Configuración de la Firma Electrónica en macOS

Autor: Javier Batista.
Versión: 1.3

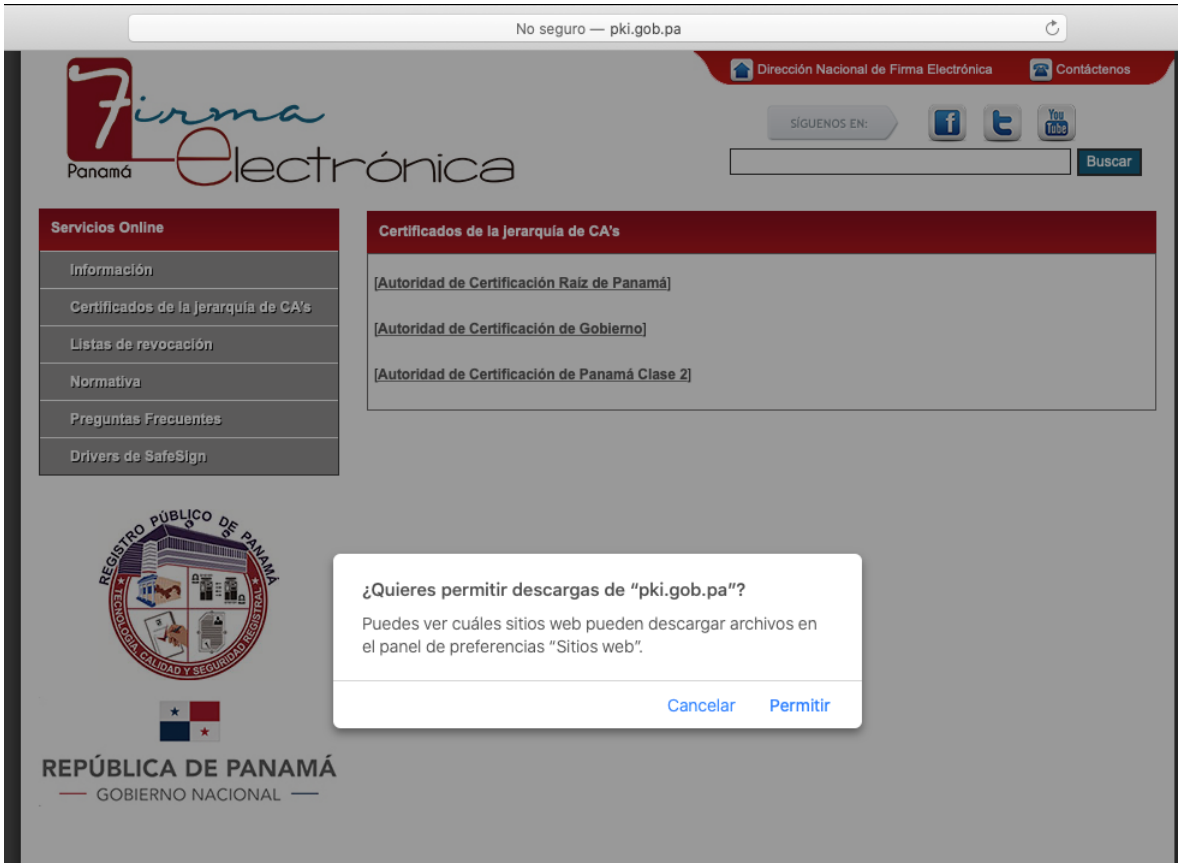
1. Descarga de los 3 Certificados de la jerarquía de CA's

Como primer paso, se debe ingresar a la dirección http://www.pki.gob.pa -> **Certificados de la jerarquía de CA's** y descargar los 3 certificados (http://www.pki.gob.pa/cert.htm):

http://www.pki.gob.pa/cacerts/caraiz.crt (Autoridad de Certificación Raíz de Panamá)

http://www.pki.gob.pa/cacerts/cagob.crt (Autoridad de Certificación de Gobierno)

http://www.pki.gob.pa/cacerts/capc2.crt (Autoridad de Certificación de Panamá Clase 2)



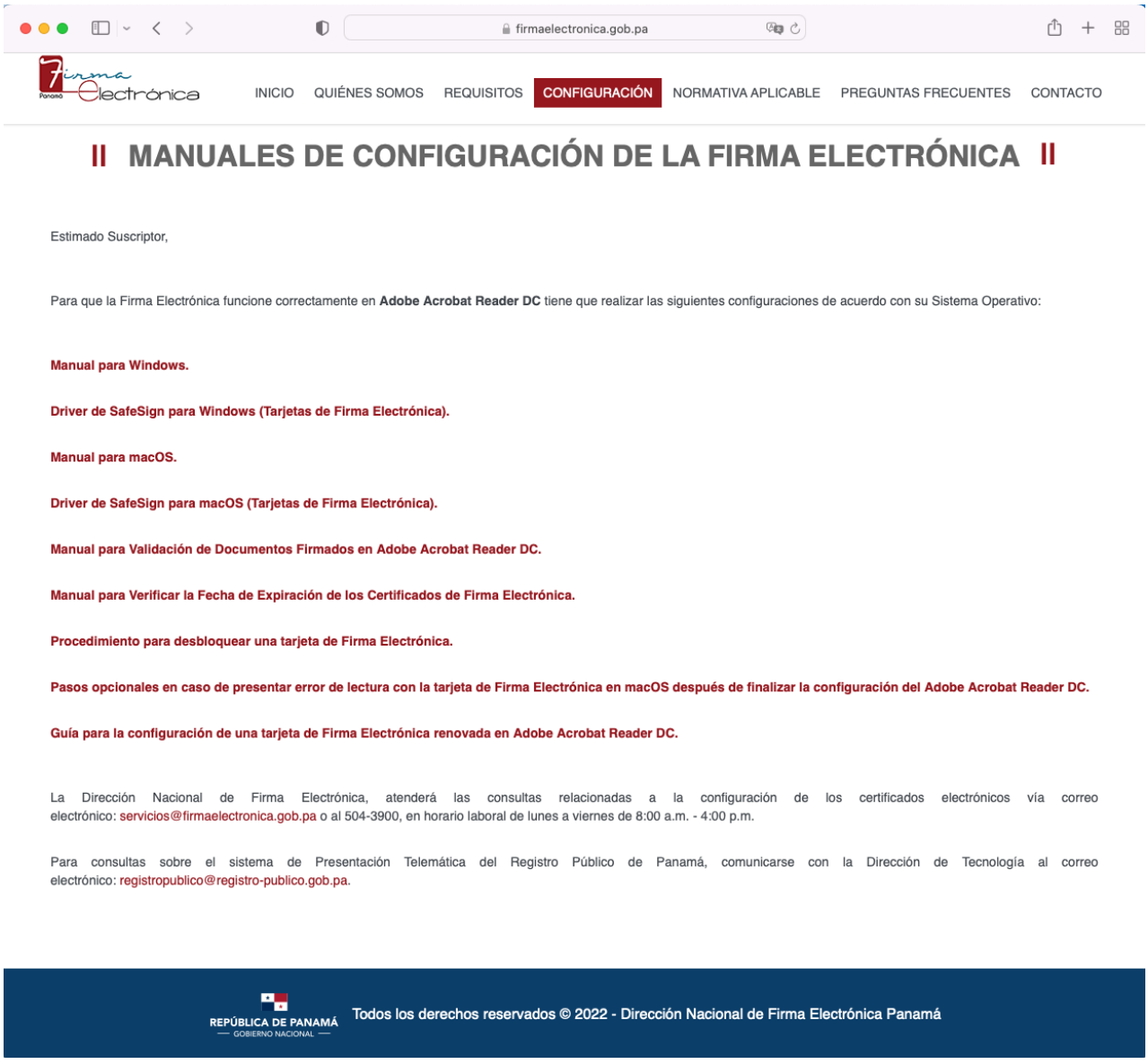
Al utilizar un navegador como Safari y al dar click en cada uno de los enlaces se debe permitir la descarga, posteriormente los archivos quedarán en la carpeta de **Descargas** o la seleccionada por el usuario.

2. Descarga e instalación del controlador de SafeSign para las tarjetas inteligentes

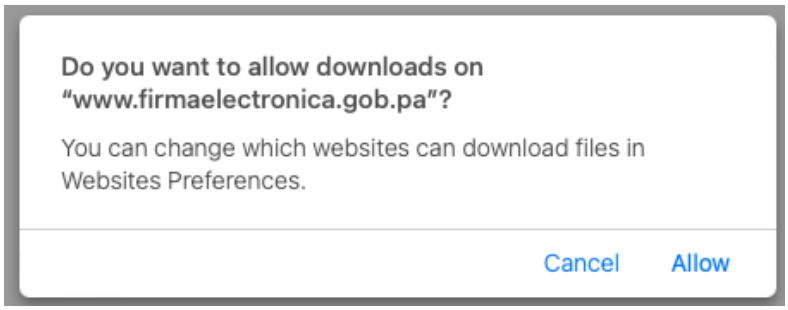
Utilizando el navegador de preferencia, por ejemplo: Safari, se debe ingresar a la dirección https://www.firmaelectronica.gob.pa/ -> **Configuración** y descargar el instalador de SafeSign para macOS, el cual es utilizado por las tarjetas de Firma Electrónica:

https://www.firmaelectronica.gob.pa/drivers/SafeSign_IC_Standard_MacOS_3.7.0.1-AET.000_universal.dmg.zip

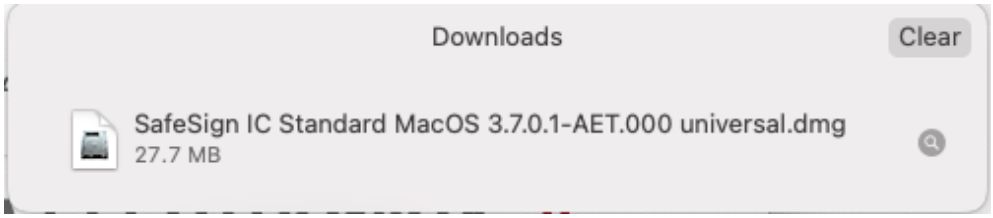
Al finalizar la descarga, se debe descomprimir el archivo para ejecutar el instalador **SafeSign_IC_Standard_MacOS_3.7.0.1-AET.000_universal.dmg** presionando doble click con el **Mouse** y posteriormente se deben seguir las instrucciones por defecto en pantalla.



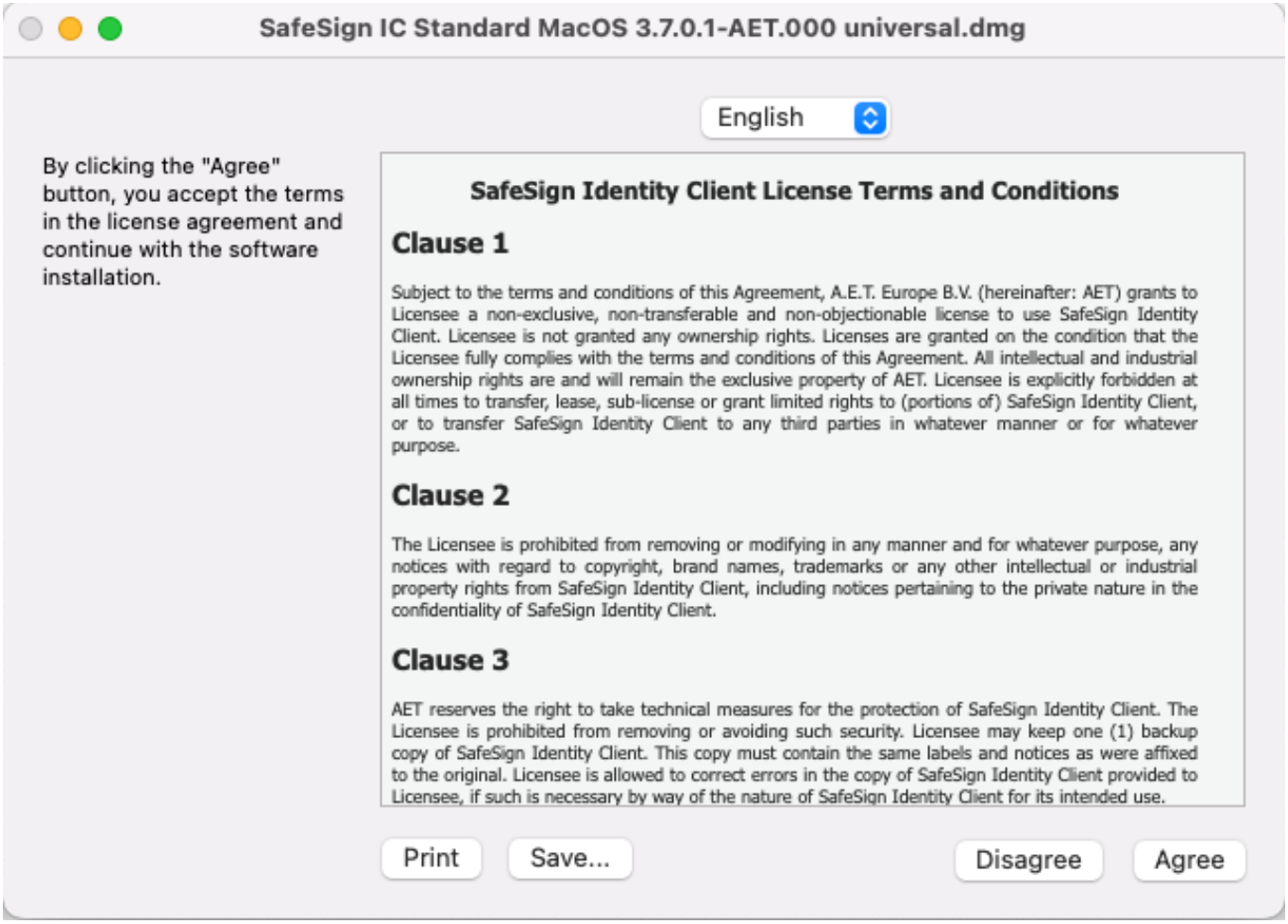
Página web de Configuración de la Firma Electrónica, donde se deberá presionar el enlace "Driver de SafeSign para macOS (Tarjetas de Firma Electrónica)".



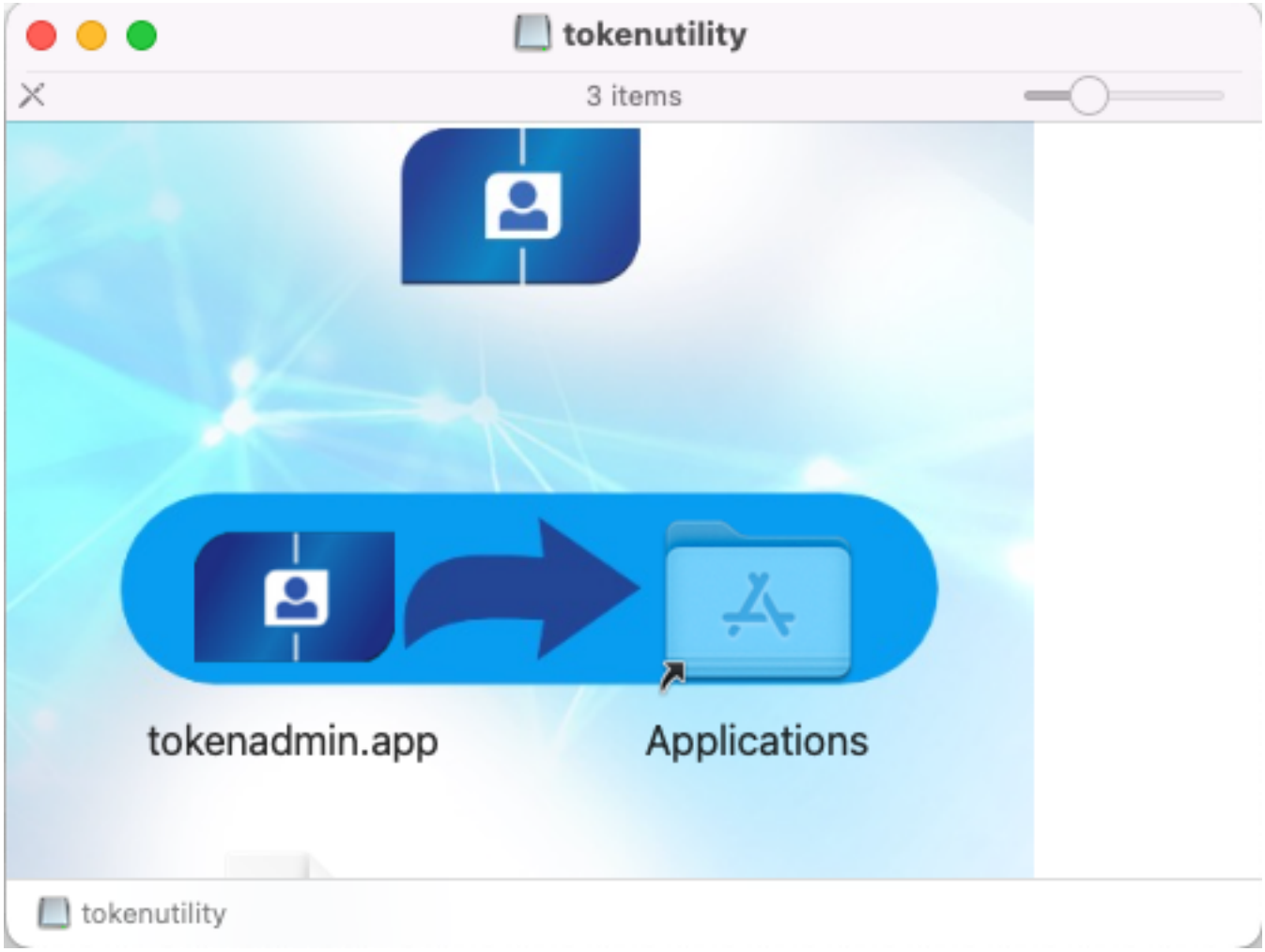
Si se utiliza Safari, se debe permitir la descargar.



Se ejecuta el archivo SafeSign IC Standard MacOS 3.7.0.1-AET.000 universal.dmg.

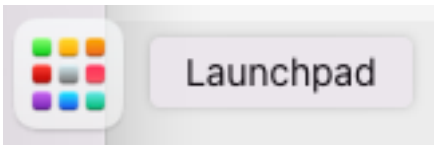


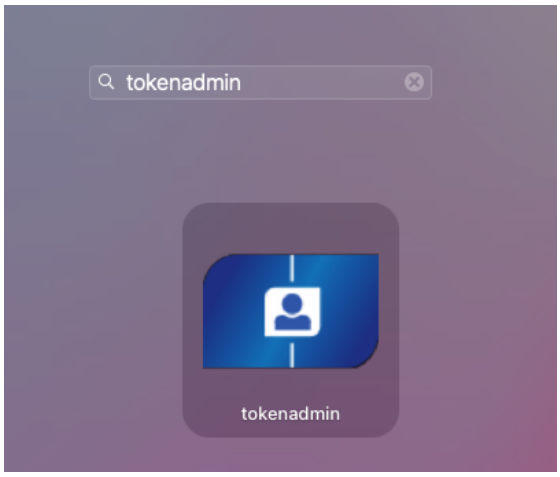
Se presiona el botón Agree para continuar con la instalación.



Se debe arrastrar el icono tokenadmin.app a la carpeta de Aplicaciones.

Al finalizar la instalación, podrá encontrar el programa escribiendo **tokenadmin** en la opción de búsqueda del **Launchpad**.

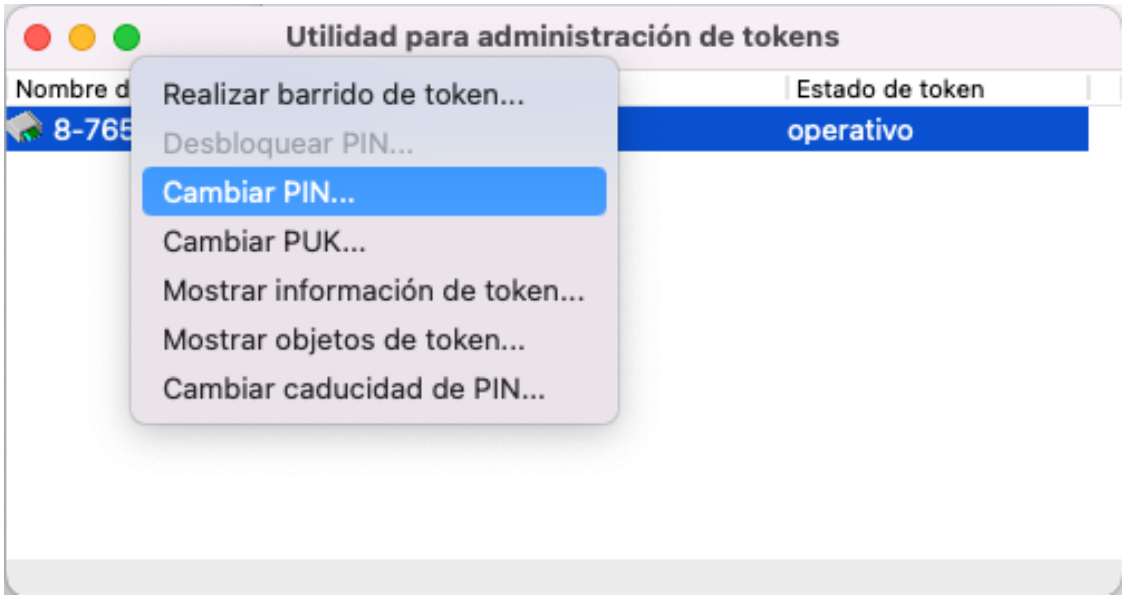


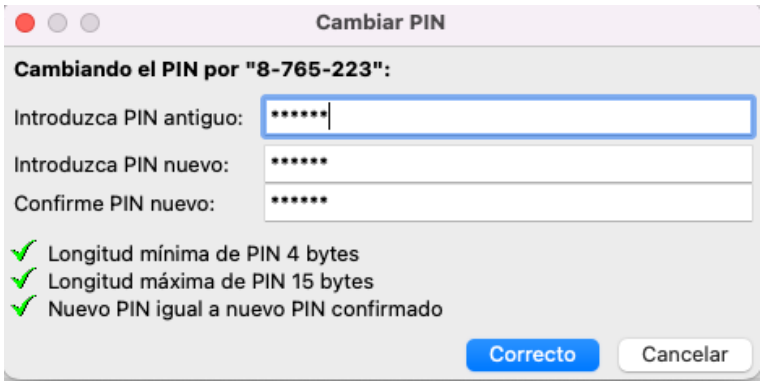


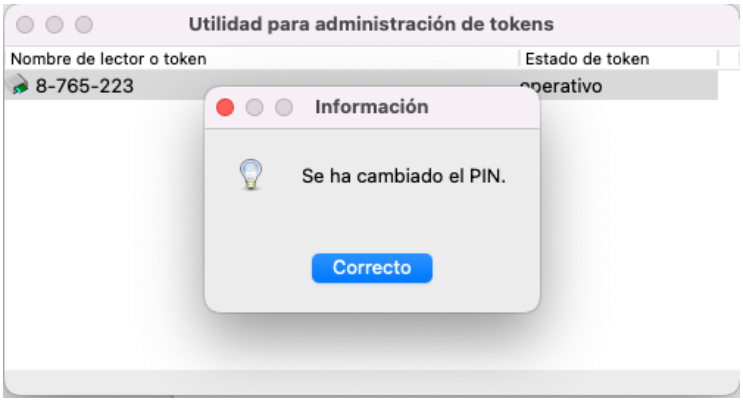
Al ejecutar el **TokenAdmin** la primera vez, se deberá presionar el botón de **Abrir** para que pueda ser ejecutado y posteriormente, aparecerá el programa **Utilidad para administración de tokens** con la cédula de su tarjeta, si la misma se encuentra insertada en el lector USB conectado a su computadora.

Nota importante: en ocasiones y principalmente en el sistema operativo **macOS**, puede ocurrir un error de lectura con la tarjeta y el lector al momento de conectarlo al puerto USB, el cual provoca que la cédula no aparezca en la ventana del programa **TokenAdmin** y en ese caso, se puede desconectar el lector desde el puerto USB (sin retirar la tarjeta del mismo) y volverlo a conectar, manteniendo la ventana del **TokenAdmin** abierta, donde la luz verde del lector debería encenderse y mostrar la cédula en pantalla (si de casualidad la cédula sigue sin mostrarse pero la luz verde encendida, se puede cerrar y volver abrir el programa **TokenAdmin** donde ya debería aparecer la cédula). Para mayor referencia, puede consultar la siguiente guía donde se detalla el problema mencionado: https://www.firmaelectronica.gob.pa/manuales/Error-de-Lector-macOS.pdf.

Cuando la cédula aparece en el programa **TokenAdmin**, con el botón derecho del Mouse sobre el número de la cédula y la opción de **Cambiar PIN**, podrá cambiar el número de PIN de su tarjeta por si desea utilizar una contraseña propia, colocando el PIN actual y el nuevo dos veces (dicha opción se encuentra también disponible en el menú **Token -> Cambiar PIN)**.







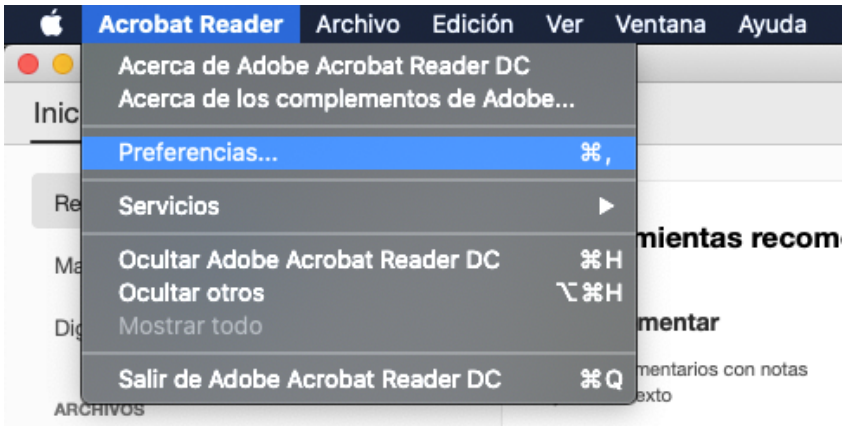
Si se escribe el número PIN de forma incorrecta 3 veces, la tarjeta se bloqueará y la única forma de desbloquearla es con el código PUK del sobre y para ese propósito se puede usar la opción de **Desbloquear PIN** que aparece con el botón derecho del **Mouse** en la cédula. De igual forma, las opciones de cambiar el PIN y desbloquearlo se encuentran también en el menú superior de **Token**.

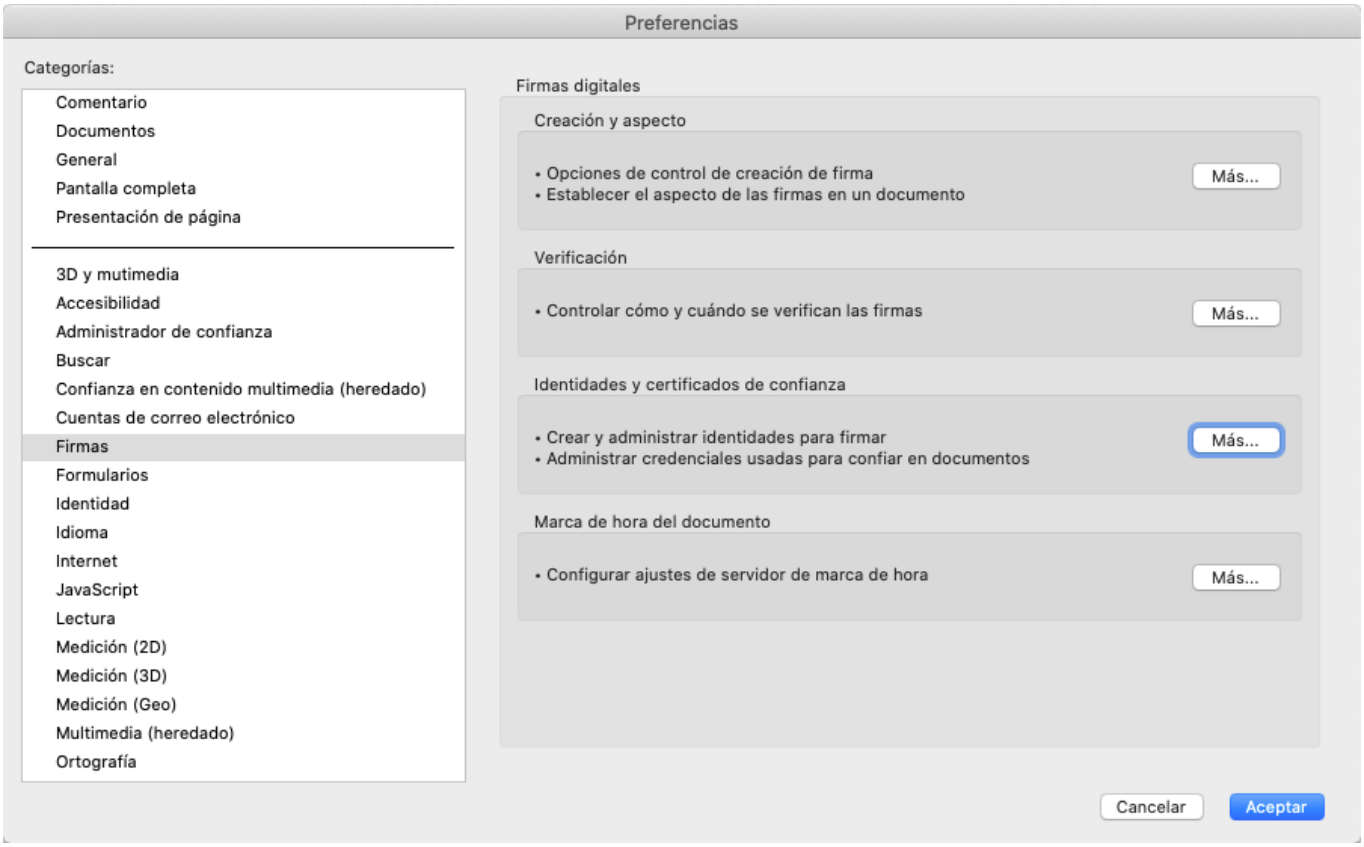
3. Configuración del Adobe Acrobat Reader DC para utilizar la Firma Electrónica.

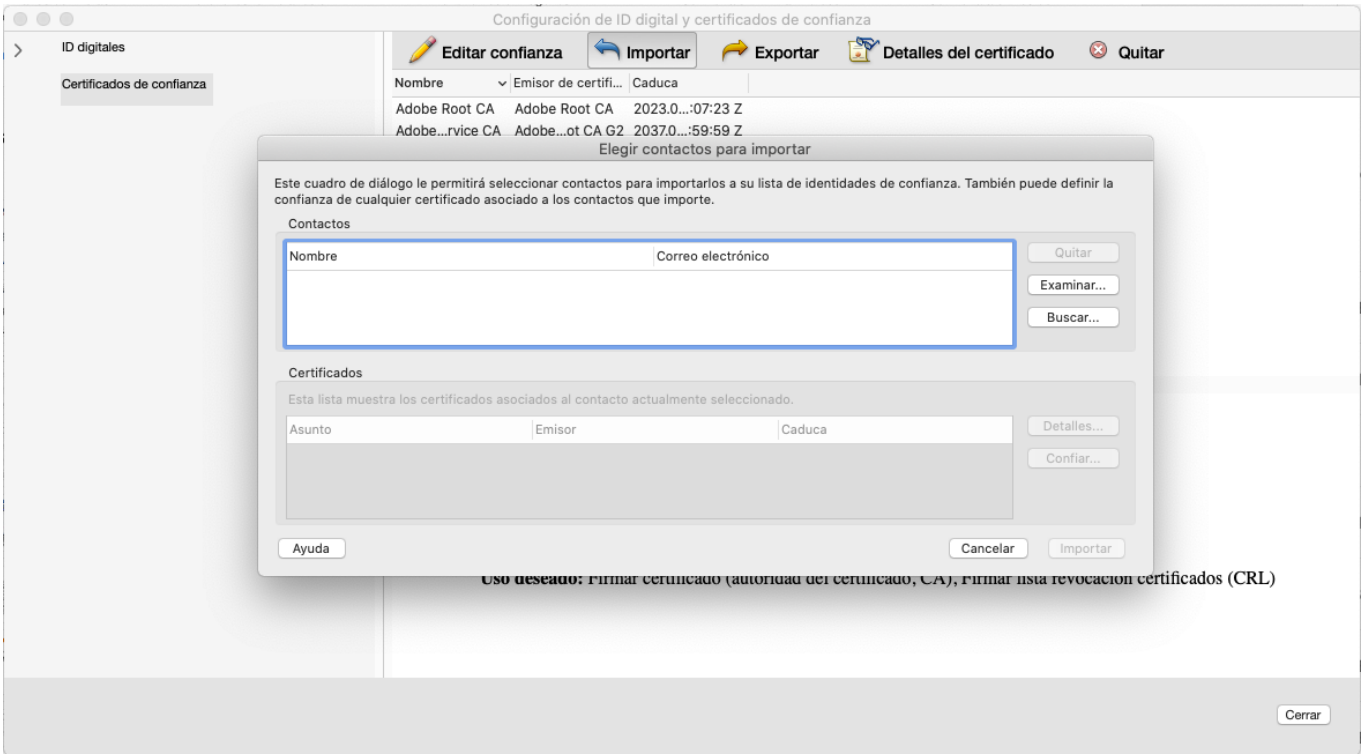
Importación de los 3 certificados de la CA Raíz e Intermedias

Para firmar documentos PDF existen diversos programas que brindan dichas opciones, donde algunos son gratuitos y otros con licencia comercial. En este tutorial recomendamos utilizar la versión gratuita del Adobe Acrobat Reader DC que cuenta con las opciones de firmar electrónicamente los documentos con sellado de tiempo. En caso de no tenerlo instalado, se puede descargar desde la siguiente dirección: https://get.adobe.com/es/reader/ y se instala siguiendo las instrucciones.

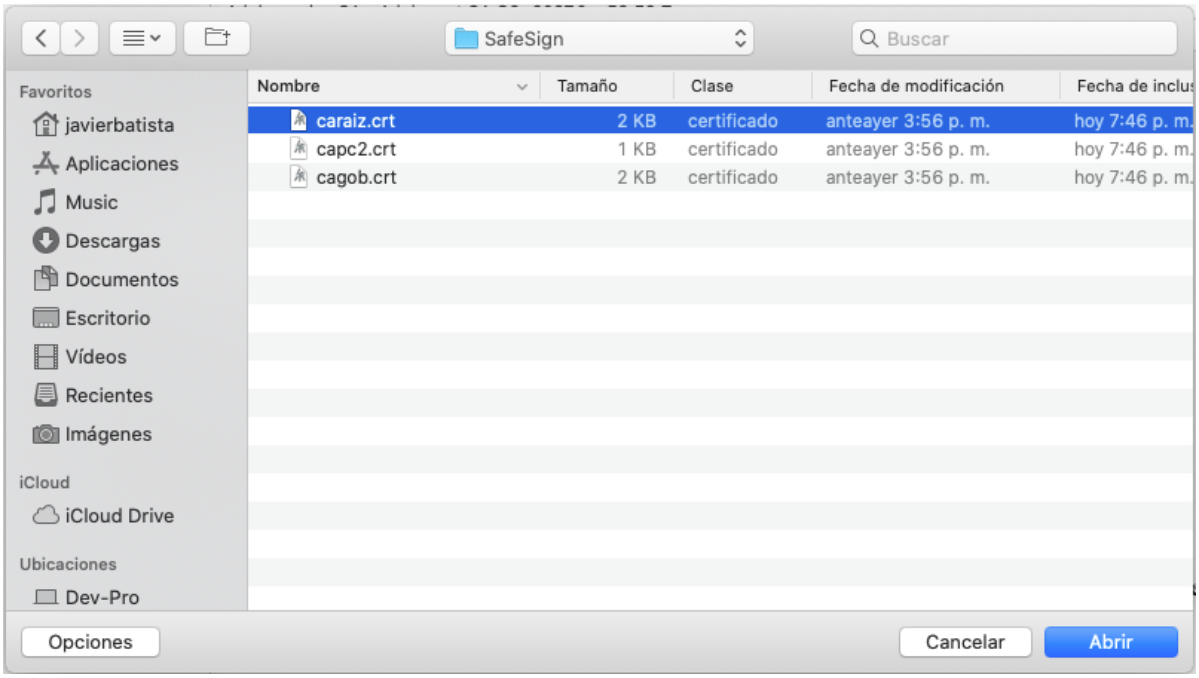
Posteriormente se deben importar los 3 certificados de la CA descargados en el primer punto y se habilitan en el Adobe Reader para que pueda validar los documentos firmados con las tarjetas. Para lograr esto, nos dirigimos a la opción de **Acrobat Reader -> Preferencias -> Firmas ->** botón de **Más** en **Identidades y certificados de confianza** (tercero) **-> Certificados de confianza -> Importar.**

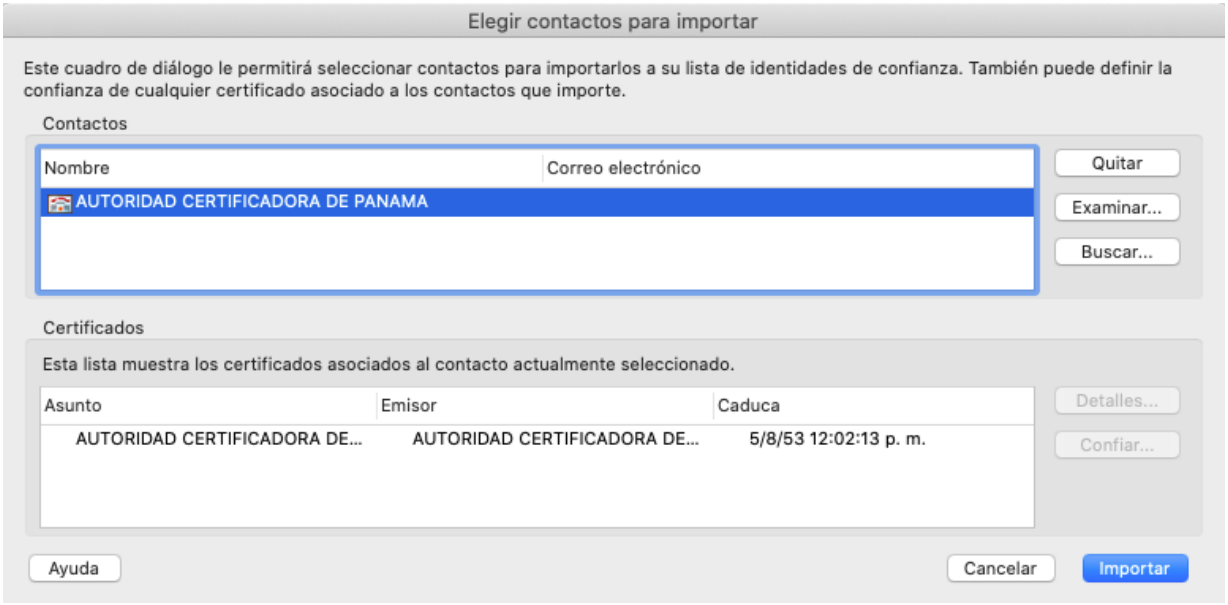




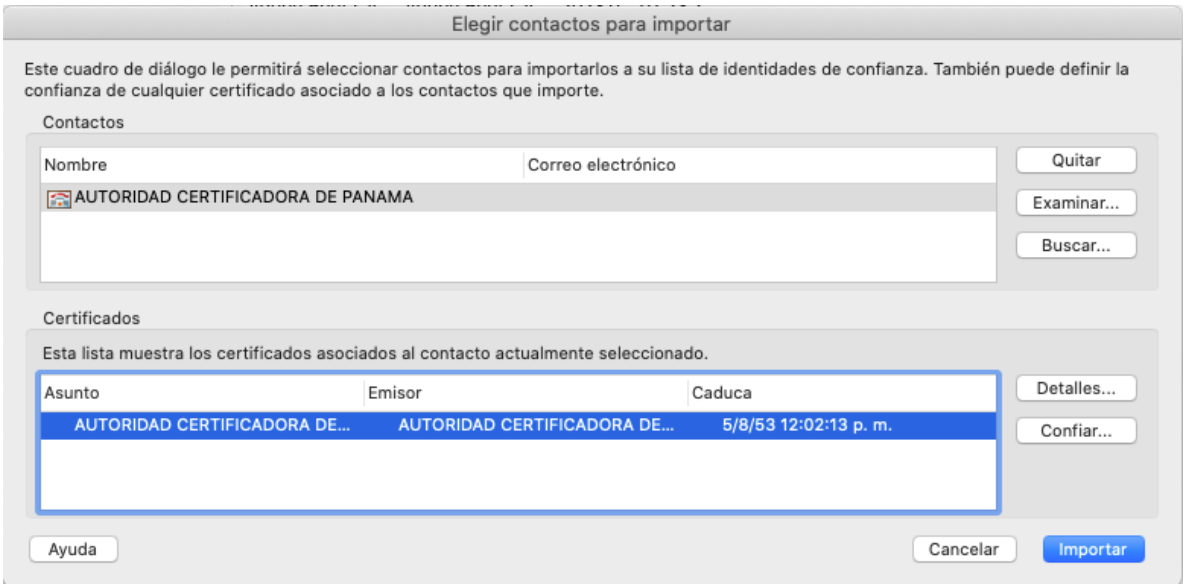


En la opción de **Importar** aparecerá la ventana de **Elegir contactos para importar** y se presiona el botón de **Examinar…** para buscar primero el certificado **caraiz**, se selecciona y se da click en el botón de **Abrir**.

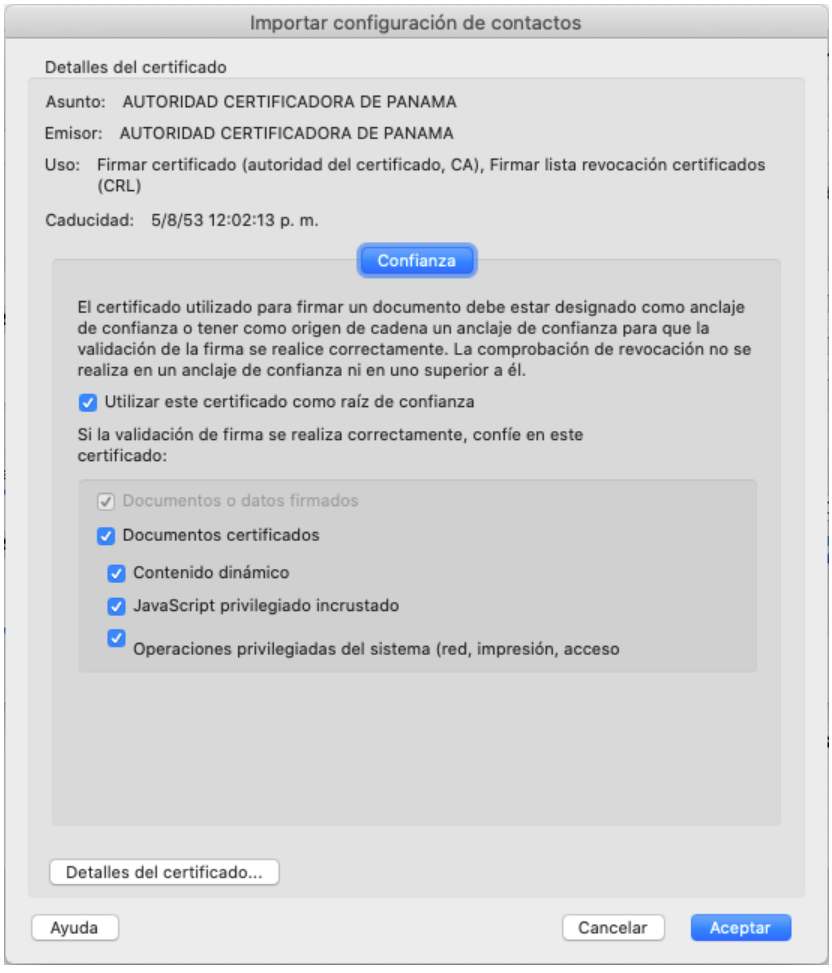


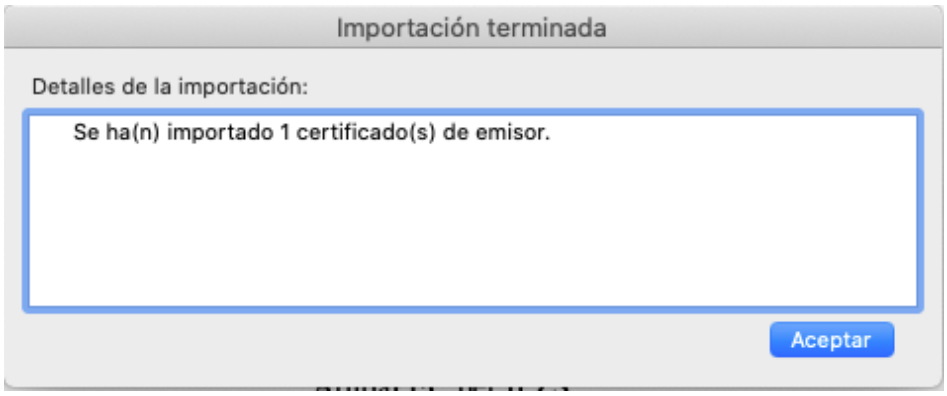


El certificado **AUTORIDAD CERTIFICADORA DE PANAMA** quedará en la ventana de **Contactos**, se debe seleccionar para que también aparezca debajo en **Certificados**. Se vuelve a seleccionar el mismo nombre en el área de Certificados (ver imagen inferior) para que se habilite el botón de **Confiar**.

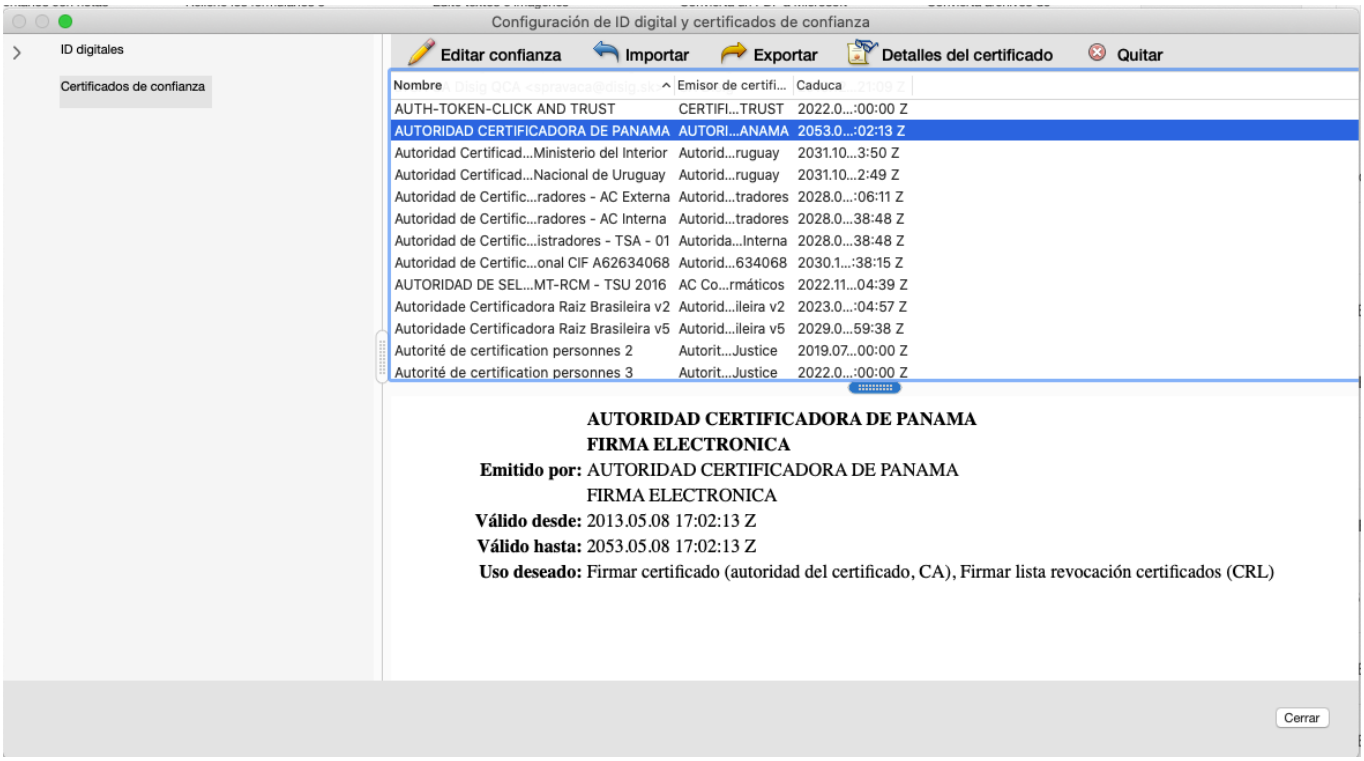


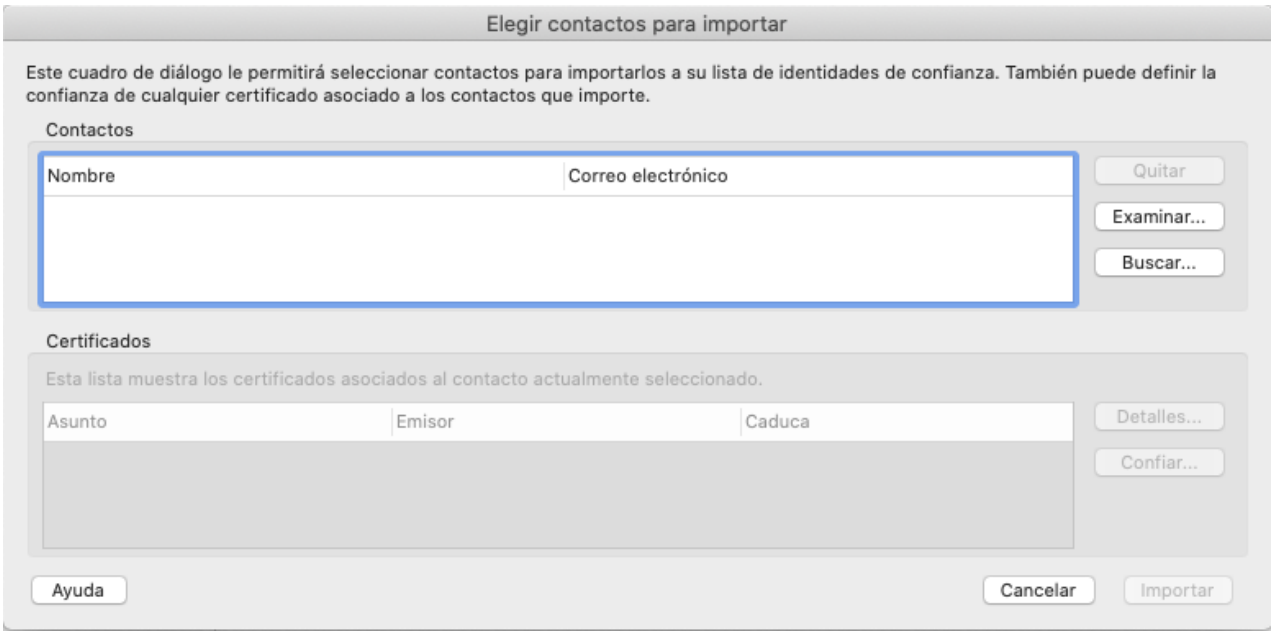
Al dar click en **Confiar…** aparecerá otra ventana llamada **Importar configuración de contactos**, donde se deben marcar todas las casillas empezando con "**Utilizar este certificado como raíz de confianza**" hasta la última. Se presiona el botón de **Aceptar** y luego **Importar** en la ventana anterior. Al final deberá aparecer un mensaje indicando que la importación ha sido terminada.

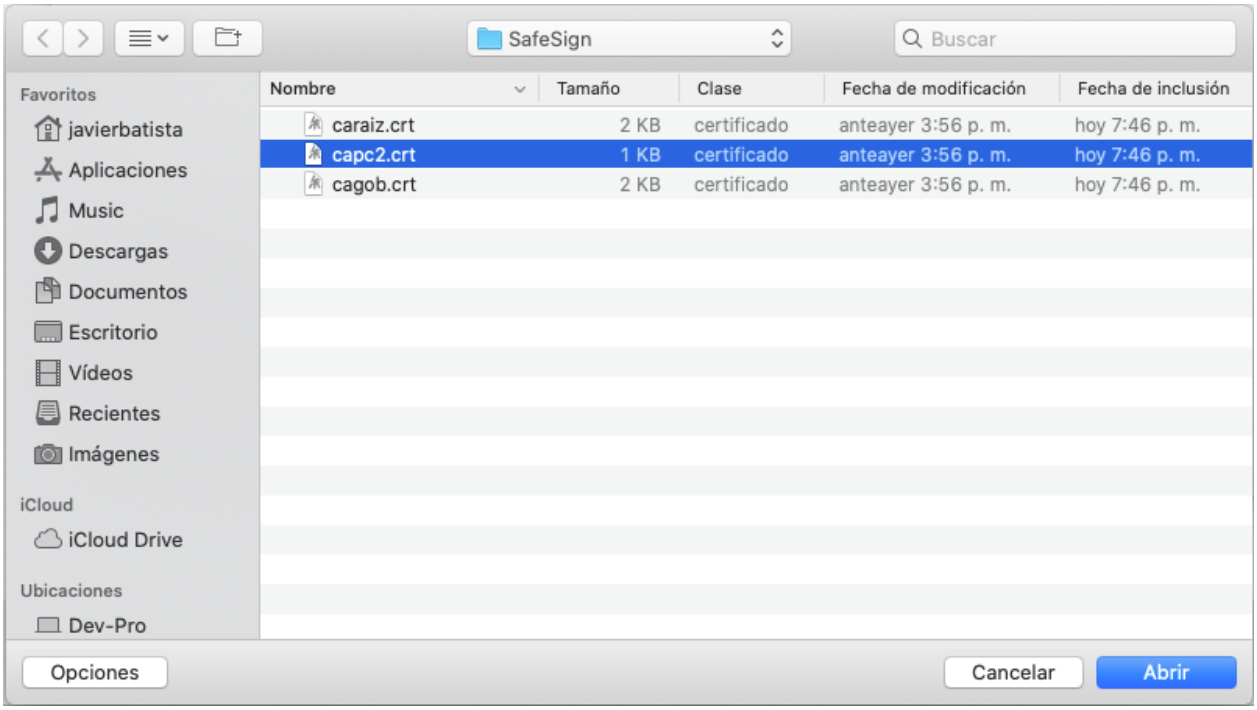


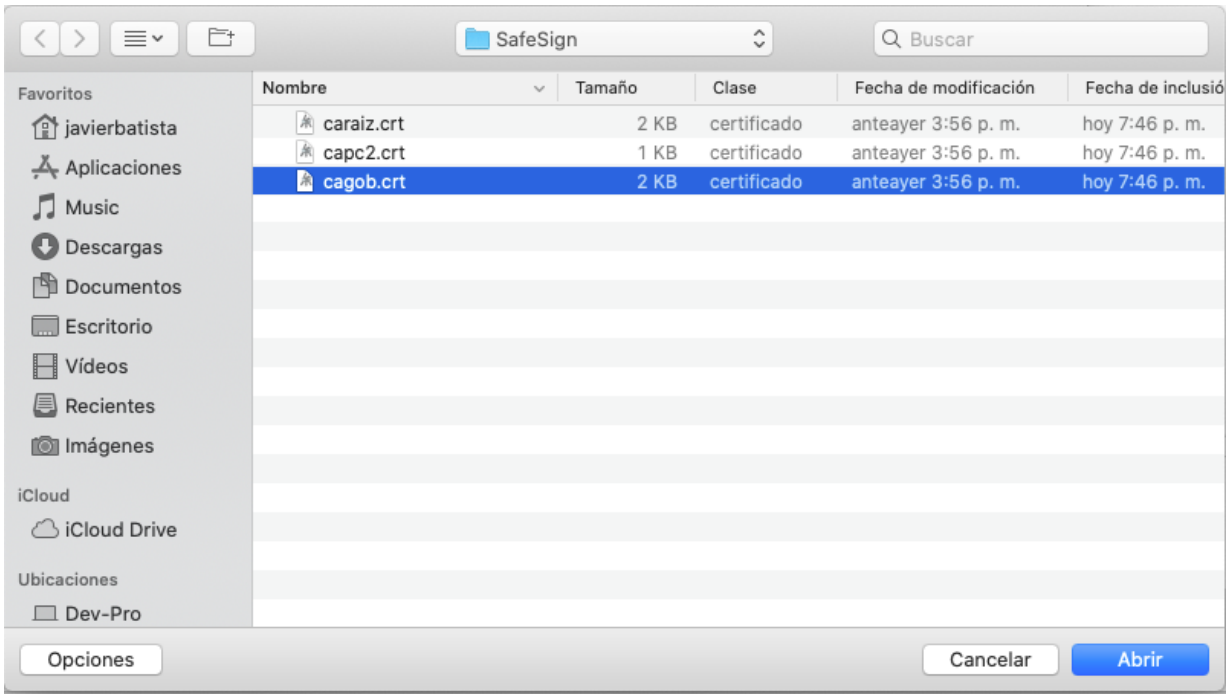


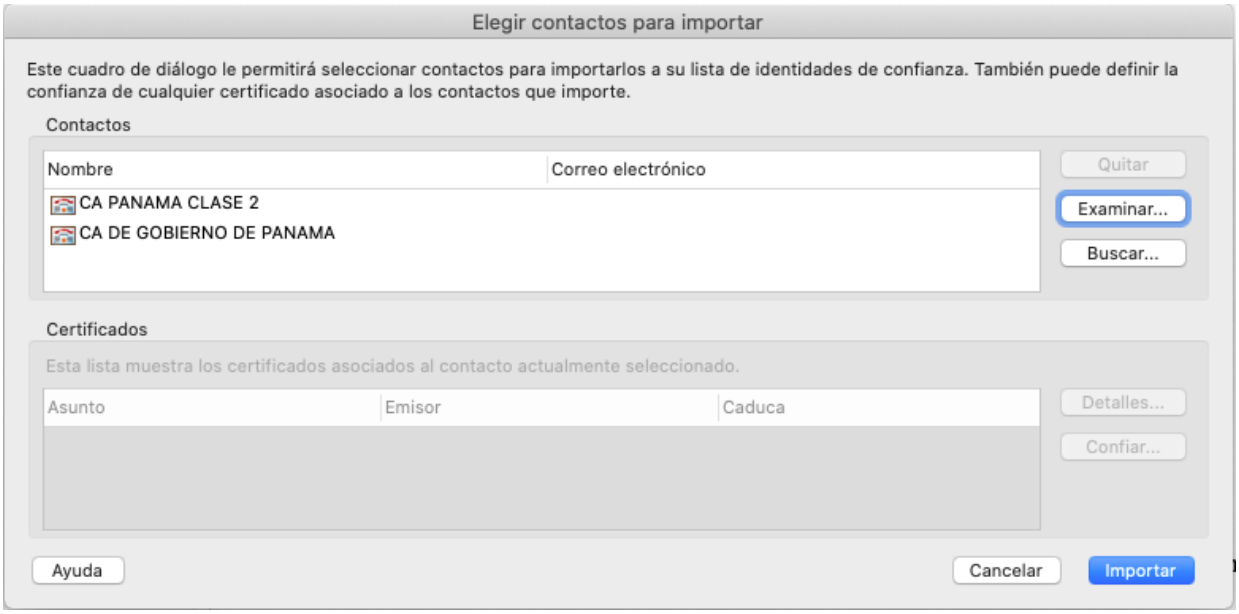
Se deben repetir los pasos mencionados con los certificados **capc2** y **cagob**, sólo que no será necesario presionar el botón de **Confiar** en la ventana de **Elegir contactos para importar** ya que ellos deben heredar la confianza del certificado raíz.

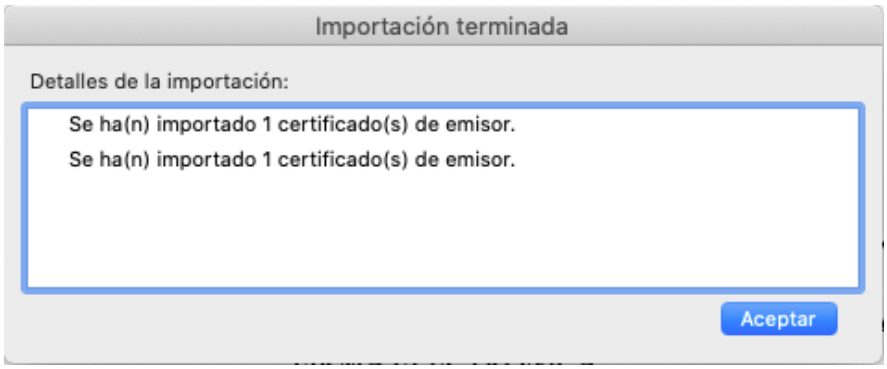



Elegir contactos para importar
Este cuadro de diálogo le permitirá seleccionar contactos para importarlos a su lista de identidades de confianza. También puede definir la confianza de cualquier certificado asociado a los contactos que importe.
Contactos
Nombre
Correo electrónico
Quitar
Examinar...
Buscar...
Certificados
Esta lista muestra los certificados asociados al contacto actualmente seleccionado.
Asunto
Emisor
Caduca
Detalles...
Confiar...
Ayuda
Cancelar
Importar

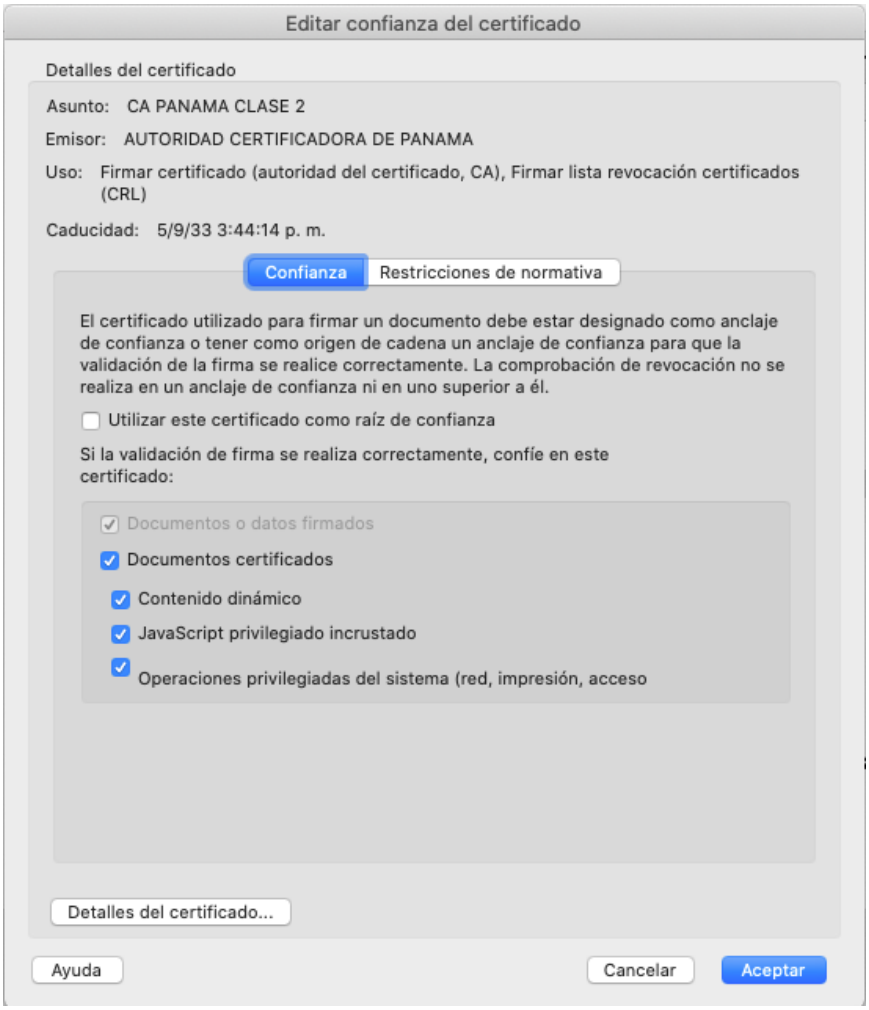

SafeSign
Buscar
Favoritos
javierbatista
Aplicaciones
Music
Descargas
Documentos
Escritorio
Vídeos
Recientes
Imágenes
iCloud
iCloud Drive
Ubicaciones
Dev-Pro
Nombre
Tamaño
Clase
Fecha de modificación
Fecha de inclusión
caraiz.crt 2 KB certificado anteayer 3:56 p. m. hoy 7:46 p. m.
capc2.crt 1 KB certificado anteayer 3:56 p. m. hoy 7:46 p. m.
cagob.crt 2 KB certificado anteayer 3:56 p. m. hoy 7:46 p. m.
Opciones
Cancelar
Abrir

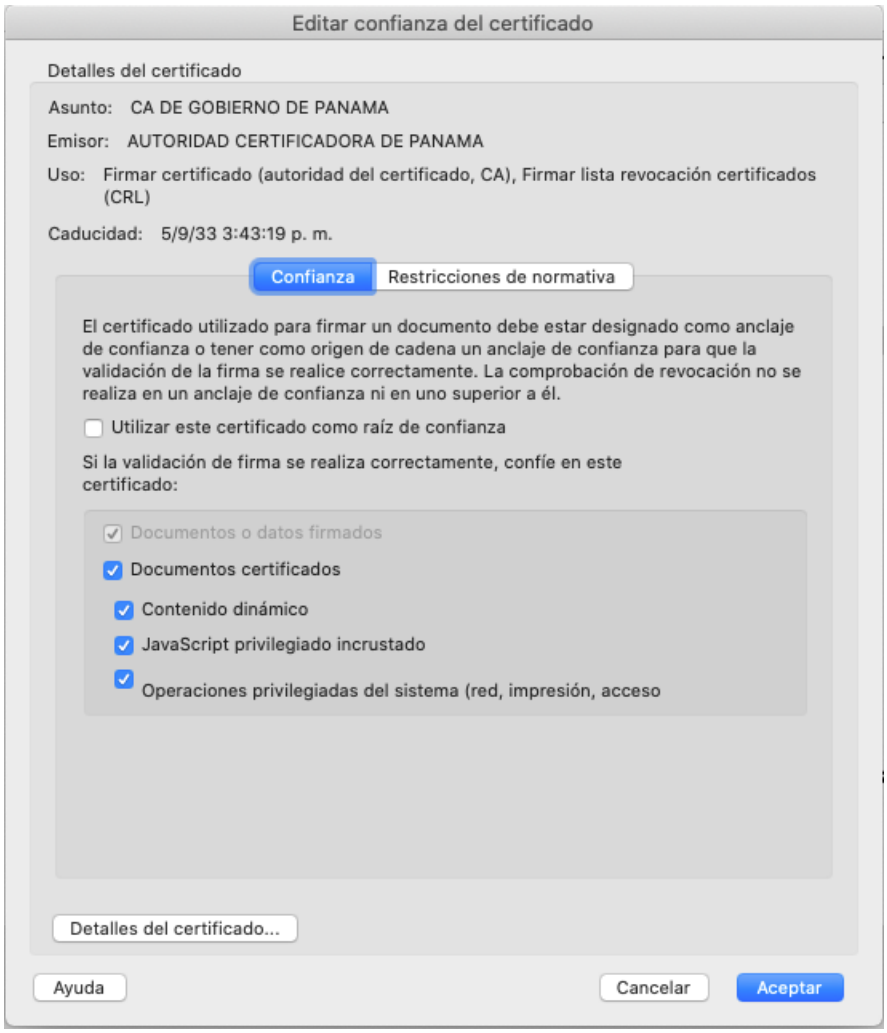

SafeSign
Buscar
Favoritos
javierbatista
Aplicaciones
Music
Descargas
Documentos
Escritorio
Vídeos
Recientes
Imágenes
iCloud
iCloud Drive
Ubicaciones
Dev-Pro
Nombre
Tamaño
Clase
Fecha de modificación
Fecha de inclusió
caraiz.crt 2 KB certificado anteayer 3:56 p. m. hoy 7:46 p. m.
capc2.crt 1 KB certificado anteayer 3:56 p. m. hoy 7:46 p. m.
cagob.crt 2 KB certificado anteayer 3:56 p. m. hoy 7:46 p. m.
Opciones
Cancelar
Abrir


Elegir contactos para importar
Este cuadro de diálogo le permitirá seleccionar contactos para importarlos a su lista de identidades de confianza. También puede definir la confianza de cualquier certificado asociado a los contactos que importe.
Contactos
Nombre
Correo electrónico
CA PANAMA CLASE 2
CA DE GOBIERNO DE PANAMA
Quitar
Examinar...
Buscar...
Certificados
Esta lista muestra los certificados asociados al contacto actualmente seleccionado.
Asunto
Emisor
Caduca
Detalles...
Confiar...
Ayuda
Cancelar
Importar


Importación terminada
Detalles de la importación:
Se ha(n) importado 1 certificado(s) de emisor.
Se ha(n) importado 1 certificado(s) de emisor.
Aceptar

Una vez que se finaliza con la importación de los 3 certificados de las CA, se pueden verificar que tengan los permisos correspondientes, buscándolos en el listado de **Certificados de confianza**, se selecciona y click en **Editar confianza**, donde **AUTORIDAD CERTIFICADORA DE PANAMA** debe tener todas las casillas marcadas pero **CA DE GOBIERNO DE PANAMA** y **CA PANAMA CLASE 2** tendrán todas las casillas menos la primera de “Utilizar este certificado como raíz de confianza” ya que esa opción sólo la debe tener el certificado de la Autoridad Raíz.

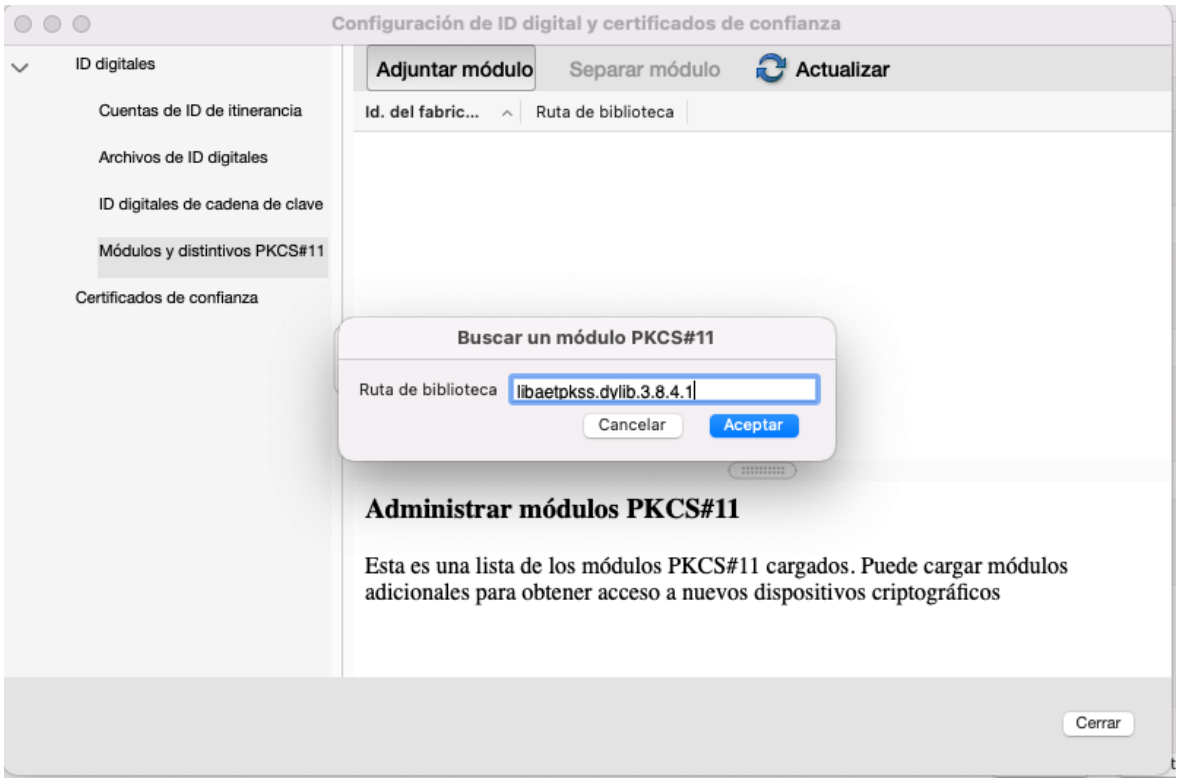




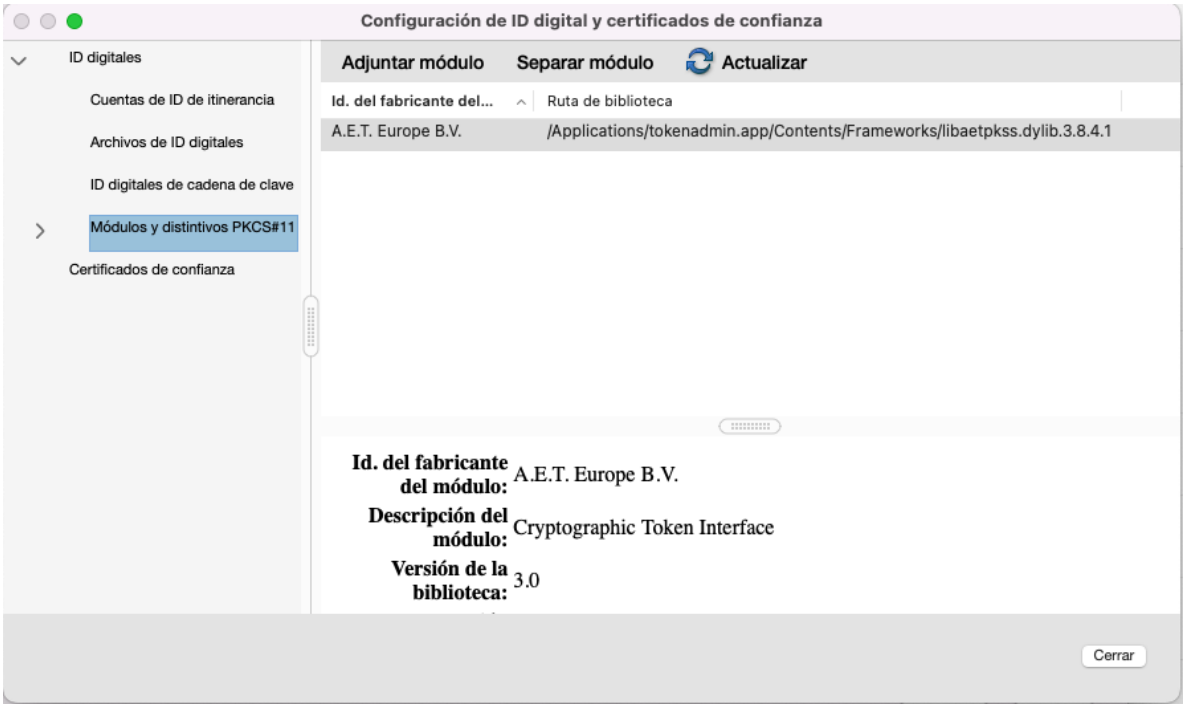
Configuración del controlador de SafeSign en el Adobe Reader

Luego de importar los 3 certificados, podemos proceder a configurar la librería de **SafeSign** en la ventana de **Configuración de ID digital y certificados de confianza**, la cual debe permanecer abierta al momento de terminar las importaciones, pero en caso de haberla cerrado, siempre se podrá encontrar en **Acrobat Reader -> Preferencias -> Firmas ->** botón de **Más** en **Identidades y certificados de confianza** (tercero)**.** En esa ventana, expandimos la opción de **ID digitales,** damos click en **Módulos y distintivos PKCS#11** y presionamos el botón de **Adjuntar módulo** para copiar (tecla command C) y pegar (tecla command V) la siguiente línea:

/Applications/tokenadmin.app/Contents/Frameworks/libaetpkss.dylib.3.8.4.1

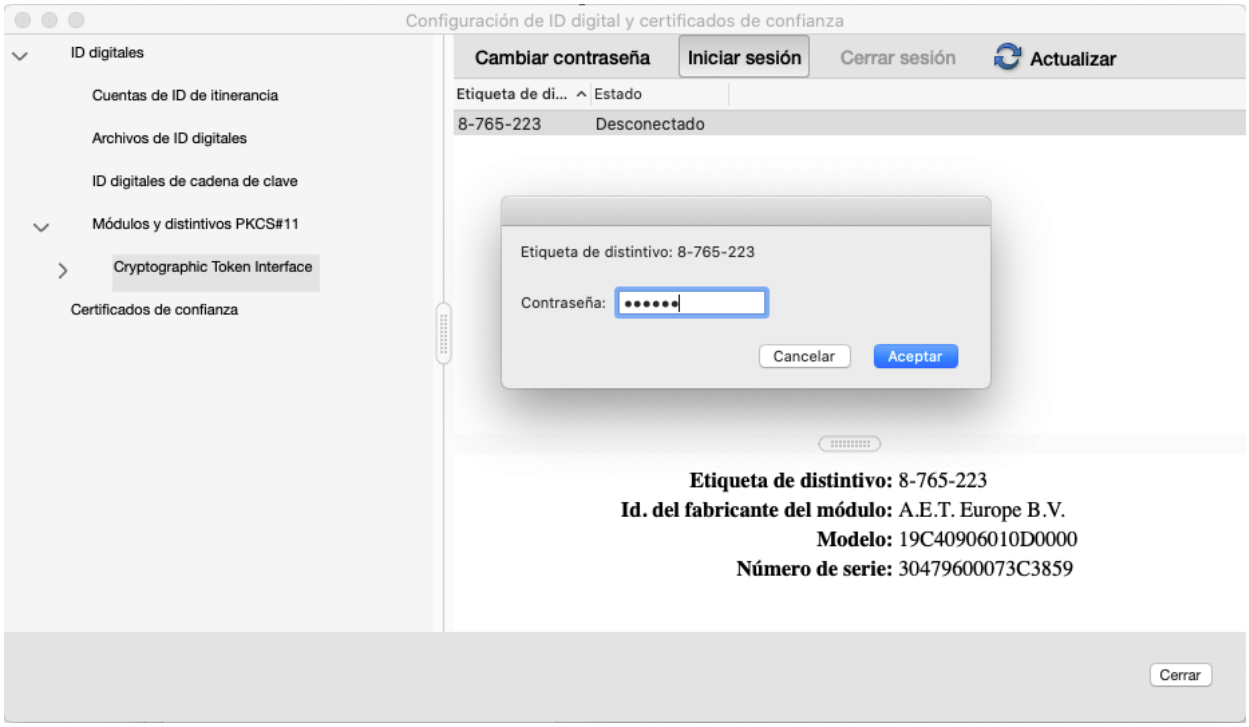


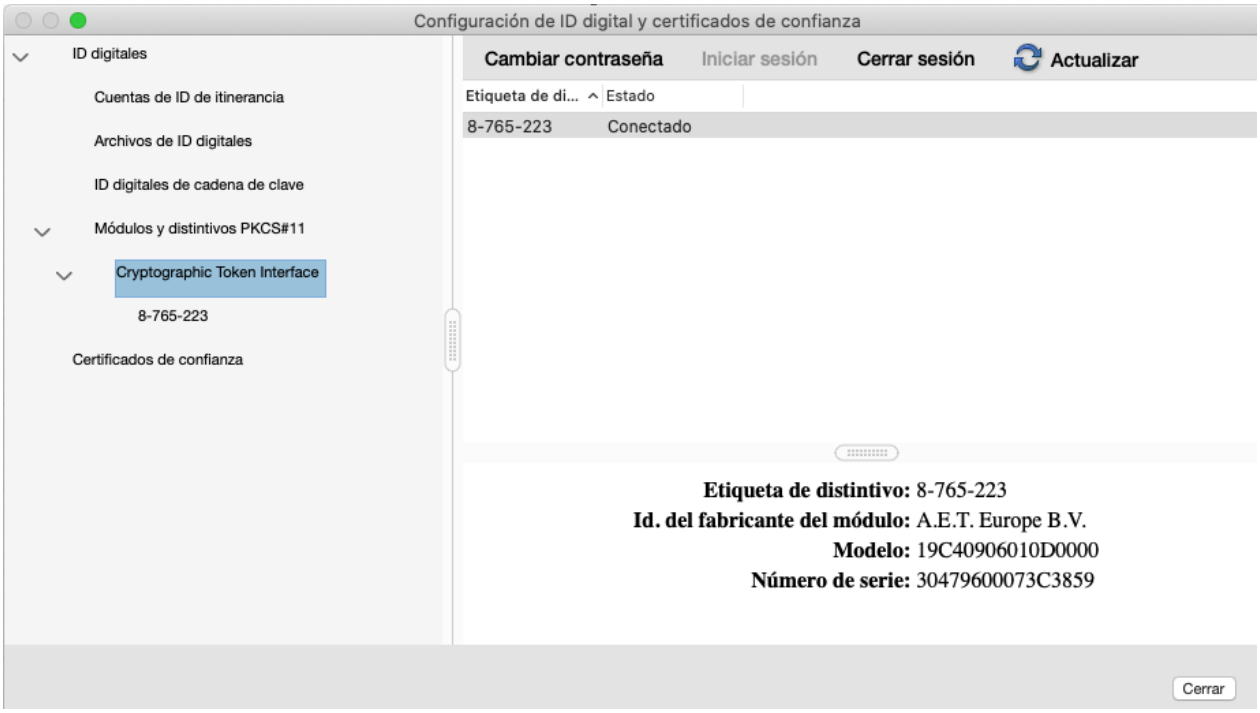
Al presionar **Aceptar**, deberá aparecer el nombre del controlador **A.E.T. Europe B.V.** en la ventana de **Id. del fabricante del módulo.**



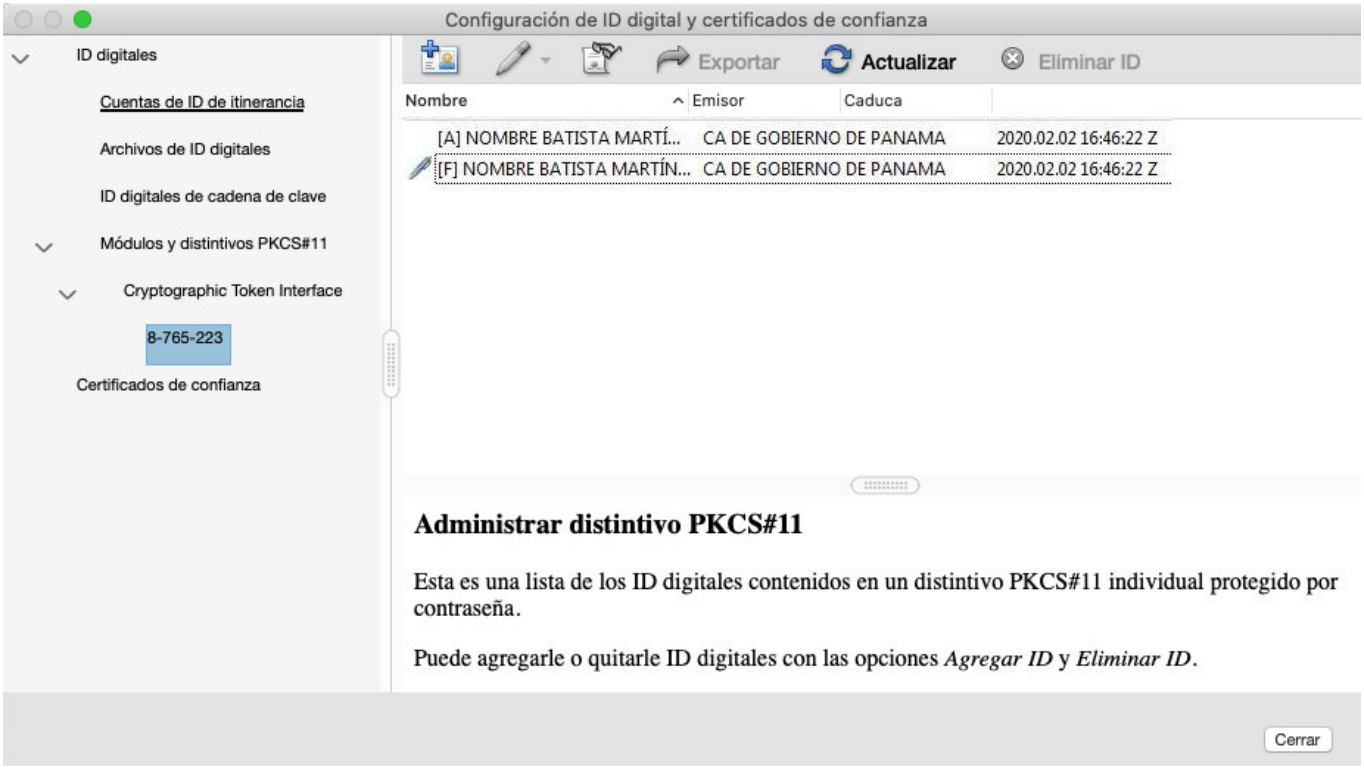
Teniendo la tarjeta insertada en el lector USB conectado a la computadora, se expande la opción de **Módulos y distintivos PKCS#11**, seleccionamos **Cryptographic Token Interface** y se podrá apreciar la cédula con el estado **Desconectado**, por lo que se deberá presionar el botón

de **Iniciar sesión** colocando el número PIN de la tarjeta (teniendo en cuenta que, si se escribe 3 veces mal, se podrá bloquear), se presiona **Aceptar** y la tarjeta aparecerá con el estado de **Conectado**.



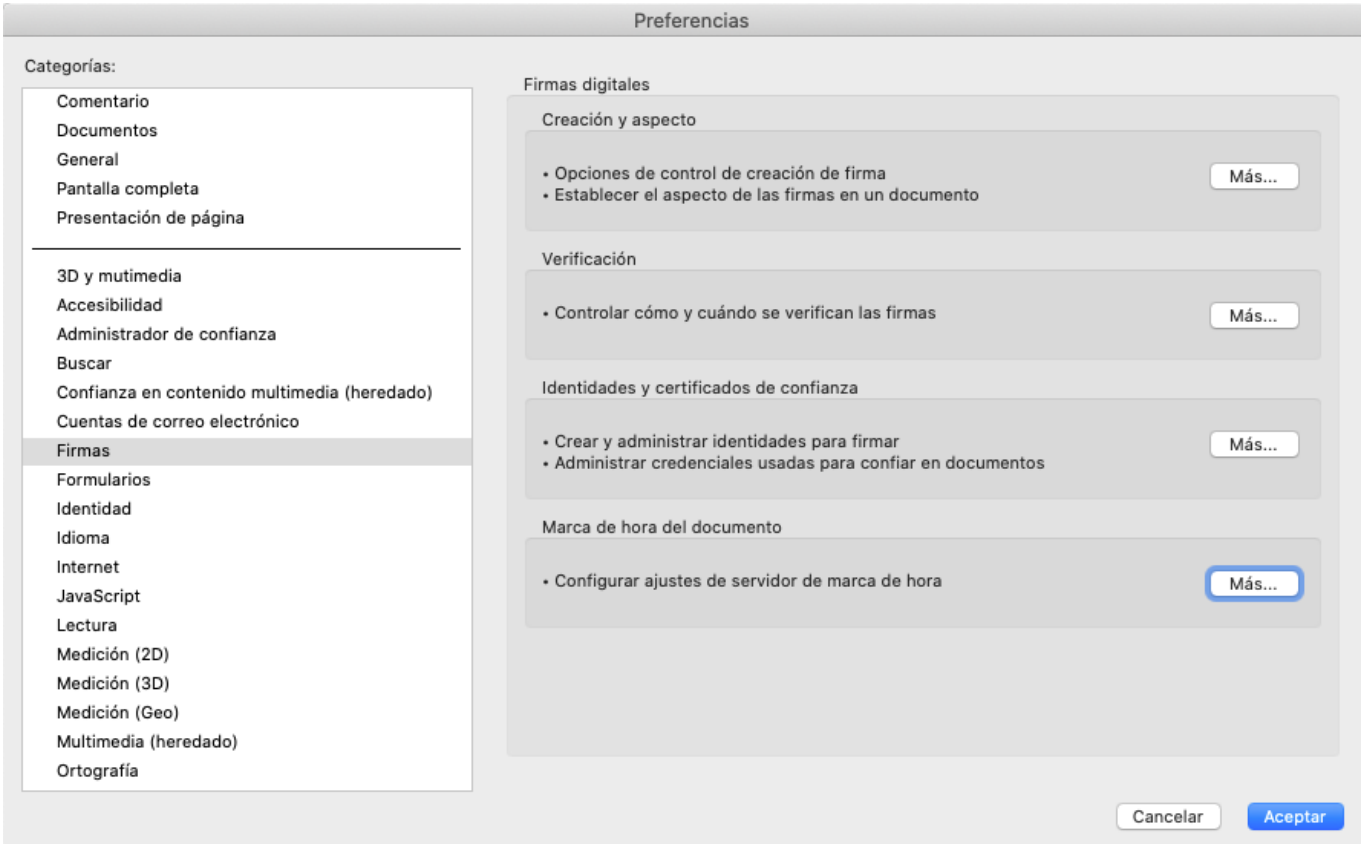


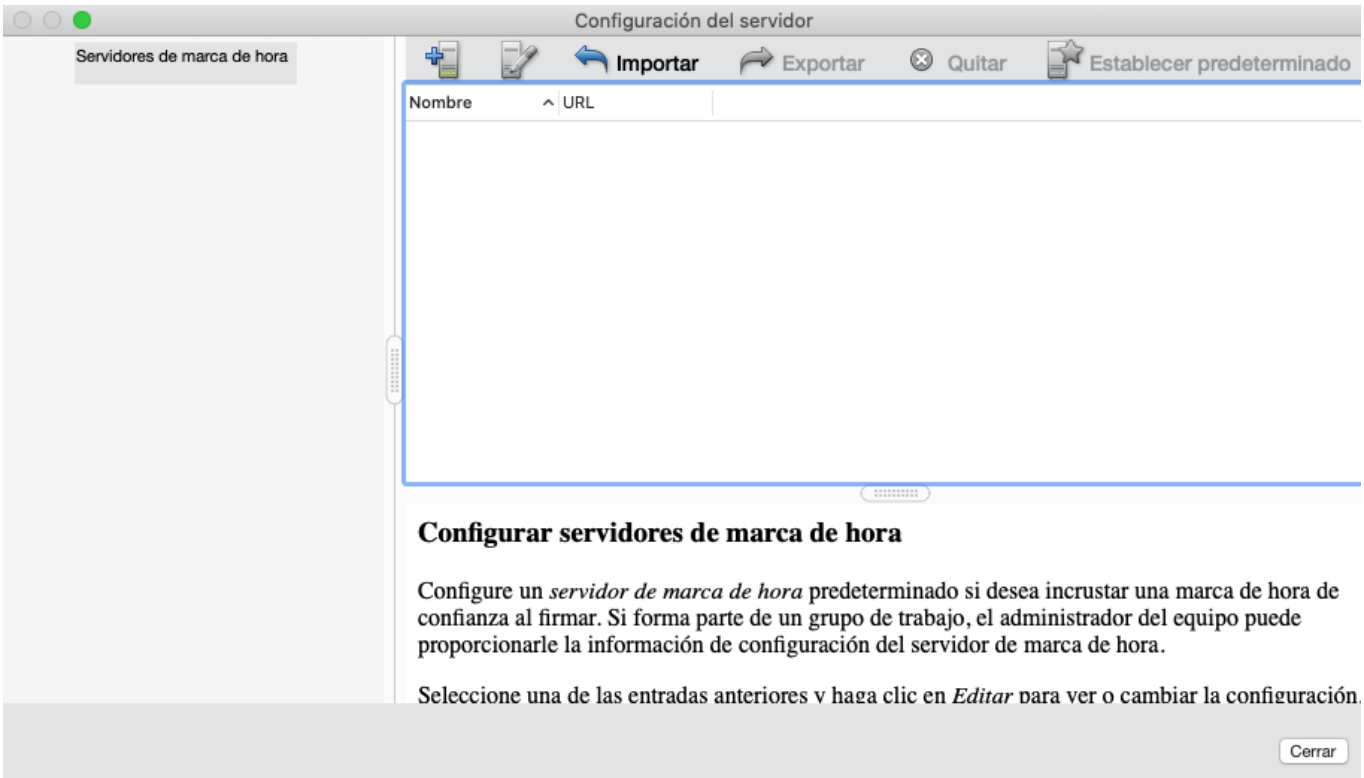
Posteriormente, se expande la opción de **Cryptographic Token Interface**, se selecciona la cédula, aparecerán los dos certificados de la tarjeta, se debe marcar el que empieza con [F] NOMBRE... y damos click en el botón superior del lápiz -> **Usar para firmar.** Con esta opción, el certificado de firma siempre estará seleccionado por defecto en la computadora.

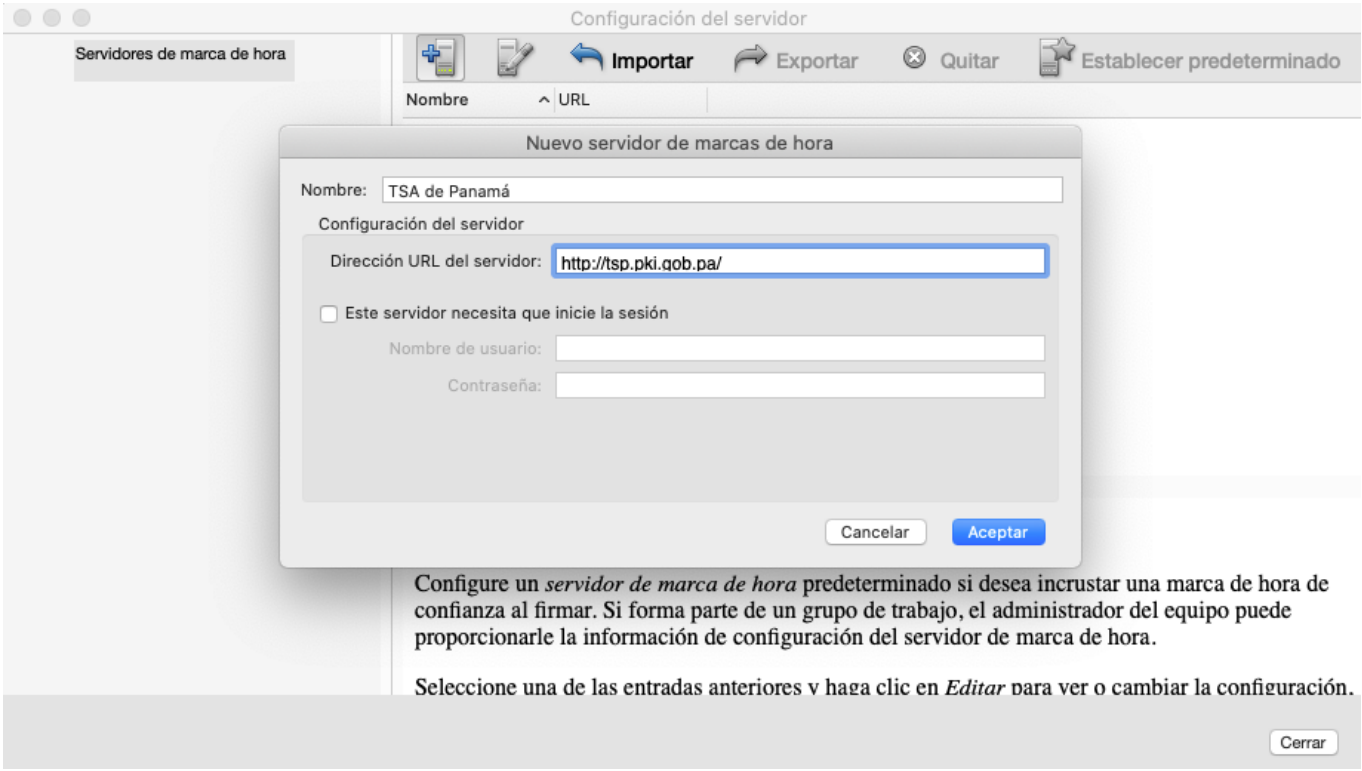


Configuración del Servidor de Marca de Hora

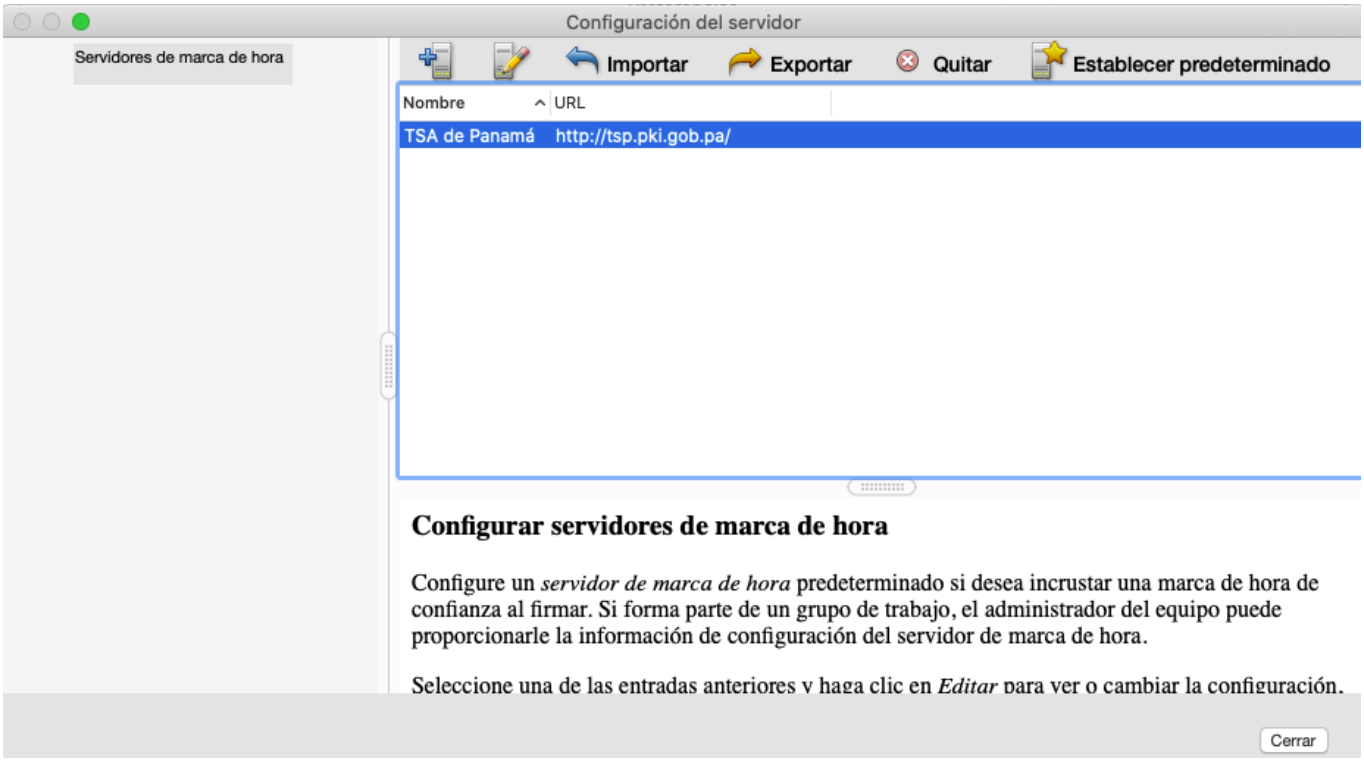
Al presionar el botón de **Cerrar** de la ventana de **Configuración de ID digital y certificados de confianza** de la imagen anterior, quedaremos en la ventana de **Firmas** en **Preferencias** (**Acrobat Reader -> Preferencias -> Firmas**) y damos click en el cuarto botón de **Más** en **Marca de hora del documento.** Luego aparecerá la ventana de **Configuración del servidor**, se presiona el botón **Nuevo** (símbolo de más + azul) y en el campo **Nombre:** se puede colocar la descripción **TSA de Panamá** y en la **Dirección URL del Servidor:** http://tsp.pki.gob.pa/ , la cual se puede verificar con la ayuda de un navegador web, donde se debe mostrar una página en blanco con el texto: **- Welcome to KeyOne TSA - .**

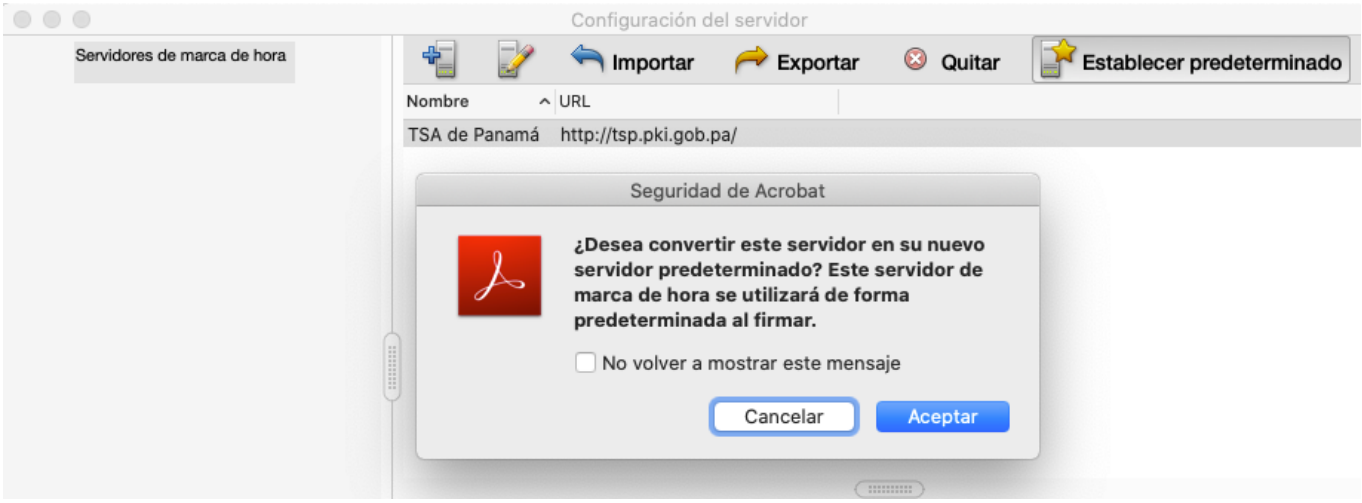

Preferencias
Categorías:
Comentario
Documentos
General
Pantalla completa
Presentación de página
3D y mutimedia
Accesibilidad
Administrador de confianza
Buscar
Confianza en contenido multimedia (heredado)
Cuentas de correo electrónico
Firmas
Formularios
Identidad
Idioma
Internet
JavaScript
Lectura
Medición (2D)
Medición (3D)
Medición (Geo)
Multimedia (heredado)
Ortografía
Firmas digitales
Creación y aspecto
• Opciones de control de creación de firma
• Establecer el aspecto de las firmas en un documento
Más...
Verificación
• Controlar cómo y cuándo se verifican las firmas
Más...
Identidades y certificados de confianza
• Crear y administrar identidades para firmar
• Administrar credenciales usadas para confiar en documentos
Más...
Marca de hora del documento
• Configurar ajustes de servidor de marca de hora
Más...
Cancelar
Aceptar

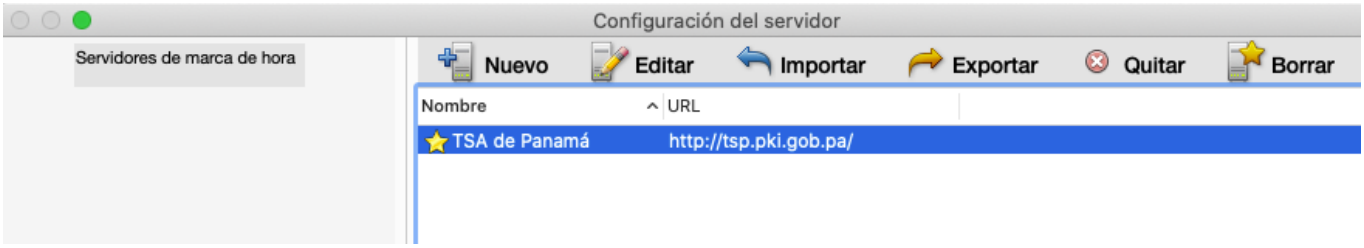

Configuración del servidor
Servidores de marca de hora
Importar
Exportar
Quitar
Establecer predeterminado
Nombre
URL
Configurar servidores de marca de hora
Configure un servidor de marca de hora predeterminado si desea incrustar una marca de hora de confianza al firmar. Si forma parte de un grupo de trabajo, el administrador del equipo puede proporcionarle la información de configuración del servidor de marca de hora.
Seleccione una de las entradas anteriores y haga clic en Editar para ver o cambiar la configuración.
Cerrar



Al completa los dos campos y presionar **Aceptar**, en la ventana aparecerá el servidor **TSA de Panamá**, por lo que se deberá seleccionar, presionar el botón de **Establecer predeterminado** y **Aceptar** para que quede con el icono de la estrella ☆ por delante de su descripción. Al finalizar este paso, se puede cerrar la ventana de **Configuración del servidor** y dar click en el botón **de Aceptar** de **Preferencias**.

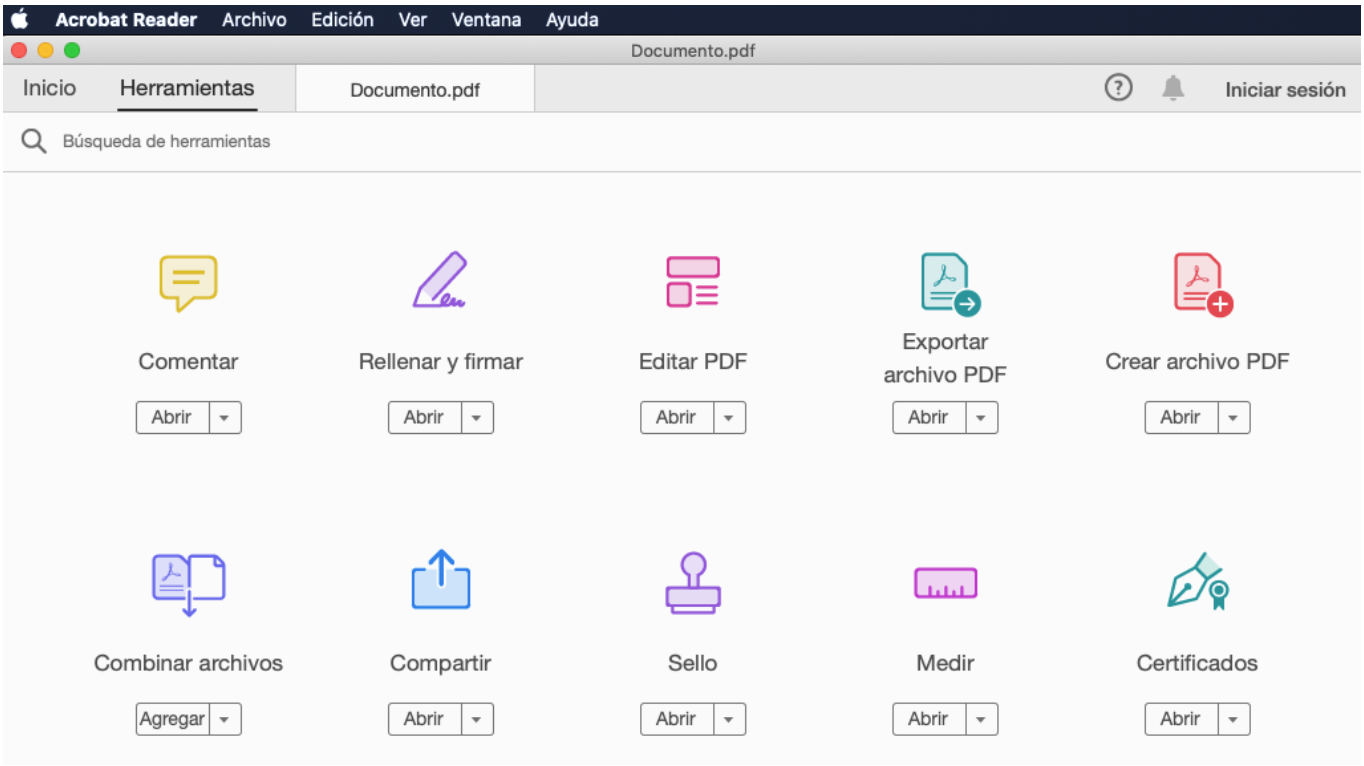

Configuración del servidor
Servidores de marca de hora
Importar
Exportar
Quitar
Establecer predeterminado
Nombre
URL
TSA de Panamá
http://tsp.pki.gob.pa/
Configurar servidores de marca de hora
Configure un servidor de marca de hora predeterminado si desea incrustar una marca de hora de confianza al firmar. Si forma parte de un grupo de trabajo, el administrador del equipo puede proporcionarle la información de configuración del servidor de marca de hora.
Seleccione una de las entradas anteriores y haga clic en Editar para ver o cambiar la configuración.
Cerrar

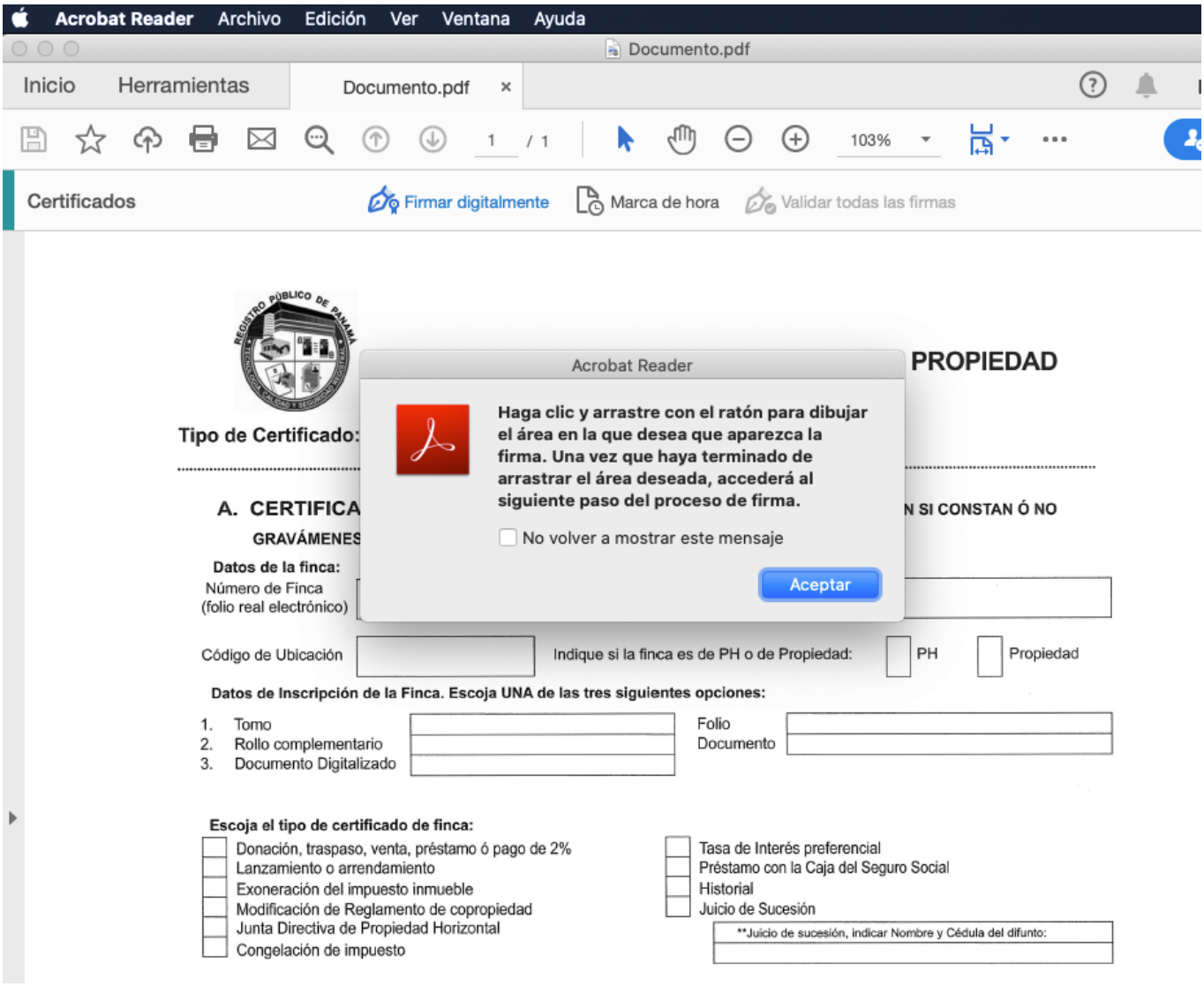

Configuración del servidor
Servidores de marca de hora
Importar
Exportar
Quitar
Establecer predeterminado
Nombre
URL
TSA de Panamá
http://tsp.pki.gob.pa/
Seguridad de Acrobat
¿Desea convertir este servidor en su nuevo servidor predeterminado? Este servidor de marca de hora se utilizará de forma predeterminada al firmar.
No volver a mostrar este mensaje
Cancelar
Aceptar


Configuración del servidor
Servidores de marca de hora
Nuevo
Editar
Importar
Exportar
Quitar
Borrar
Nombre
URL
TSA de Panamá
http://tsp.pki.gob.pa/

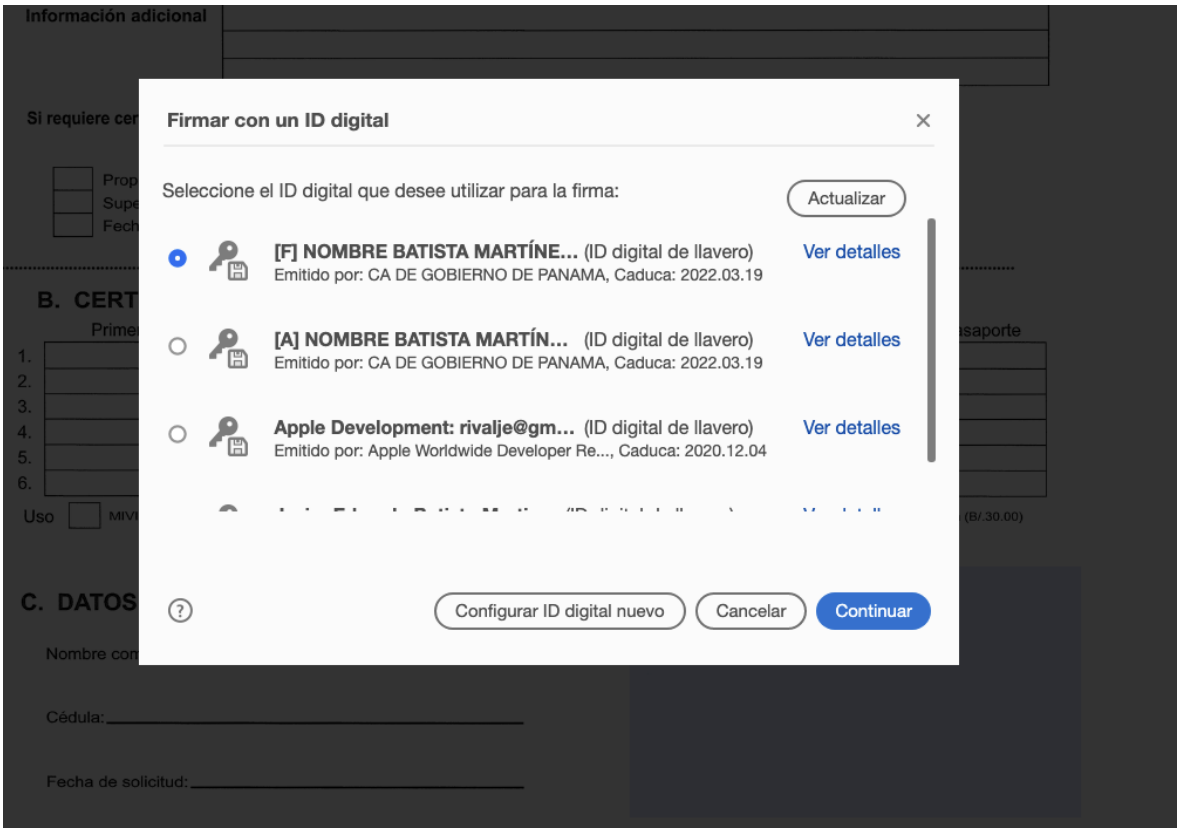
Prueba para firmar un documento PDF

Con el Adobe Reader configurado, buscamos el documento PDF que deseamos firmar y nos dirigimos a la pestaña de **Herramientas** -> **Certificados**. Esto habilitará la barra de **Certificados** en el documento PDF abierto y damos click en **Firmar digitalmente.**

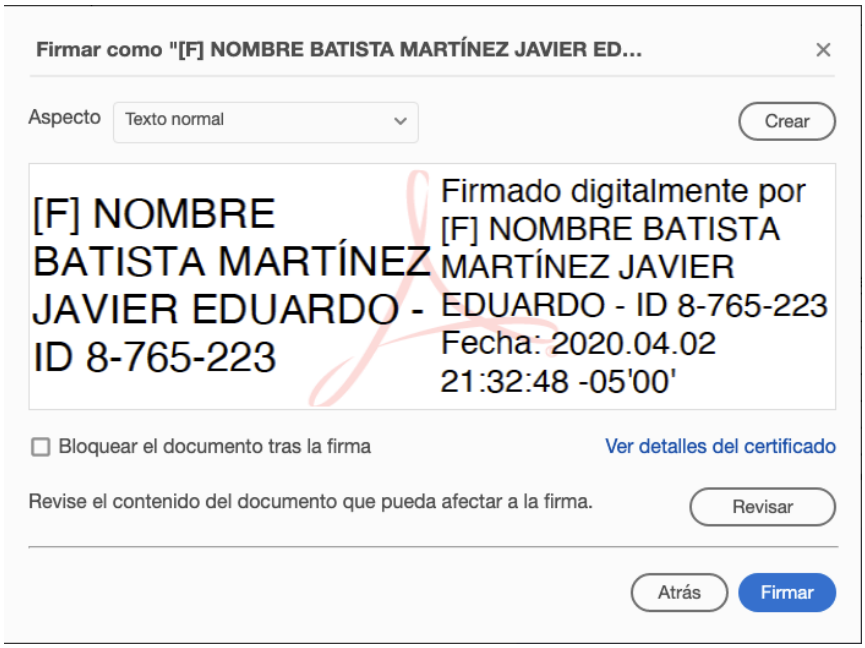




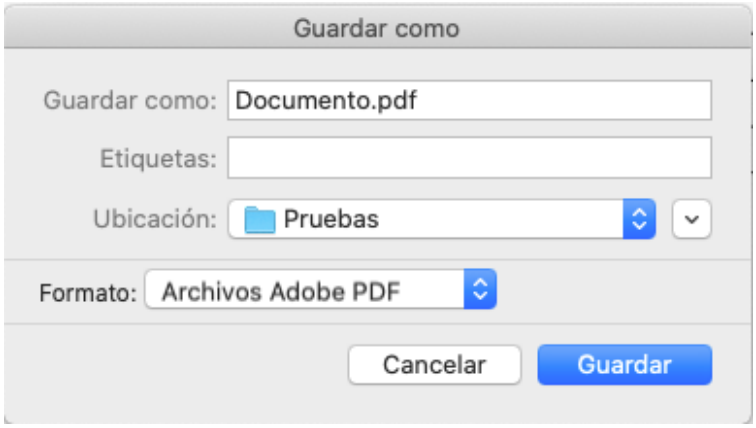
Al presionar el botón de **Firmar digitalmente** aparecerá un mensaje del **Acrobat Reader** que indica que debemos dibujar con el **Mouse** un área (preferiblemente rectangular) donde aparecerá la imagen de la firma, la cual podemos colocar en cualquier parte del documento donde no se cubra el contenido (algún área en blanco al inicio o final del archivo). Al soltar el botón del **Mouse** después de dibujar el cuadro, se mostrará una ventana blanca que lista los certificados configurados en la computadora, donde debería aparecer seleccionado el que empieza con [F] NOMBRE... y se presiona el botón de **Continuar**.

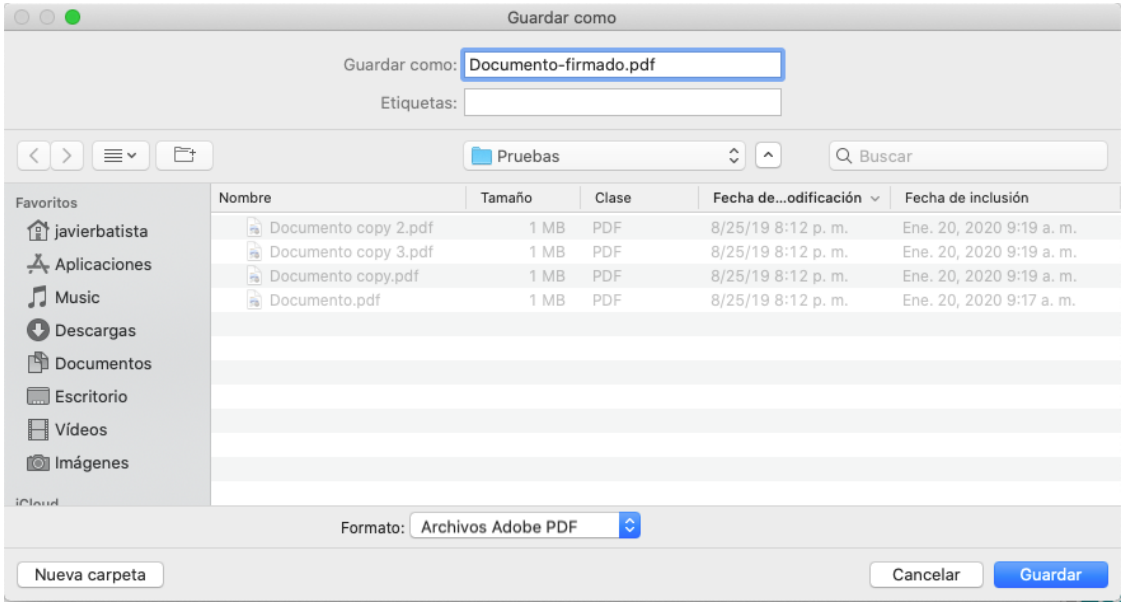


En la siguiente ventana (imagen inferior) se presiona el botón de **Firmar**, donde normalmente en esta pantalla se coloca el número PIN de la tarjeta, pero si se inició sesión previamente cuando se configuró el certificado de firma o se haya firmado un documento previo, no se pedirá el PIN por segunda vez al menos que se cierre el Adobe Reader y se vuelva a ejecutar.



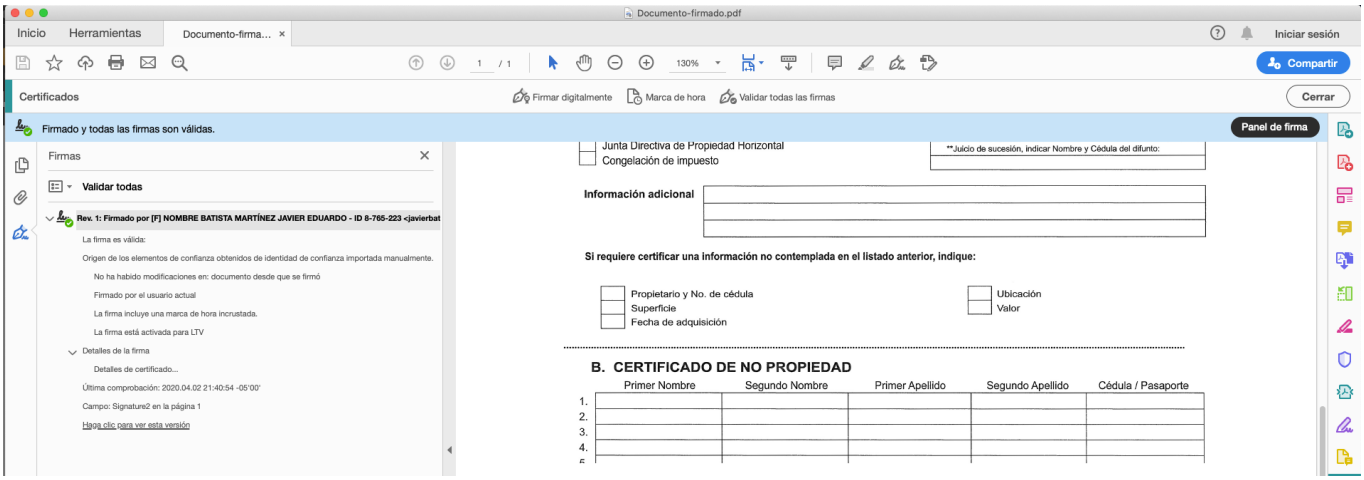
Al presionar el botón de **Firmar**, se pedirá guardar el documento como uno nuevo (se le puede cambiar el nombre o guardarlo en otra carpeta para no afectar el documento original).





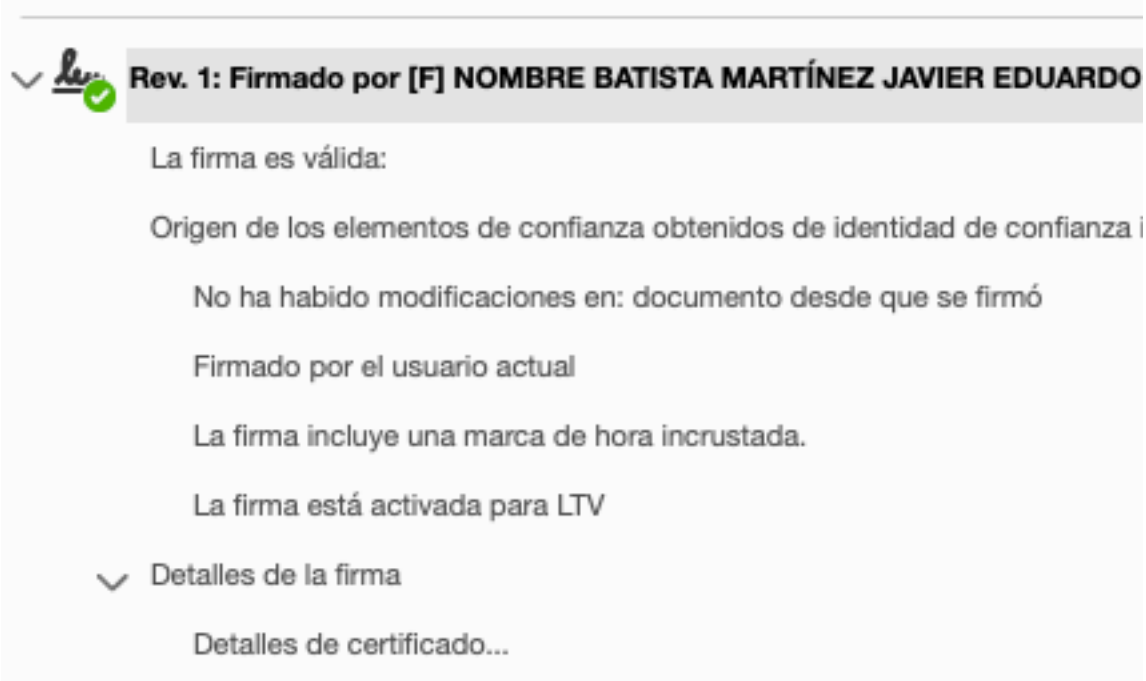
Durante el proceso de firma se establecerá conexión con el servidor de Marca de Hora http://tsp.pki.gob.pa/ por lo que podría aparecer una advertencia donde se debe permitir y marcar la opción de recordar para que el documento firmado quede con la hora del servidor y no de la computadora del usuario, ya que la fecha y hora del servidor es la que tiene validez legal.

Un documento firmado debe quedar con la imagen visual de la firma ubicada en el área donde se dibujó el cuadro con el **Mouse** y también debe tener una barra celeste superior indicando que el archivo está “Firmado y todas las firmas son válidas” (en ocasiones esta barra celeste no aparece la primera vez y se debe cerrar y abrir nuevamente el archivo firmado para que se aprecie ese mensaje).



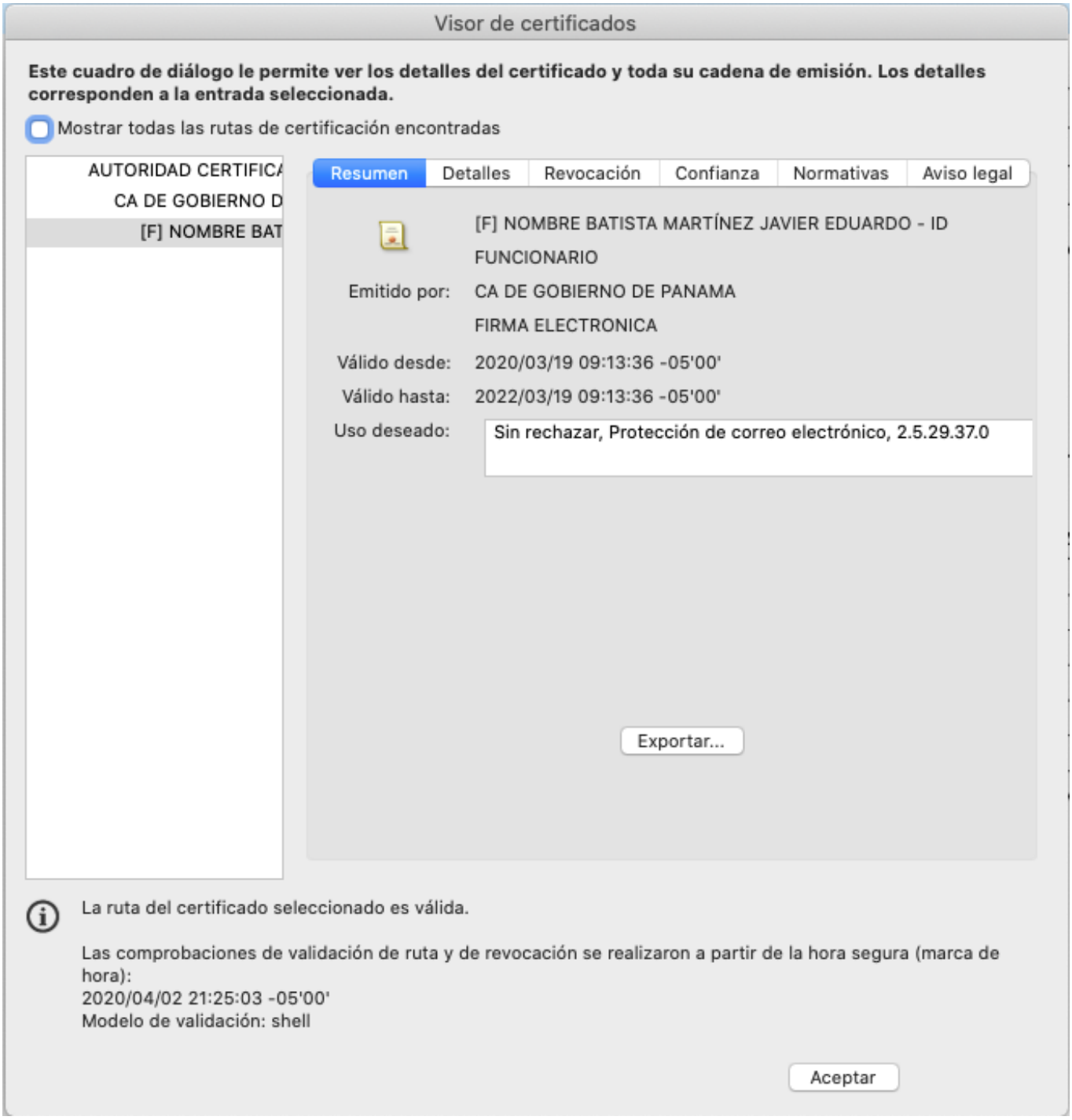
Adicionalmente se puede dar click en el botón de **Panel de firma** de la barra celeste para verificar la información del certificado donde es muy importante que aparezca el texto: “La firma incluye

una marca de hora incrustada” y “La firma está activada para LTV” al momento de expandir el menú del icono con el gancho verde .



Si se ingresa en la opción de **Detalles de la firma -> Detalles de certificado…** se verá una ventana llamada **Visor de certificados** con la información completa del firmante y debajo, antes del botón de **Aceptar**, deberá aparecer el siguiente escrito: “**Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora segura (marca de hora)**” con su respectiva fecha y hora, la cual se generó gracias al servidor de marca de hora.

Con estos pasos, tendríamos oficialmente un documento PDF firmado con una tarjeta emitida por la Autoridad Certificadora de Panamá.


Visor de certificados
Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.
Mostrar todas las rutas de certificación encontradas
AUTORIDAD CERTIFICA
CA DE GOBIERNO D
[F] NOMBRE BAT
Resumen
Detalles
Revocación
Confianza
Normativas
Aviso legal
[F] NOMBRE BATISTA MARTÍNEZ JAVIER EDUARDO - ID FUNCIONARIO
Emitido por: CA DE GOBIERNO DE PANAMA FIRMA ELECTRONICA
Válido desde: 2020/03/19 09:13:36 -05'00'
Válido hasta: 2022/03/19 09:13:36 -05'00'
Uso deseado: Sin rechazar, Protección de correo electrónico, 2.5.29.37.0
Exportar...
La ruta del certificado seleccionado es válida.
Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora segura (marca de hora):
2020/04/02 21:25:03 -05'00'
Modelo de validación: shell
Aceptar