Certificados y firmas

Herramienta de Administración

Este documento es propiedad de SIATEL.
No puede ser reproducido ni comunicado sin autorización escrita de SIATEL.

Tabla de contenidos

Requisitos para la firma

Licencia específica

Las funciones de firma que aquí se describen no están incluidas en todas las instalaciones de Gargantua. Si quiere disponer de ellas, su organización debe adquirir una licencia específica: a partir de ese momento, tendrá acceso a la rama **Certificados** de la Herramienta de Administración, así como a todas las funciones asociadas.

Requisitos para el uso de dispositivos USB eToken

Instalar SafeNet Authentication Client

Las funciones de firma con dispositivo USB securizado ofrecidas por Gargantua 7 han sido desarrolladas a partir de las avanzadas soluciones de autenticación de SafeNet (www.safenet-inc.com).

Para firmar documentos usando un dispositivo USB en Gargantua, necesita:

- En cuanto a software, instalar la aplicación SafeNet Authentication Client en cada uno de los equipos de usuario;
- En cuanto a material, los dispositivos USB eToken correspondientes.

Para instalar la aplicación SafeNet Authentication Client, proceda como se indica a continuación:

1. Ejecute el archivo SafeNetAuthenticationClient_x32_x64_8.00-SP1.exe contenido en el kit de instalación proporcionado por SIATEL (**SafeNetAuthenticationClient8_0_SP1** > **32X64 Installer**).

   Se abre el asistente de instalación.

2. Haga clic en **Next**.
3. En la lista desplegable, escoja la lengua apropiada y haga clic en **Next**.
4. Seleccione el botón de radio **I accept the license agreement** y haga clic en **Next**.
5. Seleccione el tipo de instalación **Standard** y haga clic en **Next**.
6. Seleccione la carpeta de su disco duro donde se instalará la aplicación: puede utilizar el valor por defecto o escoger otra ubicación a través del botón **Explorar**.
7. Haga clic en **Next** para iniciar la instalación y espere a que se muestre el mensaje que indica que la instalación se ha completado correctamente.
8. Haga clic en **Finish**.

   Ya dispone de SafeNet Authentication Client en su equipo: ahora puede utilizar Gargantua para firmar documentos a través de un dispositivo USB eToken.

Usar SafeNet Authentication Client

SafeNet Authentication Client dispone de su propio manual de usuario, incluido en el kit de instalación de la aplicación (**SafeNetAuthenticationClient8_0_SP1** > **Documentation** > **SAC_User_Guide_8.0_SP1_Windows_Rev_A.pdf**).

Al utilizar SafeNet Authentication Client en conjunto con Gargantua, podrá:

- Importar certificados al dispositivo USB eToken, que podrá utilizar para firmar documentos: consulte la sección “Importing a Certificate Onto a Token”, pág. 46 del manual de usuario SafeNet;
- Exportar certificados a partir del dispositivo: consulte “Exporting a Certificate from a Token”, pág. 50 ;
- Eliminar certificados presentes en el dispositivo: consulte “Deleting a Certificate”, pág. 54 ;
- Cambiar la contraseña general del dispositivo: consulte “Changing the Token Password”, pág. 36.

Presentación de las funciones de firma

Tipos de firma

Una firma Gargantua puede ser de tipo electrónica (visible o invisible) y/o manuscrita. Se pueden llevar a cabo las siguientes combinaciones:

- La **firma electrónica** permite firmar un documento usando un certificado electrónico.
- La **firma electrónica visible** permite firmar un documento usando un certificado electrónico visible directamente en el cuerpo del documento en PDF.
- La **firma manuscrita** permite estampar una firma contenida en un archivo de imagen sin usar un certificado electrónico.
- La **firma electrónica y manuscrita** permite combinar una firma contenida en un archivo de imagen con un certificado electrónico.
- La **firma electrónica visible y manuscrita** permite combinar una firma contenida en un archivo de imagen con un certificado electrónico visible directamente en el cuerpo del documento en PDF.

Firma electrónica

La firma electrónica permite aplicar un certificado electrónico a un documento.

Un certificado electrónico es un archivo que contiene:

- Un conjunto de información sobre la identidad del propietario;
- Dos claves de cifrado:
    - La clave privada, que permite al propietario del certificado estamparlo en documentos digitales usando una contraseña.
    - La clave pública, que permite a los destinatarios del documento verificar la autenticidad del certificado, y por tanto verificar la exactitud de la información en base a su procedencia.

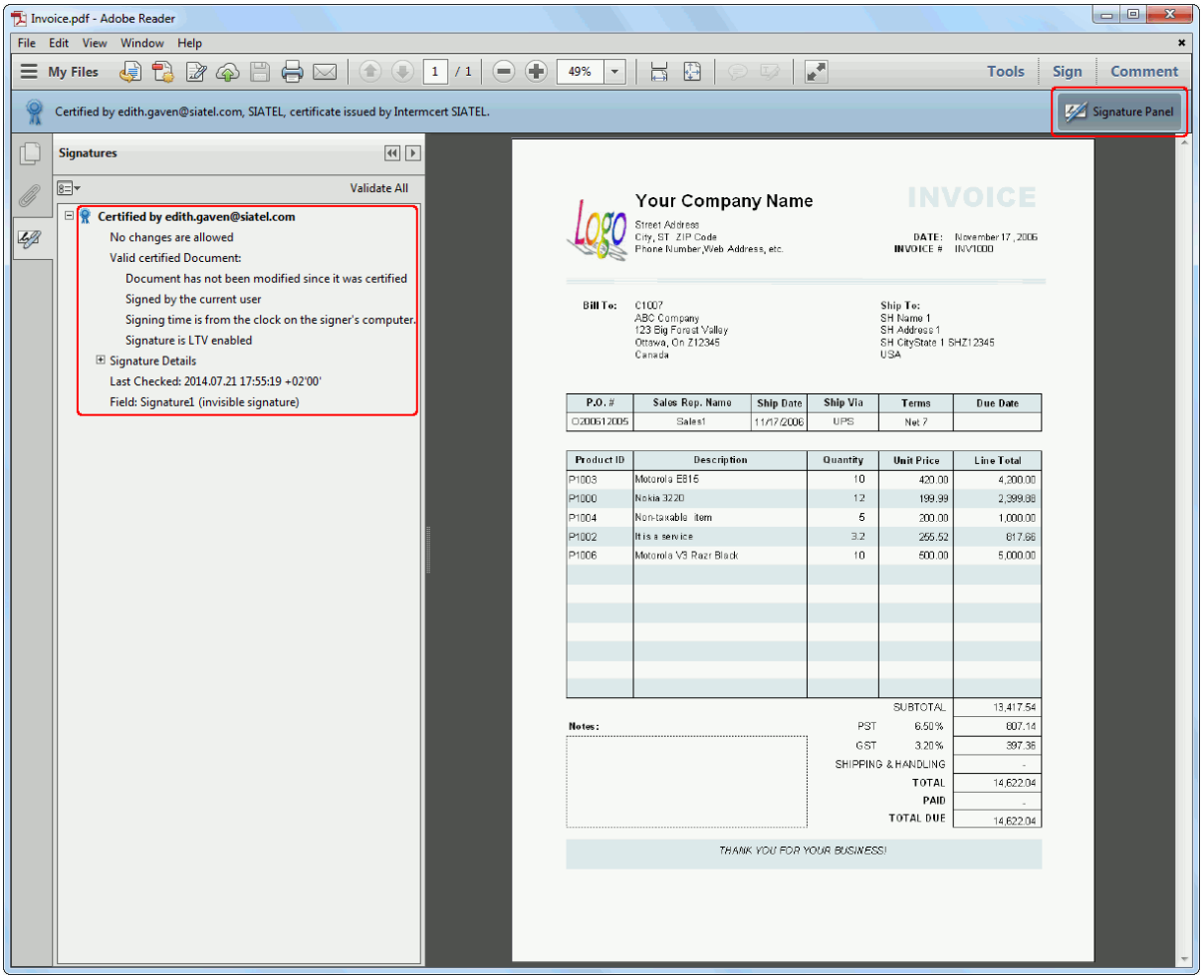
La validación de las firmas electrónicas se basa en la existencia de **autoridades de certificación** capaces de generar certificados y garantizar su autenticidad: entidades como VeriSign están especializadas en cumplir el rol de tercero de confianza, asegurando la autenticidad de los certificados. De todas formas, una organización puede también desarrollar su propia autoridad e certificación para uso interno, generando así certificados llamados “autofirmados”.

Las funciones de firma electrónica ofrecidas por Gargantua permiten utilizar ambos métodos de validación. De este modo, usted puede:

- Firmar los documentos utilizando certificados en formato .p12 o .pfx adquiridos a autoridades de certificación independientes;
- Crear una autoridad de certificación en el servidor Gargantua que le permita generar y utilizar

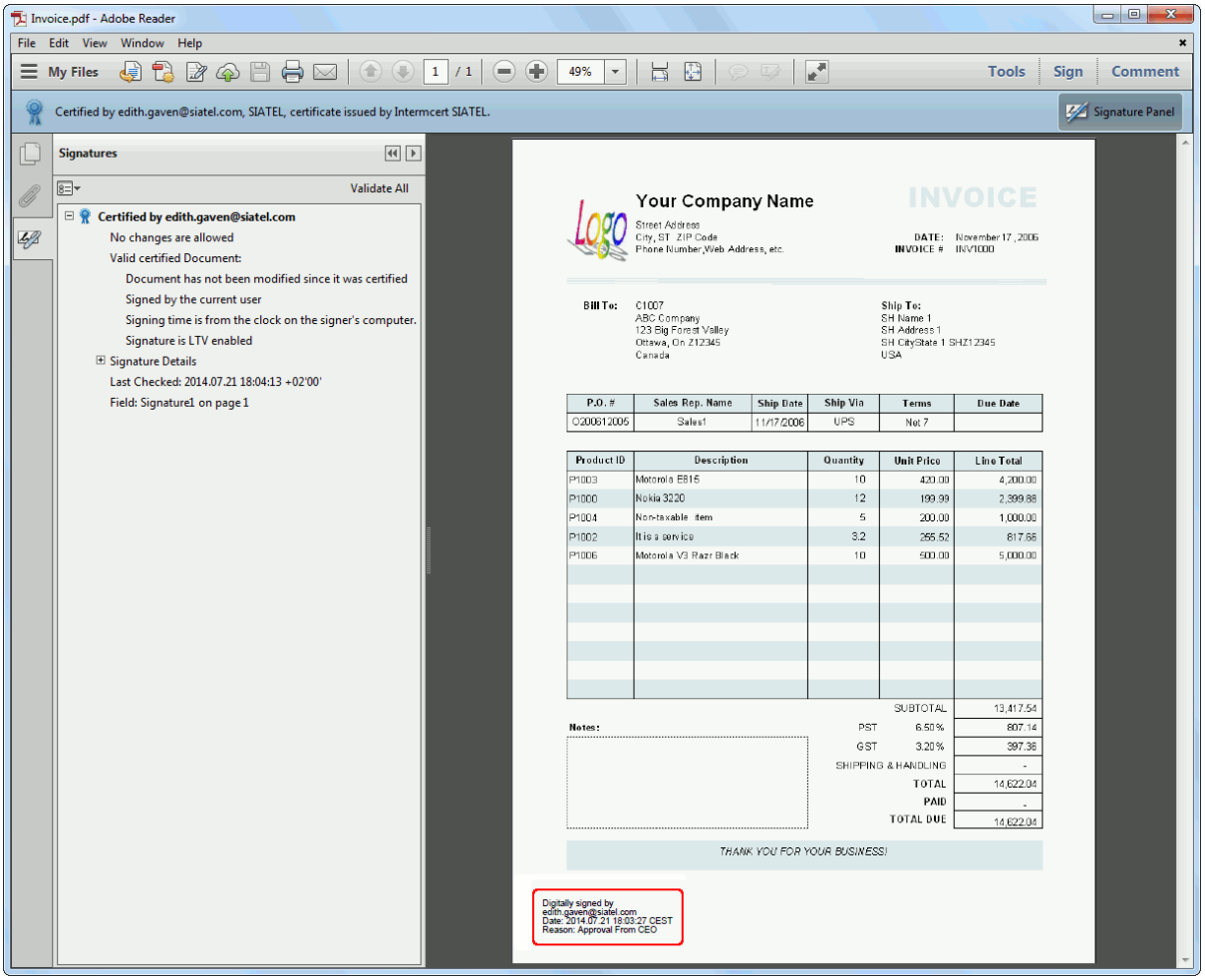
certificados autofirmados.

Los documentos firmados con Gargantua son convertidos al formato PDF. La información acerca del propietario y la autenticidad del certificado utilizado están accesibles en el **Panel de firmas** de Adobe Acrobat Reader:



Firma electrónica visible

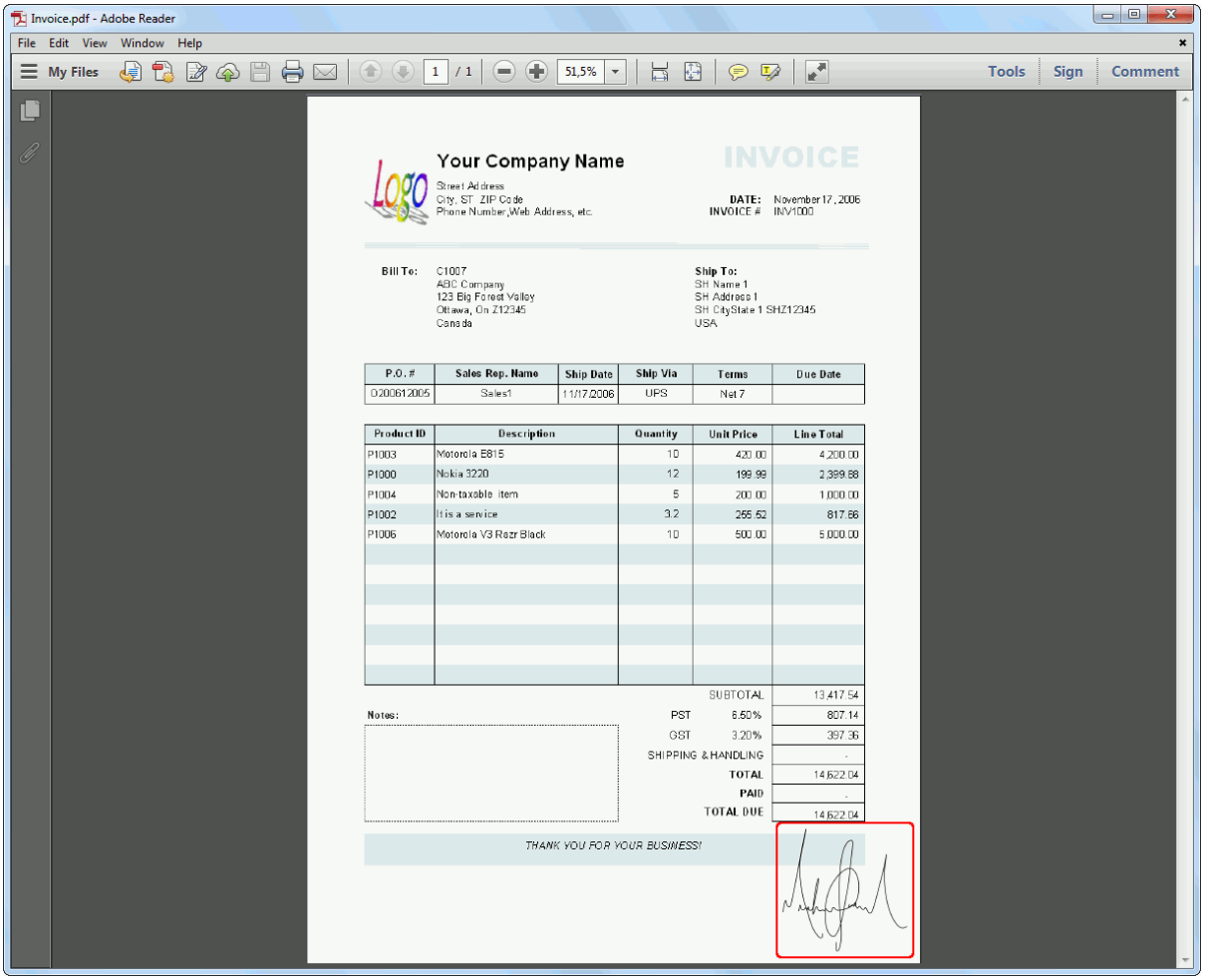
Una firma electrónica está siempre visible en el **Panel de firmas** de Adobe Acrobat Reader. Sin embargo, si quiere que esté visible directamente en el cuerpo del **documento PDF**, puede utilizar la función de firma electrónica visible:



El usuario del Cliente Web Gargantua puede seleccionar la página del documento y la ubicación en la página donde quiere estampar la firma.

Firma manuscrita

La firma manuscrita permite estampar una firma **contenida en un archivo de imagen**. Puede utilizarse sola o en combinación con una firma electrónica:



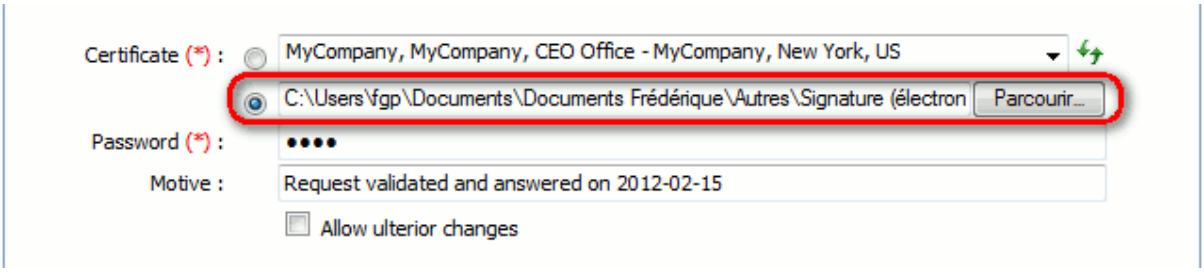
Tipos de certificados electrónicos

Al estampar una firma electrónica (visible o no), los usuarios pueden elegir entre tres tipos de certificados electrónicos.

> ***Para acceder a la firma electrónica, los usuarios deben seleccionar los documentos deseados y hacer clic en la herramienta "Estampar firma electrónica" o en la herramienta "Estampar firma visible" (pero no en la opción "Firma manuscrita").***

Certificado almacenado en local

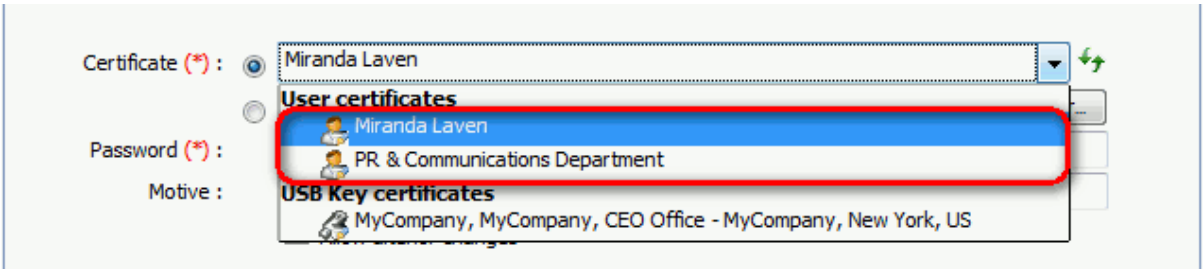
Los usuarios del Cliente Web Gargantua pueden estampar una firma electrónica en uno o más documentos utilizando un archivo de certificado en formato .p12 o .pfx almacenado en su disco duro:



Certificado almacenado en el servidor

Los usuarios del Cliente Web Gargantua pueden estampar una firma electrónica utilizando un certificado subido y almacenado para su uso en el servidor Gargantua.

Los certificados asignados al usuario actual aparecen en la lista desplegable **Certificado**:

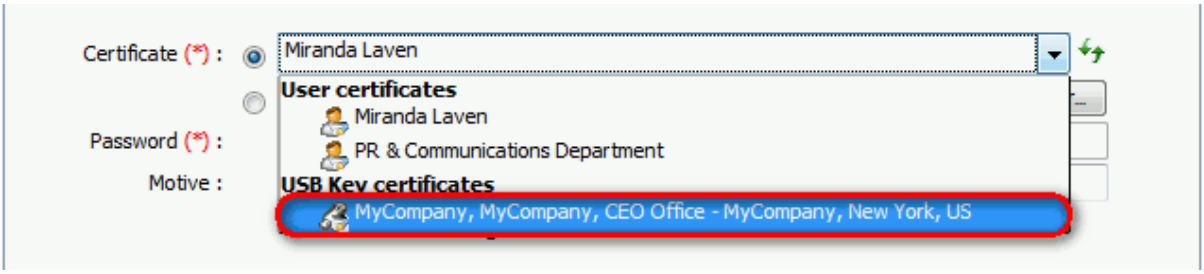


Este método aporta la ventaja de que los certificados estarán disponibles desde cualquier equipo, ofreciendo además protección contra robo.

Certificado en dispositivo USB eToken

Finalmente, los usuarios del Cliente Web Gargantua pueden estampar una firma electrónica utilizando un certificado almacenado en un dispositivo USB securizado de tipo eToken (ver Requisitos para el uso de dispositivos USB eToken).

Los usuarios deben conectar el dispositivo a su equipo e introducir la contraseña. La lista desplegable de certificados disponibles para el usuario se actualiza e incluye los certificados presentes en el dispositivo:



Métodos de firma

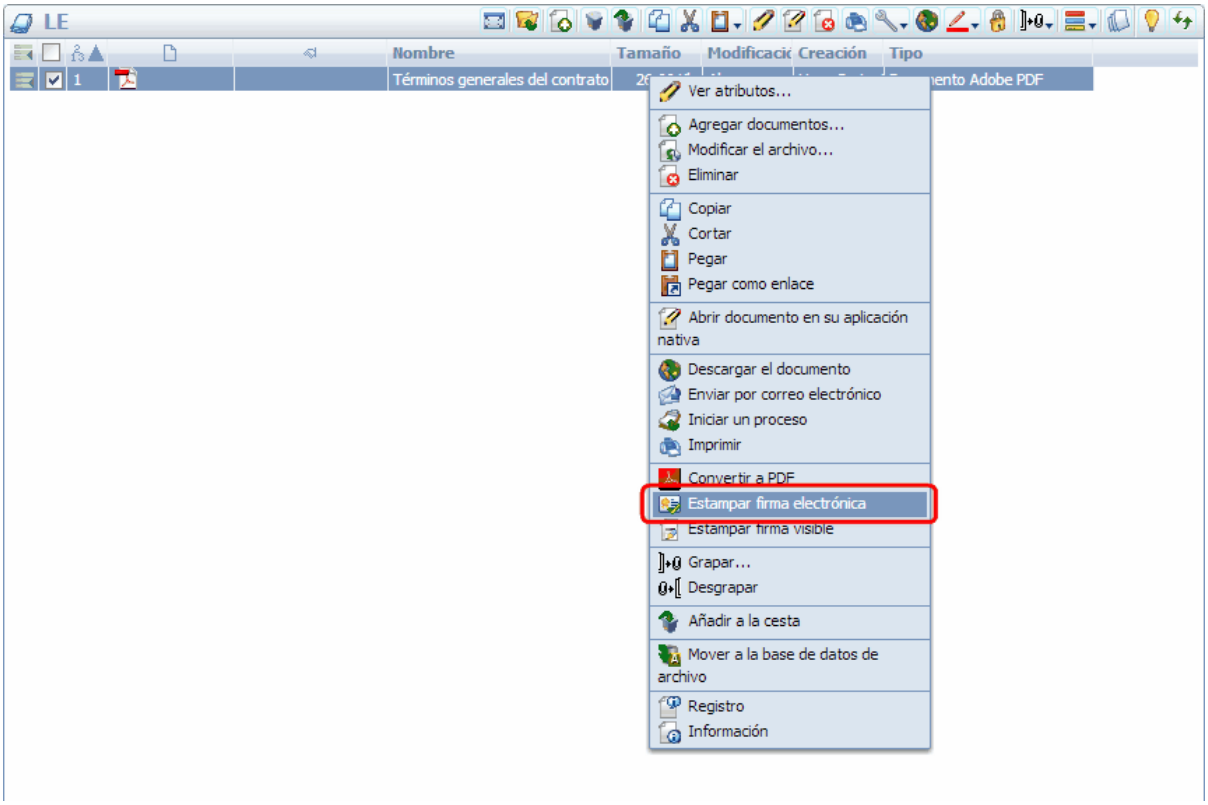
Gargantua permite firmar documentos de forma manual desde el explorador, utilizando las herramientas Estampar firma electrónica o Estampar firma visible, o de forma automática a través de una tarea de workflow de tipo firma.

Manual - Herramienta "Estampar firma electrónica"

La herramienta **Estampar firma electrónica** permite firmar utilizando únicamente un certificado electrónico **no visible** en el cuerpo del documento PDF.

> ***Para utilizar esta herramienta, los usuarios deben poseer el derecho de acceso "Estampar firma electrónica" (perfiles de seguridad) sobre los documentos correspondientes.***

Esta herramienta puede utilizarse en varios documentos al mismo tiempo.



Manual - Herramienta "Estampar firma visible"

La herramienta **Estampar firma visible** agrupa todos los tipos de firmas visibles directamente en el cuerpo del documento PDF:

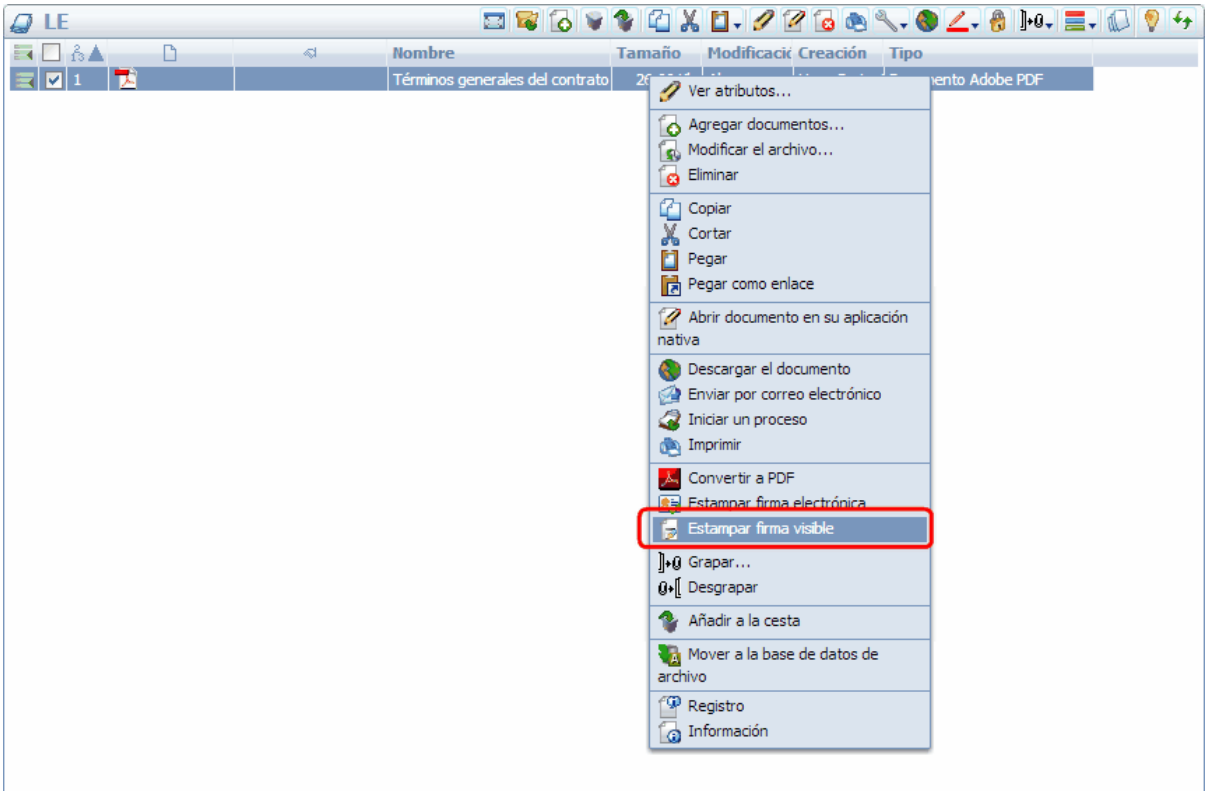
- La **firma electrónica visible** permite firmar un documento usando un certificado electrónico visible directamente en el cuerpo del documento en PDF.
- La **firma manuscrita** permite estampar una firma contenida en un archivo de imagen sin usar un certificado electrónico.
- La **firma electrónica y manuscrita** permite combinar una firma contenida en un archivo de imagen con un certificado electrónico.
- La **firma electrónica visible y manuscrita** permite combinar una firma contenida en un archivo de imagen con un certificado electrónico visible directamente en el cuerpo del documento en PDF.

Para que esta herramienta esté presente en su barra de herramientas, los usuarios deben poseer el privilegio ***"Estampar firma visible"*** *(panel de administración del usuario, grupo o rol).*

Para utilizar esta herramienta, los usuarios deben poseer el derecho de acceso ***"Estampar firma electrónica"*** *(perfiles de seguridad) sobre los documentos correspondientes.*

*Para utilizar esta herramienta, previamente se debe haber subido una imagen de firma al servidor (***"Configuración"*** >* ***"Configuración de firma y certificados"*** *>* ***"Firma manuscrita"****).*

Esta herramienta sólo se puede utilizar en un documento a cada vez.



Automático - Tarea de proceso "Firma electrónica"

Los documentos pueden ser firmados automáticamente como parte de un proceso de workflow, a través de tareas de firma electrónica establecidas por los administradores de Gargantua.

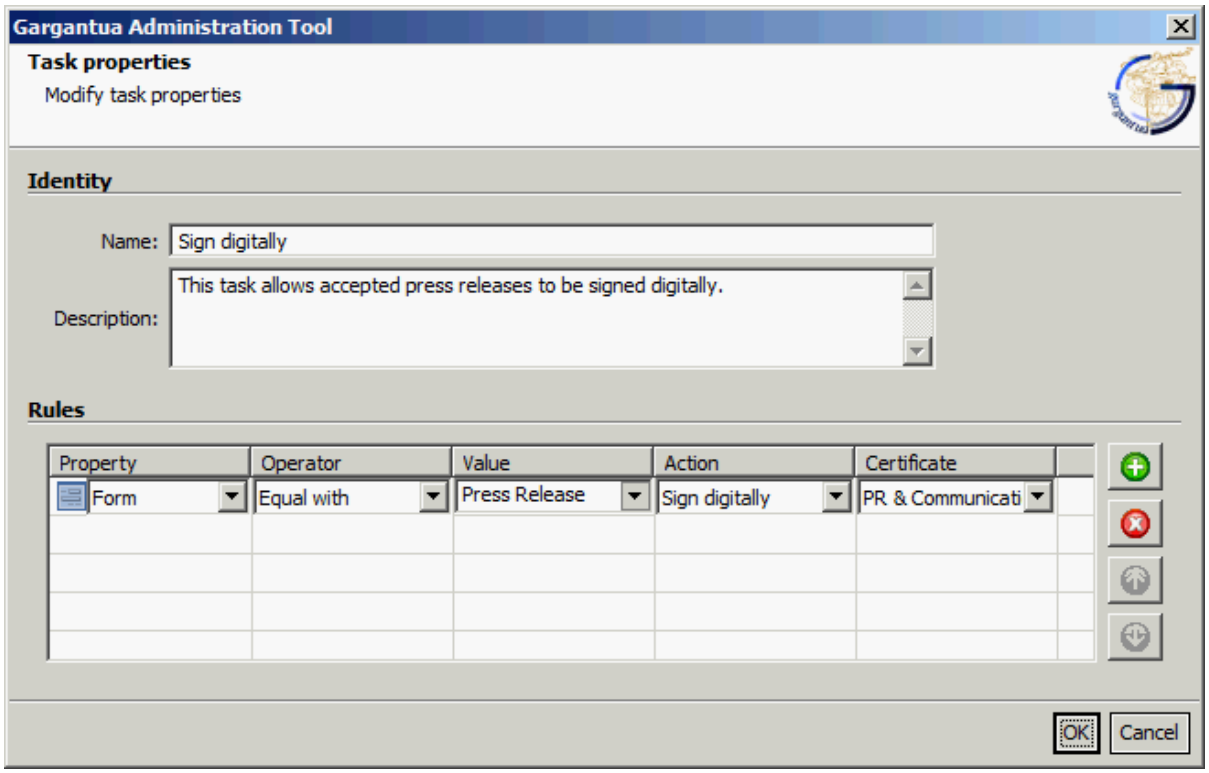
Para crear y configurar una tarea de firma electrónica, proceda como se indica a continuación:

1. En el panel izquierdo de la Herramienta de Administración, despliegue las ramas correspondientes y haga clic en el nombre del proceso en el que quiere insertar una tarea de firma.

   El panel **Administrador de procesos** se abre en el panel derecho.

2. Si la pantalla **Gráfico** no se abre automáticamente, haga clic en la pestaña correspondiente.
3. En la barra de selección de elementos de proceso, haga clic en el icono  y arrástrelo al área de creación del proceso para agregar una **Tarea de firma electrónica**.
4. Una vez agregados los conectores necesarios, haga doble clic en la nueva tarea  .

   Se abre el cuadro de diálogo **Propiedades del elemento**:



5. Introduzca un nombre y, si es necesario, una descripción de la tarea.
6. Haciendo clic en el botón  , agregue al menos una regla que defina las condiciones y modos de firma de los documentos adjuntos al proceso:
   - **Criterio**: Seleccione un criterio que permita clasificar los documentos para saber si deben o no ser firmados y, en caso de que lo sean, qué certificado utilizar. El criterio puede hacer referencia al formulario del documento, al tipo de archivo (.doc, .tif, .txt...), o incluso al contenido del campo **nombre** del formulario.
   - **Operador**: Seleccione el operador de comparación apropiado.
   - **Valor**: Introduzca o seleccione el valor a comparar con las propiedades de cada documento para saber si se cumple la condición de firma.
   - **Tipo de firma**: Seleccione **Estampar firma electrónica**. La opción **Cifrar** permite transformar los documentos en PDF cifrados, accesibles en modo sólo lectura y protegidos contra toda modificación y contra los comandos copiar-pegar.
   - **Certificado**: Seleccione el certificado que se utilizará para firmar los documentos correspondientes a la regla. Sólo estarán disponibles los certificados asignados al servidor (ver

Asignar un certificado a uno o más usuarios).

> ***Un documento sólo puede ser firmado electrónicamente una sola vez, por lo tanto las reglas son mutuamente exclusivas. Si un documento cumple varias condiciones, sólo se aplicará la primera regla.***

7. Si es necesario, puede eliminar o mover las reglas utilizando los botones , y .
8. Una vez haya terminado, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Los documentos que cumplan las reglas especificadas se firmarán automáticamente como parte del proceso.

Administración de certificados en la Herramienta de Administración Gargantua

Importar un certificado almacenado en local

La rama **Certificados** de la Herramienta de Administración le permite almacenar y administrar de forma centralizada (en el servidor) los diferentes certificados utilizados por los usuarios de Gargantua para validar y autentificar los documentos.

Para subir al servidor un certificado almacenado en su disco duro, proceda como se indica a continuación:

1. En el panel izquierdo de Herramienta de Administración, haga clic en la rama **Certificados**.

   El panel **Administrador de certificados** se abre en el panel derecho.

2. En la parte inferior derecha del panel derecho, haga clic en el botón **Importar**.

   Se abre el explorador de archivos.

3. Vaya a la ubicación en que se encuentra almacenado el archivo de certificado a importar, selecciónelo y haga clic en **Abrir**.

   Los certificados importados deben estar obligatoriamente en formato .p12 o .pfx.

   Se abre un cuadro de diálogo.

4. Introduzca la contraseña del certificado y haga clic en **Aceptar**.

   Se abre un cuadro de diálogo.

5. Complete el campo **Nombre** con un valor que le permita identificar fácilmente el certificado en la **Lista de certificados** de ahora en adelante.
6. Decida si quiere asignar el certificado a uno o varios usuarios o personas físicas (campo **Asignar a**), o si quiere asignarlo al servidor para que pueda ser utilizado en las tareas de firma electrónica y procesos de workflow (opción **Certificado de tipo servidor**).
7. Una vez haya terminado, haga clic en **Aceptar**.

   El certificado se ha importado correctamente y se ha agregado a la **Lista de certificados** almacenados en el servidor.

> ***Los usuarios que posean privilegios que les concedan acceso al enlace "Configuración" también pueden subir certificados al servidor a través del Cliente Web ("Configuración" > "Configuración de firma y certificados" > "Configuración de certificados de usuario"). Los certificados importados utilizando este método aparecerán en la "Lista de certificados" de la Herramienta de Administración, donde el administrador los puede gestionar, reasignar y eliminar.***

Crear una Autoridad de Certificación interna en Gargantua

Si no quiere adquirir un certificado generado por un tercero de confianza para cada uno de los usuarios (por ejemplo, debido a su coste) Gargantua le permite crear en el servidor su propia autoridad de certificación y utilizarla para generar certificados autofirmados para uso interno.

Para crear una autoridad de certificación en la Herramienta de Administración, proceda como se indica a continuación:

1. En el panel izquierdo de Herramienta de Administración, haga clic en la rama **Certificados**.

   El panel **Administrador de certificados** se abre en el panel derecho.

2. En la parte inferior del panel derecho, haga clic en el botón **Crear mi certificado raíz ahora**.

   Se abre un cuadro de diálogo.

3. Introduzca la información solicitada y haga clic en **Aceptar**.

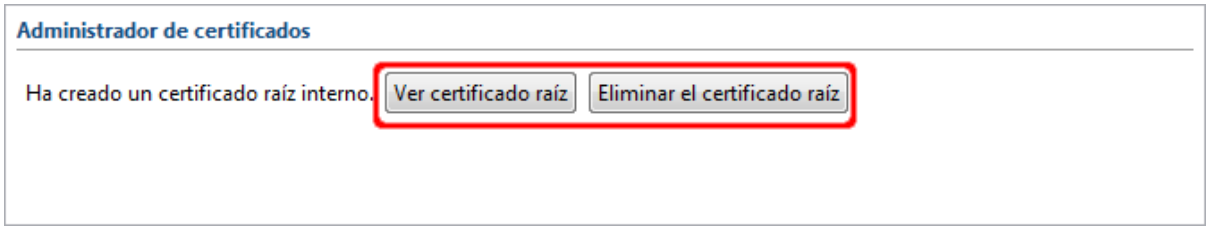
   Se abre un cuadro de diálogo.

4. Introduzca la contraseña que desee atribuir al certificado raíz y haga clic en **Aceptar**.

   La autoridad de certificación se ha creado correctamente.

   El botón **Crear mi certificado raíz ahora** será sustituido de ahora en adelante por otros dos botones:

   - **Ver certificado raíz**: permite ver la información contenida en el certificado raíz;
   - **Eliminar certificado raíz**: permite eliminar la autoridad de certificación y todos los certificados autofirmados que dependen de ésta.



Agregar certificados autofirmados

Una vez haya creado su autoridad de certificación en el servidor Gargantua, podrá agregar certificados autofirmados. Proceda como se indica a continuación:

1. En el panel izquierdo de la Herramienta de Administración, haga clic en la rama **Certificados**.

   El panel **Administrador de certificados** se abre en el panel derecho.

2. En la parte inferior izquierda del panel derecho, haga clic en el botón **Agregar**.

   Se abre el cuadro de diálogo **Nuevo certificado de usuario**.

3. Introduzca la información solicitada; en concreto, debe:
   - Escoger un **Nombre** fácil de recordar, que le permita identificarlo fácilmente en la **Lista de certificados**;
   - Decidir si quiere asignar el certificado a uno o varios usuarios o personas físicas (campo **Asignar a**), o si quiere asignarlo al servidor para que pueda ser utilizado en las tareas de firma electrónica y procesos de workflow (opción **Certificado de tipo servidor**).
4. Haga clic en **Aceptar**.

   Se abre el cuadro de diálogo **Contraseña**.

5. Introduzca la contraseña que quiera asignar al certificado y haga clic en **Aceptar**.

   En función de las características de su sistema, es posible que la longitud máxima de las contraseñas de certificado no pueda exceder 7 caracteres. (Consulte el manual de instalación, "Instalación de Java" > "Extensión Java de criptografía sin limitación de potencia".)

   El nuevo certificado autofirmado aparece en la **Lista de certificados**: ahora puede utilizarlo para firmar documentos de uso interno.

En la "Lista de certificados", los certificados autofirmados están indicados por el icono , mientras que los certificados importados están indicados por el icono .

Asignar un certificado a uno o más usuarios

En lo que respecta a su asignación, existen dos grandes tipos de certificados:

- Los certificados de tipo **Servidor**, utilizados para firmar documentos automáticamente como parte de procesos de workflow;
- Los certificados asignados a un usuario, grupo o rol, utilizados para firmar documentos uno por uno en el Cliente Web.

Para asignar un certificado al servidor, proceda como se indica a continuación:

1. En la **Lista de certificados**, marque la casilla ☐ Servidor correspondiente.

   Se muestra un mensaje de confirmación.

2. Haga clic en **Sí**.

   Se abre un cuadro de diálogo.

3. Introduzca la contraseña del certificado y haga clic en **Aceptar**.

   La asignación se ha realizado correctamente: el certificado estará disponible a partir de ahora para configurar tareas de firma electrónica de workflow.

Para asignar un certificado a un usuario, grupo o rol, proceda como se indica a continuación:

1. En la **Lista de certificados**, haga clic en el icono 🔍 correspondiente.

   Se abre un cuadro de diálogo.

2. En el campo **Nombre**, introduzca las primeras letras del nombre del usuario, grupo o rol al que quiere asignar el certificado.
3. En la lista que se muestra, haga doble clic en el nombre del usuario, grupo o rol apropiado.

   La asignación se ha realizado correctamente: el certificado estará disponible para los usuarios correspondientes en la lista **Certificados de usuario** del Cliente Web.

Asignar un certificado a uno o más usuarios

En lo que respecta a su asignación, existen dos grandes tipos de certificados:

- Los certificados de tipo **Servidor**, utilizados para firmar documentos automáticamente como parte de procesos de workflow;
- Los certificados asignados a un usuario, grupo o rol, utilizados para firmar documentos uno por uno en el Cliente Web.

Para asignar un certificado al servidor, proceda como se indica a continuación:

1. En la **Lista de certificados**, marque la casilla ☐ Servidor correspondiente.

   Se muestra un mensaje de confirmación.

2. Haga clic en **Sí**.

   Se abre un cuadro de diálogo.

3. Introduzca la contraseña del certificado y haga clic en **Aceptar**.

   La asignación se ha realizado correctamente: el certificado estará disponible a partir de ahora para

configurar tareas de firma electrónica de workflow.

Para asignar un certificado a un usuario, grupo o rol, proceda como se indica a continuación:

1. En la **Lista de certificados**, haga clic en el icono  correspondiente.

   Se abre un cuadro de diálogo.

2. En el campo **Nombre**, introduzca las primeras letras del nombre del usuario, grupo o rol al que quiere asignar el certificado.
3. En la lista que se muestra, haga doble clic en el nombre del usuario, grupo o rol apropiado.

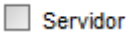
   La asignación se ha realizado correctamente: el certificado estará disponible para los usuarios correspondientes en la lista **Certificados de usuario** del Cliente Web.

Asignar un certificado a uno o más usuarios

En lo que respecta a su asignación, existen dos grandes tipos de certificados:

- Los certificados de tipo **Servidor**, utilizados para firmar documentos automáticamente como parte de procesos de workflow;
- Los certificados asignados a un usuario, grupo o rol, utilizados para firmar documentos uno por uno en el Cliente Web.

Para asignar un certificado al servidor, proceda como se indica a continuación:

1. En la **Lista de certificados**, marque la casilla 

correspondiente.

   Se muestra un mensaje de confirmación.

2. Haga clic en **Sí**.

   Se abre un cuadro de diálogo.

3. Introduzca la contraseña del certificado y haga clic en **Aceptar**.

   La asignación se ha realizado correctamente: el certificado estará disponible a partir de ahora para configurar tareas de firma electrónica de workflow.

Para asignar un certificado a un usuario, grupo o rol, proceda como se indica a continuación:

1. En la **Lista de certificados**, haga clic en el icono  correspondiente.

   Se abre un cuadro de diálogo.

2. En el campo **Nombre**, introduzca las primeras letras del nombre del usuario, grupo o rol al que quiere asignar el certificado.
3. En la lista que se muestra, haga doble clic en el nombre del usuario, grupo o rol apropiado.

La asignación se ha realizado correctamente: el certificado estará disponible para los usuarios correspondientes en la lista **Certificados de usuario** del Cliente Web.

Ver la información acerca de un certificado

Para ver la información de firma contenida en un certificado, proceda como se indica a continuación:

1. Seleccione el certificado en la **Lista de certificados**
2. Haga clic en el botón **Ver detalles** en la parte inferior izquierda del panel derecho.

   La información contenida en el certificado aparece sombreada: puede consultarla pero no modificarla.

   A mayores, cierta información protegida es sustituida por la mención **Desconocido**.

3. Para acceder a la información protegida, haga clic en el botón **Identificarse** e introduzca la contraseña del certificado.

   Se muestra la información protegida.

4. Una vez haya terminado, haga clic en **Aceptar**.

Exportar un certificado

La Herramienta de Administración le permite exportar certificados almacenados en el servidor a su disco duro o a un dispositivo USB eToken, ya sean certificados autofirmados o externos.

Para exportar un certificado a su disco duro, proceda como se indica a continuación:

1. En la parte inferior derecha del panel **Administrador de certificados**, haga clic en el botón **Exportar a disco**.

   Se abre el explorador de carpetas.

2. Seleccione la ubicación en la que quiere exportar el certificado y haga clic en **Guardar**.

   Se muestra un mensaje de confirmación.

3. Haga clic en **Aceptar**.

   El certificado está ahora disponible en la ubicación seleccionada de su disco duro.

Para exportar un certificado a un dispositivo USB eToken, proceda como se indica a continuación:

1. Compruebe que el dispositivo está correctamente conectado a su equipo.
2. En la parte inferior derecha del panel **Administrador de certificados**, haga clic en la flecha ▼ situada a la derecha del botón **Exportar a disco**.
3. En la lista que se muestra, seleccione **Exportar a dispositivo USB**.

   Se abre un cuadro de diálogo.

4. Introduzca la contraseña general del dispositivo y haga clic en **Aceptar**.

   Se abre un cuadro de diálogo.

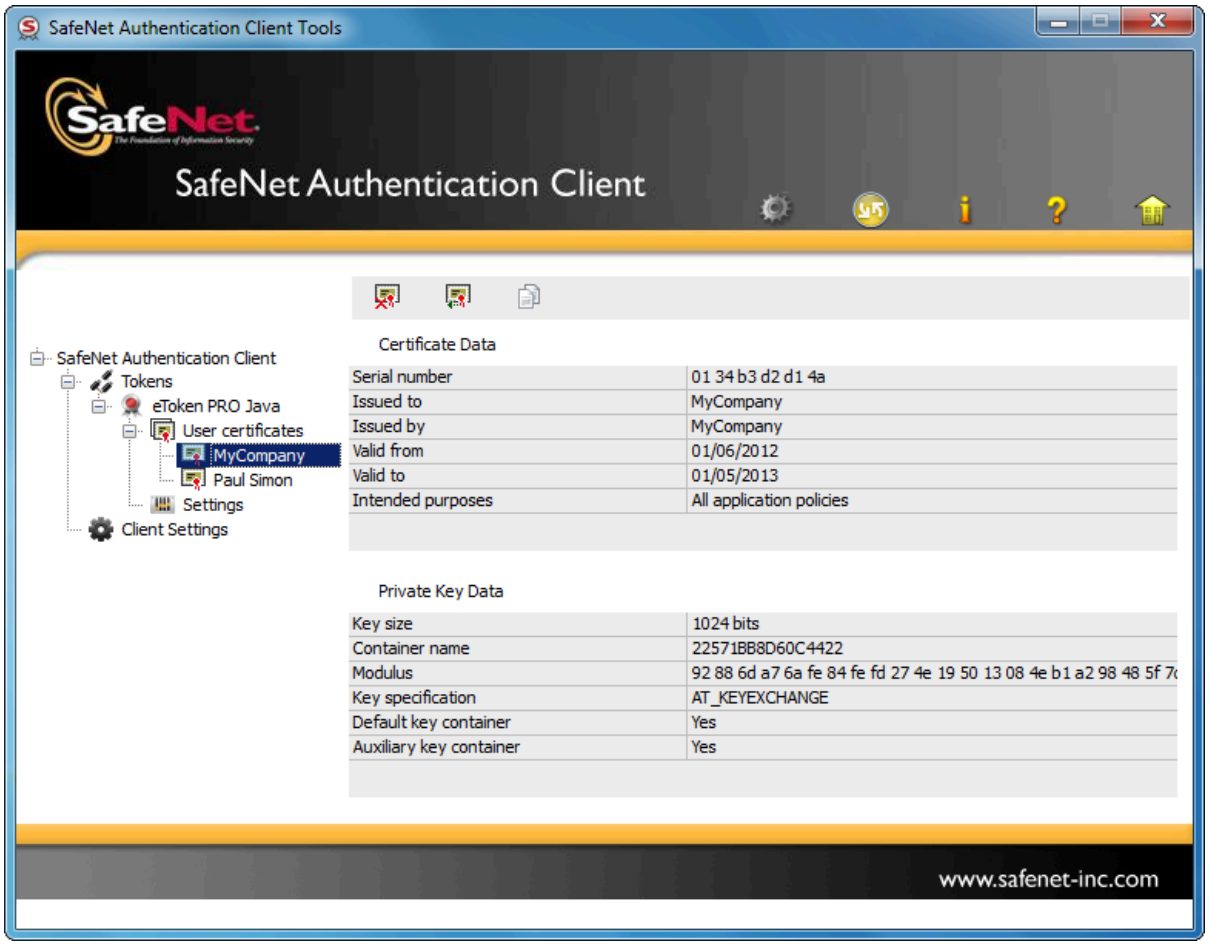
5. Introduzca la contraseña del certificado y haga clic en **Aceptar**.

   Se muestra un mensaje de confirmación.

6. Haga clic en **Aceptar**.

   El certificado se ha exportado correctamente al dispositivo USB.

   Al explorar el contenido del dispositivo a través de SafeNet Authentication Client, su certificado debería aparecer en la sección **Certificados de usuario** si se trata de un certificado externo, o en la sección **Certificados AC** si se trata de un certificado autofirmado:



Eliminar un certificado almacenado en el servidor

Para eliminar un certificado almacenado en el servidor, proceda como se indica a continuación:

1. En la **Lista de certificados**, seleccione el certificado correspondiente.
2. En la parte inferior derecha del panel **Administrador de certificados**, haga clic en el botón **Eliminar**.

Se muestra un mensaje de advertencia.

3. Haga clic en **Sí**.

El certificado se ha eliminado correctamente: ya no aparecerá en la **Lista de certificados**.

> ***Los usuarios que posean privilegios que les concedan acceso al enlace "Configuración" también pueden eliminar certificados a través del Cliente Web, siempre y cuando se trate de certificados subidos por ellos mismos y éstos no hayan sido reasignados a uno o más usuarios por un administrador (ver Importar un certificado almacenado en local).***