



**P-42**

## **GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS**

Última versión: 1.2	Fecha de implementación: 15 de marzo de 2024	
Preparado por: JULIETH DIAZ	Revisado por: JAVIER BATISTA	Aprobado por: JAVIER BATISTA

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS  CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS  EN EL PROGRAMA ADOBE ACROBAT READER DC EN  MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 2 de 27

## 1.0 PROPÓSITO

Especificar el procedimiento utilizado para la instalación y configuración de los certificados de las Autoridades Raíz e Intermedias de la PKI de Panamá en el programa Adobe Acrobat Reader DC, incluyendo el controlador del lector de tarjetas inteligentes.

## 2.0 ALCANCE

Inicia con la descargar de los certificados y termina con una prueba de firma de un documento PDF.

## 3.0 DOCUMENTOS DE REFERENCIA

<https://helpx.adobe.com/es/acrobat/using/validating-digital-signatures.html>

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 3 de 27

## 4.0 PROCEDIMIENTO

### 4.1 Descarga e instalación de los certificados de las Autoridades de Certificación Raíz e Intermedias.

Para que los certificados emitidos por la **Dirección Nacional de Firma Electrónica** puedan ser utilizados sin que marquen error en los documentos que se firmen, es necesario descargarlos de la siguiente dirección: <https://www.firmaelectronica.gob.pa/configuracion-firma-electronica.html>.


**REPÚBLICA DE PANAMÁ**  
 GOBIERNO NACIONAL

**REGISTRO PÚBLICO  
DE PANAMÁ**

**DIRECCIÓN NACIONAL  
DE FIRMA ELECTRÓNICA**

Inicio   Nosotros   Requisitos   Configuración   Normativa   Políticas de Certificación   Preguntas   Contacto

Solicitar

|| CONFIGURACIÓN DE LA FIRMA ELECTRÓNICA ||

Manuales de Configuración

Certificados de la jerarquía de CA's
 

- Autoridad de Certificación Raíz de Panamá.
- Autoridad de Certificación de Gobierno.
- Autoridad de Certificación de Panamá Clase 2.

Drivers de SafeSign

En la página se muestran tres (3) enlaces en el menú desplegable de **Certificados de la jerarquía de CA's**. Cada uno corresponde a un archivo de certificado (con extensión .crt), los cuales podrán ser descargados con el botón derecho del ratón sobre el enlace y seleccionando **Guardar enlace como** para así guardarlos en una carpeta en nuestros computadores.

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS  CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS  EN EL PROGRAMA ADOBE ACROBAT READER DC EN  MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 4 de 27

## 4.2 Instalación del controlador del lector para tarjetas inteligentes SafeSign

Para que las tarjetas sean reconocidas en la computadora donde se usará el Adobe Reader para firmar los documentos, será necesario primero descargar el controlador correspondiente para el Sistema Operativo en uso en el menú desplegable de **Drivers de SafeSign** en la siguiente dirección:  
<https://www.firmaelectronica.gob.pa/configuracion-firma-electronica.html>



**REGISTRO PÚBLICO  
DE PANAMÁ**

**DIRECCIÓN NACIONAL  
DE FIRMA ELECTRÓNICA**

Inicio   Nosotros   Requisitos   **Configuración**   Normativa   Políticas de Certificación   Preguntas   Contacto

Solicitar

### || CONFIGURACIÓN DE LA FIRMA ELECTRÓNICA ||

Manuales de Configuración



Certificados de la jerarquía de CA's



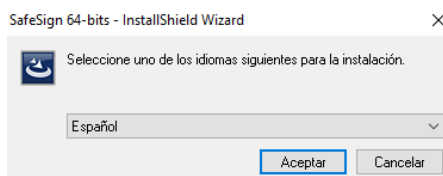
Drivers de SafeSign



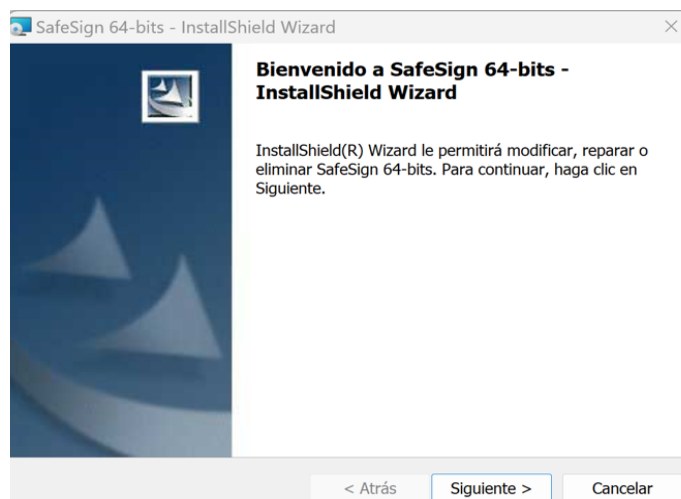
- [Driver de SafeSign para Windows \(Tarjetas de Firma Electrónica\).](#)
- [Driver de SafeSign para Windows x86 \(32 bits\) \(Tarjetas de Firma Electrónica\).](#)
- [Driver de SafeSign para macOS \(Tarjetas de Firma Electrónica\).](#)
- [Driver de SafeSign para macOS i386-x86 \(Tarjetas de Firma Electrónica\).](#)

Procedemos a darle doble clic al instalador **Driver de SafeSign para Windows (Tarjetas de Firma Electrónica)** para poder instalarlo en el equipo. Al terminar la descarga del instalador, debemos darle doble clic. Luego, el sistema preguntará si desea permitir que este programa realice cambios en el equipo, donde indicaremos que **Sí**. Luego seleccionaremos el idioma deseado, ejemplo **Español** y empezará el proceso para descomprimir los archivos para la instalación.

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 5 de 27

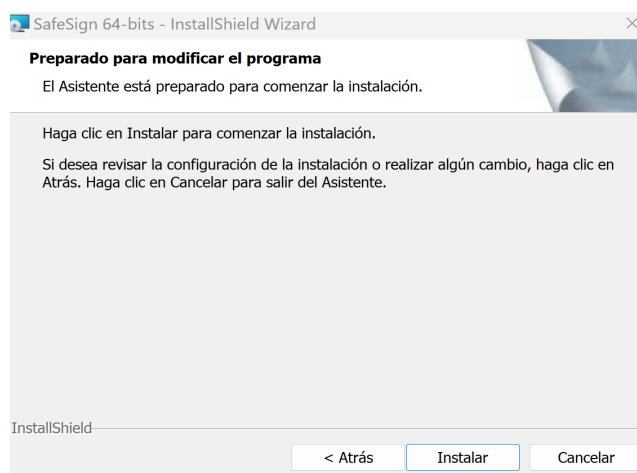
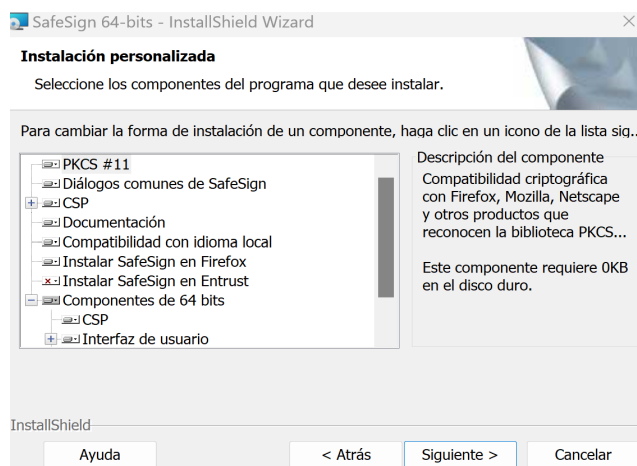


Cuando finaliza el proceso de descompresión, aparecerá la ventana de bienvenida, se da clic en **Siguiente**, se selecciona la opción de **Acepto los términos del contrato de licencia**, y luego **Siguiente** nuevamente.



Antes de iniciar con la instalación del controlador SafeSign, se muestran los componentes que se incluirán, los cuales podemos dejarlos tal como están y dar clic en **Siguiente** para así presionar el botón de **Instalar** en la próxima ventana.

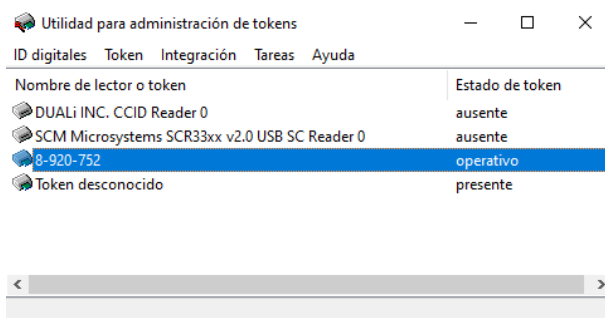
	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA		
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS</b>		
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 6 de 27



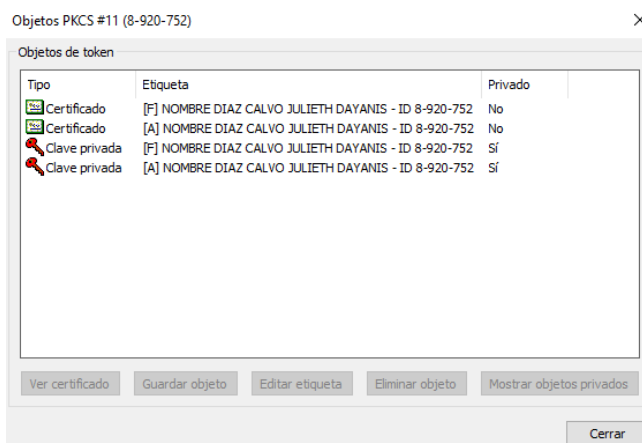
Posteriormente iniciará el proceso de instalación y si todo culmina de forma correcta, podrá dar clic a **Finalizar**.

Podrá observar un programa llamado **Administración de Tokens** en el menú de inicio de Windows, que al ejecutarse mostrará una ventana con el lector de tarjetas (que debe estar conectado a un puerto USB de la computadora) y si se introduce la tarjeta que contiene la firma electrónica, se mostrará el ID de dicho documento (número de cédula) en la posición del lector.

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 7 de 27	



Si presionamos doble clic sobre el número de cédula, se debe mostrar otra ventana con los certificados incluidos en dicha tarjeta, lo cual nos indica que la instalación del controlador fue realizada de forma correcta.



Con el **Administrador de Tokens** se pueden efectuar distintas operaciones, donde la más común sería el cambio del número PIN de la tarjeta, el cual se realiza con la tarjeta insertada en el lector, seleccionando el número de cédula y la opción del menú **Token -> Cambiar PIN**. Luego introducimos el número PIN actual y el nuevo dos veces. Es importante considerar que las tarjetas tienen un máximo tres (3) intentos de números PIN fallidos antes de bloquearse como medida de seguridad cuando se están utilizando, ya sea en operaciones de firma o autenticación, donde si nos llega a suceder este inconveniente, se puede utilizar el número PUK suministrado en el sobre para así desbloquearlas (opción **Token -> Desbloquear PIN**).

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA		
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS  CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS  EN EL PROGRAMA ADOBE ACROBAT READER DC EN  MICROSOFT WINDOWS</b>		
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 8 de 27

Cambiar PIN

Cambiando el PIN por "8-920-752":

Introduzca PIN antiguo:

Introduzca PIN nuevo:

Confirme PIN nuevo:

✗ Longitud mínima de PIN 4 bytes  
✓ Longitud máxima de PIN 15 bytes  
✓ Nuevo PIN igual a nuevo PIN confirmado

Aceptar

Cancelar

### 4.3 Configuración del Adobe Acrobat Reader DC para firmar y validar documentos PDF con los certificados de las Autoridades de la PKI de Panamá

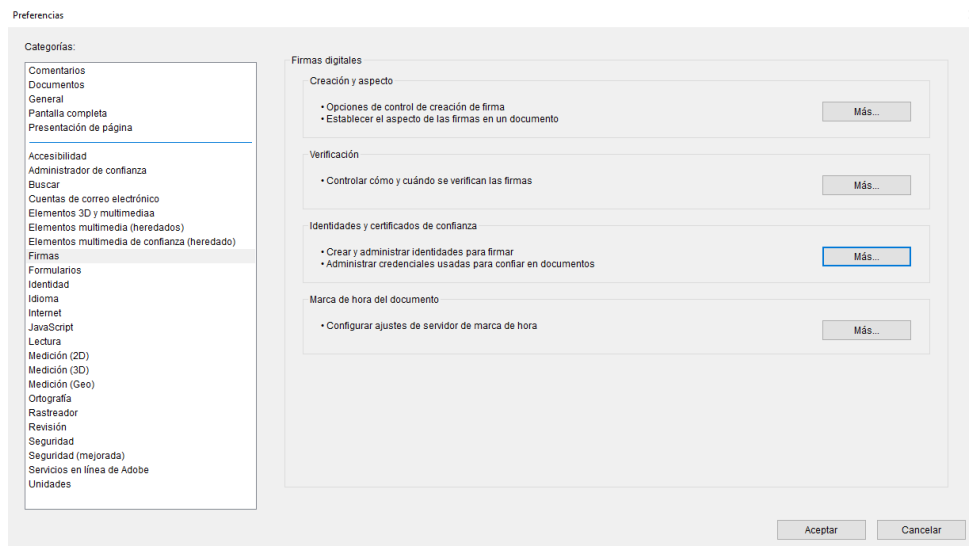
En la actualidad, se pueden utilizar diversos programas para realizar operaciones de firma de documentos electrónicos, sin embargo, en este punto, cubriremos los aspectos necesarios para utilizar el programa gratuito de Adobe Reader, cuya versión actual permite realizar firma de documentos. Si no contamos con este programa, podemos descargarlo desde la siguiente dirección: <https://get.adobe.com/es/reader/> y realizar el proceso de instalación, según las instrucciones que ofrezca esa web o el mismo instalador.

#### 4.3.1 Instalación de los Certificados de las CA Raíz e Intermedias

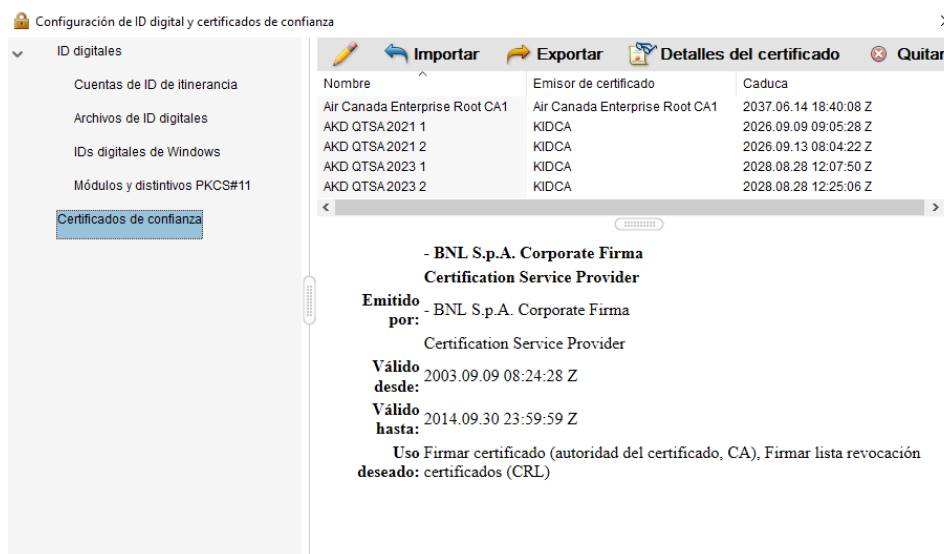
Una vez que ejecutamos el Adobe Reader, debemos configurar los certificados de las **Autoridades Certificadoras Raíz e Intermedias**, descargados según las explicaciones del primer punto de este documento. Para esto, nos dirigimos a la opción del menú **Edición -> Preferencias**, seleccionamos **Firmas** y damos clic en el tercer botón **Más (Identidades y certificados de confianza)**.



 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> <b>DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA</b>		
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS  CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS  EN EL PROGRAMA ADOBE ACROBAT READER DC EN  MICROSOFT WINDOWS</b>		
<b>Código:</b> P-42	<b>Versión:</b> 1.2	<b>Fecha de implementación:</b> <b>15 de marzo de 2024</b>	<b>Página:</b> 9 de 27



Al realizar la acción anterior, se visualizará otra ventana llamada **Configuración de ID digital y certificados de confianza**. Allí seleccionamos la opción **Certificados de confianza** donde se listarán aquellos que están incluidos en el repositorio de Adobe (es posible que la primera vez se pregunte si se desean descargar, donde indicamos que sí).

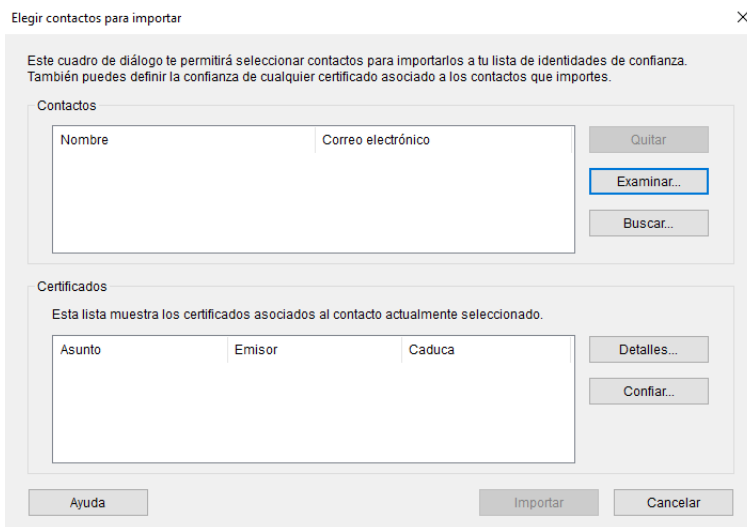


Nombre	Emisor de certificado	Caduca
Air Canada Enterprise Root CA1	Air Canada Enterprise Root CA1	2037.06.14 18:40:08 Z
AKD QTSA 2021 1	KIDCA	2026.09.09 09:05:28 Z
AKD QTSA 2021 2	KIDCA	2026.09.13 08:04:22 Z
AKD QTSA 2023 1	KIDCA	2028.08.28 12:07:50 Z
AKD QTSA 2023 2	KIDCA	2028.08.28 12:25:06 Z

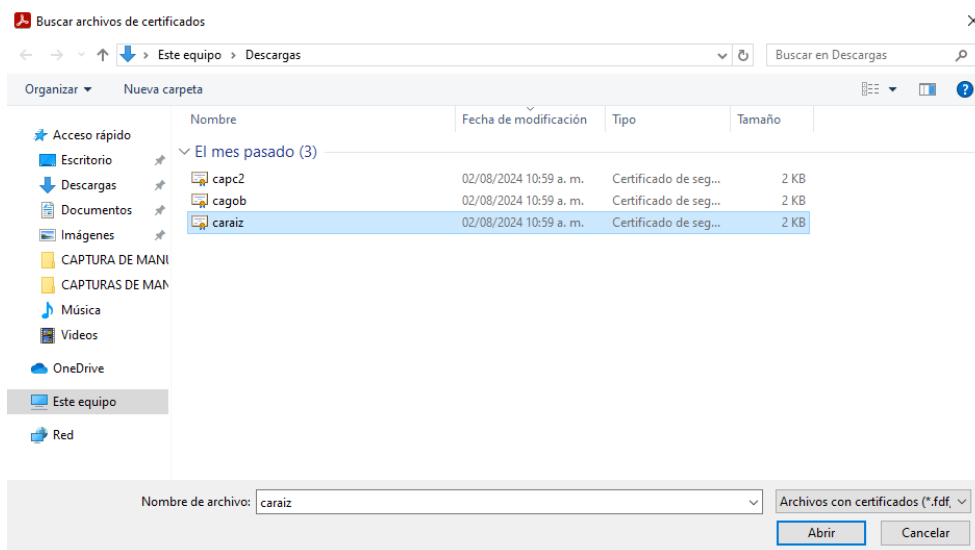
**Emitido por:** - BNL S.p.A. Corporate Firma Certification Service Provider  
**Válido desde:** 2003.09.09 08:24:28 Z  
**Válido hasta:** 2014.09.30 23:59:59 Z  
**Uso Firmar certificado (autoridad del certificado, CA), Firmar lista revocación deseado: certificados (CRL)**

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 10 de 27	

En el listado debemos incluir los 3 certificados de las Autoridades de la PKI de Panamá, empezando con la Raíz (archivo **caraiz.crt**), utilizando el botón de **Importar**, el cual muestra la ventana **Elegir contactos para importar**.



En esa ventana presionamos **Examinar** y buscamos el archivo **caraiz.crt** en la carpeta donde lo descargamos, se selecciona y damos clic en **Abrir**.





## REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

### GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS

Código:  
P-42

Versión:  
1.2

Fecha de implementación:  
15 de marzo de 2024

Página: 11 de 27

En la ventana de **Elegir contactos para importar** se mostrará el nombre del certificado raíz **AUTORIDAD CERTIFICADORA DE PANAMÁ**, por lo que debemos seleccionar ese nombre pero en la lista inferior llamada **Certificados**, el cual habilita el botón **Confiar...** que debemos presionar y que muestra otra ventana llamada **Importar configuración de contactos** donde habilitaremos los permisos de confianza para ese certificado raíz, tal como se aprecia en las imágenes inferiores.

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
AUTORIDAD CERTIFICADORA DE PA...	

Certificados

Esta lista muestra los certificados asociados al contacto actualmente seleccionado.

Asunto	Emisor	Caduca
AUTORIDAD CERTIFICAD...	AUTORIDAD CERTIFICA...	05/08/2053 12:02:13 p. m.

Ayuda Importar Cancelar

Importar configuración de contactos

Detalles del certificado

Asunto: AUTORIDAD CERTIFICADORA DE PANAMÁ

Emisor: AUTORIDAD CERTIFICADORA DE PANAMÁ

Uso: Firmar certificado (autoridad del certificado, CA), Firmar lista revocación certificados (CRL)

Caducidad: 05/08/2053 12:02:13 p. m.

Confiar

El certificado utilizado para firmar un documento debe estar designado como anclaje de confianza o tener como origen de cadena un anclaje de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un anclaje de confianza ni en uno superior a él.

☒ Utilizar este certificado como raíz de confianza

Si la validación de firma se realiza correctamente, confíe en este certificado:

- ☒ Documentos o datos firmados
- ☒ Documentos certificados
  - ☒ Contenido dinámico
  - ☒ JavaScript privilegiado incrustado
  - ☒ Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.)

Detalles del certificado...

Ayuda Aceptar Cancelar

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 12 de 27

Para el certificado raíz, debemos seleccionar la opción **Utilizar este certificado como raíz de confianza** y adicional si deseamos podemos marcar las opciones inferiores de **Documentos certificados, Contenido dinámico, JavaScript privilegiado incrustado y Operaciones privilegiadas del sistema**; por si se requieren firmar documentos PDF dinámicos. Luego presionamos **Aceptar** en la ventana de **Importar configuración de contactos** y damos clic en el botón de **Importar** de la ventana anterior **Elegir contactos para importar**, donde iniciará el proceso de importación que debe finalizar con el mensaje de **Importación terminada**, para finalmente presionar **Aceptar**.

Importación terminada

Detalles de la importación:

Se ha(n) importado 1 certificado(s) de emisor.

Aceptar

Cuando se realiza el proceso de importación, el listado en la ventana de **Certificados de confianza** se actualizará y si buscamos por orden alfabético más abajo, debe aparecer el certificado de la **AUTORIDAD CERTIFICADORA DE PANAMA**, lo cual indica que el proceso se realizó correctamente.

Los mismos pasos debemos realizarlos para los certificados de las **Autoridades de Certificación de Gobierno y Panamá Clase 2**, tal como se aprecian en las imágenes inferiores. Sólo se debe tener en cuenta que no debemos editar la confianza de dichos certificados (botón de **Confiar** en la ventana de **Importar configuración de contacto**) ya que ellos heredarán de forma automática la configuración de confianza que establecimos para el certificado raíz anteriormente, por lo que omitimos ese paso.



# REGISTRO PÚBLICO DE PANAMÁ

## DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

### GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS

Código:  
P-42

Versión:  
1.2

Fecha de implementación:  
15 de marzo de 2024

Página: 13 de 27

Elegir contactos para importar

Este cuadro de diálogo te permitirá seleccionar contactos para importarlos a tu lista de identidades de confianza. También puedes definir la confianza de cualquier certificado asociado a los contactos que importes.

**Contactos**

Nombre	Correo electrónico
<input type="text"/>	

**Certificados**

Esta lista muestra los certificados asociados al contacto actualmente seleccionado.

Asunto	Emisor	Caduca
<input type="text"/>		

Buscar archivos de certificados

Este equipo > Descargas

Organizar Nueva carpeta

Nombre	Fecha de modificación	Tipo	Tamaño
El mes pasado (3)			
capc2	02/08/2024 10:59 a. m.	Certificado de seg...	2 KB
cagob	02/08/2024 10:59 a. m.	Certificado de seg...	2 KB
caraiz	02/08/2024 10:59 a. m.	Certificado de seg...	2 KB

Nombre de archivo: cagob Archivos con certificados (\*.fdf)

Buscar archivos de certificados

Este equipo > Descargas

Organizar Nueva carpeta

Nombre	Fecha de modificación	Tipo	Tamaño
El mes pasado (3)			
capc2	02/08/2024 10:59 a. m.	Certificado de seg...	2 KB
cagob	02/08/2024 10:59 a. m.	Certificado de seg...	2 KB
caraiz	02/08/2024 10:59 a. m.	Certificado de seg...	2 KB

Nombre de archivo: capc2 Archivos con certificados (\*.fdf)

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
	Código: <b>P-42</b>	Versión: <b>1.2</b>	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 14 de 27

Elegir contactos para importar

Este cuadro de diálogo te permitirá seleccionar contactos para importarlos a tu lista de identidades de confianza. También puedes definir la confianza de cualquier certificado asociado a los contactos que importes.

**Contactos**

Nombre	Correo electrónico
CAPANAMA CLASE 2	
CADE GOBIERNO DE PANAMA	

Quitar Examinar... Buscar...

**Certificados**

Esta lista muestra los certificados asociados al contacto actualmente seleccionado.

Asunto	Emissor	Caduca
--------	---------	--------

Detalles... Confiar...

Ayuda Importar Cancelar

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

#### 4.3.2 Desactivación del modo protegido del Adobe Reader para interactuar con el lector de tarjetas inteligentes

Con los 3 certificados de las Autoridades de la PKI de Panamá configurados, el Adobe Reader es capaz de validar documentos PDF firmados con certificados emitidos por la **Dirección Nacional de Firma Electrónica de Panamá**, sin embargo, para realizar las operaciones de firma, es necesario que el Adobe pueda acceder al lector de tarjetas inteligentes, cuyo controlador de SafeSign instalamos anteriormente. Para realizar dicha acción, nos dirigimos primero a **Edición -> Preferencias -> Seguridad (mejorada)** y desactivamos la opción **Activar modo protegido al iniciar** desmarcándola, se presiona el botón de **Sí** y luego **Aceptar** en esa ventana de **Seguridad (mejorada)**, para así reiniciar el Adobe Reader (cerrándolo y volviéndolo a ejecutar).



# REGISTRO PÚBLICO DE PANAMÁ

## DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

### GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS

Código:  
P-42

Versión:  
1.2

Fecha de implementación:  
15 de marzo de 2024

Página: 15 de 27

Preferencias

Categorías:

- Comentario
- Documentos
- General
- Pantalla completa
- Presentación de página
- 3D y multimedia
- 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
- Rastreador
- Revisión
- Seguridad
- Seguridad (mejorada)
- Servicios en línea de Adobe
- Unidades

Protecciones de la zona de pruebas

☐ Activar modo protegido al iniciar ☒ Ejecutar en AppContainer ☐ Crear un archivo de registro en modo protegido [Visualizar registro](#)

Vista protegida ☒ Desactivado

☐ Archivos de ubicaciones potencialmente no seguras

☐ Todos los archivos

Seguridad mejorada

☒ Activar seguridad mejorada ☐ Archivo de registro entre dominios [Ver](#)

Ubicaciones privilegiadas

Si tiene flujos de trabajo que dependen de la seguridad, utilice la forma selectiva de seguridad. La forma selectiva de seguridad otorga confianza a los elementos de su flujo de trabajo.

☐ Confiar automáticamente en los documentos con una certificación válida

☒ Confiar automáticamente en sitios de las zonas de seguridad de mi Win OS [Ver sitios de confianza de Windows](#)

[¿Qué es el modo protegido?](#) [¿Qué es la seguridad mejorada?](#) [¿Qué son las ubicaciones privilegiadas?](#)

[Aceptar](#) [Cancelar](#)

Preferencias

Categorías:

- Comentarios
- Documentos
- General
- Pantalla completa
- Presentación de página
- Accesibilidad
- Administrador de confianza
- Buscar
- Cuentas de correo electrónico
- Elementos 3D y multimedia
- Elementos multimedia (heredados)
- Elementos multimedia de confianza (heredado)
- Firmas
- Formularios
- Identidad
- Idioma
- Internet
- JavaScript
- Lectura
- Medición (2D)
- Medición (3D)
- Medición (Geo)
- Ortografía
- Rastreador
- Revisión
- Seguridad
- Seguridad (mejorada)
- Servicios en línea de Adobe
- Unidades

Protecciones de la zona de pruebas

☐ Habilitar modo protegido al iniciar ☐ Ejecutar en AppContainer

Vista protegida ☒ Desactivado

☐ Archivos de ubicaciones potencialmente no seguras

☐ Todos los archivos

Seguridad mejorada

☒ Activar seguridad mejorada ☐ Archivo de registro entre dominios [Ver](#)

Ubicaciones privilegiadas

Si tienes flujos de trabajo que se vean afectados de forma negativa por la configuración de seguridad, utiliza Ubicaciones privilegiadas para confiar en archivos, carpetas y hosts de forma selectiva para excluirlos de las restricciones establecidas en la configuración de seguridad. Las ubicaciones privilegiadas te permiten trabajar de forma segura mientras otorga confianza a los elementos de tu flujo de trabajo.

☐ Confiar automáticamente en los documentos con una certificación válida

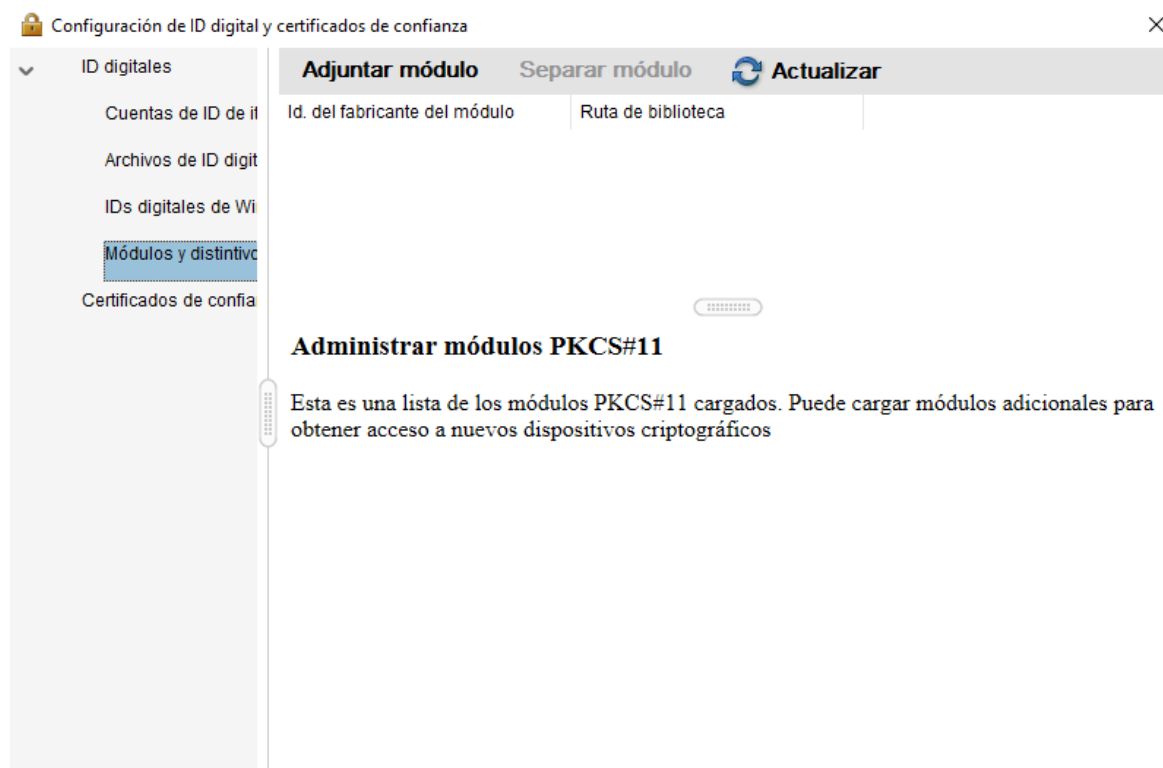
☒ Confiar automáticamente en sitios de las zonas de seguridad de mi Win OS [Ver sitios de confianza de Windows](#)

[¿Qué es el modo protegido?](#) [¿Qué es la seguridad mejorada?](#) [¿Qué son las ubicaciones privilegiadas?](#)

[Aceptar](#) [Cancelar](#)

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 16 de 27

Cuando se vuelve a iniciar el Adobe Reader, volvemos al menú de **Edición** -> **Preferencias** -> **Firmas** y damos clic en el tercer botón de **Más (Identidades y certificados de confianza)**, pero esta vez expandimos la opción **ID digitales** y seleccionamos **Módulos y distintivos PKCS#11**. Usamos la opción de **Adjuntar módulo** (la cual debe estar habilitada y si no lo está, es porque el Adobe se sigue ejecutando en modo protegido y debemos desactivarlo según las indicaciones anteriores) y luego saldrá la ventana para que busquemos al archivo **aetpkss1.dll** en la carpeta **C:\Windows\System32**, lo seleccionamos y presionamos **Abrir**.







## REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

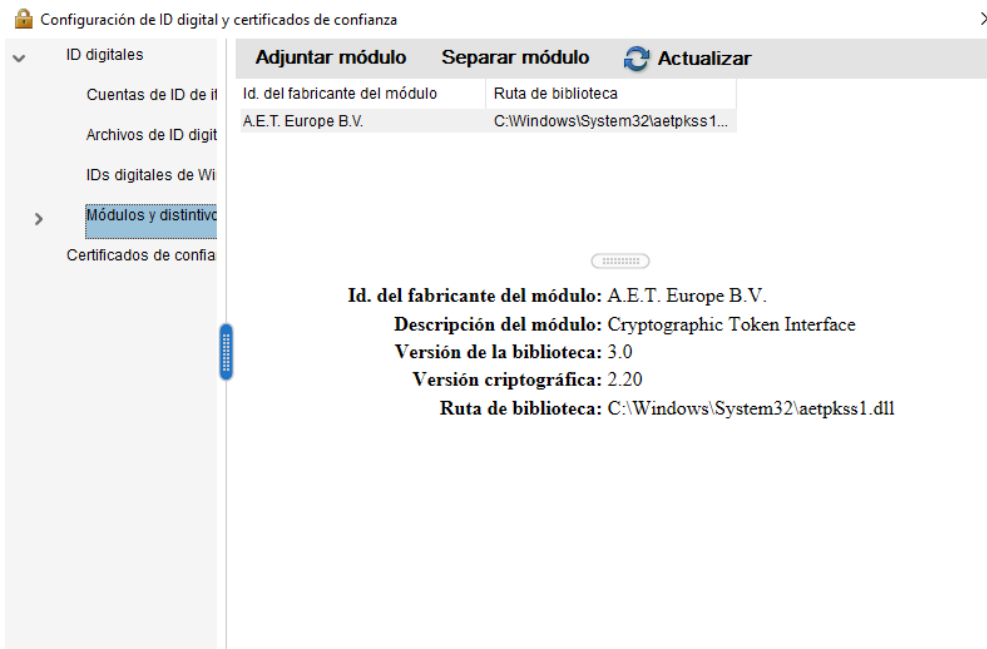
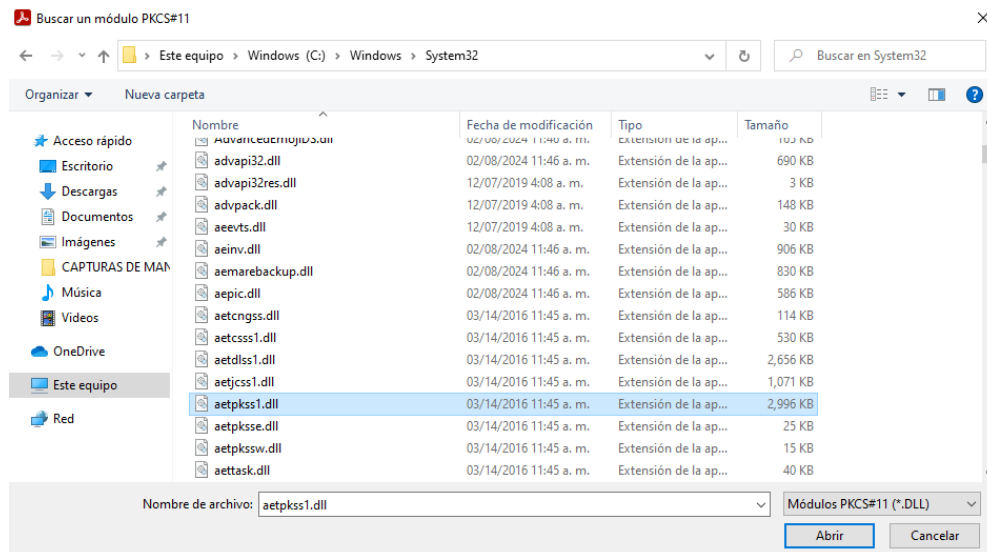
### GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS

Código:  
P-42

Versión:  
1.2

Fecha de implementación:  
15 de marzo de 2024

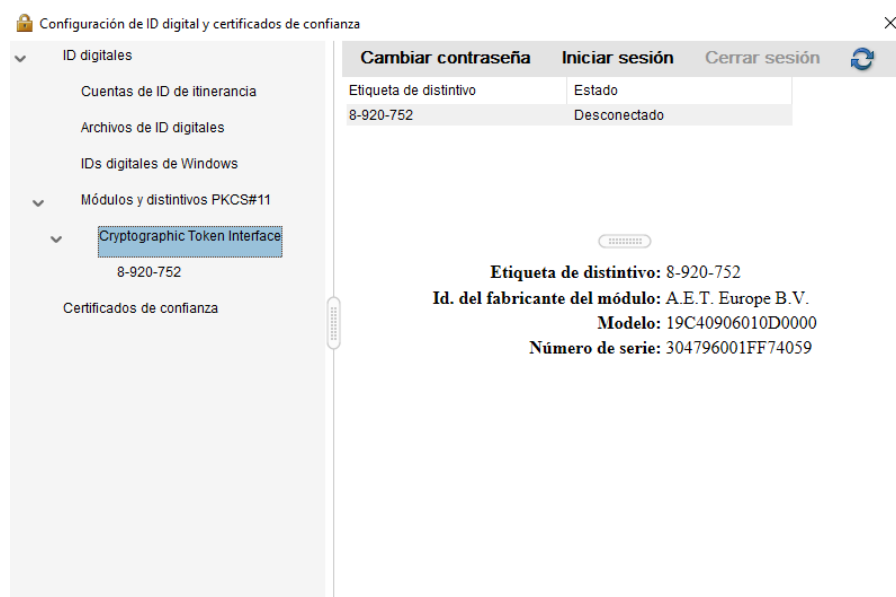
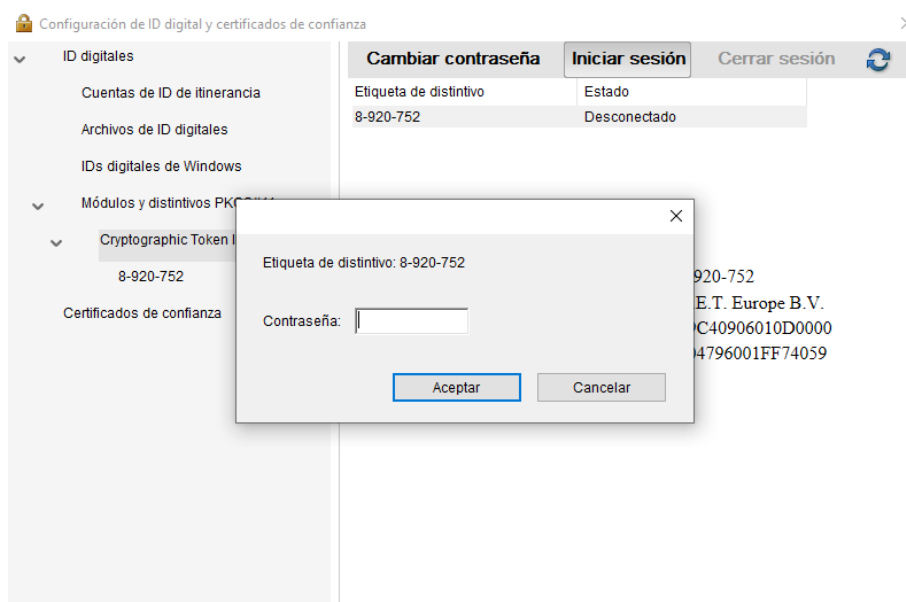
Página: 17 de 27



Después de seleccionar y abrir el archivo **aetpkss1.dll** en la ventana, se mostrará el controlador de la tarjeta, tal como se aprecia en la imagen inferior y si ingresamos en la opción de **Módulos y distintivos PKCS#11 -> Cryptographic Token Interface**, saldrá la cédula con el estado

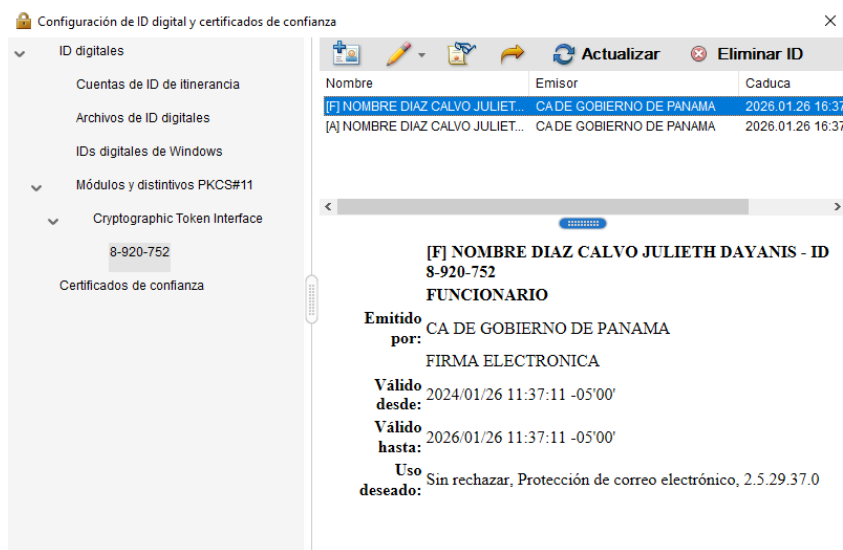
 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 18 de 27

**Desconectado** que representa el ID de la tarjeta insertada en el lector. Se presiona 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**.

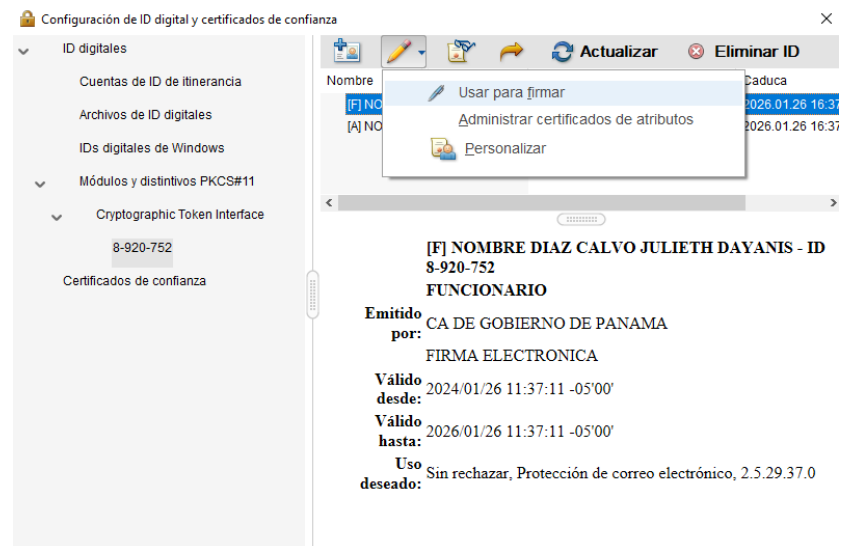
 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA		
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>		
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 19 de 27

Si seleccionamos el ID de la cédula, se visualizarán en la pantalla los dos certificados que están en la tarjeta ([A] Autenticación y [F] Firma). Es importante seleccionar el de firma [F] y dar clic en el icono del lápiz (**Opciones de uso**) indicando **Usar para firmar**, para que el Adobe Reader pueda utilizar dicho certificado en la firma de documentos PDF. Luego cerramos esa ventana y presionamos **Aceptar** en preferencias.



Nombre	Emitor	Caduca
[F] NOMBRE DIAZ CALVO JULIETH...	CA DE GOBIERNO DE PANAMA	2026.01.26 16:37
[A] NOMBRE DIAZ CALVO JULIETH...	CA DE GOBIERNO DE PANAMA	2026.01.26 16:37

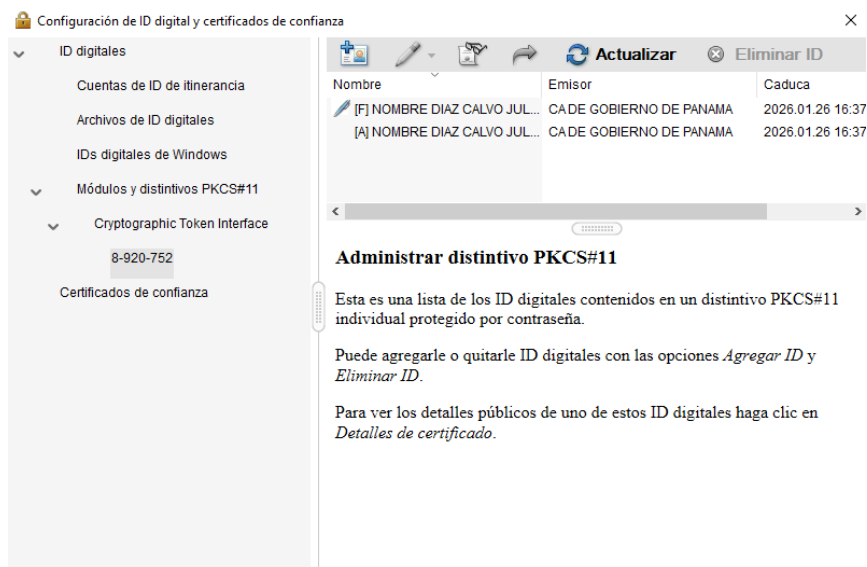
**[F] NOMBRE DIAZ CALVO JULIETH DAYANIS - ID 8-920-752**  
**FUNCIONARIO**  
 Emitido por: CA DE GOBIERNO DE PANAMA  
 FIRMA ELECTRONICA  
 Válido desde: 2024/01/26 11:37:11 -05'00'  
 Válido hasta: 2026/01/26 11:37:11 -05'00'  
 Uso deseado: Sin rechazar, Protección de correo electrónico, 2.5.29.37.0



Nombre	Emitor	Caduca
[F] NOMBRE DIAZ CALVO JULIETH...	CA DE GOBIERNO DE PANAMA	2026.01.26 16:37
[A] NOMBRE DIAZ CALVO JULIETH...	CA DE GOBIERNO DE PANAMA	2026.01.26 16:37

**[F] NOMBRE DIAZ CALVO JULIETH DAYANIS - ID 8-920-752**  
**FUNCIONARIO**  
 Emitido por: CA DE GOBIERNO DE PANAMA  
 FIRMA ELECTRONICA  
 Válido desde: 2024/01/26 11:37:11 -05'00'  
 Válido hasta: 2026/01/26 11:37:11 -05'00'  
 Uso deseado: Sin rechazar, Protección de correo electrónico, 2.5.29.37.0

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 20 de 27	



Nombre	Emisor	Caduca
[F] NOMBRE DIAZ CALVO JUL...	CA DE GOBIERNO DE PANAMA	2026.01.26 16:37
[A] NOMBRE DIAZ CALVO JUL...	CA DE GOBIERNO DE PANAMA	2026.01.26 16:37

**Administrar distintivo PKCS#11**

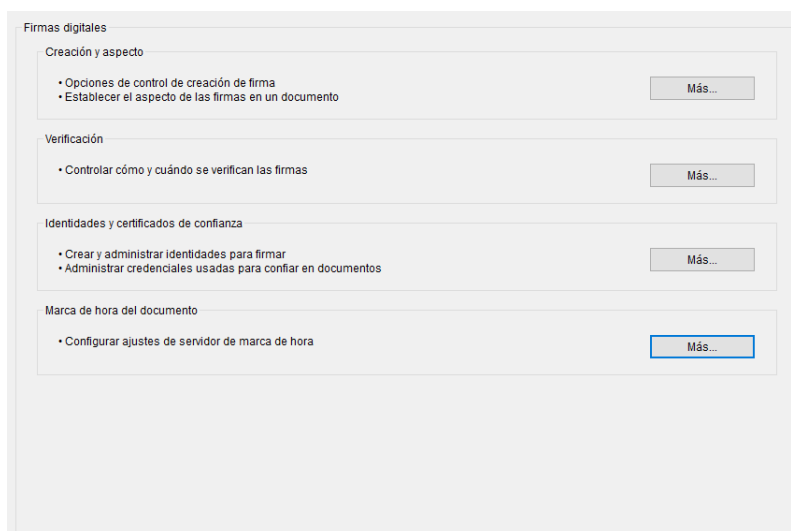
Esta es una lista de los ID digitales contenidos en un distintivo PKCS#11 individual protegido por contraseña.

Puede agregarle o quitarle ID digitales con las opciones *Agregar ID* y *Eliminar ID*.

Para ver los detalles públicos de uno de estos ID digitales haga clic en *Detalles de certificado*.

#### 4.4 Configuración del servidor de Sellado de tiempo

Lo ideal es que cada documento que firmemos lleve incrustado una marca de hora ofrecida por un servidor de Sellado de tiempo y para configurar esa opción en el Adobe Reader volvemos al menú de **Firmas (Edición -> Preferencias -> Firmas)** y damos clic en el último botón de **Más (Marca de hora del documento)**.



**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

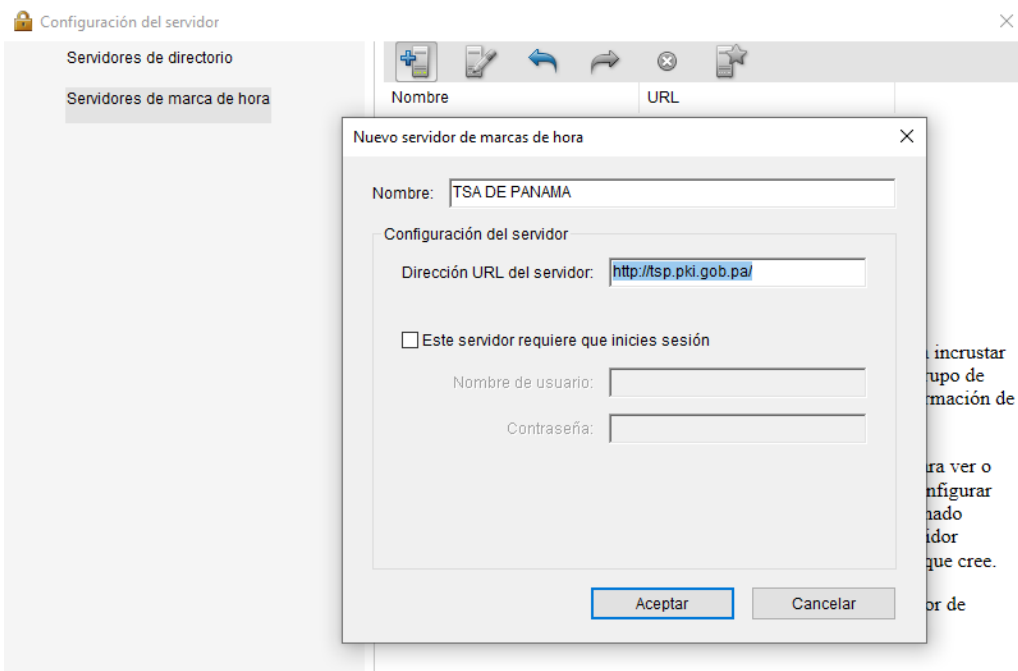
Más...

**Marca de hora del documento**

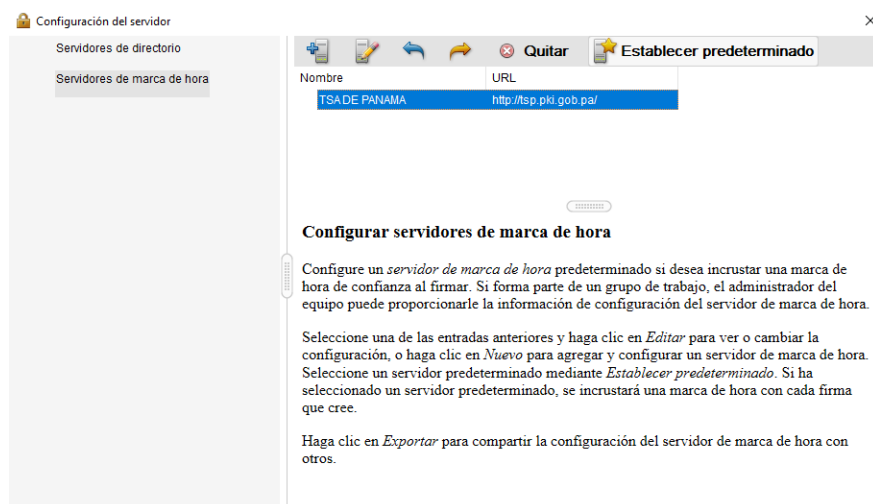
- Configurar ajustes de servidor de marca de hora

Más...

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA		
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>		
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 21 de 27



En la siguiente ventana (**Configuración del servidor**) seleccionamos **Servidores de marca de hora** y damos clic en **Nuevo** para colocar un **Nombre** que identifique a nuestro servidor (puede ser **TSA Panamá** o el nombre que deseen), luego en la **Dirección URL del servidor** escribimos <http://tsp.pki.gob.pa/> y presionamos **Aceptar**.



**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, o haga clic en *Nuevo* para agregar y configurar un servidor de marca de hora. Seleccione un servidor predeterminado mediante *Establecer predeterminado*. Si ha seleccionado un servidor predeterminado, se incrustará una marca de hora con cada firma que cree.

Haga clic en *Exportar* para compartir la configuración del servidor de marca de hora con otros.

	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA		
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS  CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS  EN EL PROGRAMA ADOBE ACROBAT READER DC EN  MICROSOFT WINDOWS</b>		
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>
			Página: 22 de 27

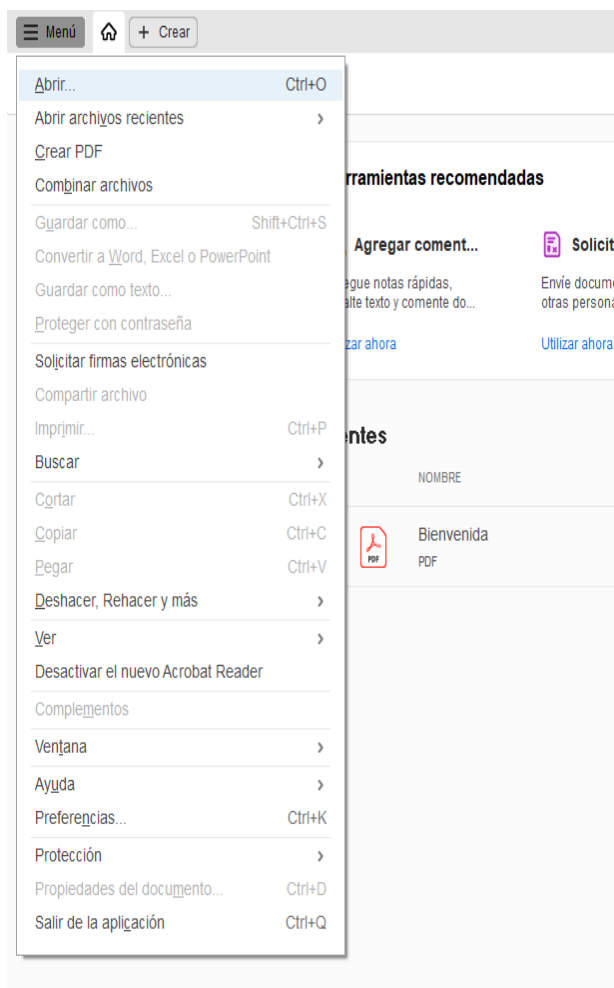
Posteriormente se podrá apreciar que la dirección de la **Autoridad de Sellado de Tiempo de Panamá** aparecerá en la ventana de **Configuración del servidor** y es importante seleccionarla para presionar el botón de **Establecer predeterminado**, donde indicaremos **Aceptar** en la pregunta de seguridad de Acrobat. Al finalizar, debe mostrarse el servidor de TSA como predeterminado y se puede cerrar la ventana, para luego presionar **Aceptar** en la ventana de **Preferencias**.



#### 4.5 Prueba para firmar un documento PDF con el Adobe Reader

Si se han configurado los certificados de las CA, se ha desactivado el modo protegido del Adobe Reader indicando la ruta del controlador y si se ha indicado el servidor del Sellado de Tiempo, podemos realizar una prueba firmando un documento PDF. Para realizar esta acción, abrimos el documento deseado, dando doble clic sobre el archivo en el explorador de Windows (o el sistema operativo en uso) o utilizando la misma opción del Adobe Reader **Archivo -> Abrir**.

 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA		
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS  CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS  EN EL PROGRAMA ADOBE ACROBAT READER DC EN  MICROSOFT WINDOWS</b>		
Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 23 de 27



Una vez que tenemos el documento abierto, se abrirá automáticamente la barra de **Herramientas** a mano izquierda del documento abierto. Bajaremos y daremos clic en **Ver más**. Luego daremos clic en **Utilizar un certificado**. Esa opción habilitará otra barra de herramientas a mano izquierda de la pestaña que muestra al documento PDF abierto con las opciones de **Firmar digitalmente**, **Marca de hora** y **Validar todas las firmas**. Seleccionamos **Firmar digitalmente**.



# REGISTRO PÚBLICO DE PANAMÁ

## DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

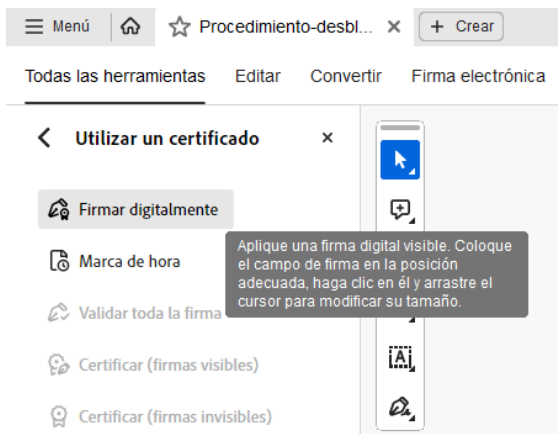
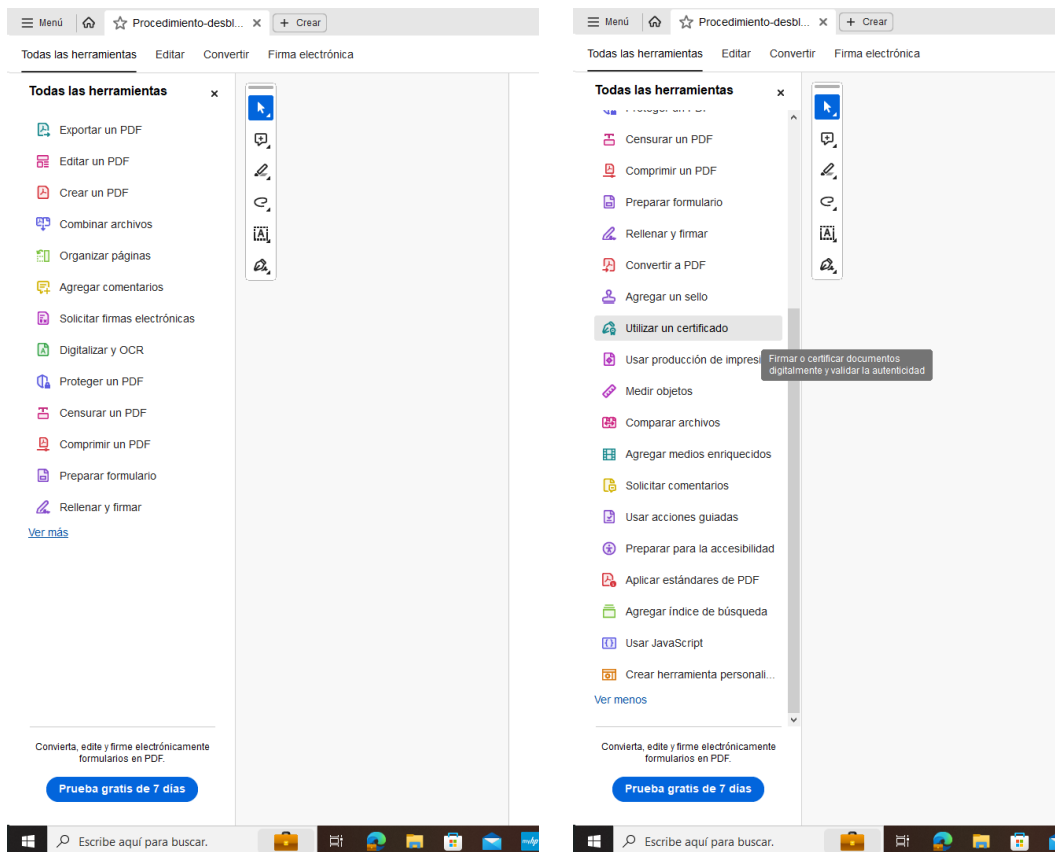
### GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS

Código:  
P-42

Versión:  
1.2

Fecha de implementación:  
15 de marzo de 2024

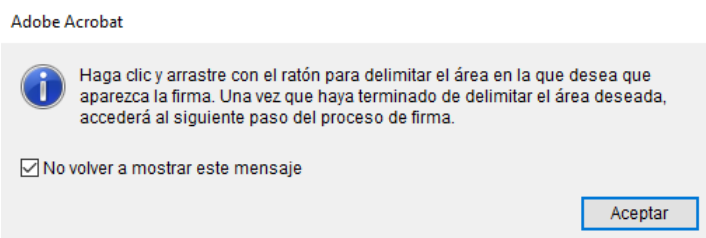
Página: 24 de 27



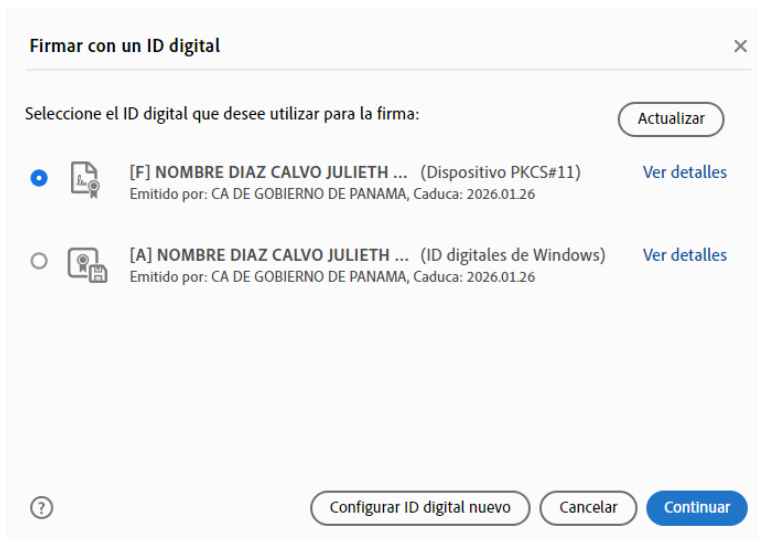


 	<b>REGISTRO PÚBLICO DE PANAMÁ</b> DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA			
	<b>GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS          CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS          EN EL PROGRAMA ADOBE ACROBAT READER DC EN          MICROSOFT WINDOWS</b>			
	Código: P-42	Versión: 1.2	Fecha de implementación: <b>15 de marzo de 2024</b>	Página: 25 de 27

Luego saldrá un mensaje indicando que podemos dibujar con el Mouse un cuadro en cualquier parte del documento donde se añadirá una imagen visual que representa la firma, se presiona **Aceptar** y se procede a dibujar en el área deseada como lo muestran las imágenes inferiores.



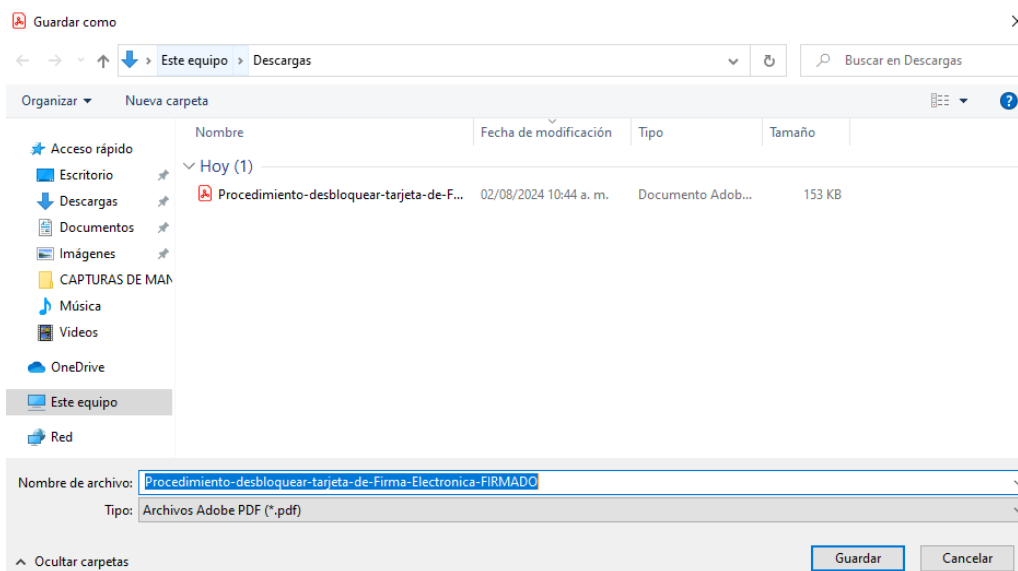
Cuando hemos seleccionado el área del documento donde estará la imagen de la firma, se mostrará una ventana para escoger el certificado que se utilizará para firmar. Normalmente se mostrarán los certificados incluidos en el repositorio de Windows, donde deben salir también los que están en la tarjeta insertada en el lector. Escogemos el certificado que empieza con **[F] NOMBRE ....**, damos clic en **Continuar** donde aparece una imagen por defecto que genera el Adobe con el nombre del certificado y la cédula (se puede dejar esa o cambiarla por una imagen personalizada usando las opciones que se brindan), se escribe el número PIN de la tarjeta y finalmente se indica **Firmar**.





# GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS

Página: 26 de 27



La impresión de este documento se convierte en una copia NO CONTROLADA.



## REGISTRO PÚBLICO DE PANAMÁ DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA

### GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE LOS CERTIFICADOS DE LAS AUTORIDADES RAÍZ E INTERMEDIAS EN EL PROGRAMA ADOBE ACROBAT READER DC EN MICROSOFT WINDOWS

Código:  
P-42

Versión:  
1.2

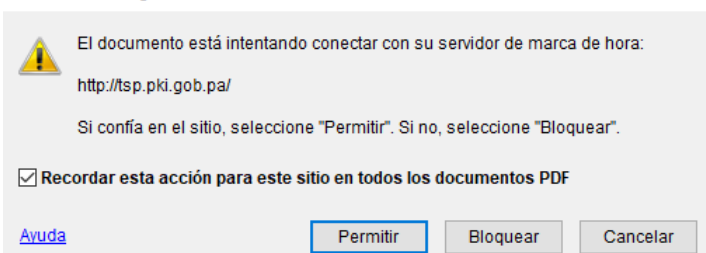
Fecha de implementación:  
15 de marzo de 2024

Página: 27 de 27

Luego de esto aparecerá en nuestras pantallas una advertencia de seguridad debido a que el documento está intentando conectarse con nuestro servidor de marca de hora. Presionaremos **Recordar esta acción para este sitio en todos los documentos PDF y Permitir**.

Advertencia de seguridad

X



Si todo se realiza correctamente, se debe mostrar el documento PDF con la imagen representativa de la firma y una leyenda indicando que el documento está **Firmado y todas las firmas son válidas**.

Firmado y todas las firmas son válidas. Panel de firma

el código PUK que está en su sobre (si lo cambio deberá usar el nuevo) para desbloquearla con el siguiente procedimiento:

1. Debe ejecutar el programa **Utilidad para administración de tokens** (se puede buscar con el nombre **Tokenadmin** en el menú de inicio de **Windows** o en el **Launchpad** en **macOS**).
2. Con la tarjeta insertada en el lector, se selecciona la cédula en el **Tokenadmin** con el botón derecho del mouse y se da click en **Desbloquear PIN** (dicha opción también se encuentra en el menú **Token -> Desbloquear PIN**). Luego escribe el número PUK (que también tiene sólo 3 intentos y si se agotan la tarjeta quedaría bloqueada de forma definitiva) y el PIN que desee utilizar dos veces para que así se desbloquee la tarjeta después de presionar el botón de **Aceptar**.
3. Al final, después de desbloquear la tarjeta, debería poder firmar nuevamente; donde en ocasiones si se utilizan programas como el Adobe Reader, es recomendable salir y volver a entrar en para evitar errores.

[F] NOMBRE DIAZ  
CALVO JULIETH  
DAYANIS - ID  
8-920-752

Firmado digitalmente  
por [F] NOMBRE DIAZ  
CALVO JULIETH DAYANIS  
- ID 8-920-752  
Fecha: 2024.02.08  
11:46:19 -05'00'