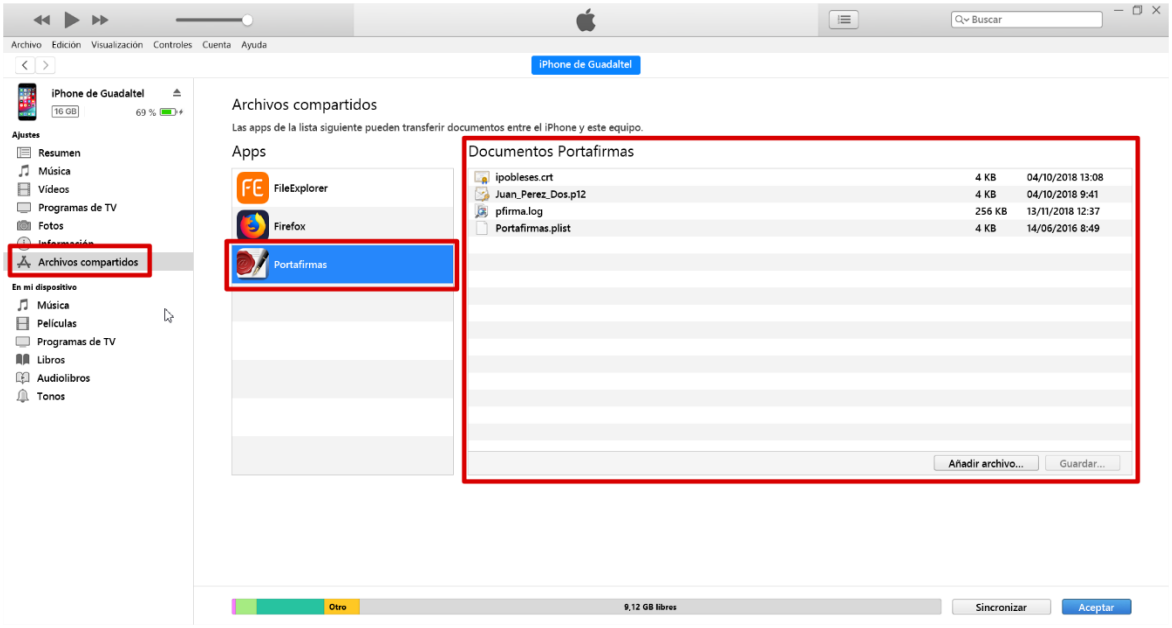
El proceso de instalación del certificado en un dispositivo iOS se realiza a través de la herramienta iTunes y a continuación se describe el proceso:

- Arrancar herramienta iTunes y conectar por USB nuestro dispositivo iOS. Una vez conectado se mostrará una pantalla inicial con un menú en la parte superior izquierda. En dicho menú, pinchar sobre el icono del dispositivo que acabamos de conectar.



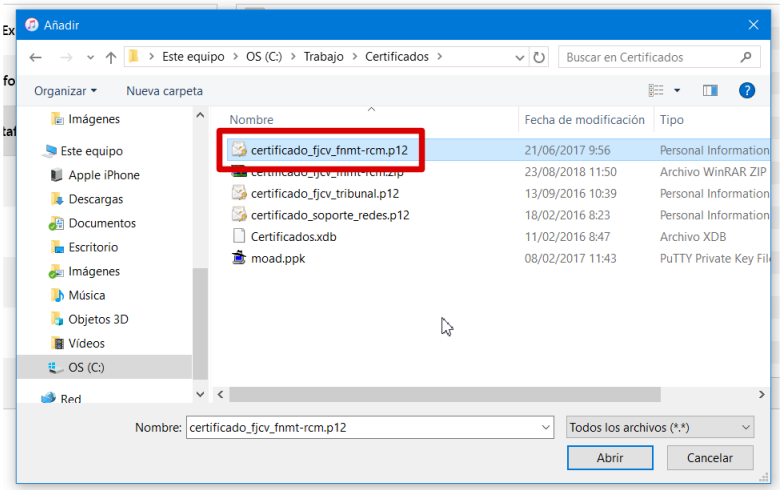
Pantalla resumen de dispositivo seleccionado

- En el apartado "Archivos compartidos" se mostrará una lista con las aplicaciones instaladas en el dispositivo seleccionado que soporten dicha funcionalidad, entre las que debe de aparecer la aplicación Portafirmas. Pulsando sobre Portafirmas, se mostrará en la lista de la derecha los "Documentos Portafirmas", que aparecerá la relación de archivos que ya dispone la aplicación, entre ellos los certificados que ya hayamos subido.



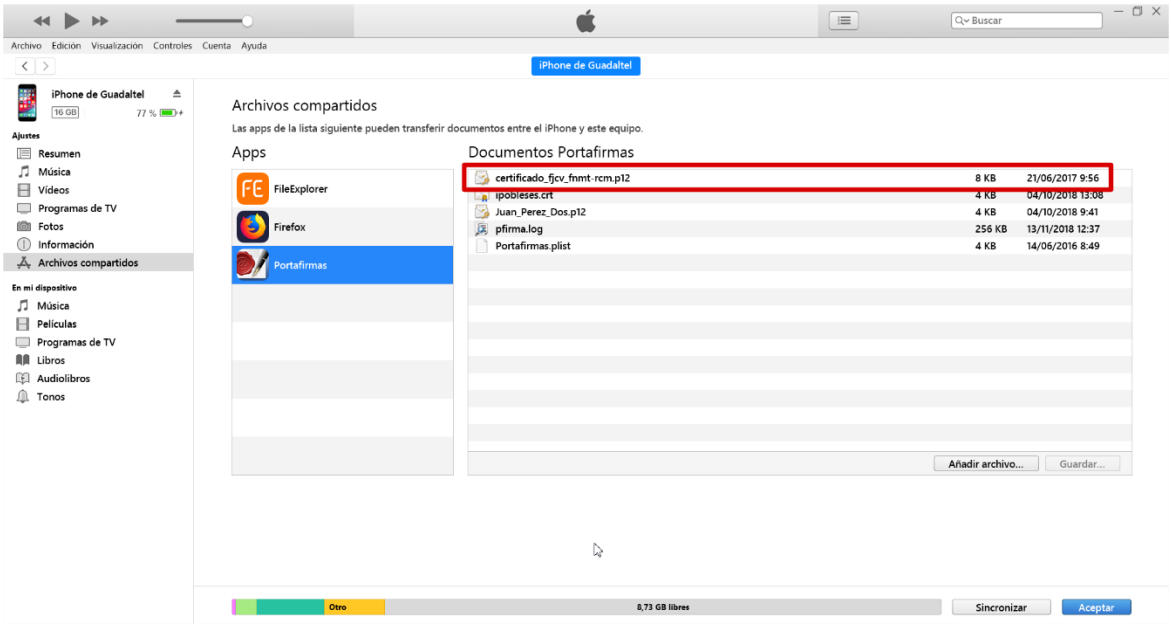
Selección de aplicación Portafirmas

- Para instalar el/los certificados se pulsará sobre el botón "Añadir archivo" tras lo que aparecerá en pantalla un diálogo de selección de ficheros. En dicho diálogo se seleccionarán los ficheros de los certificados que se deseen instalar. **Dichos ficheros tienen la extensión .p12 y siguen el estándar PKCS#12 (*)**



Selección de certificados a importar

- Una vez seleccionados los certificados, si la importación ha sido correcta se refrescará la lista de documentos para la aplicación Portafirmas mostrando los certificados instalados y que podrán ser usados en la autenticación y firma iOS.



Lista de certificados instalados en Portafirmas

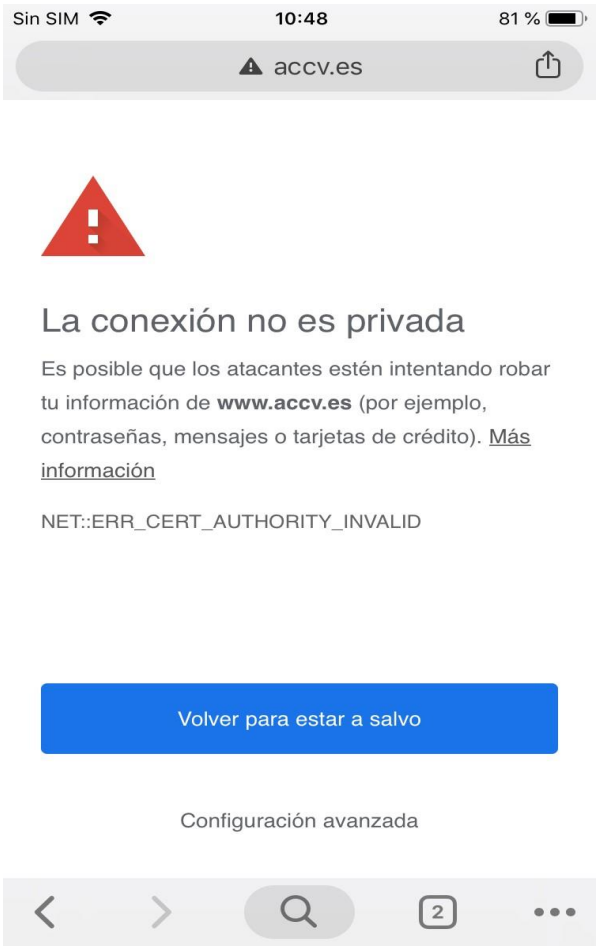
1.3. Configuración HTTPs en iOS

Si tenemos el entorno de la aplicación securizada bajo entorno HTTPs/SSL, hay que hacer una serie de configuraciones adicionales en nuestro dispositivo en función de la entidad emisora de nuestro certificado usado para el cifrado de las comunicaciones.

Apple por defecto tiene importadas una serie de entidades de confianza de ámbito internacional y nacional (FNMT y Camerfirma por ejemplo), pero en éstas no se incluye de momento algunas de ámbito más nacional (por ejemplo ACCV).

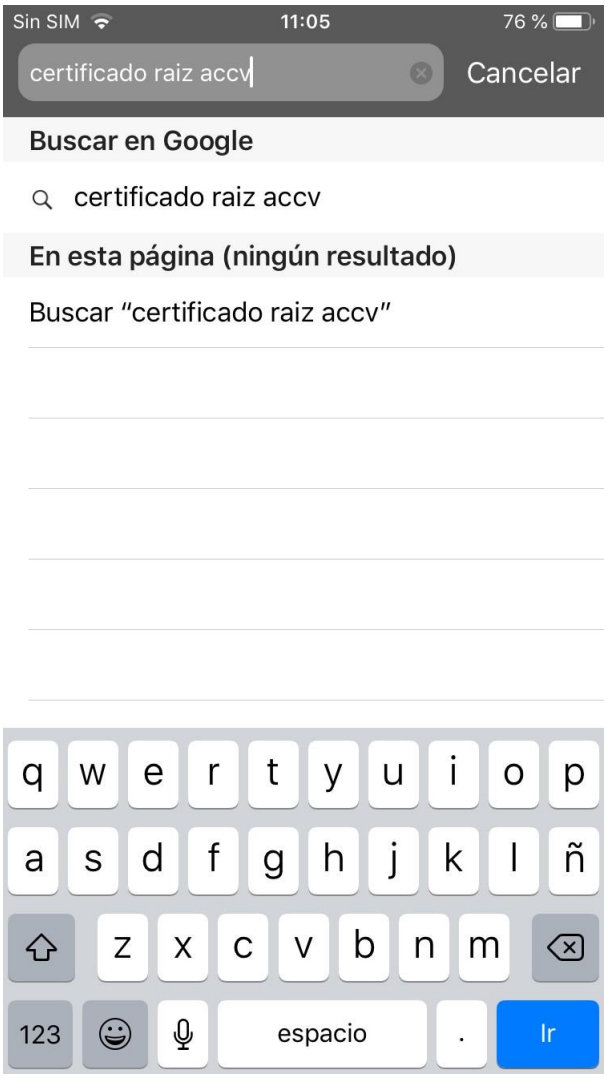
Para comprobarlo, basta con que intentemos acceder desde el navegador del dispositivo. Si nos sale la pantalla de bienvenida de portafirmas no hay problema, pero si salta un diálogo como el siguiente es cuando debemos realizar los siguientes pasos de configuración.

IMPORTANTE: Las instrucciones indicadas a continuación pueden resultar complejas a nivel técnico, si tiene alguna duda, es preferible que contacte primero con el equipo de soporte de su entidad.



Acceso a web bajo https con certificado no autorizado

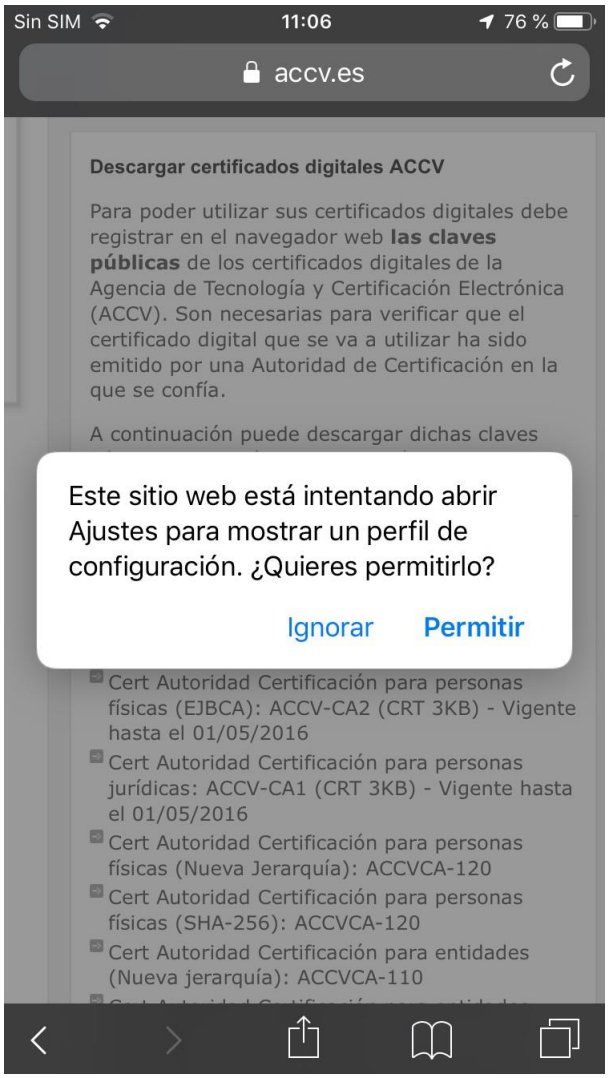
Para solucionar este problema deberemos importar el certificado raíz de la entidad emisora de nuestro certificado SSL dentro de la configuración de nuestro dispositivo. Para ello basta con buscar desde el propio dispositivo por el mismo. Siguiendo el caso de ejemplo, vamos a importar el certificado raíz de la ACCV.



Buscando el certificado raíz

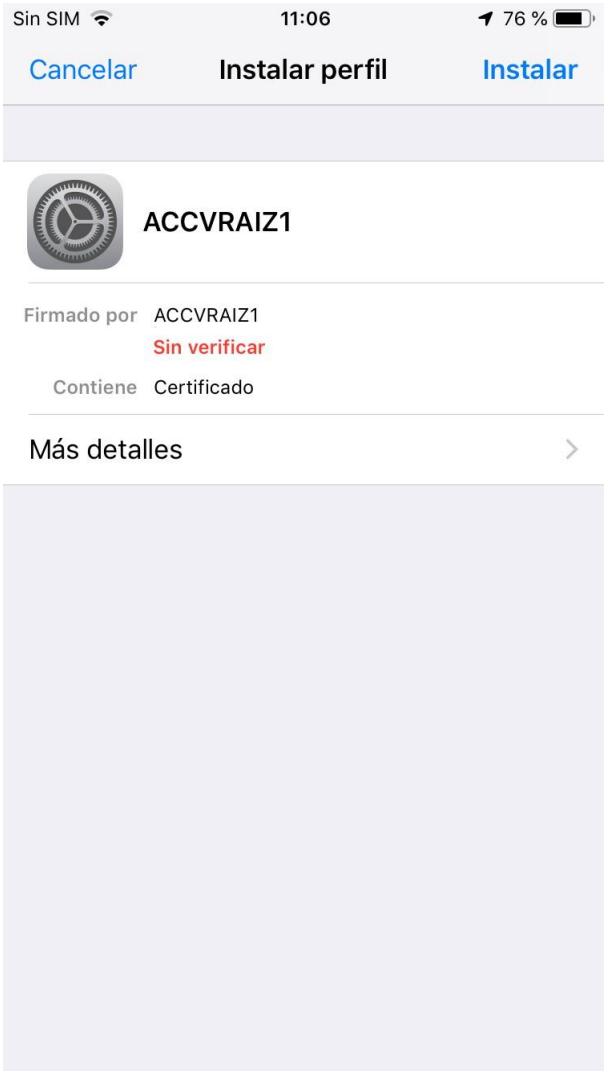
Accedemos a la primera opción que nos ofrece el buscar. Es probable que salte de nuevo el dialogo de "La conexión no es privada", si pulsamos en configuración avanzada podemos autorizar el acceso temporalmente.

Llegaremos a la relación de certificados de confianza de la entidad, y pulsaremos sobre el certificado raíz.



Descargando el certificado raíz

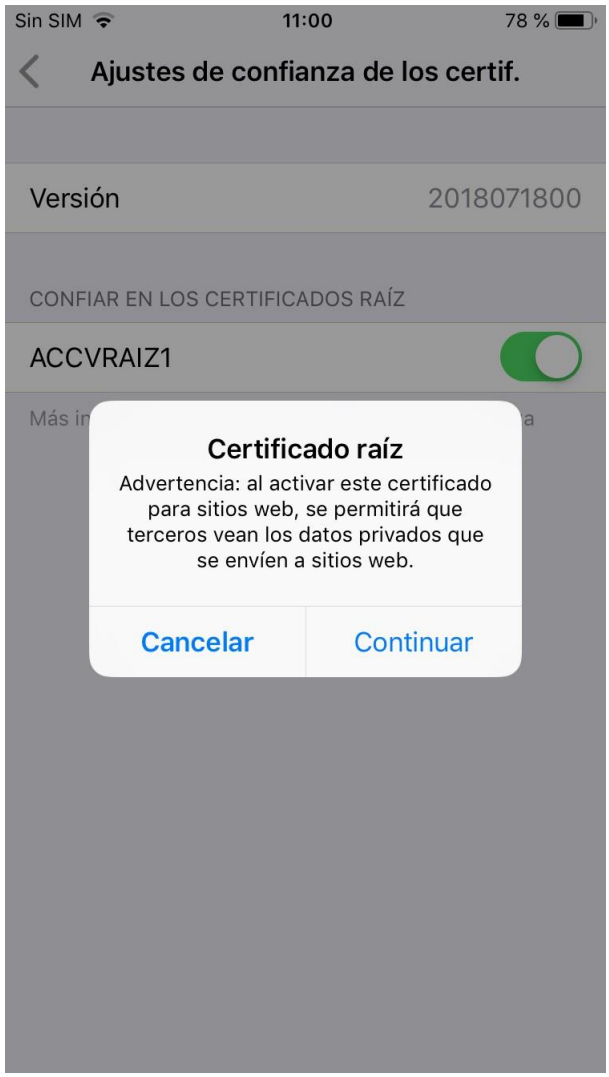
Le damos a permitir y nos saldrá este diálogo.



Instalando el certificado raíz

Pulsamos sobre "Instalar" y seguimos el asistente hasta el final. Tras esto ya tenemos instalado el certificado raíz en nuestro dispositivo.

En **el caso que tengamos una versión iOS 10.3 o superior**, hay que hacer un paso adicional final. Por defecto, al importar este certificado, éste no se autoriza aún, deberemos acceder dentro de la configuración, ***General > Información > Ajustes de confianza de los certificados*** y nos mostrará una pantalla donde aparece el recién certificado importado, pero todavía sin activar la confianza. Bastará con activar la misma aceptando el diálogo como se muestra a continuación.



Autorizando el certificado raíz

Tras esto, ya podemos acceder desde nuestro navegador, así como la app de Portafirmas, a nuestro portal securizado por HTTPs sin problemas.

2. Cliente de firma Android

Portafirmas integra mecanismos de autenticación y firma móvil para dispositivos basados en Android. A continuación, se detallan uno a uno los pasos para descargar e instalar el cliente de firma así como la instalación de certificados digitales en el mismo.

Para autenticar en la aplicación pulsaremos el botón Acceder mediante certificado para iniciar el proceso de autenticación, en el que arrancará el cliente de firma Android y se nos mostrará una ventana con los certificados que tengamos instalados. Seleccionando nuestro certificado y pulsando sobre Firmar accederemos al sistema.

Selección de certificados en cliente Android de Portafirmas

2.1. Descarga e instalación del cliente Android

Para poder autenticar y firmar peticiones en el sistema desde un dispositivo que funcione bajo Android es necesario descargar el cliente ligero de firma de Portafirmas desde la Google Play Store.

Tras pulsar sobre el botón instalar la aplicación quedará instalada en el dispositivo y podremos pasar al siguiente punto, la instalación del certificado en el dispositivo. Una vez instalada no es necesario ejecutar la aplicación, de hecho, si se intenta ejecutar la aplicación no ofrece ninguna funcionalidad, únicamente muestra un mensaje describiendo la misma.

Pantalla bienvenida

El cliente se ejecutará automáticamente cuando se vaya a realizar una autenticación o una firma desde Portafirmas.

2.2. Instalación de certificado Android

Al igual que con el cliente de firma de escritorio, es necesario poseer un certificado personal de usuario o usuaria admitido por la plataforma @firma para poder realizar autenticación y firmas en Portafirmas.

Para instalar los certificados que deseemos usar debemos conectar el dispositivo al PC. Este paso lo podemos hacer:
- Con la herramienta particular de cada marca para intercambiar archivos, música, ... con el dispositivo. Algunas de estas herramientas son Kies de Samsung, PC Companion de Sony, ...
- Con alguna aplicación Android que permita intercambiar ficheros con el dispositivo.
- Conectando el dispositivo en modo "**Almacenamiento Masivo USB / Transferencia de archivos**".

Android 9 e inferiores

Tras conectarnos al dispositivo con alguna de las maneras del paso anterior debemos crear la carpeta "**portafirmas**" en el raíz. Una vez creada se copian dentro todos los certificados que queramos usar desde nuestro dispositivo Android.

Desde el PC estamos trabajando en el raíz pero realmente nuestro directorio de trabajo Android es: **/mnt/sdcard/portafirmas/**

La instalación del certificado o certificados debe quedar de la siguiente manera:

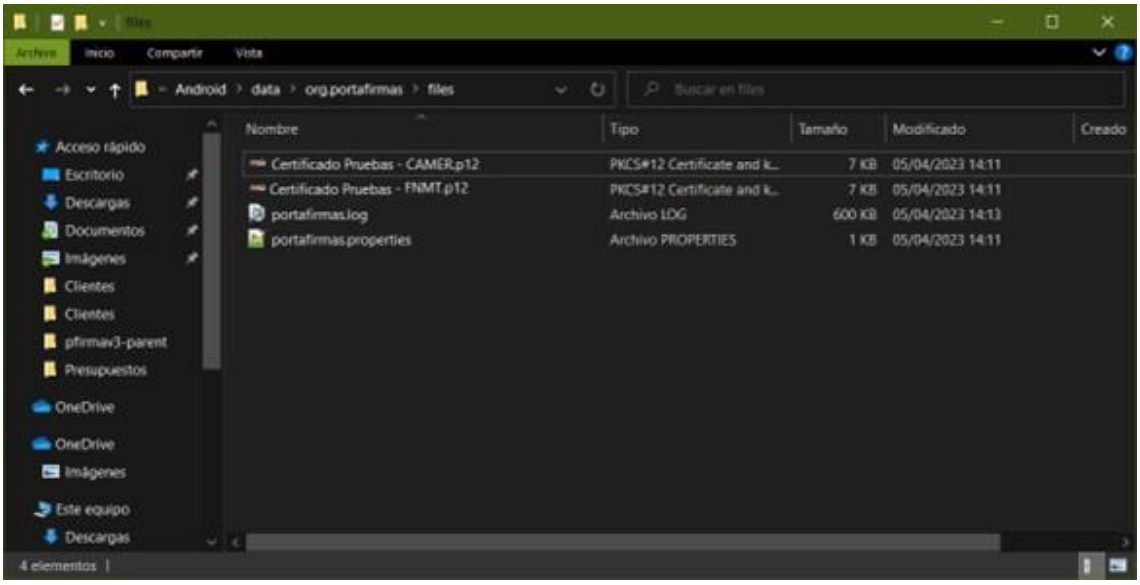
Importación correcta de certificados

Android 10 y superiores

A partir de la versión 10 de Android las aplicaciones sólo pueden usar su ruta específica para lectura y escritura de ficheros. En nuestro caso, al instalar la aplicación, se creará una carpeta dónde debe/n colocarse el/los certificado/s que vamos a usar.

Desde el PC estamos trabajando en **/Android/data/org.portafirmas/files** pero realmente nuestro directorio de trabajo completo es: **/storage/emulated/0/Android/data/org.portafirmas/files** (aunque puede variar dependiendo del fabricante)

La instalación del certificado o certificados debe quedar de la siguiente manera:

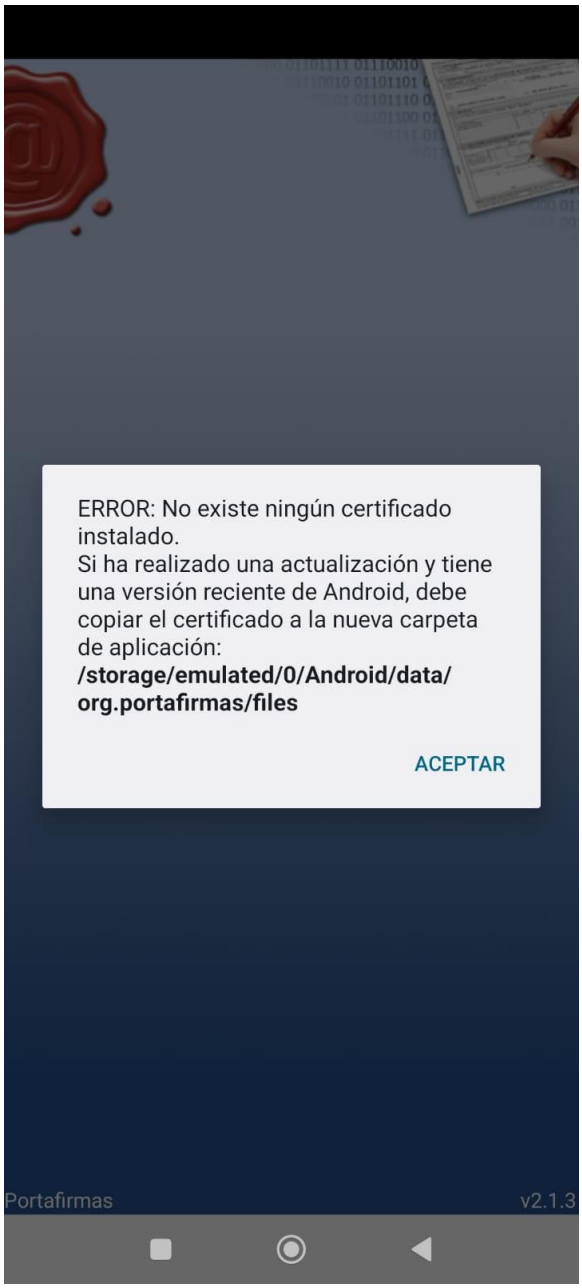


Importación correcta de certificados Android v10 y superiores

Recordar, que al igual que en iOS, el certificado debe tener la extensión "**p12**".

En esta carpeta se almacenará también el fichero "**portafirmas.properties**", que contiene la configuración de las trazas de logs, y el fichero de trazas en sí (**portafirmas.log**).

Si realiza una actualización de la aplicación y su versión de Android es igual a superior a 10, debe mover los certificados del directorio antiguo (no soportado) al nuevo. La aplicación le avisará con un mensaje como el siguiente:



Error de certificado no encontrado e información de cambio de ruta