

ANEXO 4

Manual Para la Creación y Firma de los Documentos PDF requeridos para el Registro de Productos de Seguros para la Versión 5.0 de Adobe Acrobat

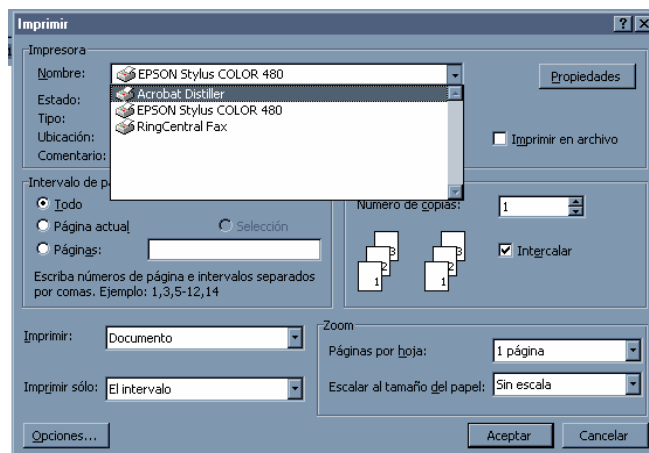
Introducción

El presente manual tiene como objetivo orientar en lo referente a la creación y validación de firmas a través del software denominado Adobe Acrobat, enfocado únicamente a los procedimientos para llevar a cabo el registro de productos de seguros, a través de la página Web de esta Comisión.

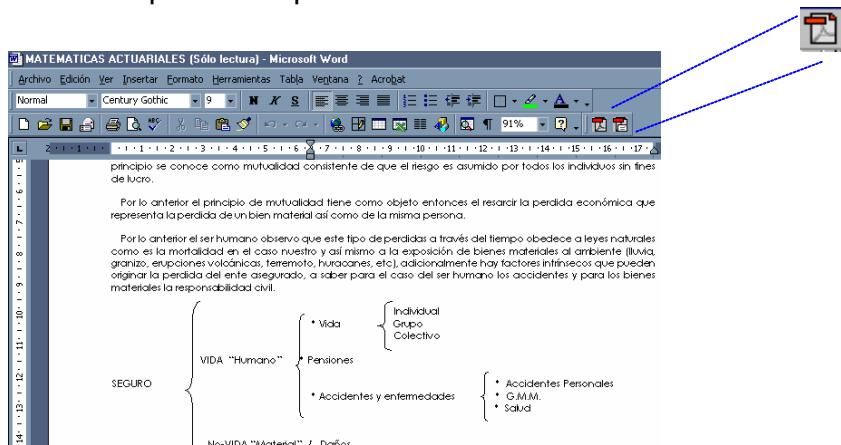
En concordancia con la Disposición Cuarta de la presente Circular todos los documentos requeridos para el registro de un producto deberán conformarse en archivos de formato PDF (Portable Document Format) y serán enviados a través de la página Web de esta Comisión. Estos archivos deberán crearse mediante el software denominado Adobe Acrobat, versión 5.0 o posterior.

Los documentos PDF conservan fielmente el contenido y la apariencia de los documentos originales, incluyendo gráficos y fuentes, y pueden distribuirse por cualquier medio magnético para hacerlos accesibles a otros usuarios.

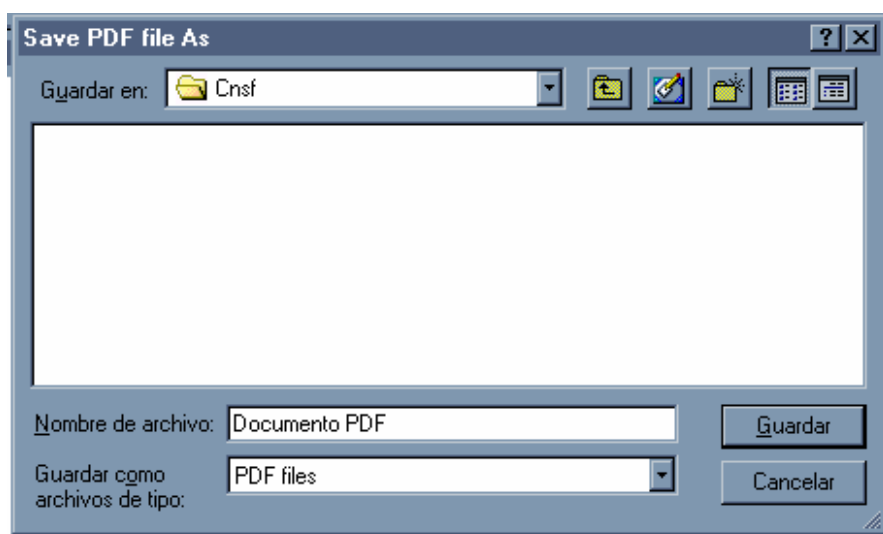
El proceso de creación de documentos en Acrobat empieza con la conversión del material de origen o los documentos existentes a formato PDF (en el caso de productos, serán por lo regular archivos de word o excel). Acrobat crea una copia del material de origen a formato PDF (sin modificarlo). Para convertir un archivo electrónico a formato PDF, puede “imprimir” el archivo a dicho formato desde otra aplicación (word, excel), como si se imprimiera en papel, pero se debe seleccionar una de las impresoras del Adobe Acrobat (Acrobat Distiller o Acrobat PDFWriter) de manera indistinta; se sugiere seleccionar Acrobat Distiller ya que es un poco más rápida la conversión del documento a PDF cuando éste tiene imágenes o símbolos matemáticos.



Si dentro de la aplicación del material de origen existe en la barra de herramientas el ícono de Acrobat, deberá hacer clic en éste una vez configurando previamente el archivo para su impresión.



En ese momento aparecerá la siguiente pantalla:



en la cual se deberá elegir nombre y ruta en la que desee guardar el documento en formato PDF; posteriormente se deberá oprimir el botón “Guardar”, con esto se creará el documento PDF preservando visualmente el contenido del material de origen.

En el caso de Windows, se puede convertir un documento simplemente abriéndolo desde el propio Acrobat.

Los documentos PDF proporcionan un alto nivel de seguridad, permiten agregar, validar y controlar firmas digitales para acreditar su estatus. También pueden verse todas las firmas que se han añadido al documento, comprobar la validez de éstas, y retroceder a una versión del documento firmada anteriormente.

Firmas Electrónicas

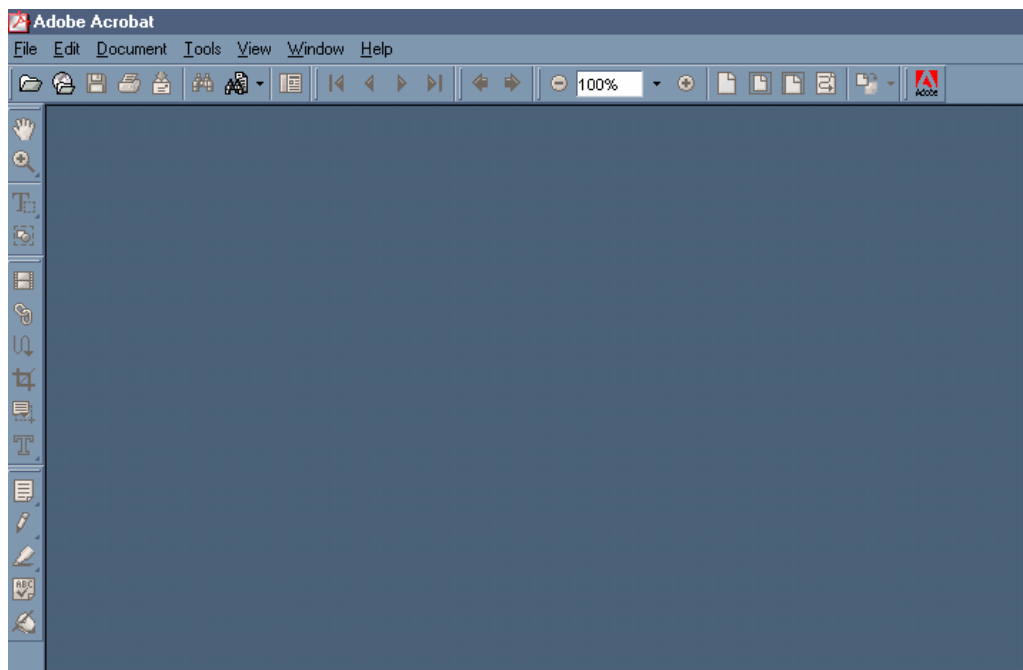
Una firma electrónica, como cualquier otra firma autógrafa, identifica a la persona que firma un documento y además puede reconocer la entidad a la que pertenece. Cada firma digital almacena información invisible sobre la persona firmante y el estado exacto del documento en el momento de la firma. Cuando se visualiza un documento firmado en Acrobat, se puede validar su firma para confirmar la identidad del firmante y verificar que el documento no se ha alterado desde que se firmó.

Un documento en formato PDF puede ser firmado más de una vez y por más de una persona. Cada firma se asocia con una versión del documento, que representa el estado de éste en el momento de ser firmado por esa persona. Solamente la primera vez que se firma un documento, el Acrobat requiere que se guarde como un nuevo PDF. A partir de ese momento, cada vez que se vuelva a firmar el documento, la nueva firma y los cambios que se introduzcan sobre la versión precedente se anexan al archivo. Al visualizar un documento con más de

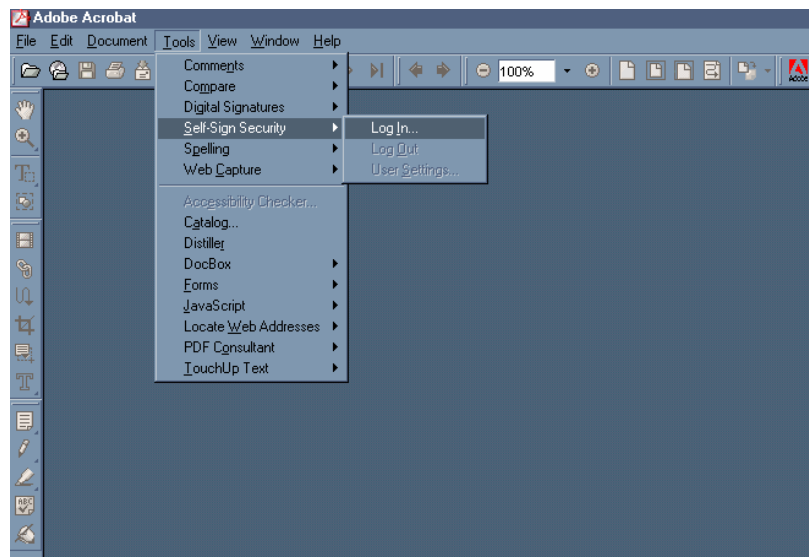
una firma se ve su versión más reciente, pero se puede abrir una versión anterior en un archivo distinto para compararlas y ver qué cambios se han realizado.

Creación de firmas

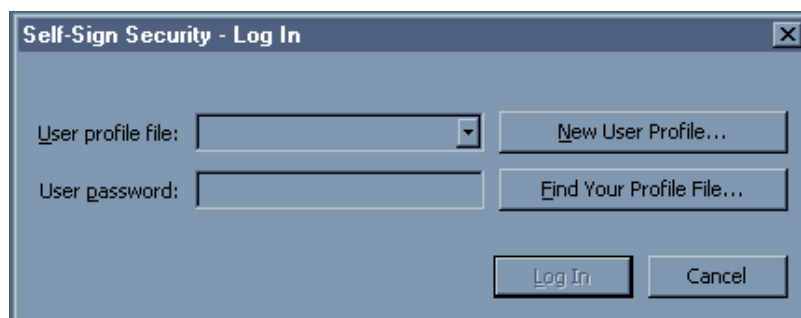
La ventana principal del Adobe Acrobat es:



Antes de iniciar el proceso de creación de firmas se debe acceder al controlador de firmas denominado Acrobat Self-Sign, el cual proporciona una forma fácil y rápida de firmar documentos, y usa un sistema de llaves privadas y públicas para verificar la autenticidad de las firmas y la integridad de las versiones del documento. Para usar el controlador de firmas será necesario configurar un perfil de usuario, posicionándose en el menú superior y seleccionando, "Tools", "Self-Sign Security", "Log in...", tal como se muestra a continuación:



Al hacer clic en “Log In...” aparecerá la siguiente ventana:



El usuario debe oprimir el botón “New User Profile...”, al hacer esto visualizará la pantalla de captura que se muestra a continuación, y estará en posibilidad de configurar su perfil. El perfil es una serie de datos del usuario y de seguridad, que se almacenan en un archivo:

Create New User

Create a 1024-bit RSA private key and X.509 public key certificate, and store in a password-protected profile file.

User Attributes

Name (e.g. John Smith):

Organization name: (optional)

Organization Unit: (optional)

Country: (optional)

Profile File

Choose a password: (6 characters minimum)

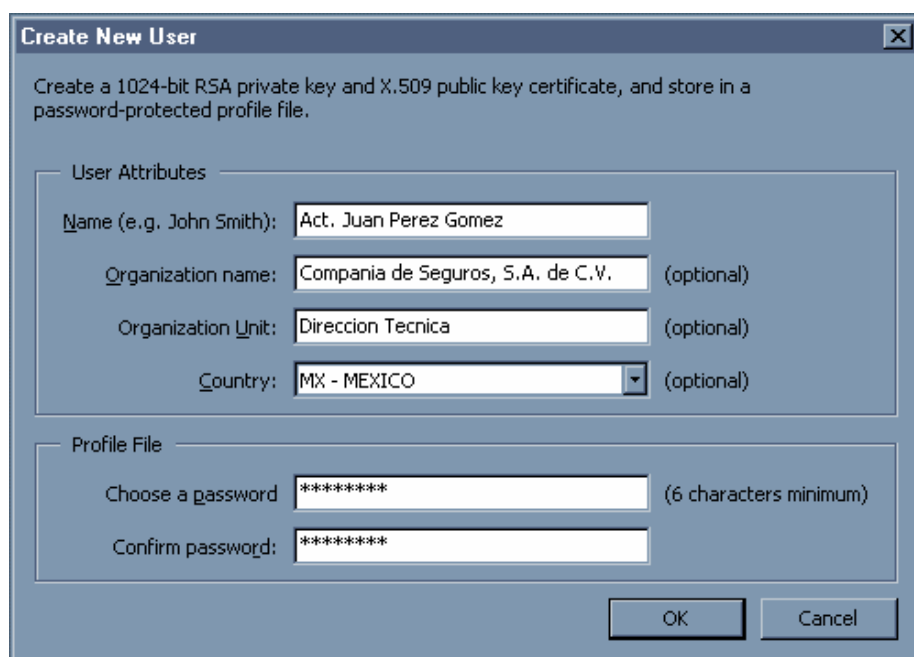
Confirm password:

OK Cancel

La pantalla de captura anterior debe ser llenada con los datos solicitados; en la sección “User Attributes” se requiere nombre del signatario, nombre de la organización a la que pertenece, unidad de la organización y país. Es importante señalar que sólo se admiten caracteres romanos, por lo que los siguientes caracteres no son válidos para llenar el perfil: ! @ # \$ % ^ & *, comillas dobles, | \ ; < > _ ñ y acentos ortográficos.

En el apartado “Profile File”, el usuario debe teclear y confirmar una contraseña de al menos seis caracteres, ésta será conocida únicamente por la persona que está dando de alta una nueva firma.

Ejemplo:



Create New User [X]

Create a 1024-bit RSA private key and X.509 public key certificate, and store in a password-protected profile file.

User Attributes

Name (e.g. John Smith):

Organization name: (optional)

Organization Unit: (optional)

Country: (optional)

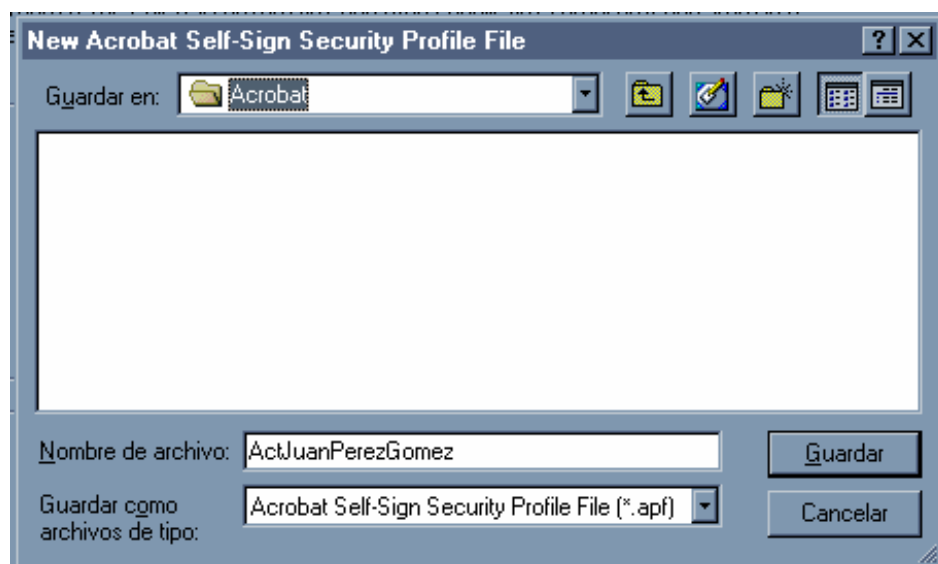
Profile File

Choose a password: (6 characters minimum)

Confirm password:

OK Cancel

Una vez que todos los campos mínimos fueron debidamente capturados se debe oprimir el botón “Ok”, y aparecerá un recuadro que permite guardar el perfil en la ruta que se desee. La ubicación predeterminada del archivo de perfil es la carpeta de Acrobat. Una vez seleccionada la ubicación deseada haga clic en “Guardar”.



New Acrobat Self-Sign Security Profile File [?] [X]

Guardar en: [Icons]

Nombre de archivo:

Guardar como archivos de tipo:

Guardar Cancelar

Con lo anterior se ha creado y guardado un archivo que contiene el perfil del firmante, con lo que quedará predefinido. Es importante enfatizar que los signatarios de los documentos que integran un producto, señalados en la

Disposición Cuarta de la presente Circular a efecto de que puedan utilizar su firma electrónica, deberán generar un perfil cada cinco años, que es el periodo de vigencia del certificado digital.

El usuario debe invocar a su perfil e identificarse a través del controlador de firmas cada vez que desee firmar un documento, o validar la firma de otra persona.

El archivo que contiene el perfil almacena la llave privada (codificada), la llave pública empaquetada en un certificado y una sección de “Trusted Certificates”¹ con los certificados de otros usuarios, entre otros datos. El nombre de este archivo es el nombre que se asigna al perfil, más la extensión .apf.

El nombre de los archivos asociados a los certificados digitales deberá corresponder al nombre completo del responsable de la firma de los documentos que conforman el producto, con objeto de lograr uniformidad para el control eficiente de las validaciones que se realizarán en esta Comisión

 ActJuanPerezGomez

No será necesario efectuar el procedimiento descrito anteriormente, relativo a la generación de los perfiles que contienen las llaves públicas y privadas, cada vez que se pretenda someter a registro un producto, en virtud de que los mencionados perfiles quedan predefinidos.

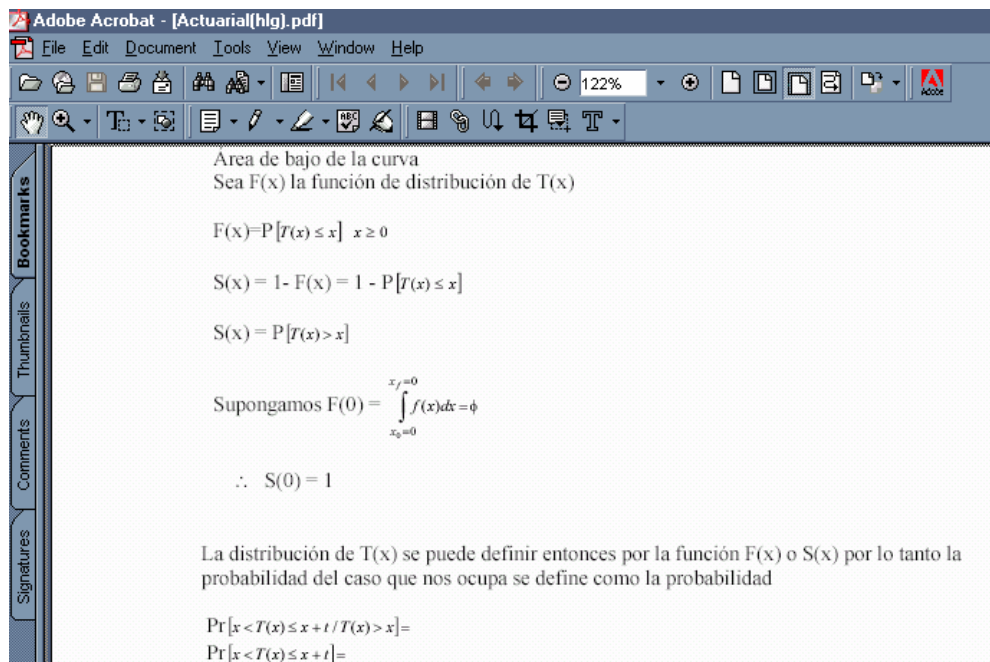
Firma de Documentos

Una vez creado el certificado se puede firmar cualquier documento en formato PDF, siempre y cuando el signatario se identifique con su perfil.

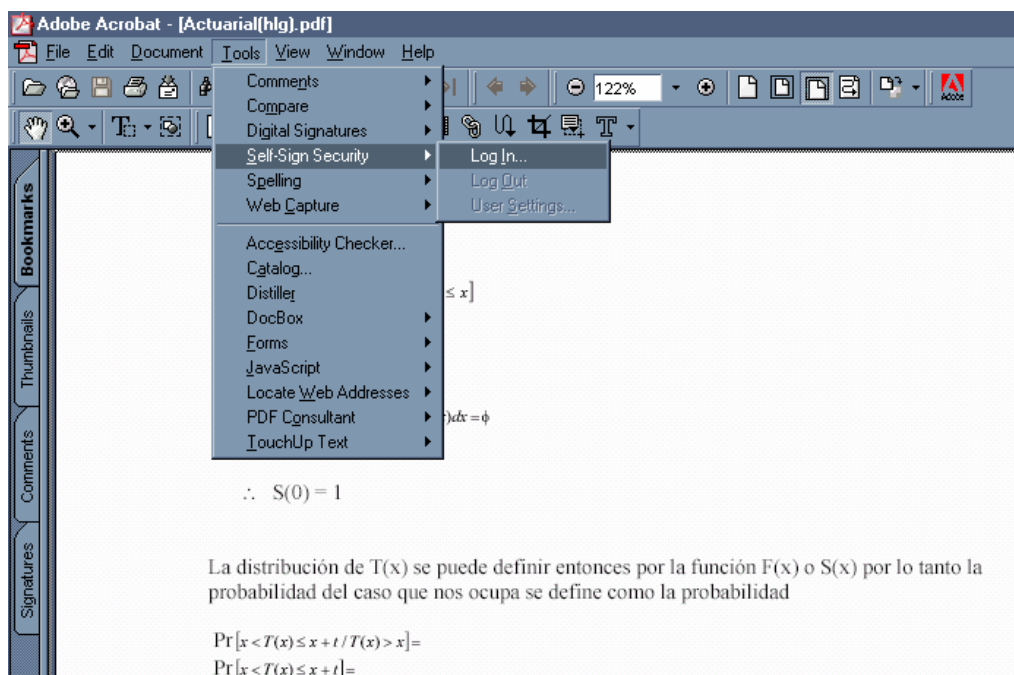
La firma en un archivo PDF, y la información contenida en ella, se almacenan en un campo de firma insertado en una página del documento. La firma puede añadirse en cualquier zona del documento, por lo que no es necesario aplicarla en cada página del mismo.

Para firmar un documento en formato PDF, primeramente debe tenerse visible.

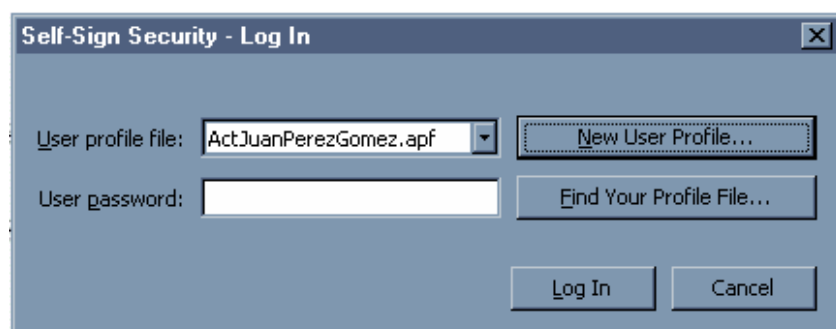
¹ Para mayor información de cómo integrar las llaves públicas de los usuarios en la sección de “Trusted Certificates”, deberá remitirse a la sección “Generación y entrega de llaves públicas” del presente Anexo



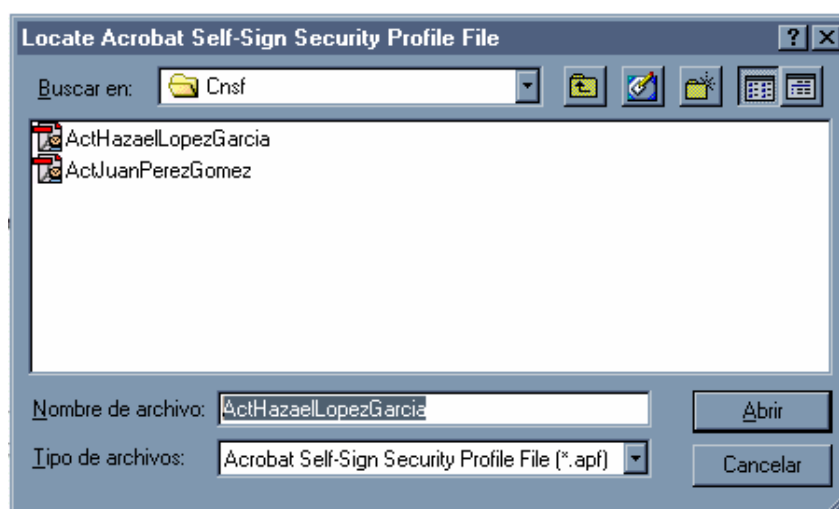
En seguida, se debe “llamar” al perfil del usuario, mediante el controlador de firmas; para lo cual el usuario debe posicionarse el menú superior y seleccionar, “Tools”, “Self-Sign Security”, “Log in...”, tal como se muestra a continuación:



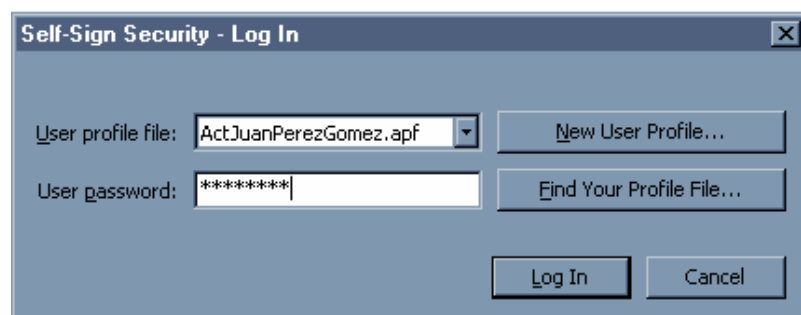
Al hacer clic en “Log in...”, se visualiza la siguiente ventana:



Si el perfil que se muestra en el cuadro de “User Profile file” no es el de la persona que pretende firmar, ésta deberá hacer clic en el botón “Find Your Profile File,,,”; en ese momento aparecerá un visor que permitirá buscar el perfil deseado en la ruta dónde se almacenó. Una vez seleccionado, bastará con hacer clic en el botón “Abrir”



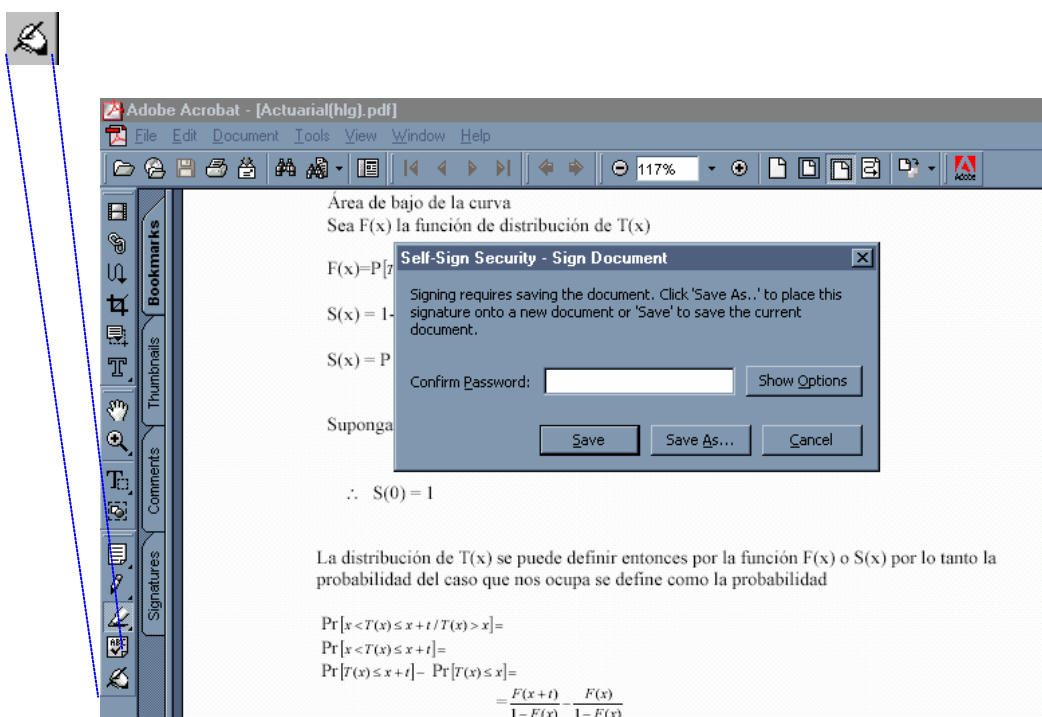
Entonces aparecerá el cuadro de “Log In”, en el cual el usuario deberá teclear su contraseña:



Si la contraseña es la correcta, el controlador de firmas identificará al usuario de acuerdo con su perfil.

Para plasmar una firma en el documento, el usuario deberá hacer clic en el ícono “Firma digital”. Con el puntero del “ratón” (mouse) se deberá trazar el área del documento donde se desee insertar la firma. Deberá procurarse que la zona se encuentre en blanco, en cercanía al nombre del firmante, a fin de visualizarla claramente.

De forma inmediata aparecerá el cuadro de diálogo “Sign Document”, en el cual deberá teclearse la contraseña del signatario, con lo cual el documento quedará firmado.



En caso de oprimir “Show Options”, aparecerá el siguiente cuadro de diálogo:



The image shows a Windows-style dialog box titled "Self-Sign Security - Sign Document". It contains the following elements: a text box for "Confirm Password:" with a "Hide Options" button to its right; a dropdown menu for "Reason for signing document: (select or edit)" currently showing "<none>"; a text box for "Location, e.g. city name: (optional)"; a text box for "Your contact information, e.g. phone number: (optional)"; a "Signature Appearance:" section with a dropdown menu showing "Standard Text" and "Preview..." and "New..." buttons; and a bottom row with "Save", "Save As...", and "Cancel" buttons.

Es mediante este cuadro de diálogo, donde se puede configurar la firma electrónica.

En el campo "Reason for signing document", el usuario puede elegir dentro de un catálogo predeterminado el motivo por el cual se firma el documento, o elegir la opción "<none>" para hacer una descripción personalizada, la cual formará parte del catálogo, a partir de su creación. Para el caso de los documentos relacionados con los productos, esta personalización deberá decir: "Se firma la presente para efecto de lo dispuesto en la Circular S-8.1 de la Comisión Nacional de Seguros y Fianzas".

Adicionalmente, dentro del cuadro de información, existe la opción "Location, e.g. city name:" en la cual se puede teclear la ubicación del firmante; asimismo el cuadro de diálogo contiene el campo "Your contact information, e.g. phone number". Estos campos son de llenado opcional. Ejemplo:

Self-Sign Security - Sign Document

Signing requires saving the document. Click 'Save As..' to place this signature onto a new document or 'Save' to save the current document.

Confirm Password: Hide Options

Reason for signing document: (select or edit)
Se firma la presente para efecto de lo dispuesto en la circular S-8.

Location, e.g. city name: (optional)
Mexico, D. F.

Your contact information, e.g. phone number: (optional)
57 - 24 - 74 - 82

Signature Appearance:
Standard Text Preview... New...

Save Save As... Cancel

El botón “Preview...” muestra una vista previa de la firma.

Por último, el firmante deberá confirmar su contraseña en el campo correspondiente.

Self-Sign Security - Sign Document

Signing requires saving the document. Click 'Save As..' to place this signature onto a new document or 'Save' to save the current document.

Confirm Password: ***** Hide Options

Reason for signing document: (select or edit)
Se firma la presente para efecto de lo dispuesto en la circular S-8.

Location, e.g. city name: (optional)
Mexico, D. F.

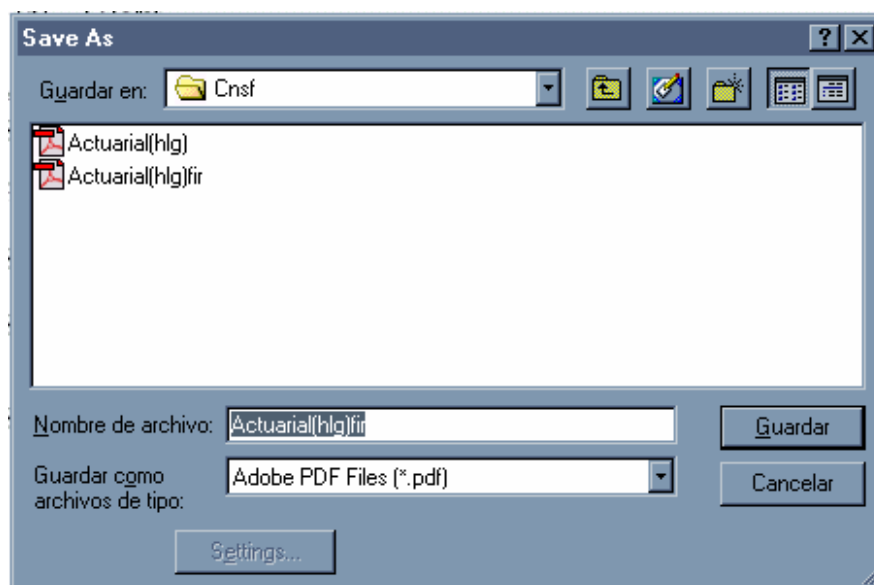
Your contact information, e.g. phone number: (optional)
57 - 24 - 74 - 82

Signature Appearance:
Standard Text Preview... New...

Save Save As... Cancel

Si se hace clic en el botón “Save”, el documento se guarda en una versión ya firmada con el mismo nombre y en la misma ruta que el archivo original.

En caso de que se haga clic en el botón “Save As...”, aparecerá el cuadro de diálogo “Save As”.



Deberá teclearse el nombre del archivo conforme a la estructura definida a continuación:

Documento	Prefijo	Tipo de seguro	Número de Compañía	Nombre designado por la compañía (libre) y extensión
Nota Técnica	NT-	X	xxxx-	*.pdf
Documentación Contractual	DC-	X	xxxx-	*.pdf
Dictamen Jurídico	DJ-	X	xxxx-	*.pdf
Análisis de Congruencia	AC-	X	xxxx-	*.pdf
Folleto Explicativo	FE-	H	xxxx-	*.pdf
Contratos Tipo	CT-	H	xxxx-	*.pdf

Para efecto de los registros señalados en el segundo y tercer párrafo de la Disposición Décima Tercera, así como los establecidos en el tercer párrafo de la

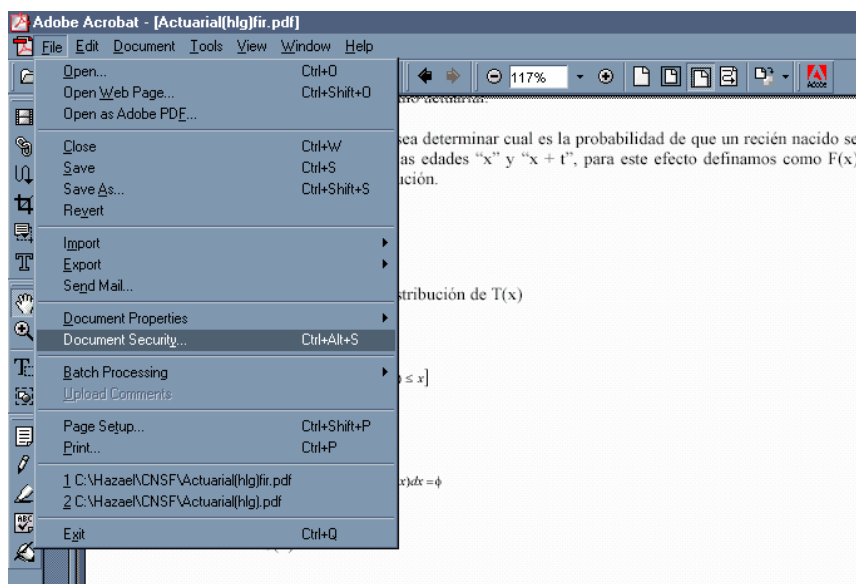
Disposición Décima Séptima de la presente Circular, deberá respetarse la estructura definida en la tabla anterior para nombrar los documentos correspondientes.

Donde el identificador de la operación será S para seguros, P para los seguros de pensiones derivados de las leyes de seguridad social y H para las instituciones de seguros especializadas en salud (ISES). El número de la compañía será el mismo que se utiliza actualmente para efectos de recepción e identificación del Sistema Integral de Información Financiera (SIIF). El nombre designado por la compañía no deberá tener espacios, o bien en caso de necesitar separar palabras se debe utilizar “guiones bajos” (_).

Para efecto del registro de productos, todos los documentos en PDF que conforman un producto, deberán tener una contraseña que permita su apertura, ésta será la única medida de seguridad estándar, de toda la gama de opciones que ofrece el Adobe Acrobat.

Esta contraseña será creada libremente por cada institución o sociedad mutualista de acuerdo al tipo de operación de que se trate, y deberá ser entregada a esta Comisión de manera previa a la solicitud de registro de sus productos bajo el esquema vía página Web, en concordancia con lo establecido en la Disposición Tercera y el Anexo 1 de la presente Circular.

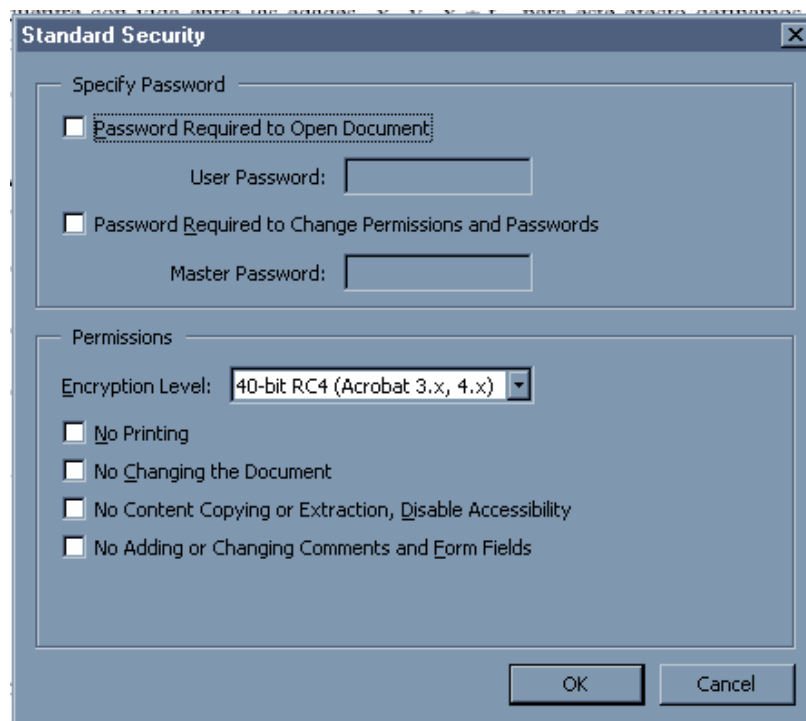
Para dar a los documentos esta opción de seguridad, **previo a la firma de un documento** se debe seleccionar dentro del menú principal “File”, “Document Security...”.



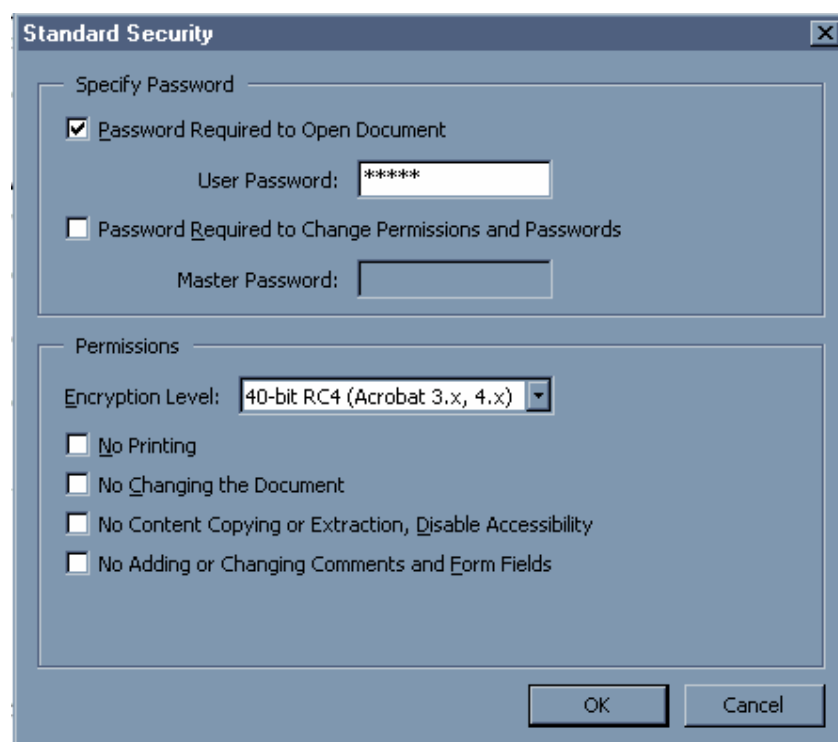
En ese instante aparecerá la ventana “Document Security”



Dentro de la lista, se debe seleccionar la opción “Acrobat Standard Security”



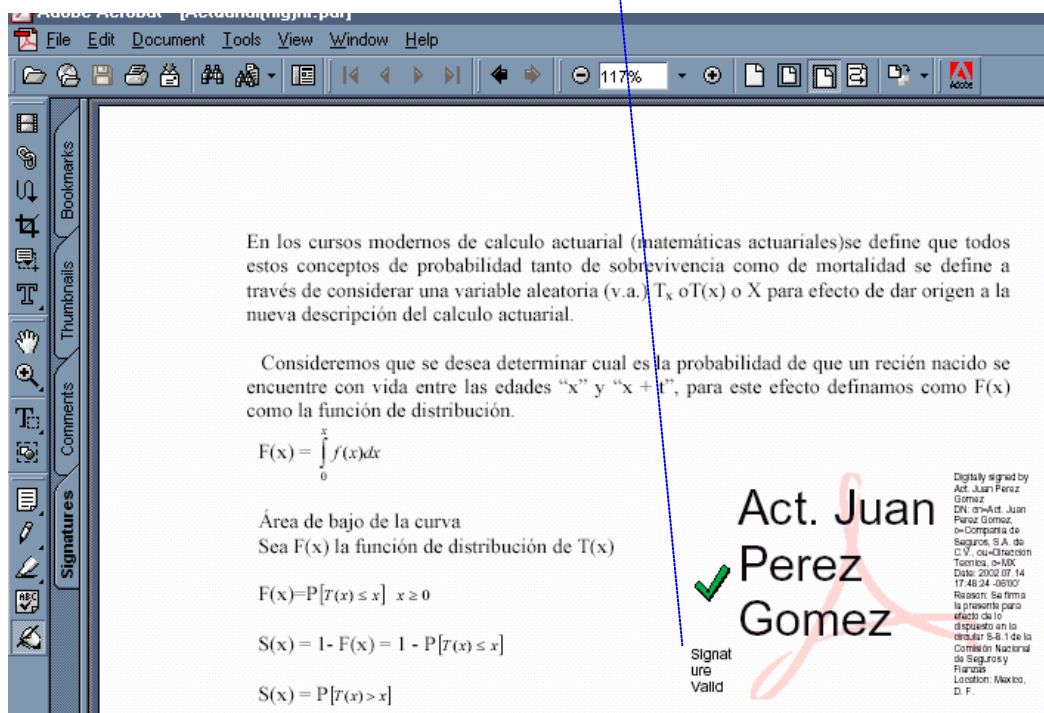
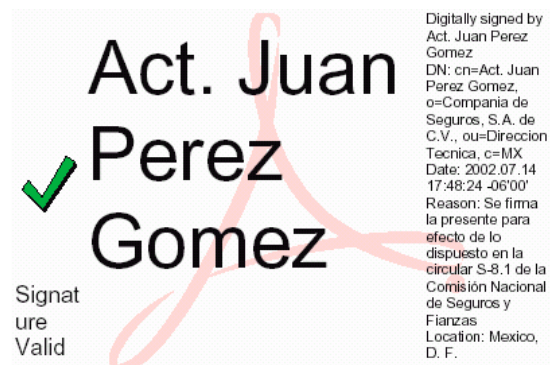
Dentro de la sección “Specify Password”, se deberá seleccionar únicamente la opción “Password Required to Open Document” y se deberá teclear el password de apertura.



Las instituciones y sociedades mutualistas de seguros no deberán aplicar las demás opciones de seguridad que ofrece el Adobe Acrobat a sus documentos electrónicos, permitiendo así su lectura, impresión y firma por parte de los funcionarios de esta Comisión.

Haga clic en “Ok”, confirme la contraseña para abrir el documento en la siguiente ventana y posteriormente haga clic en el ícono de “Guardar”

Cada uno de los documentos del producto requiere de una contraseña para abrir el documento, la cual es solicitada por el Acrobat para concluir cada aplicación de una nueva firma, posterior a la primera. Así que una vez confirmada la contraseña de signatario el documento quedará firmado.



La firma electrónica no sólo se hace presente de forma visual, sino que se encuentra de manera intrínseca en las características electrónicas del archivo.

Puede cambiar o eliminar una firma, pero, como ocurre con cualquier otro cambio introducido en un documento PDF firmado, esto añade otra versión al mismo sin alterar las versiones precedentes. Los lectores del documento pueden retroceder a una versión anterior para ver la firma original. Sin embargo, cualquier documento que en su última versión carezca de firma no tendrá ninguna validez para efecto de lo dispuesto en la presente Circular.

Validación de firmas electrónicas

Se puede validar una firma electrónica para verificar que la versión del documento no se ha alterado y para confirmar la identidad del firmante.

El controlador Acrobat Self-Sign asocia a cada perfil, datos de seguridad exclusivos que pueden utilizarse para validar las firmas aplicadas con ese perfil. El perfil almacena un valor numérico llamado llave privada que le representa como firmante; para poder firmar un documento debe poder usar esta llave. El perfil también almacena una llave pública que se incrusta en todas las firmas que se añadan a un documento; cuando el documento se valida, Self-Sign usa la llave pública para verificar matemáticamente sus firmas, es decir, la llave privada codifica una suma de comprobación que se almacena con la firma, y la llave pública decodifica la suma cuando alguien valida.

La llave pública se incluye en un certificado que puede distribuirse a otros usuarios para que éstos la almacenen en la sección de "Trusted Certificates" de su propio perfil. Esto les proporciona un método más seguro para comprobar la autenticidad de las firmas que se introduzcan en los documentos que reciban. La llave pública es entregada por el usuario a las entidades que requieran validar que la firma es auténtica, es decir, que corresponde al usuario previamente registrado.

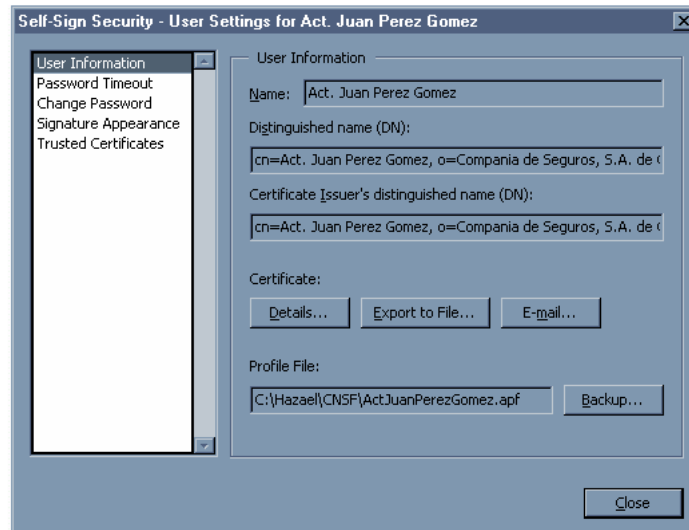
Ambas llaves son complementarias una de la otra; una firma electrónica es válida si la llave privada y la llave pública son compatibles.

Por lo anterior, todas las personas que firmarán algún documento que forme parte de un producto, deben entregar a esta Comisión las llaves públicas de sus correspondientes firmas electrónicas, en concordancia con la Disposición Quinta de la presente Circular. De la misma manera, a través de su página Web, la Comisión pondrá a disposición de las instituciones y sociedades mutualistas de seguros, las llaves públicas de los servidores públicos autorizados para firmar los acuses de cada uno de los documentos que integran el producto que se somete a registro.

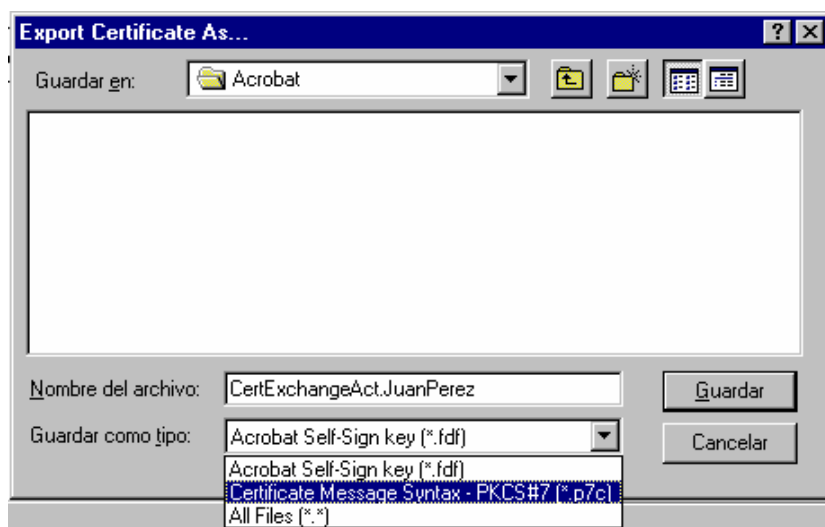
Generación y entrega de llaves públicas

Con objeto de que la llave pública incluida en un certificado pueda ser distribuida a otros usuarios para que estos la almacenen en la sección "Trusted Certificates" de su propio perfil, primeramente deberá exportarse dicho certificado, atendiendo a lo siguiente:

1. Elija "Tools", "Self-Sign Security", "User Settings". Si aún no ha abierto ninguna sesión, elija "Tools", "Self-Sign Security", "Log In" para conectarse a su perfil, y luego haga clic en el botón "User Settings" de la ventana que aparece. Posteriormente aparecerá la ventana:



2. Haga clic en el botón "Export to File...".
3. Especifique la ubicación en la que desee exportar el certificado que contiene la llave pública y seleccione en el apartado "Guardar como tipo" la opción "**Certificate Message Syntax-PKCs#7(*.p7c)**" y haga clic en "Guardar". Por "default" el nombre del certificado corresponderá al nombre capturado durante el proceso de la creación del perfil, es decir, el nombre del firmante. Este nombre no deberá modificarse cuando se remita a esta Comisión.

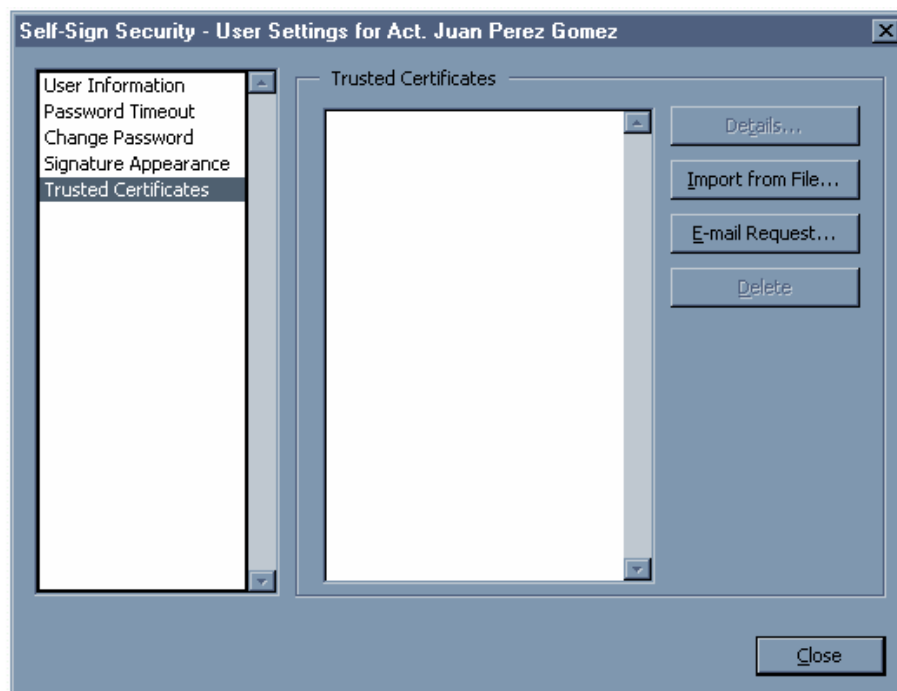


4. Inmediatamente al paso anterior, aparecerá un cuadro de diálogo que contendrá el dato **'MD5 Fingerprint'** la cual corresponde a la exportación y cuyas cifras deberán incluirse en el formato descrito en el **Anexo 2** de la presente Circular como la **"Cadena de validación"**. La cadena de validación deberá coincidir con la contenida en el certificado entregado a esta Comisión, de lo contrario éste será rechazado. Haga clic en "Ok" y posteriormente en "Close".

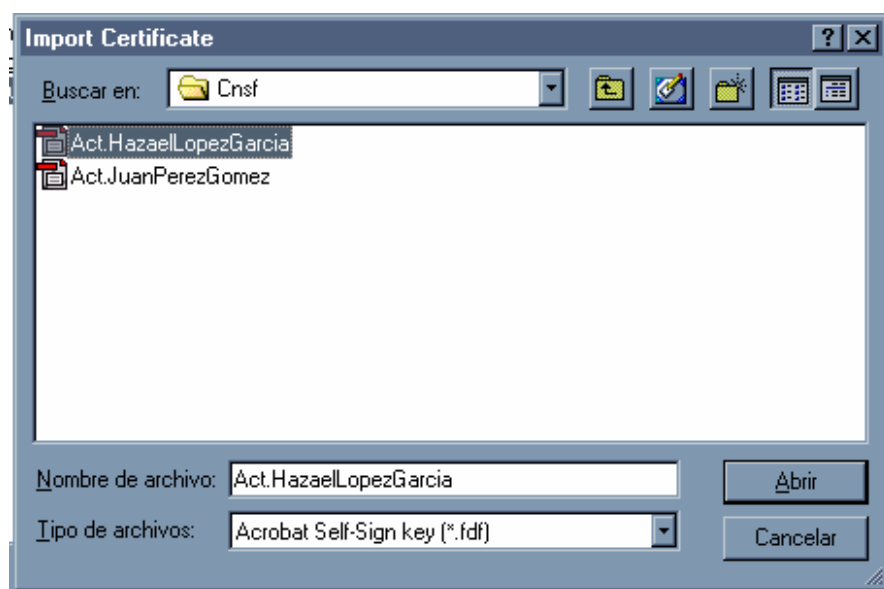


Análogamente, para importar a la sección "Trusted Certificates" de nuestro perfil, un certificado de otro usuario cuya firma se quiere validar, como será en el caso de la de un servidor público de esta Comisión, se procederá de la forma siguiente:

1. Elija "Tools", "Self-Sign Security", "User Settings". Si aún no ha abierto ninguna sesión, elija "Tools", "Self-Sign Security", "Log In" para conectarse a su perfil, y luego haga clic en el botón "User Settings" de la ventana que aparece.
2. Seleccione en la ventana de la izquierda la opción "Trusted Certificates".

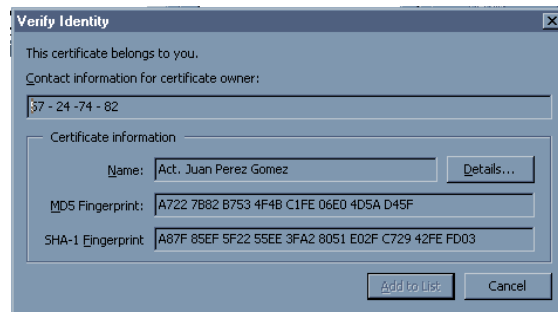


3. Haga clic en "Import from File...", y elija la ubicación de donde se desee importar la llave pública del signatario cuya firma se quiere validar; haga clic en "Abrir".

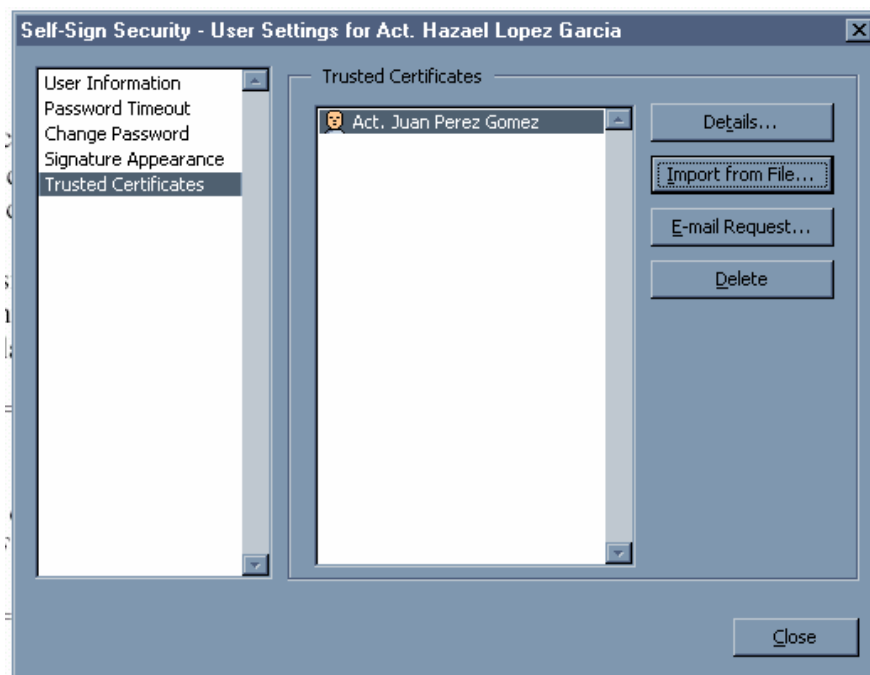


4. En el cuadro de diálogo "verify Identity", copie la cadena de validación (**"MD5 Fingerprint"**) y haga clic en "Aceptar". Deberá corroborarse que este dato

coincida con el contenido en el certificado entregado por el funcionario de esta Comisión.



5. En la “sección de Trusted Certificates” quedará almacenada la llave pública importada”

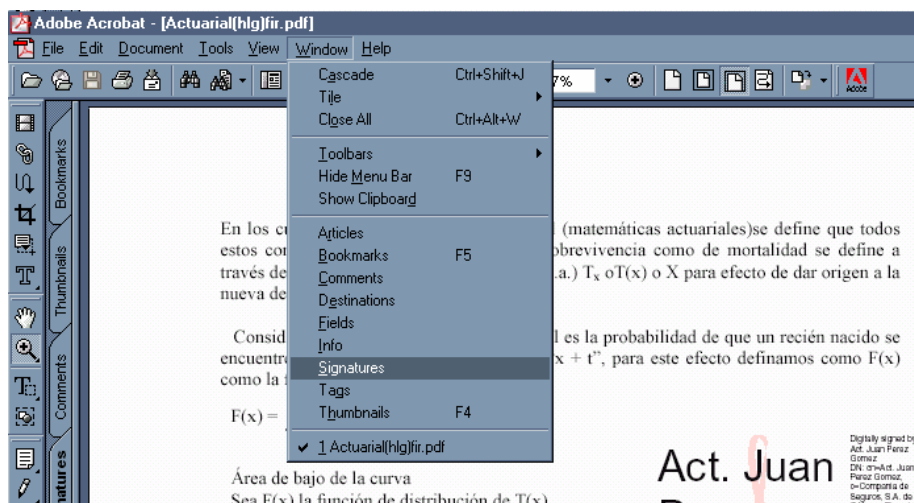


6. Haga clic en “Close”

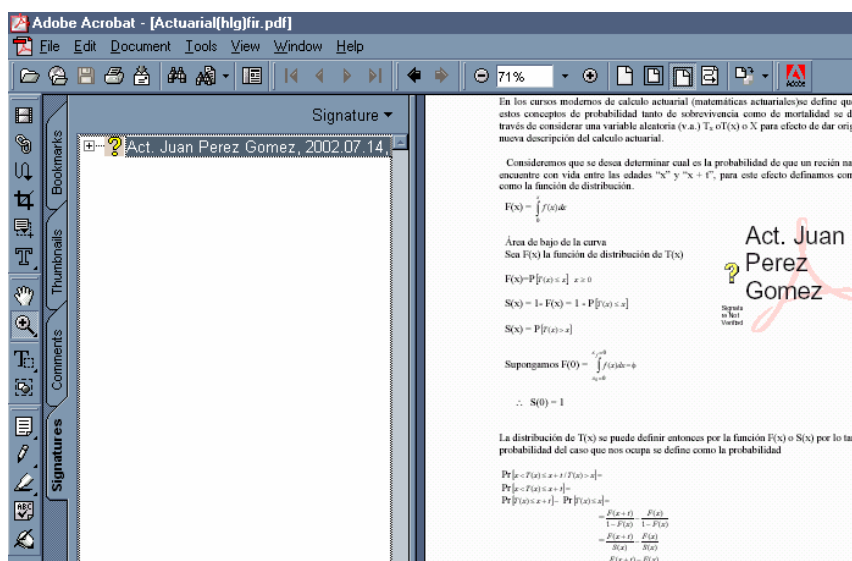
Procedimiento para validar una firma

Acrobat permite hacer la validación de una firma al abrir la paleta de firmas (ventana del lado izquierdo). Elija “Window”, “Signatures”, o bien elija “Show Signatures” en el menú emergente de la llave de seguridad  que aparece en

la barra de estado. Este menú sólo se muestra cuando un documento tiene firmas u otras propiedades de seguridad.



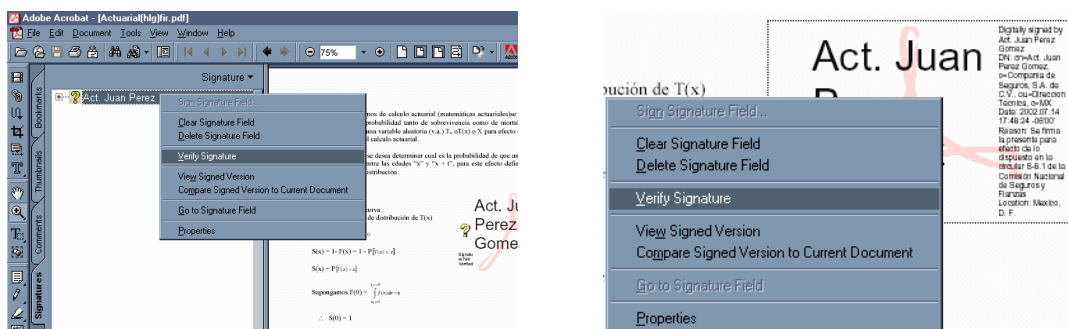
La paleta “Signatures” contiene la lista de todas las firmas contenidas en el documento, en el orden en que se han añadido. Puede contraer una firma para ver sólo su nombre, fecha y hora, o expandirla para ver más información.



Puede desplazar la paleta “Firmas” como una ventana flotante, integrarla en un grupo de paletas, y en general trabajar con ella del mismo modo que con otras paletas de Acrobat.

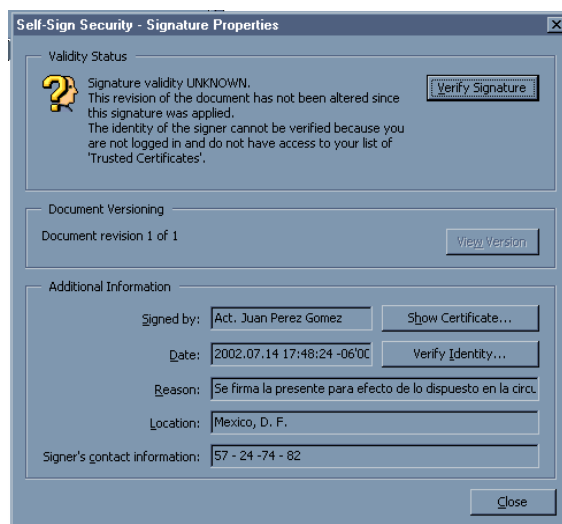
Haga clic en el signo “más” situado a la izquierda de la firma para expandirla, o en el signo “menos” para contraerla.

Cada firma de la paleta tiene un pequeño ícono que indica su estado actual de validación; para conocerlo seleccione la pestaña correspondiente a “Signatures”, coloque el puntero en la firma con el “ratón” (mouse), haga clic con el botón derecho, seleccione “verify signature” y posteriormente “properties”.



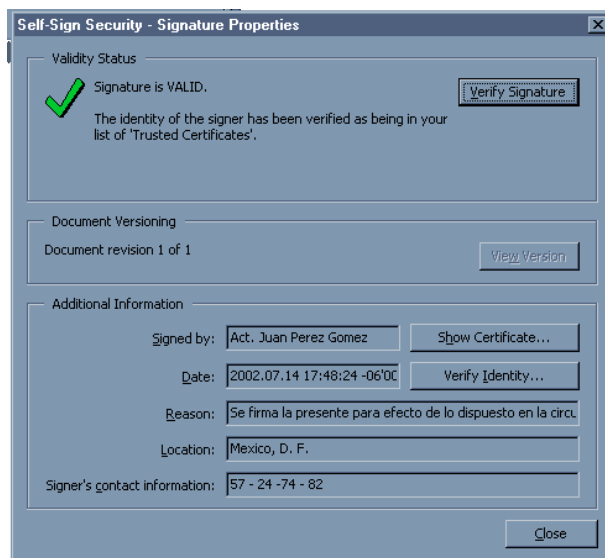
Aparecerán las propiedades de la firma y se indicará el estado de la validación. Cuando se valida una firma mediante Acrobat Self-Sign, Acrobat puede confirmar la autenticidad de la firma de dos maneras:

Si hay una sesión de perfil abierta y el certificado del firmante está en la libreta de direcciones del perfil, Acrobat compara la información de la firma con el certificado para verificar la identidad del firmante. Si Acrobat determina que ni el documento ni la firma han sido alterados, la firma es parcialmente válida y aparece en la paleta “Firmas” con un signo de interrogación y una cara.



Este nivel de validación lo único que indica es que el documento no ha sido alterado y que la firma que contiene es una firma creada mediante Adobe Acrobat, sin embargo, **no garantiza que la firma corresponda a la llave pública de la persona cuyo nombre aparece.**

Si además la firma se ajusta a un certificado de la sección de “Trusted Certificates”, significa que es totalmente válida (corresponde a la llave pública de la persona cuyo nombre aparece) y se muestra en la paleta una marca de comprobación:



Si se edita o modifica un documento firmado, aparecerá una línea con una señal de atención en la paleta para indicar que el documento se ha alterado. Si más tarde se firma el documento, la señal se preservará para indicar que ha firmado una versión alterada.

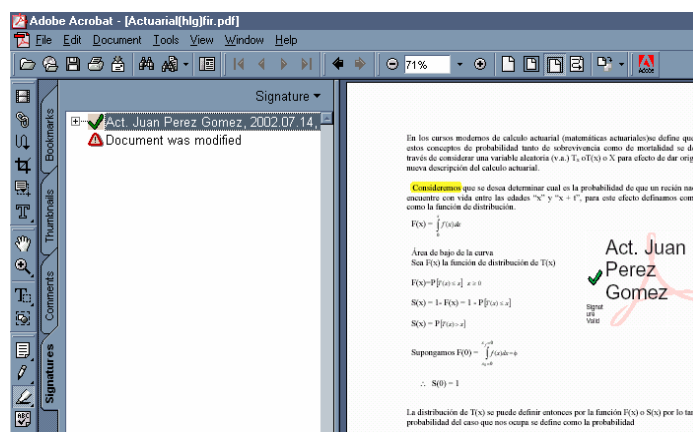
Puede verse el estado de validación de una firma en la página del documento y en la paleta “Firmas”. En la siguiente tabla se describe cómo se muestra la información en los controladores Acrobat.

Estado de validación	Icono en paleta
Sin firmar	ninguno
Firmado pero no validado	Signo de interrogación 
Parcialmente válido	Marca de comprobación 
Totalmente válido	Marca de comprobación 
No válido	

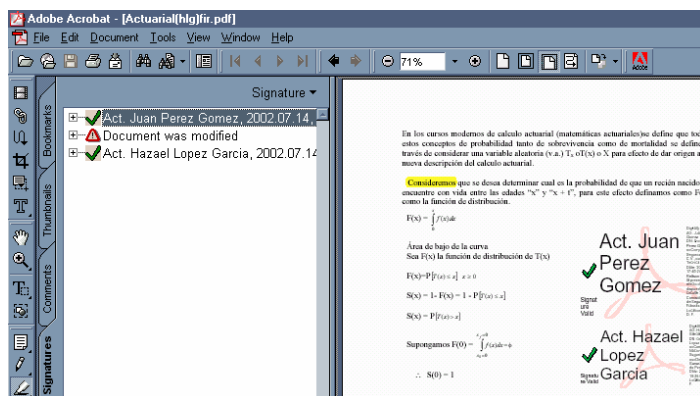
El registro del producto sólo podrá acreditarse siempre y cuando la validación de todas las firmas contenidas en los documentos que lo conforman sea completa. En cualquier otro caso el documento en cuestión no será válido.

Es posible realizar cualquier cambio en un documento firmado, por lo que las versiones de documento almacenadas en un archivo PDF pueden diferir. Sin embargo, siempre es posible conocer si el documento ha sido modificado.

En este caso, los documentos alterados se considerarán inválidos. La siguiente ilustración ejemplifica cómo se refleja una alteración en la paleta de “Firmas”:



Si una firma incorpora cambios introducidos después de realizar la firma precedente, el ícono de paleta  indica que su versión incluye alteraciones.

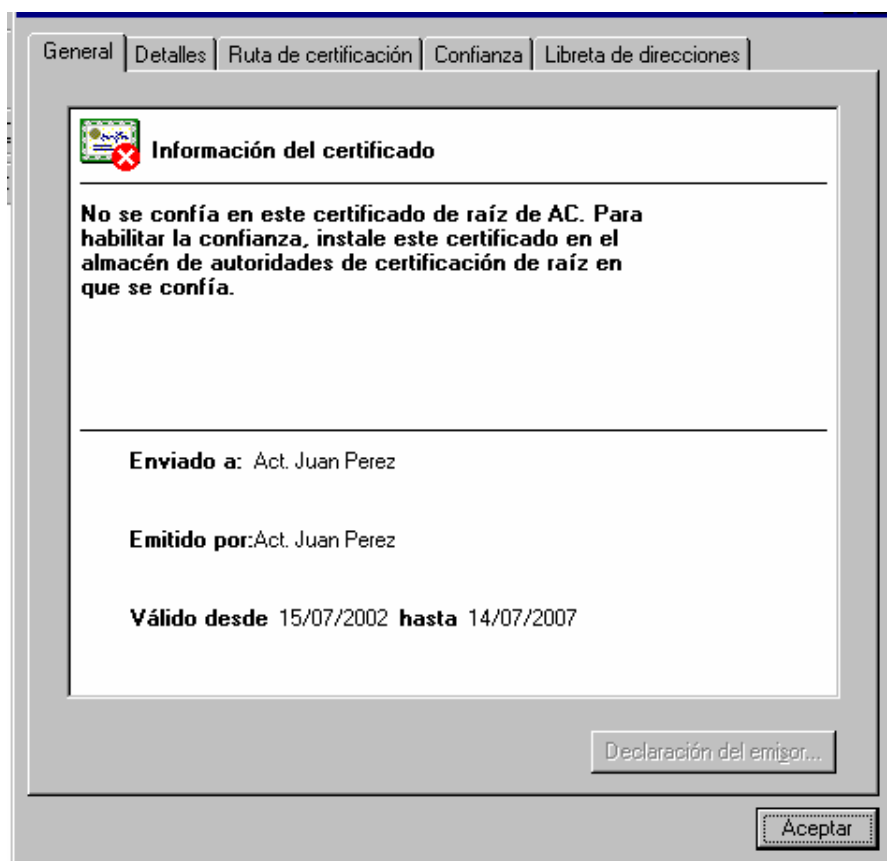


La forma más segura de ver exactamente lo que se ha firmado es retroceder a la versión de esa firma. Acrobat abre la versión anterior en un archivo PDF temporal. Los cambios que se introduzcan en ese archivo se anexan a él, de modo que ni siquiera retrocediendo se puede alterar una versión una vez firmada.

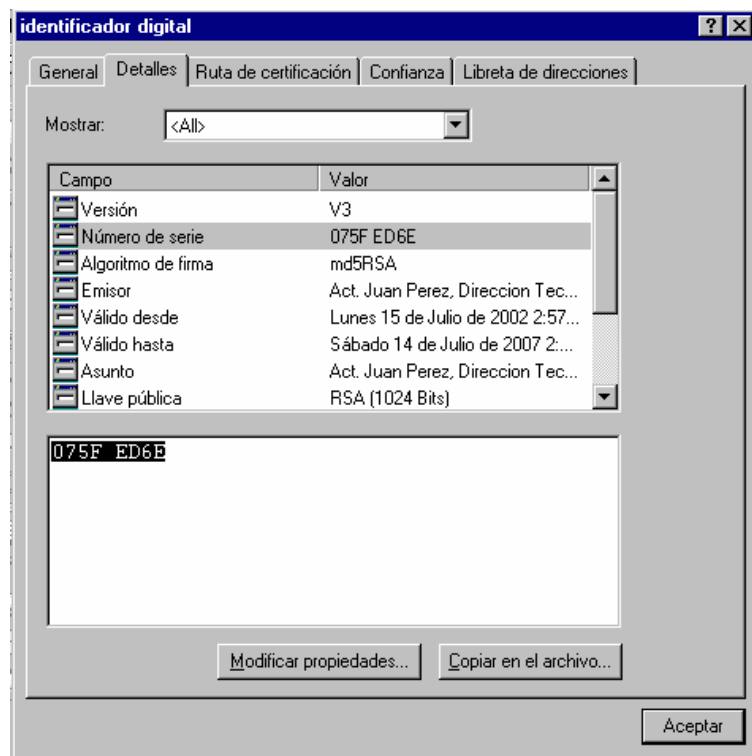
Para todos los efectos, siempre que aparezca una señal de atención en cualquiera de los documentos que integran el producto, éste será considerado inválido. Para que un producto se considere registrado de forma definitiva, todos los documentos

deberán estar firmados conforme a la presente Circular y cada una de las firmas deberá aceptar una validación completa.

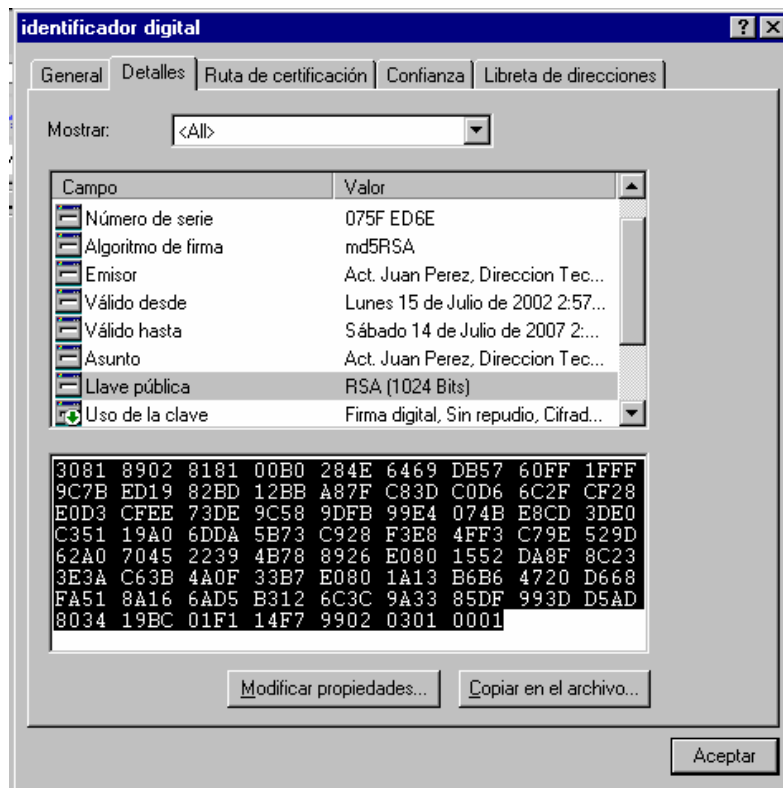
Para conocer los datos de identificación requeridos en el Anexo 2 de la presente Circular en lo relativo a las propiedades de la llave pública, salvo el de la cadena de validación, deberá abrir el archivo correspondiente al certificado exportado desde el explorador de Windows, y aparecerá la siguiente pantalla:



Seleccione la pestaña "Detalles" para consultar cada uno de los datos de identificación solicitados en el Anexo 2, a fin de copiarlos para su remisión a esta Comisión en conformidad a lo dispuesto en la presente Circular.



Número de serie



Llave pública