

# MANUAL DE INSTALACIÓN DE CERTIFICADOS EN DISPOSITIVOS iOS

## 1. Requisitos

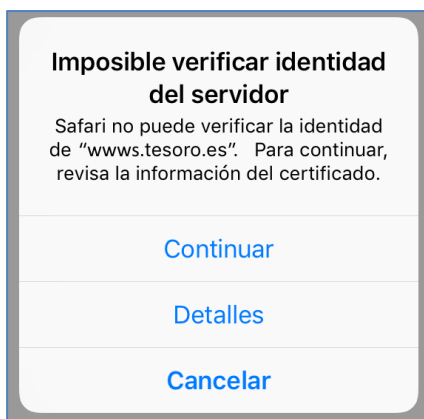
El acceso al SCVV deberá obligatoriamente realizarse con el navegador Safari disponible por defecto en todos los dispositivos iOS. Safari es el único navegador que permite acceder al almacén de certificados en dispositivos iOS.

## 2. Importación de certificados

- 1) Acceder a la página del Servicio de Compra y Venta de Valores (en adelante SCVV) desde un navegador Safari con la URL siguiente:

<https://www.tesoro.es>

Al acceder por primera vez el navegador le dirá que es imposible verificar la identidad del servidor al no tener instalados los certificados del SCVV. Deberá pulsar en **Continuar**.



En el punto siguiente instalaremos los certificados del SCVV para que este aviso no le vuelva a aparecer.

- 2) Se muestra la página de instalación de certificados del SCVV

Al no tener todavía el certificado de usuario se le dirigirá automáticamente 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)

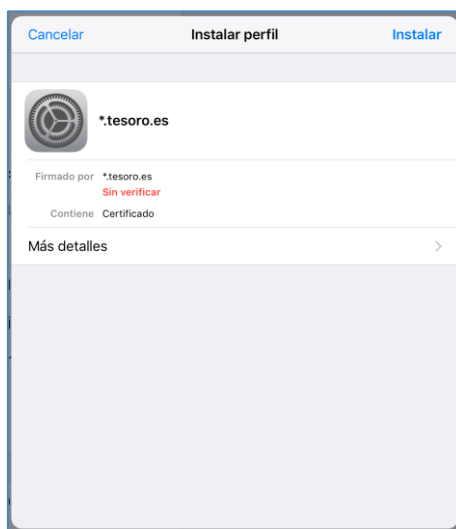
Elija la opción adecuada a su Sistema Operativo para descargar AutoFirma y después proceda a su instalación tras descomprimir el archivo zip:

- 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

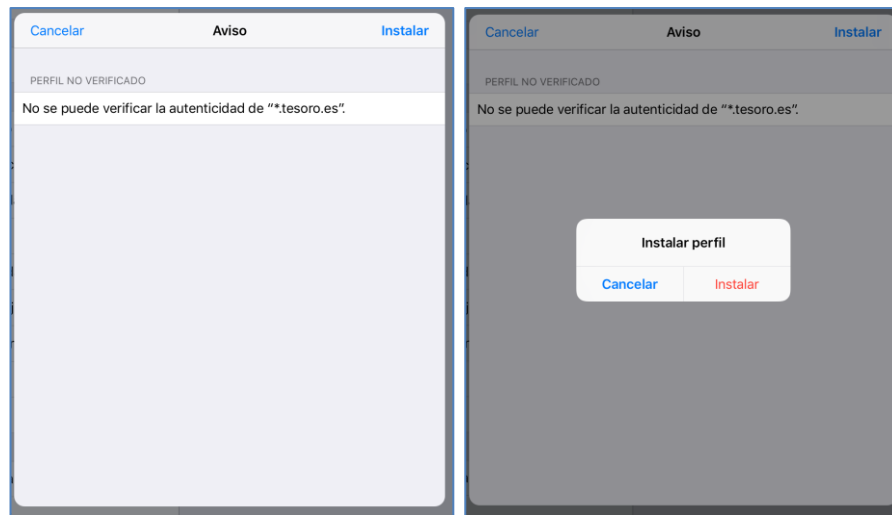
3) Pulsar sobre los enlaces indicados para los tres certificados del SCVV del apartado superior de la página

- 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

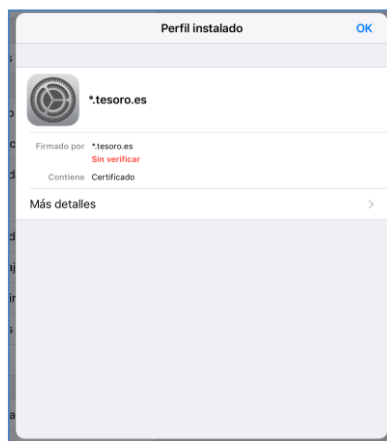
- Al pulsar sobre **\*.tesoro.es** le muestra el aviso siguiente:



Pulse sobre **Instalar** para proceder a la instalación de este certificado y siga los pasos indicados. La validez de este certificado se actualizará automáticamente cuando haya instalado los tres certificados. El sistema vuelve a preguntar si desea instalar el certificado, pulse de nuevo sobre **Instalar**.



Finalmente se mostrara el aviso de instalación correcta del certificado **\*.tesoro.es**, pulse sobre **OK** para salir del asistente y vuelva a Safari.



Repita todos los pasos anteriores para los demás certificados.

- Al pulsar sobre **AC RAIZ FNMT-RCM** se nos muestra el aviso siguiente:



Siga los mismos pasos anteriores para instalar este certificado.

- Al pulsar sobre **AC Componente Informáticos** se nos muestra el aviso siguiente:



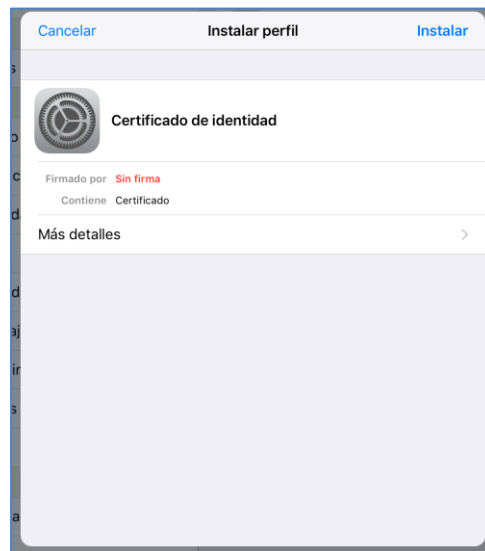
Siga los mismos pasos anteriores para instalar este certificado.

- 4) Para instalar su certificado de usuario en el dispositivo **el usuario deberá enviarse un correo adjuntando su certificado digital** (fichero con extensión “.pfx”).

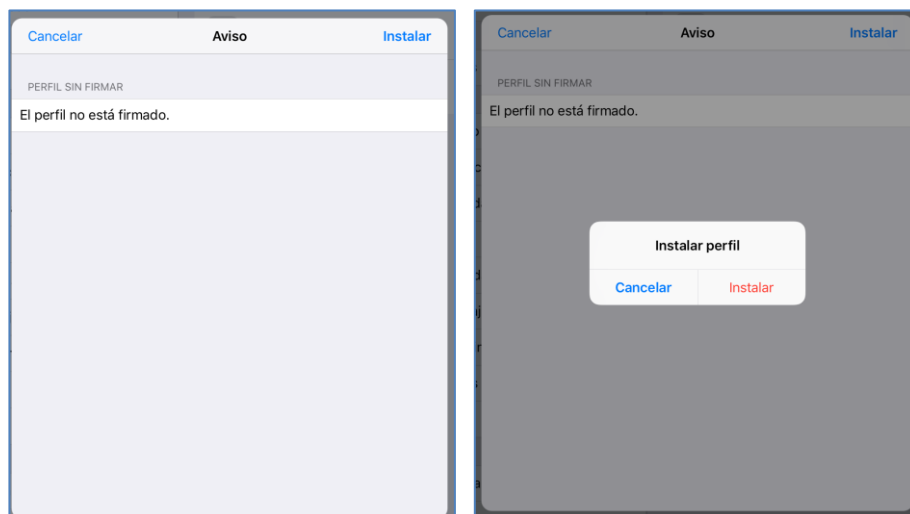
Nota para los usuarios que dispongan del DNle v3 con tecnología sin contacto NFC:

A fecha de hoy Apple no permite la utilización del DNle v3 en los dispositivos más recientes, que disponen de NFC (tecnología de comunicación inalámbrica, de corto alcance que permite el intercambio de datos entre dispositivos), pero las futuras actualizaciones de iOS probablemente lo permitirán y su utilización dependerá de la implementación efectuada en el Cliente móvil @firma (aplicación gratuita), totalmente independiente del Servicio de Compra y Venta de Valores del Tesoro.

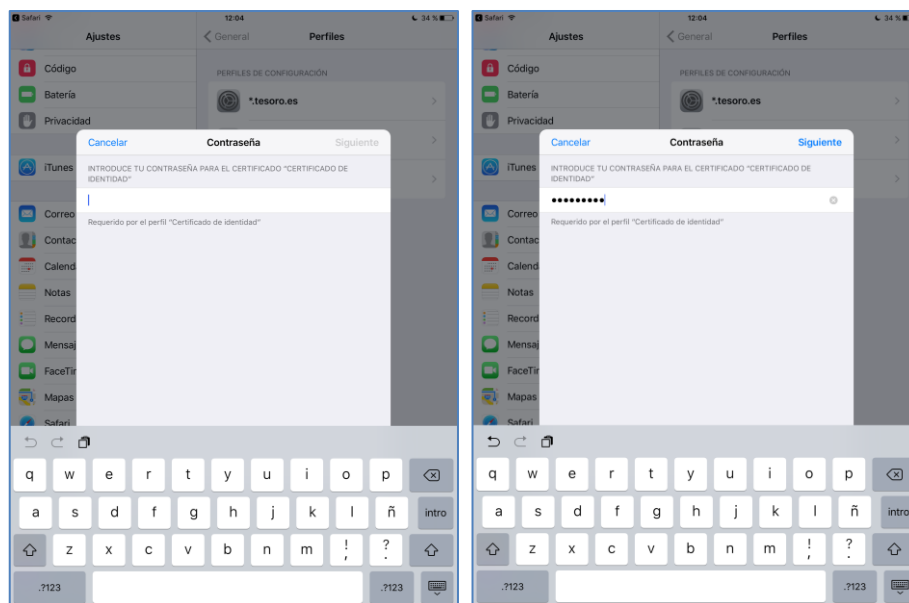
Desde su propio correo cuando pulse sobre su certificado de usuario se le mostrara el asistente de importación de su certificado.



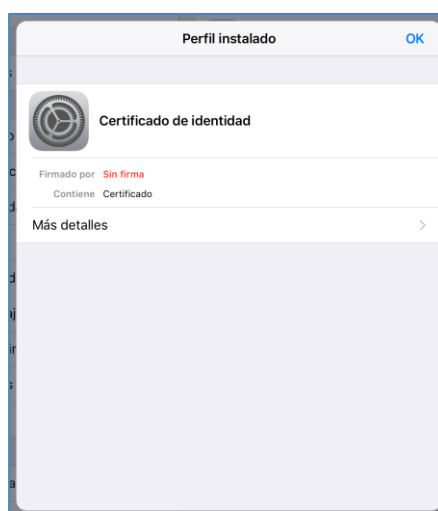
Pulse sobre **Instalar** para proceder a su instalación y siga los pasos indicados:



Introduzca la contraseña de su certificado cuando se le solicite y pulse **Siguiente**:



Al finalizar la instalación de su certificado de usuario, pulse sobre **OK**:



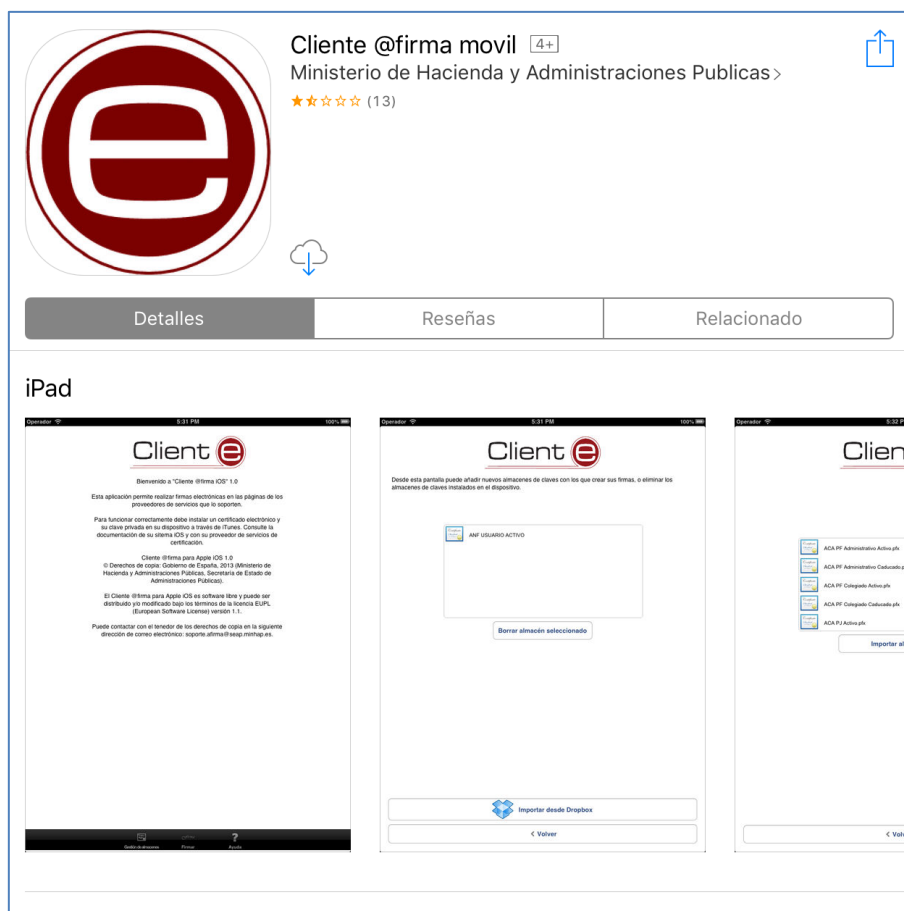
### 3. Instalación cliente móvil @firma y configuración

Desde la página de descargas seleccione la opción Cliente móvil @firma (aplicación gratuita del App Store) para sistemas Apple iOS. Desde este enlace accederá a la tienda del App Store 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 (mantener pulsado para abrir el enlace en el App Store):

<https://itunes.apple.com/es/app/cliente-firma-movil/id627410001>



- Si ya tenía el Cliente móvil @firma instalado previamente en el dispositivo:

No es necesario importar su certificado de usuario en el Cliente móvil de @firma para poder firmar operaciones. Al haberse ya previamente realizado ésta importación en su dispositivo la aplicación lo utilizara automáticamente avisándole para que confirme su utilización.

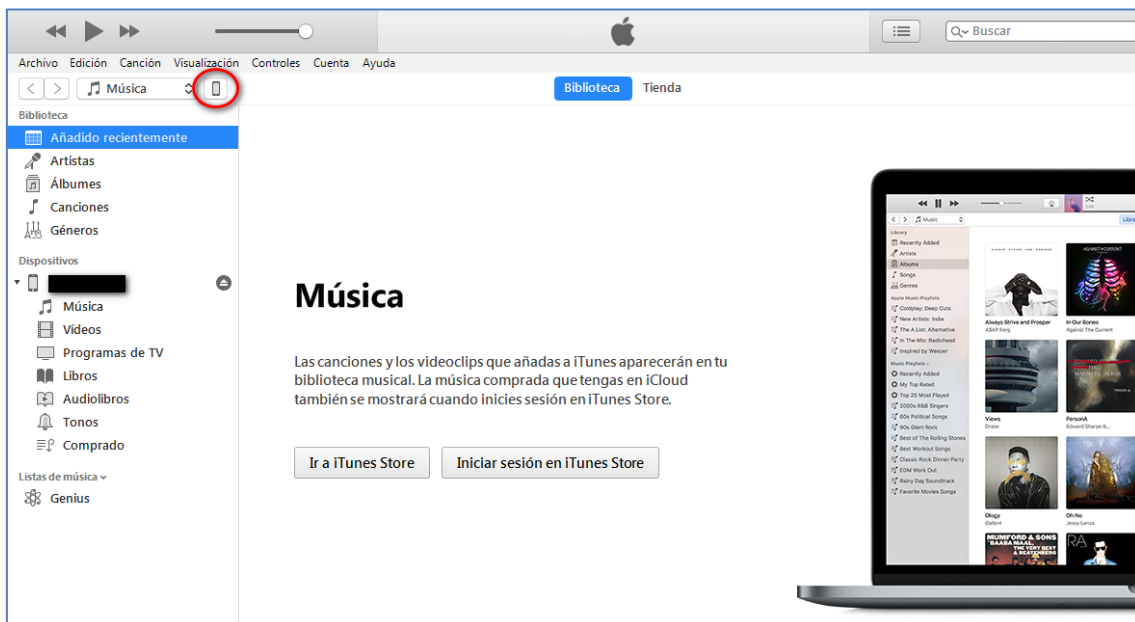
- Si es la primera instalación del Cliente móvil @firma en el dispositivo:

**Nota:** estas indicaciones son propias del Cliente móvil @firma y pueden estar sujetas a cambios según las actualizaciones del propio Cliente móvil @firma disponible en el App Store.

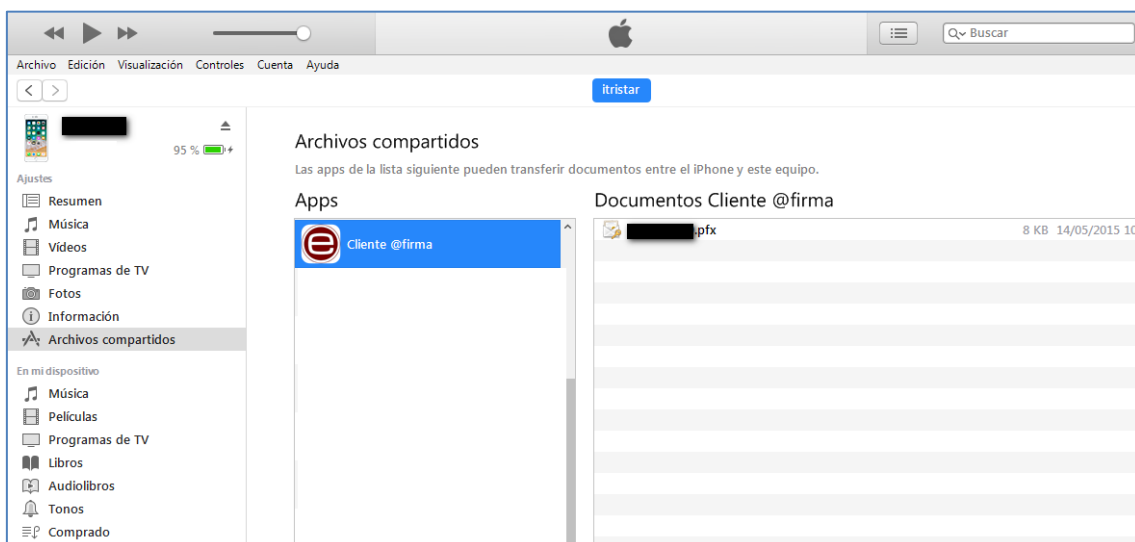
Deberá importar su certificado de usuario, para esto es obligatoria la instalación de la aplicación **iTunes de Apple** en un ordenador de escritorio. Para efectuarlo acceda a la página de Apple para efectuar su descarga e instalación.

<https://www.apple.com/es/itunes/download/>

Una vez correctamente instalado iTunes, conecte su dispositivo y le aparecerá un aviso preguntándole si confía en éste ordenador. Tras haber seleccionado que confía en su ordenador verá su dispositivo móvil en el panel de navegación.

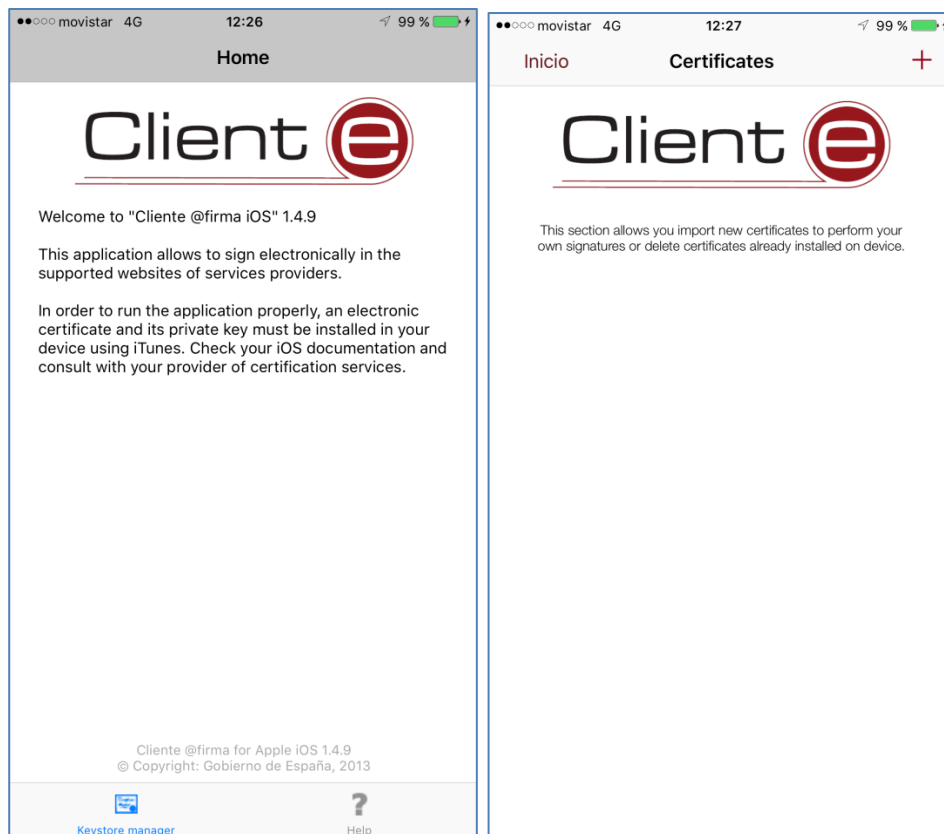


Pulse sobre el icono indicado con un círculo rojo, en la imagen anterior, para acceder a los **Archivos compartidos** (imagen siguiente) de su dispositivo. En la parte derecha, indicada por **Apps**, seleccione el **Cliente @firma** y sobre el panel de la derecha **Documentos Cliente @firma** arrastre el fichero PFX de su certificado para que este sea accesible desde la aplicación del Cliente móvil @firma de su dispositivo.

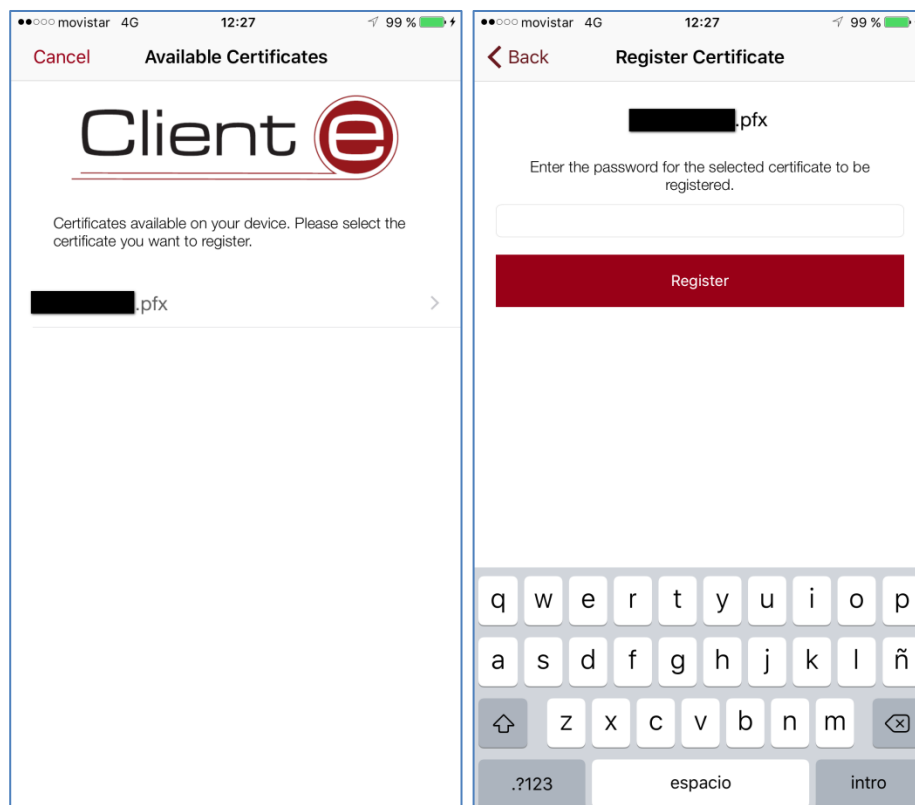


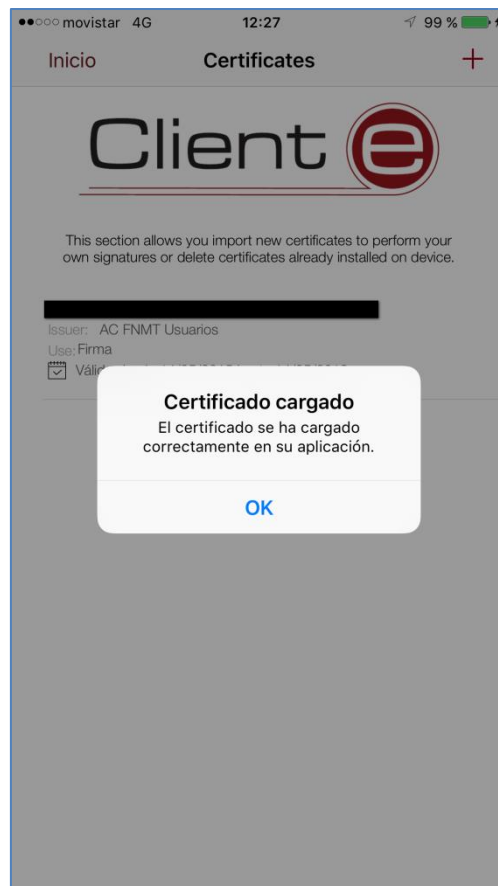
Una vez realizada esta operación, desconecte su dispositivo del ordenador y abra la aplicación Cliente móvil @firma para importar su certificado de usuario. En el menú del Cliente móvil @firma encontrará una opción de instalación de certificados **Keystore Manager** en la parte inferior.





Pulse sobre el símbolo **+** de la parte superior para agregar su certificado (añadido desde iTunes) e introduzca la contraseña del certificado cuando se le solicite.



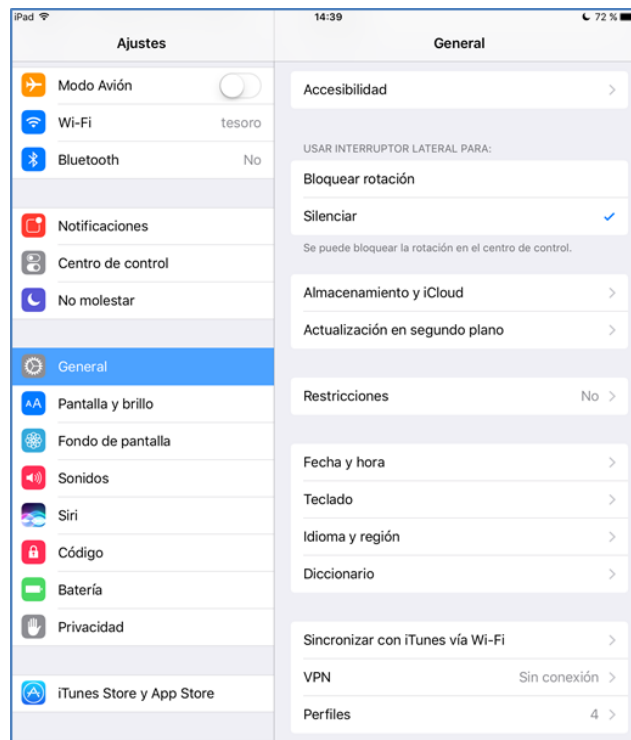


Este será el certificado que se usará en todas las operaciones de firma del SCVV.

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

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

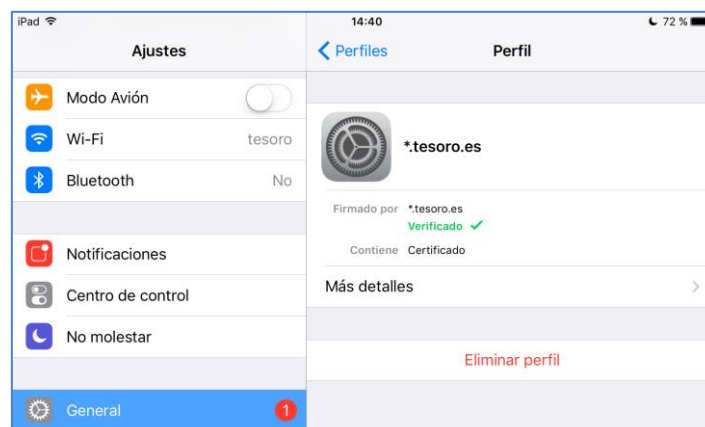
Si desea eliminar todos sus certificados del dispositivo, deberá acceder a las Ajustes de su dispositivo, ir a las opciones Generales y seleccionar la opción Perfiles:



Se muestran los perfiles existentes en el sistema:



Para eliminarlos es necesario seleccionarlos de uno en uno y pulsar sobre **Eliminar perfil**:



En la propia aplicación del Cliente móvil @firma, para eliminar el certificado arrastre hacia la izquierda el certificado para que le aparezca la opción de **Eliminar**:

