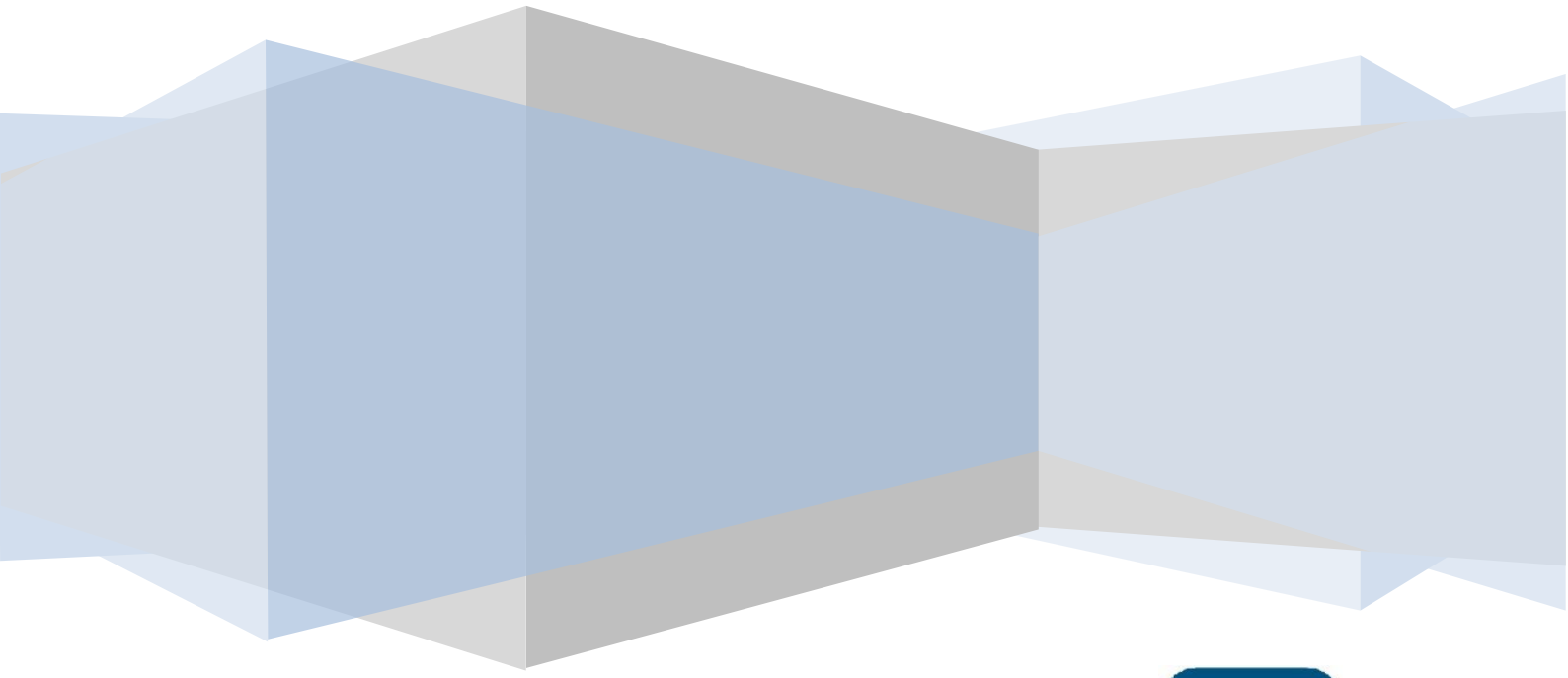
Tarjeta Virtual

v.2.3



CONTENIDO

1. INTRODUCCIÓN

El cliente *Tarjeta Virtual* permite acceder localmente a certificados de usuario en la nube de Izenpe bien BAKQ o bien Profesional, en función de la configuración del mismo. De este modo, las aplicaciones que se ejecutan en su ordenador pueden utilizar estos certificados y las claves de firma como si hubieran sido instalados directamente por el sistema operativo del mismo.

2. CASOS DE USO

Este capítulo describe los principales casos de uso de la tarjeta virtual.

- Almacén de certificados de Windows
- Almacén de certificados PKCS #11
- Integración

2.1. ALMACÉN DE CERTIFICADOS DE WINDOWS

Dichos certificados pueden ser utilizados por cualquier aplicación de escritorio que emplee el almacén de certificados de Windows. La gestión remota de los certificados es totalmente transparente a las aplicacions.

Importante

Los certificados gestionados por la tarjeta virtual no se pueden importar ni eliminar mediante el almacén de certificados de Windows.

2.1.1. FIRMA DE DOCUMENTOS Y FORMULARIOS

Firma de documentos mediante herramientas de edición de Microsoft Office (p.ej Word, Excel) o Adobe (Acrobat, Reader).

Firma de documentos o formularios web mediante componentes de firma ejecutados desde exploradores como Google Chrome.

2.1.2. FIRMA DE CORREOS

Firma de correos electrónicos mediante aplicaciones cliente como Microsoft Outlook.

2.1.3. AUTENTICACIÓN SSL/TLS

Acceso a sitios remotos que requieran autenticación SSL/TLS. Por ejemplo, acceso a sitios seguros mediante exploradores Microsoft Edge o Google Chrome.

2.2. ALMACÉN DE CERTIFICADOS PKCS #11

Las aplicaciones sin acceso al almacén de claves de Windows pueden acceder a las claves de usuario gracias al cliente PKCS #11 proporcionado con *Tarjeta Virtual*. Al configurar la aplicación, debe indicarse la ruta de la librería `p11rss.dll`

- Aplicaciones de 32 bits: `C:\Windows\SysWOW64\p11rss.dll`
- Aplicaciones de 64 bits: `C:\Windows\System32\p11rss.dll`

Las siguientes secciones ilustran ejemplos de uso del cliente PKCS #11.

2.2.1. FIRMA DE DOCUMENTOS Y FORMULARIOS

Firma de documentos y formularios web mediante componentes de firma ejecutados desde exploradores como Mozilla Firefox.

2.2.2. FIRMA DE CORREOS

Firma de correos electrónicos mediante aplicaciones cliente como Mozilla Thunderbird.

2.2.3. AUTENTICACIÓN SSL/TLS

Acceso a sitios web que requieran autenticación SSL/TLS mediante exploradores como Mozilla Firefox.

Importante

Los certificados gestionados por la tarjeta virtual no se pueden importar ni eliminar mediante el navegador.

2.3. INTEGRACIÓN

Los certificados gestionados por la tarjeta virtual pueden ser utilizados por aplicaciones con interfaces como los siguientes.

2.3.1. NETWORK SECURITY SERVICES

La tarjeta virtual se integra con las librerías criptográficas Network Security Services (NSS). Para ello, en las aplicaciones que utilicen dichas librerías, la tarjeta virtual puede registrarse como dispositivo PKCS #11.

La integración con NSS permite registrar la tarjeta virtual como dispositivo de seguridad de las aplicaciones Mozilla (e.g. Firefox, Thunderbird). De este modo, los usuarios de dichas aplicaciones pueden utilizar los certificados de la tarjeta virtual.

Para registrar la tarjeta virtual como dispositivo Firefox:

1. En el navegador Firefox, seleccione la opción **Ajustes** para acceder al cuadro de configuración.
2. En el menú de configuración haga clic sobre la opción **Privacidad & Seguridad** .
3. En la opción **Seguridad > Certificados**, haga clic sobre el botón **Dispositivos de seguridad** para acceder al administrador de dispositivos criptográficos .
4. En el administrador de dispositivos, haga clic sobre **Cargar** para añadir un dispositivo con las propiedades descritas a continuación.

2.3.2. NOMBRE DEL MÓDULO

Nombre del nuevo dispositivo de seguridad (e.g. DesktopCard).

Importante

Por limitaciones del navegador, se aconseja omitir los espacios en blanco en el nombre del módulo.

2.3.3. NOMBRE DEL ARCHIVO DEL MÓDULO

Proporcione la ruta de la librería `p11rss.dll` instalada (32 o 64 bits) de acuerdo a lo que se explica en el apartado Almacén de certificados PKCS #11.

2.3.4. OPENSC

La tarjeta virtual se integra con las librerías criptográficas OpenSC. Por ello, en las aplicaciones que utilicen dichas librerías, la tarjeta virtual puede registrarse como dispositivo PKCS #11. Por ejemplo, la siguiente linea de comandos genera un par de claves a través de la interfaz PKCS # 11 de la tarjeta virtual:

```
pkcs11-tool.exe --module "C:\Windows\SysWOW64\p11rss.dll" -l -k --key-type rsa:1024
```

Observe que el argumento del comando `--module` es la ruta de la librería `p11rss.dll` .

Nota

El `engine_pkcs11` de OpenSC permite integrar la tarjeta virtual con OpenSSL.

2.3.5. JAVA

La tarjeta virtual se puede integrar en las aplicaciones desarrolladas mediante Java SE (versión 6 o superiores), por ejemplo, aplicaciones en de escritorio Para ello, deben utilizarse los siguientes proveedores criptográficos que permiten el acceso a la tarjeta virtual mediante PKCS #11 o a través del almacén de Windows:

- `SunPKCS11`
- `SunMSCAPI`

3. REQUISITOS DE SISTEMA

Este capítulo describe los requisitos de sistema para instalar y ejecutar *Tarjeta Virtual*.

- Sistema operativo
- Dependencias
- Proxy
- Navegadores
- Aplicaciones
- Integración

3.1. SISTEMA OPERATIVO

Tarjeta Virtual puede ejecutarse sobre las versiones del sistema operativo Windows descritas a continuación.

3.1.1. WINDOWS 10

Sistemas para 64 bits de Windows 10.

3.2. DEPENDENCIAS

Tarjeta Virtual requiere las siguientes dependencias en el equipo.

3.2.1. .NET FRAMEWORK

La versión 4.6 o superior es necesaria. Tenga en cuenta que forma parte de la instalación estándar de Windows 10.

3.2.2. MICROSOFT EDGE WEBVIEW2

Es necesario disponer del *Runtime* de Microsoft Edge Webview2. Se recomienda emplear la última actualización disponible.

Si el instalador de *Tarjeta Virtual* detecta que no está presente en el sistema, descarga el instalador *bootstrapper* para satisfacer este requisito.

Si no se dispone del Runtime Microsoft Edge Webview2 en el equipo antes de instalar la aplicación y la configuración de Windows requiere el uso de proxy, durante la instalación se descargará el instalador bootstrapper del *runtime* pero éste no podrá descargar la última versión del mismo porque no soporta el uso de proxy.

Como solución, debe instalarse previamente el instalador del *runtime* preparado para instalaciones *offline*.

3.3. PROXY

Tarjeta Virtual soporta configurar manual y automáticamente un proxy en Windows para establecer las conexiones hacia el servidor.

3.4. NAVEGADORES

Las claves y certificados de *Tarjeta Virtual* pueden ser utilizados desde los siguientes navegadores.

3.4.1. MICROSOFT EDGE

Últimas versiones de Microsoft Edge.

3.4.2. GOOGLE CHROME

Últimas versiones de Google Chrome para 32 y 64 bits.

3.4.3. MOZILLA FIREFOX

Últimas versiones de Mozilla Firefox para 32 y 64 bits.

3.5. APLICACIONES

Además de los navegadores ya descritos, aplicaciones como las siguientes pueden utilizar las claves y certificados de *Tarjeta Virtual*.

3.5.1. MICROSOFT OFFICE

Versiones a partir de la 2007 para 32 y 64 bits.

3.5.2. ADOBE

Versiones X, XI y DC de Adobe Reader y Adobe Acrobat.

3.6. INTEGRACIÓN

Tarjeta Virtual puede integrarse con los siguientes entornos.

3.6.1. OPENSC

La librería OpenSC permite integrar *Tarjeta Virtual* con tarjetas inteligentes.

3.6.2. JAVA SE

Tarjeta Virtual puede integrarse con aplicaciones desarrolladas con Java SE para 32 y 64 bits (versión 6 o superior). Para ello, deben utilizarse los siguientes proveedores:

- Sun PKCS #11 Provider
- Sun MSCAPI Provider

4. INSTALACIÓN Y DESINSTALACIÓN

Este capítulo describe las modalidades de instalación soportadas por la aplicación *Tarjeta Virtual*.

- Características del instalador
- Instalación
- Desinstalación

NOTA: En caso de que exista una versión anterior instalada, es recomendable la desinstalación de la misma y reiniciar el equipo previamente a la instalación de la la última versión

4.1. CARACTERÍSTICAS DEL INSTALADOR

4.1.1. FORMATO MSI

El instalador se genera en formato MSI (Windows Installer), para facilitar su distribución e instalación en los equipos de los usuarios.

4.1.2. MULTIUSUARIO

La instalación y desinstalación de la aplicación debe realizarla únicamente un usuario con permisos de administrador en el equipo.

Una vez instalada, todos los usuarios del mismo equipo pueden emplearla, aunque su cuenta local del equipo se cree posteriormente. La desinstalación es también efectiva para todos los usuarios del equipo.

4.1.3. RUTA DE INSTALACIÓN POR DEFECTO

La aplicación se instala de manera predeterminada en la carpeta definida en el sistema como

`<ProgramFiles>\Izenpe\Tarjeta Virtual [BAK|Profesionales]`, pero puede cambiarse durante la instalación.

4.1.4. ARRANQUE AUTOMÁTICO

La aplicación arranca automáticamente tras completarse la instalación.

Por otro lado, la aplicación arranca automáticamente tras cada inicio de sesión de Windows, pero puede cambiarse este comportamiento durante la instalación

4.1.5. DEPENDENCIAS

Si el instalador de *Tarjeta Virtual* detecta que no está presente en el sistema el *Runtime* de *Microsoft Edge Webview2*, descarga el instalador *bootstrapper* y lo ejecuta a continuación para satisfacer esta dependencia.

4.2. INSTALACIÓN

4.2.1. INSTALACIÓN INTERACTIVA

En este caso, el usuario instala la aplicación interactivamente siguiendo un asistente.

Para instalar en modo interactivo:

1. Acceda al equipo con permisos de administrador
2. Ejecute el instalador de aplicación
3. El asistente del instalador requiere la aceptación de los términos de la licencia. Seleccione **Acepto los términos de la licencia** para continuar.
4. El asistente del instalador ofrece continuar con la instalación por defecto (pulse **Instalar**) o con la avanzada (pulse **Avanzado**).
   a. La instalación predeterminada instala la aplicación en el directorio

`<ProgramFiles>\Izenpe\Tarjeta Virtual [BAK|Profesionales]` e instala la opción **Ejecutar la aplicación al iniciar sesión** (ejecutar la aplicación automáticamente cuando se inicia sesión en Windows).La instalación avanzada permite cambiar el directorio y escoger si se deshabilita la opción **Ejecutar la aplicación al iniciar sesión**.El instalador ofrece reiniciar el equipo antes de usar la aplicación si detecta cualquier conflicto de librerías durante la instalación.

4.2.2. INSTALACIÓN DESATENDIDA

En este caso, el usuario instala la aplicación en modo desatendido. Esto es, sin mostrar un asistente gráfico.

Para instalar en modo desatendido:

1. Acceda al equipo con permisos de administrador
2. Ejecute la siguiente línea de comandos `msiexec /i [nombre instalador] /quiet [APPLICATIONFOLDER="<path>"] [INSTALLLEVEL="<level>"]`

El comando opcional `APPLICATIONFOLDER` instala la aplicación en el directorio `<path>` . Cuando no se indica, `<ProgramFiles>\Izenpe\Tarjeta Virtual [BAK|Profesionales]` se emplea como valor.

El comando opcional `INSTALLLEVEL` instala la aplicación con la opción **Ejecutar la aplicación al iniciar sesión** (ejecutar la aplicación automáticamente cuando se inicia sesión en Windows) cuando se define `<level>` con valor 2 o sin ella (`<level>` 1).

4.3. DESINSTALACIÓN

4.3.1. DESINSTALACIÓN INTERACTIVA

Para desinstalar en modo interactivo:

1. Acceda al equipo con permisos de administrador.
2. En el panel de desinstalación de aplicaciones de Windows, seleccione **Tarjeta Virtual**.

4.3.2. DESINSTALACIÓN DESATENDIDA

Para desinstalar en modo desatendido:

1. Acceda al equipo con permisos de administrador.
2. Ejecute el comando `msiexec /x [nombre instalador.msi] /quiet`

5. USO

Este capítulo explica cómo el usuario emplea la aplicación *Tarjeta Virtual* y la operativa habitual que permite.

- Estado de la aplicación
- Gestión de la sesión
- Uso de la identidad de firma
- Otras opciones de la aplicación

5.1. ESTADO DE LA APLICACIÓN

5.1.1. ACCESO A LOS CERTIFICADOS

Para que las identidades de firma en servidor estén visibles como certificados en el equipo del usuario y puedan emplearse desde otras aplicaciones, *Tarjeta Virtual* debe estar arrancada. Adicionalmente, el usuario debe haber iniciado sesión en la aplicación.

5.1.2. ARRANCAR LA APLICACIÓN

Para arrancar la aplicación, haga clic sobre el acceso directo **Tarjeta Virtual** del menú **Inicio** de Windows. Cuando se arranca la aplicación se solicita automáticamente el inicio de la sesión al usuario.

Este comportamiento es configurable con el atributo OpenSessionOnStart del fichero csprss.cnf ubicado en el directorio settings de la ruta de instalación. Si tiene valor true, se solicitará automáticamente el inicio de sesión y false, en caso contrario.

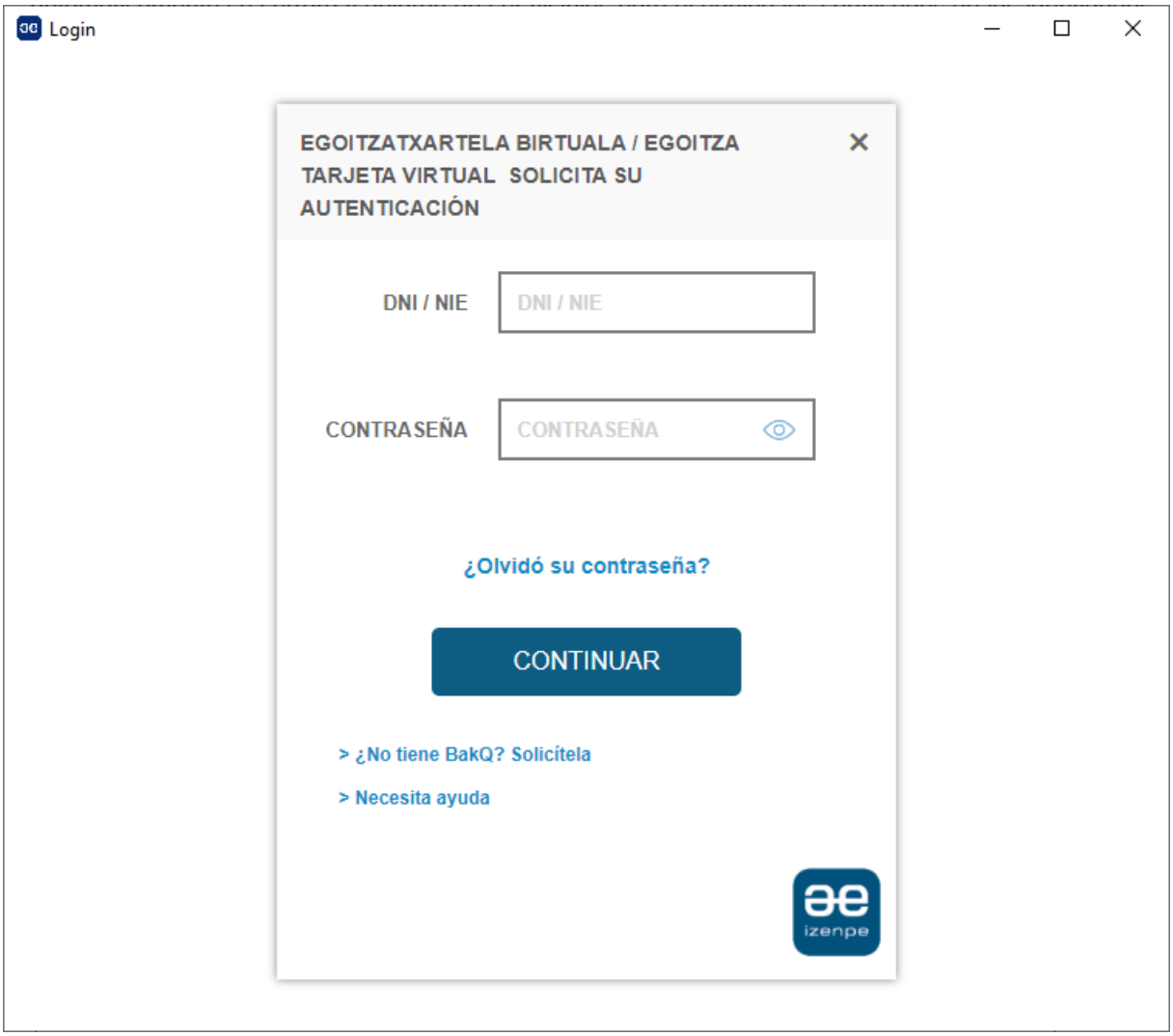
5.1.3. SALIR DE LA APLICACIÓN

Para cerrar la la aplicación *Tarjeta Virtual*, haga clic con el botón derecho sobre el icono de la aplicación en la barra de tareas y seleccione el comando **Salir**. Si la aplicación tenía la sesión del usuario iniciada, automáticamente se cerrará y dejarán de ser visibles para el equipo los certificados de las identidades de firma en servidor.

5.2. GESTIÓN DE LA SESIÓN

5.2.1. INICIO DE SESIÓN

Para iniciar una sesión en la aplicación haga clic con el botón derecho sobre el icono de la aplicación en la barra de tareas y seleccione el comando contextual **Iniciar sesión** o haga doble clic sobre el icono. De este modo, al usuario se le presenta un formulario de inicio de sesión en el que se ofrecerán las opciones de autenticación establecidas en el servidor. Por ejemplo, el siguiente:



Tras arrancar *Tarjeta Virtual*, el usuario dispone de un icono en la barra de tareas de Windows. Como veremos a continuación, tanto la apariencia como las notificaciones de dicho icono permiten consultar fácilmente el estado de la sesión.

5.2.2. NOTIFICACIONES DE CAMBIO DE ESTADO

Cuando el usuario de *Tarjeta Virtual* selecciona las opciones descritas en esta capítulo, los cambios de estado en la aplicación son notificados mediante los siguientes avisos en la barra de tareas de Windows.

5.2.2.1. INICIANDO SESIÓN

La aplicación está iniciando una sesión con las credenciales introducidas por el usuario.

5.2.2.2. SESIÓN INICIADA

La sesión de usuario se ha iniciado con éxito.

5.2.2.3. SESIÓN FINALIZADA

La sesión ha sido finalizada.

5.2.2.4. CERRAR SESIÓN

Para finalizar la sesión en curso, haga clic con el botón derecho sobre el icono de la aplicación de la barra de tareas cuando hay una sesión iniciada y seleccione el comando contextual **Cerrar sesión**. Al cerrar la sesión, los certificados gestionados por la tarjeta virtual dejan de estar disponibles en el equipo.

5.3. USO DE LA IDENTIDAD DE FIRMA

Una vez se inicia sesión en la aplicación *Tarjeta Virtual*, los certificados correspondientes a las identidades de firma en servidor pasan a estar disponibles en todas las aplicaciones que emplean el almacén de certificados de Windows.

Alternativamente, algunas aplicaciones de escritorio (por ejemplo, el navegador Firefox) pueden requerir el uso del interfaz PKCS #11 para tener acceso a los certificados. En este caso, además de iniciar sesión en la aplicación *Tarjeta Virtual* es necesario registrarla en la aplicación como dispositivo PKCS #11. Vea en Casos de uso los detalles este caso.

Las aplicaciones que permitan escoger el certificado a emplar en un proceso de firma o autenticación, en caso de disponer de varios certificados disponibles en el equipo, mostrarán también los correspondientes a las identidades de firma custodiadas en Remote Signing Engine. En caso de que empleen el nombre descriptivo del certificado registrado en Windows, se mostrará el campo CN del Subject del certificado.

5.4. OTRAS OPCIONES DE LA APLICACIÓN

La aplicación, adicionalmente, permite realizar otras operaciones. En particular:

Para consultar las identidades de firma del usuario:

1. En la barra de tareas de Windows, haga clic con el botón derecho sobre el icono de sesión iniciada.
2. Seleccione el comando contextual **Mostrar certificados** para acceder al cuadro de diálogo **Certificados**.
3. En el cuadro de de diálogo **Certificados**, haga clic sobre los diferentes certificados para consultar sus propiedades.

Para consultar la versión de Tarjeta Virtual:

1. En la barra de tareas de Windows, haga clic con el botón derecho sobre el icono d
2. Seleccione el comando contextual **Acerca de** para acceder a la vista con la información de la aplicación.
3. En la barra inferior de la vista se muestra la versión de la aplicación.

6. NOTAS DE LA VERSIÓN 2.3.0

6.1. NUEVAS FUNCIONALIDADES

6.1.1. COMPATIBILIDAD CON APLICACIONES DE 64 BITS

Se amplía la compatibilidad de *Tarjeta Virtual* en sistemas operativos de 64 bits con el soporte para las aplicaciones de 64 bits. De este modo, se pueden emplear los certificados certificados desde las aplicaciones independientemente de si corren en 32 o 64 bits.

Esta mejora permite ampliar la compatibilidad de *Tarjeta Virtual* con diversas aplicaciones. Por ejemplo, con las versiones recientes de los navegadores Mozilla Firefox, Google Chrome y Microsoft Explorer, Microsoft Edge para Windows 10, y la edición de 64 bits de las herramientas de Microsoft Office.

6.1.2. MAYOR COMPATIBILIDAD CON LAS APLICACIONES

Esta versión cambia el modo de solicitar al servidor las operaciones de firma con las identidades de firma para mejorar la compatibilidad con aplicaciones que requieren ciertos modos de firma.. Este cambio permite, por ejemplo, que esta versión de *Tarjeta Virtual* pueda emplearse desde un navegador en autenticaciones SSL/ TLS contra servidores que únicamente soportan las versiones 1.0 y 1.1 del protocolo TLS.

6.1.3. ACTUALIZACIÓN DEL NAVEGADOR EMBEBIDO

Tarjeta Virtual emplea desde esta versión el *Runtime* de *Microsoft Edge Webview2* para implementar el inicio de sesión y la autorización mediante un nuevo tipo de navegador embebido en la aplicación. Este cambio de tecnología permite ampliar la compatibilidad con servidores de autenticación que no soportan el motor de Internet Explorer y mejorar la estabilidad de la aplicación.

Funcionalmente el inicio de sesión y autorización se comporta como en versiones anteriores. No obstante, introduce una funcionalidad nueva, el autocompletado de contraseñas y valores en los formularios, que ofrece al usuario la posibilidad de decidir si desea recordar sus credenciales en el navegador embebido de la aplicación

6.1.4. SOPORTE DE CONFIGURACIÓN DE PROXY DE WINDOWS MEDIANTE SCRIPTS PAC

En la versión 2.3.0 se añade el soporte de uso de un proxy en el equipo donde se ejecuta la aplicación para conectarse al servidor. Este soporte solo permitía configuraciones de Windows donde se establecía el *proxy* en el modo manual. En esta versión se ha añadido el soporte para configuraciones de proxy de Windows mediante *scripts* PAC (Proxy *auto-config*).

6.1.5. SOPORTE DE PROXY DE SISTEMA

En esta versión se introduce el soporte de uso de un proxy en el equipo donde se ejecuta la aplicación para conectarse al servidor.

El soporte se basa en la configuración de proxy establecida en Windows en el modo manual, de modo que *Tarjeta Virtual* realizará todas las conexiones al servidor mediante proxy si en la configuración de proxy de Windows se ha establecido un servidor proxy y si el host del servidor no se ha configurado como una excepción.

Tenga en cuenta que no se soporta el modo de configuración de proxy de Windows mediante *scripts* PAC (Proxy *auto-config*). En este caso, la aplicación intentará conectarse directamente.

6.1.6. NUEVAS OPCIONES DE ARRANQUE DE LA APLICACIÓN

Esta versión modifica el comportamiento de arranque de la aplicación en dos circunstancias.

En primer lugar, arranca la aplicación tras su instalación automáticamente. En segundo lugar, permite arrancar la aplicación automáticamente tras cada inicio de sesión de Windows si así se establece al generar el instalador.

6.2. BUGS CORREGIDOS

Esta sección describe los *bugs* corregidos por la versión 2.1.0.

6.2.1. TX-26892

En algunas aplicaciones que empleaban los certificados de *Tarjeta Virtual* a través del almacén de certificados de Windows, si se cancelaba la firma en las pantallas de autorización se retornaba un código de error que podía provocar un mensaje confuso para el usuario.

6.2.2. TX-27233

La aplicación no se podía conectar al servidor mediante una conexión segura TLS con las *ciphersuites* ECDHE soportadas y recomendadas en el servidor siguientes:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA14

6.2.3. TX-28160

El uso de los certificados con el propósito de autenticación en Internet Explorer fallaba si éste iniciaba múltiples conexiones.

6.2.4. TX-28221

La versión de 32 bits instalaba el CSP de 64bits.

6.2.5. TX-28321

El inicio de sesión fallaba si se detectaba un error en los certificados instalados en el equipo.

6.2.6. TX-28556

La aplicación *Tarjeta Virtual* o la aplicación externa desde la que se usara podían cerrarse inesperadamente al intentar iniciar sesión o realizar una operación de firma o autenticación.