Tarjeta Virtual

v.4.1.0

Manual de instalación y uso

Plataforma Windows

CONTENIDO

1. Introducción

2. Casos de uso

2.1 Almacén de certificados de Windows (CNG / KSP)

2.1.1 Firma de documentos y formularios

2.1.2 Autenticación SSL/TLS

2.2 Integración con aplicaciones

2.2.1 Microsoft Office

2.2.2 Adobe Acrobat / Reader

2.2.3 Navegadores

3. Requisitos de sistema

3.1 Sistema operativo

3.2 Dependencias

3.3 Permisos y privilegios

3.4 Conectividad de red

3.5 Navegadores y aplicaciones soportadas

4. Instalación y desinstalación

4.1 Distribución y formato del instalador

4.2 Procedimiento de instalación

4.3 Instalación desatendida

4.4 Desinstalación

5. Uso

5.1 Primera ejecución y bienvenida

5.2 Vincular un certificado

5.3 Activar y desactivar certificados

5.4 Acceso a sedes electrónicas

5.5 Icono de la barra de tareas

5.6 Ajustes de la aplicación

5.7 Reportar un problema

5.8 Salir de la aplicación

6. Resolución de problemas

7. Notas de la versión 4.1.0

1. Introducción

Tarjeta Virtual es una aplicación de escritorio que permite acceder localmente a los certificados digitales del usuario custodiados en la nube de Izenpe (**BakQ** y **Profesional en la nube**), de modo que las aplicaciones del equipo (navegadores, Microsoft Office, Adobe Reader, clientes de correo, etc.) puedan utilizar dichos certificados y sus claves de firma como si hubieran sido instalados directamente en el sistema operativo.

A diferencia de las versiones anteriores de la aplicación (rama 2.x), la versión 3.x ha sido reescrita íntegramente sobre tecnología **Flutter**, con una experiencia de usuario unificada entre Windows, macOS, Android e iOS. En la plataforma Windows, la integración con el sistema se realiza mediante un *Key Storage Provider* (KSP) propio que se registra en el subsistema criptográfico CNG (*Cryptography Next Generation*) de Microsoft, junto con un módulo de firma remota (*sign bridge*) que comunica con la infraestructura HSM de Izenpe.

Este manual describe los casos de uso, los requisitos del sistema, el procedimiento de instalación y desinstalación, y la operativa habitual de la aplicación en su versión 4.1.0 para Windows.

2. Casos de uso

Este capítulo describe los principales casos de uso de Tarjeta Virtual en la plataforma Windows.

2.1 Almacén de certificados de Windows (CNG / KSP)

Una vez instalada y con un certificado activo, los certificados gestionados por Tarjeta Virtual están disponibles de manera transparente para cualquier aplicación de escritorio que utilice el almacén de certificados de Windows. La integración se realiza a través de un *Key Storage Provider* (KSP) propio de Izenpe, registrado en el subsistema criptográfico CNG mediante la API oficial `BCrypt` de Microsoft.

Importante

Los certificados gestionados por Tarjeta Virtual no pueden importarse ni eliminarse manualmente desde el almacén de certificados de Windows; su ciclo de vida se controla desde la propia aplicación.

2.1.1 FIRMA DE DOCUMENTOS Y FORMULARIOS

Firma de documentos mediante herramientas de edición de Microsoft Office (Word, Excel) o Adobe (Acrobat, Reader). Firma de formularios web mediante componentes de firma ejecutados desde navegadores como Microsoft Edge o Google Chrome. La firma se realiza siempre de forma remota contra el HSM de Izenpe a través del módulo `izenpe_sign_bridge.dll`, sin que la clave privada abandone nunca la infraestructura de Izenpe.

2.1.2 AUTENTICACIÓN SSL/TLS

Acceso a sitios remotos que requieran autenticación SSL/TLS con certificado de cliente. Por ejemplo, acceso a sedes electrónicas y oficinas virtuales mediante navegadores Microsoft Edge o Google Chrome. La aplicación instala automáticamente la cadena de certificados intermedios de Izenpe para que el sistema operativo pueda validar correctamente la confianza del certificado del usuario.

2.2 Integración con aplicaciones

Las aplicaciones de escritorio que utilizan el almacén de certificados de Windows pueden emplear los certificados de Tarjeta Virtual de manera totalmente transparente. La aplicación expone tanto una versión x64 como una versión x86 de las librerías nativas, instaladas respectivamente en `C:\Windows\System32` y `C:\Windows\SysWOW64`, para garantizar el soporte de aplicaciones de 32 y 64 bits.

2.2.1 MICROSOFT OFFICE

Word, Excel y otras aplicaciones de Microsoft Office pueden utilizar los certificados de Tarjeta Virtual para firmar documentos. Es compatible tanto con la edición de 32 bits (que carga el KSP desde SysWOW64) como con la edición de 64 bits (que lo carga desde System32).

2.2.2 ADOBE ACROBAT / READER

Adobe Acrobat y Adobe Reader pueden firmar documentos PDF utilizando los certificados de Tarjeta Virtual. La aplicación implementa las propiedades CNG requeridas por Adobe (`NCRYPT_EXPORT_POLICY`, `NCRYPT_KEY_USAGE` y `NCRYPT_WINDOW_HANDLE`), de modo que los certificados aparecen disponibles en el cuadro de selección de identidades de firma de Adobe sin configuración adicional.

2.2.3 NAVEGADORES

Microsoft Edge y Google Chrome utilizan directamente el almacén de certificados de Windows, por lo que los certificados de Tarjeta Virtual están disponibles para autenticación SSL/TLS en sedes electrónicas sin necesidad de configuración adicional. Mozilla Firefox dispone de su propio almacén interno (NSS); para utilizar los certificados de Tarjeta Virtual desde Firefox, se recomienda configurar Firefox para emplear el almacén de Windows mediante la opción `security.osclientcerts.autoload` disponible en `about:config`.

3. Requisitos de sistema

Este capítulo describe los requisitos de sistema necesarios para instalar y ejecutar Tarjeta Virtual 4.1.0 en Windows.

3.1 Sistema operativo

Tarjeta Virtual 4.1.0 puede ejecutarse sobre las siguientes versiones de Windows:

- Windows 10 (64 bits)
- Windows 11 (64 bits)

El instalador verifica la versión del sistema operativo durante la instalación y aborta el proceso si detecta una versión inferior a Windows 10. No se proporciona soporte para Windows 7, Windows 8 ni Windows 8.1.

3.2 Dependencias

3.2.1 MICROSOFT EDGE WEBVIEW2 RUNTIME

Tarjeta Virtual requiere el runtime de Microsoft Edge WebView2 para el flujo de autenticación OAuth y para mostrar las páginas embebidas dentro de la aplicación. Si el instalador detecta que el runtime no está presente en el sistema, descarga e instala automáticamente el bootstrapper oficial de Microsoft.

En equipos en los que la salida a Internet esté restringida por proxy o cortafuegos durante la instalación, se recomienda instalar previamente el runtime de WebView2 a partir del instalador *offline* disponible en el sitio oficial de Microsoft.

3.2.2 VISUAL C++ REDISTRIBUTABLE

El instalador presupone que el runtime de Visual C++ 2015–2022 (x64 y x86) está disponible en el sistema, lo cual es habitual en cualquier instalación moderna de Windows 10 u 11.

3.2.3 CERTIFICADOS INTERMEDIOS CA DE IZENPE

El propio instalador despliega de manera automática la cadena de certificados intermedios de Izenpe en el almacén "Entidades de certificación intermedias" (*Intermediate Certification Authorities*) de la máquina, de modo que aplicaciones como Adobe Reader o los navegadores puedan validar la cadena de confianza completa de los certificados de ciudadano, profesional o de Administración Pública vasca.

3.3 Permisos y privilegios

La instalación de Tarjeta Virtual requiere obligatoriamente **permisos de administrador**. Esto es necesario por varios motivos:

- Las librerías nativas `izenpe_ksp.dll` e `izenpe_sign_bridge.dll` deben copiarse a las carpetas `C:\Windows\System32` y `C:\Windows\SysWOW64`.
- El registro del Key Storage Provider (KSP) en CNG se realiza mediante la herramienta `IzenpeKspConfig.exe`, que invoca la API BCrypt y requiere acceso de escritura a la rama `HKLM\SYSTEM\CurrentControlSet\Control\Cryptography` del registro.
- Los certificados intermedios CA se instalan en el almacén de la máquina (*LocalMachine*), no en el del usuario, lo cual también requiere privilegios elevados.

Una vez instalada, la aplicación puede ser ejecutada por cualquier usuario del equipo, sin necesidad de privilegios elevados.

3.4 Conectividad de red

Tarjeta Virtual requiere acceso a Internet para autenticarse contra los servidores de Izenpe y para realizar operaciones de firma remota contra el HSM. Los dominios que deben ser accesibles son los siguientes:

Entorno	Dominio	Puerto
Producción	servicios.izenpe.com	443
Producción (HSM)	eidas.izenpe.com	8082 / 443

La aplicación respeta la configuración de proxy del sistema operativo (proxy manual y proxy automático mediante scripts PAC). En entornos corporativos con cortafuegos, debe garantizarse que estos dominios sean accesibles desde el equipo del usuario.

3.5 Navegadores y aplicaciones soportadas

Aplicación	Versiones soportadas	Notas
Microsoft Edge	Últimas versiones	Almacén de Windows
Google Chrome	Últimas (32 y 64 bits)	Almacén de Windows
Mozilla Firefox	Últimas versiones	Configurable vía about:config
Microsoft Office (Word/Excel)	2016+ (32 y 64 bits)	Firma de documentos
Adobe Acrobat / Reader	DC y posteriores	Firma de PDF
Mozilla Thunderbird	Últimas versiones	S/MIME
certutil.exe	Incluido en Windows	Diagnóstico

4. Instalación y desinstalación

Este capítulo describe el procedimiento de instalación y desinstalación de la aplicación Tarjeta Virtual.

Importante

Si en el equipo existe una versión anterior de Tarjeta Virtual (rama 2.x o anterior), se recomienda desinstalarla y reiniciar el equipo antes de instalar la versión 4.1.0, para evitar conflictos entre el antiguo proveedor PKCS #11 (`p11rss.dll`) y el nuevo Key Storage Provider (`izenpe_ksp.dll`).

4.1 Distribución y formato del instalador

La aplicación se distribuye en dos formatos, ambos firmados digitalmente con el certificado de firma de código de Izenpe S.A. y funcionalmente equivalentes:

Formato	Fichero	Uso recomendado
Inno Setup EXE	`TarjetaVirtual-Setup-4.1.0.exe`	Instalación interactiva por el usuario
MSI	`TarjetaVirtual-Setup-4.1.0.msi`	Despliegue corporativo (SCCM, Microsoft Intune, Group Policy)

Ambos instaladores contienen la aplicación, las librerías nativas (KSP y *sign bridge* en versiones x64 y x86), la herramienta de registro `IzenpeKspConfig.exe` , los certificados intermedios CA de Izenpe y los scripts de post-instalación. No requieren ningún archivo adicional para funcionar.

El MSI se genera con WiX Toolset a partir de los mismos binarios y sigue los estándares de Windows Installer, lo que permite integrarlo directamente en Microsoft Intune, SCCM, Configuration Manager o Group Policy sin necesidad de un *bootstrapper* intermedio.

4.1.1 COMPONENTES DESPLEGADOS

Tras una instalación correcta, los siguientes componentes quedan instalados en el equipo:

Componente	Ubicación
Aplicación principal	`C:\Program Files\Izenpe\Tarjeta virtual\`
KSP x64	`C:\Windows\System32\izenpe_ksp.dll`
Sign Bridge x64	`C:\Windows\System32\izenpe_sign_bridge.dll`
KSP x86	`C:\Windows\SysWOW64\izenpe_ksp.dll`
Sign Bridge x86	`C:\Windows\SysWOW64\izenpe_sign_bridge.dll`
Herramienta de registro KSP	`...\Tarjeta virtual\tools\IzenpeKspConfig.exe`
Scripts de mantenimiento	`...\Tarjeta virtual\scripts\`

4.1.2 CARACTERÍSTICAS DEL PROCESO DE INSTALACIÓN

El instalador realiza automáticamente las siguientes operaciones, en este orden:

1. Verificación de privilegios de administrador y de capacidad real de escritura en `C:\Windows\System32`.
2. Verificación de la versión del sistema operativo (Windows 10 o superior).
3. Detección y, si procede, instalación silenciosa del runtime de Microsoft Edge WebView2.
4. Detección, mediante el *Restart Manager* de Windows, de aplicaciones (navegadores, Adobe Reader, Microsoft Office, etc.) que tuvieran cargada una versión anterior del KSP. En tal caso, se solicita al usuario el cierre de dichas aplicaciones antes de continuar.
5. Copia de la aplicación a `C:\Program Files\Izenpe\Tarjeta virtual`.
6. Copia de las librerías nativas (KSP y *sign bridge*) en sus dos arquitecturas (x64 y x86).
7. Limpieza de cualquier registro previo del KSP en CNG.
8. Registro del nuevo KSP en CNG mediante `IzenpeKspConfig.exe` (API BCrypt oficial de Microsoft).
9. Verificación post-instalación del KSP mediante un script PowerShell.
10. Despliegue de la cadena de certificados intermedios CA de Izenpe (CCEER, AAPPR, AAPPNR, AAPPR2 y SUBCA QC AP) en el almacén de la máquina, mediante `certutil`.

Nota

La versión 4.1.0 NO requiere reiniciar el equipo tras la instalación. Es suficiente con cerrar y volver a abrir aquellos navegadores y aplicaciones que vayan a utilizar los certificados, para que carguen el KSP recién instalado.

4.2 Procedimiento de instalación

El procedimiento recomendado para una instalación interactiva es el siguiente:

1. Inicie sesión en el equipo con una cuenta de administrador.
2. Cierre todos los navegadores y aplicaciones de Office o Adobe que pudieran estar utilizando certificados de Tarjeta Virtual.
3. Haga doble clic sobre el fichero `TarjetaVirtual-Setup-4.1.0.exe`. Windows solicitará confirmación de elevación de privilegios (UAC); acéptela.
4. Seleccione el idioma de la instalación (Castellano o Euskera). El idioma seleccionado se aplicará también como idioma inicial de la aplicación tras el primer arranque.
5. Siga el asistente del instalador hasta su finalización.

Al completarse la instalación, la aplicación arranca automáticamente y se integra en el menú Inicio y opcionalmente en el escritorio.

> **Nota**
>
> La apariencia del asistente puede variar si la aplicación se distribuye empaquetada como MSI a través de un sistema corporativo. Las pantallas y los textos finales del asistente serán los que defina el sistema de despliegue empleado en cada caso.

4.3 Instalación desatendida

4.3.1 INNO SETUP EXE

El instalador Inno Setup admite los flags estándar para ejecución desatendida:

```
TarjetaVirtual-Setup-4.1.0.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
```

Parámetro	Descripción
`/VERYSILENT`	No muestra ninguna ventana ni barra de progreso.
`/SILENT`	Muestra barra de progreso pero suprime las pantallas del asistente.
`/SUPPRESSMSGBOXES`	Suprime los diálogos de error o aviso.
`/NORESTART`	Evita el reinicio automático del equipo.

Ejemplo de desinstalación desatendida:

```
"C:\Program Files\Izenpe\Tarjeta virtual\unins000.exe" /VERYSILENT /SUPPRESSMSGBOXES
/NORESTART
```

4.3.2 MSI (WINDOWS INSTALLER)

El paquete MSI se integra directamente con las herramientas de despliegue de Microsoft (SCCM, Intune, GPO). Ejemplo de instalación silenciosa con log:

```
msiexec /i TarjetaVirtual-Setup-4.1.0.msi /quiet /norestart /l*v
C:\Windows\Temp\tv_install.log
```

Ejemplo de desinstalación silenciosa:

```
msiexec /x TarjetaVirtual-Setup-4.1.0.msi /quiet /norestart
```

Códigos de salida más habituales de `msiexec`:

Código	Significado
`0`	Instalación / desinstalación correcta.
`1602`	Usuario canceló la elevación UAC.
`1603`	Error genérico. Consultar el log detallado (`/l*v`).
`3010`	Instalación correcta con requerimiento de reinicio.

4.3.3 CÓDIGOS DE SALIDA Y LOGS (INNO EXE)

Con el instalador Inno Setup, el código de salida del proceso (`ERRORLEVEL`) indica el resultado: 0 indica éxito y cualquier otro valor indica error. El log detallado de la instalación queda en el directorio `%TEMP%` del usuario que la ejecuta.

4.4 Desinstalación

Para desinstalar la aplicación de manera interactiva:

1. Inicie sesión en el equipo con una cuenta de administrador.
2. Acceda a *Configuración > Aplicaciones > Aplicaciones instaladas* (en Windows 11) o *Panel de control > Programas y características* (en Windows 10).
3. Localice la entrada "Tarjeta virtual" y pulse Desinstalar.

Para desinstalar de manera silenciosa desde línea de comandos:

```
"C:\Program Files\Izenpe\Tarjeta virtual\unins000.exe" /VERYSILENT /SUPPRESSMSGBOXES
/NORESTART
```

El desinstalador realiza automáticamente la limpieza completa del sistema: des-registro del KSP en CNG mediante `IzenpeKspConfig.exe -unregister`, eliminación de credenciales y logs (script `uninstall_cleanup.ps1`) y eliminación de las DLLs y archivos instalados.

5. Uso

Este capítulo describe la operativa habitual con la aplicación Tarjeta Virtual, desde la primera ejecución hasta el acceso a sedes electrónicas mediante certificado digital. Las capturas que se muestran corresponden a la versión en castellano de la aplicación; la versión en euskera mantiene la misma estructura y diseño visual.

5.1 Primera ejecución y bienvenida

La aplicación se lanza desde el icono "Tarjeta Virtual" del menú Inicio de Windows o desde el acceso directo creado en el escritorio (si fue seleccionado durante la instalación). La ventana principal tiene un tamaño fijo de 500×680 píxeles y no es redimensionable, manteniendo la coherencia visual con el resto de plataformas (macOS, Android, iOS).

En la primera ejecución, la pantalla principal muestra una franja de bienvenida con el mensaje *"¡Instalación terminada!"*, un selector de idioma (Castellano / Euskera) y un aviso sobre el icono de la barra de tareas. Bajo la franja de bienvenida se muestran las dos tarjetas de certificado disponibles (Ciudadano y Profesional), todavía sin vincular. En ejecuciones posteriores, la franja de bienvenida ya no se muestra.



Figura 1 — Pantalla principal en la primera ejecución, con la franja de bienvenida visible.

5.2 Vincular un certificado

Tarjeta Virtual permite vincular dos tipos de certificados:

- **Ciudadano:** certificado BakQ, identificado por DNI/NIE, contraseña y código SMS.
- **Profesional en la nube:** certificado profesional para empleados públicos y trabajadores autónomos / colegiados, identificado por las credenciales corporativas correspondientes.

Mientras un certificado no está vinculado, su tarjeta muestra el icono del tipo de certificado y la opción **+ Vincular**:

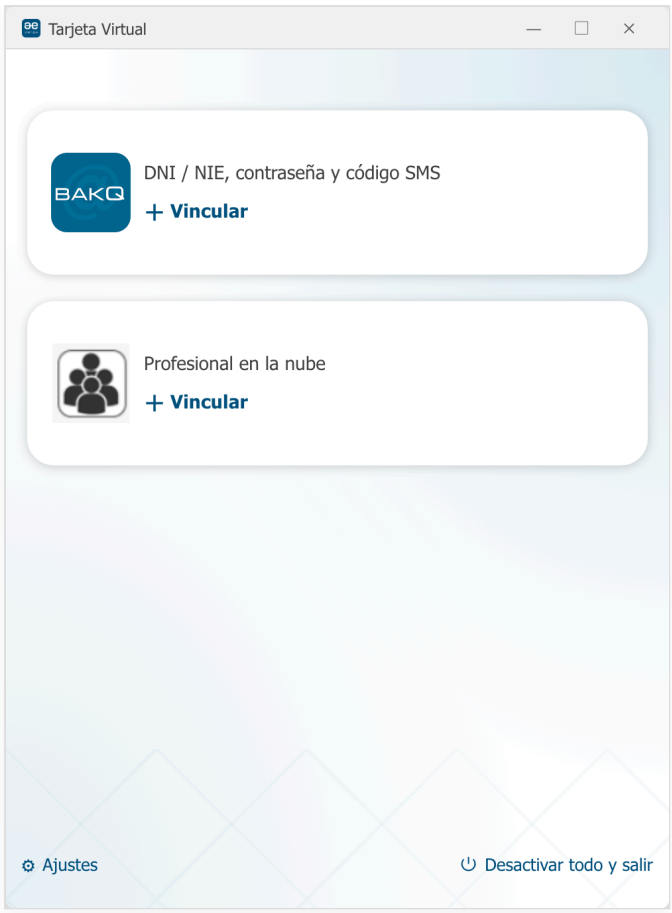


Figura 2 — Pantalla principal con ambos certificados sin vincular.

Para vincular un certificado, pulse sobre la tarjeta correspondiente. Se abrirá un navegador embebido (basado en Microsoft Edge WebView2) que mostrará el formulario de inicio de sesión de Izenpe:



Figura 3 — Formulario de inicio de sesión BakQ embebido.

Una vez introducidas las credenciales y completado el proceso de autenticación de doble factor (en el caso de BakQ, mediante código SMS), el certificado quedará vinculado a la aplicación y se mostrará en la pantalla principal con el botón de encendido correspondiente.

La vinculación es un proceso que se realiza una sola vez. Tras esta operación, las credenciales no son almacenadas localmente; en su lugar, la aplicación dispone de un *token* de refresco persistente que le permite renovar el acceso al certificado de manera transparente.

5.3 Activar y desactivar certificados

Una vez vinculado, la tarjeta del certificado cambia su aspecto: muestra el nombre del titular, el identificador (DNI / NIE para BakQ u organización para Profesional) y un **botón de encendido** circular. Este botón indica el estado del certificado y permite activarlo o desactivarlo con un solo clic:

- **Botón verde:** el certificado está activo. Su clave pública aparece publicada en el almacén de Windows y todas las aplicaciones del equipo pueden utilizarlo.
- **Botón gris oscuro:** el certificado está vinculado pero desactivado. No es visible para las aplicaciones del equipo y, por tanto, no puede emplearse para firmar ni autenticarse.

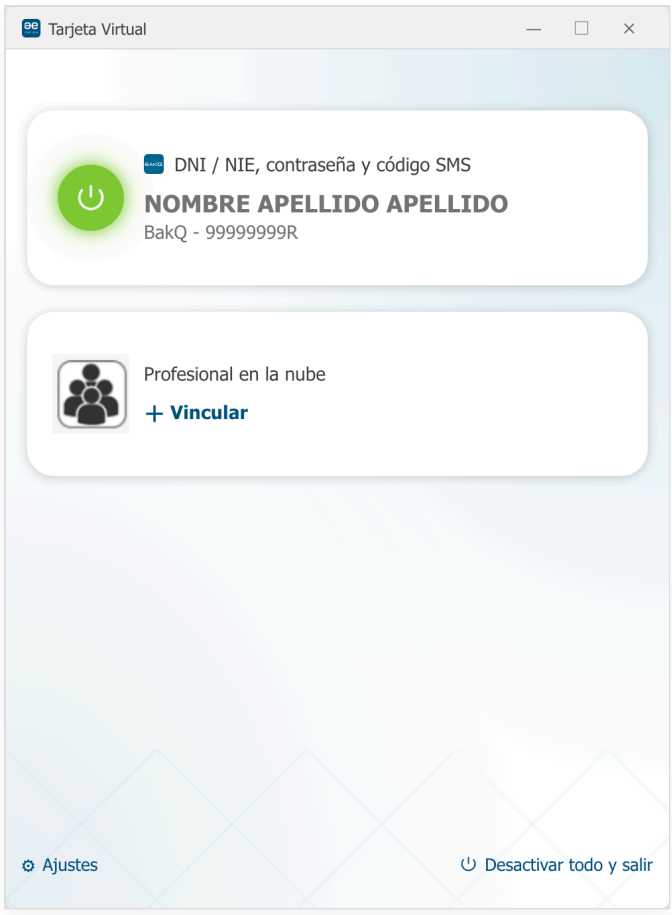


Figura 4 — Certificado BakQ vinculado y activo (botón verde).

Al pasar el cursor sobre el botón, éste muestra un brillo de color que anticipa el efecto del clic (verde si va a activar, gris si va a desactivar). La sesión activa se renueva automáticamente mientras el usuario interactúa con cualquier aplicación cliente.

Nota

Si el equipo permanece inactivo durante **8 horas o más**, al volver a la aplicación los certificados activos se desactivan automáticamente por seguridad y se muestra un aviso de sesión caducada. Basta con volver a pulsar el botón de encendido en la ficha del certificado para reactivarlo.

5.4 Acceso a sedes electrónicas

Una vez activado un certificado, el usuario puede acceder a cualquier sede electrónica directamente desde su navegador habitual (Microsoft Edge, Google Chrome, etc.). Al solicitar la autenticación, el navegador muestra el certificado de Tarjeta Virtual junto al resto de certificados que pudiera tener instalados, y el usuario lo selecciona para identificarse.

No es necesario que la ventana principal de Tarjeta Virtual esté visible; es suficiente con que la aplicación se esté ejecutando, lo cual puede comprobarse mediante el icono de la barra de tareas (apartado siguiente).

5.5 Icono de la barra de tareas

Mientras la aplicación esté en ejecución, se mantendrá visible un icono en la zona de notificaciones de la barra de tareas (*system tray*) de Windows, junto al reloj. Este icono permite consultar visualmente el estado actual de la aplicación:

- **Conectado:** existe al menos un certificado activo y la aplicación está conectada a los servidores de Izenpe.
- **Desconectado:** no hay ningún certificado activo o no hay conexión con los servidores de Izenpe.
- **Verificando:** la aplicación está comprobando la conectividad o renovando el *token* de un certificado.

Haciendo clic con el botón derecho sobre el icono se accede a un menú contextual con las acciones de mostrar / ocultar la ventana principal y salir de la aplicación:

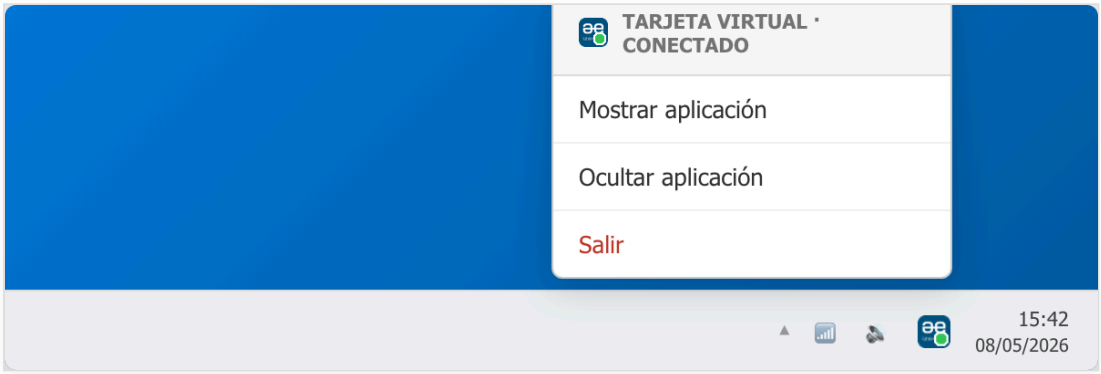


Figura 5 — Icono en la barra de tareas y menú contextual asociado.

5.6 Ajustes de la aplicación

La pantalla **Ajustes**, accesible desde el botón *Ajustes* de la esquina inferior izquierda de la ventana principal, permite configurar los perfiles visibles, gestionar los certificados vinculados, cambiar el idioma, reportar un problema y salir de la aplicación. Al entrar en Ajustes, la ventana se redimensiona automáticamente a 550×900 píxeles para acomodar todas las opciones.

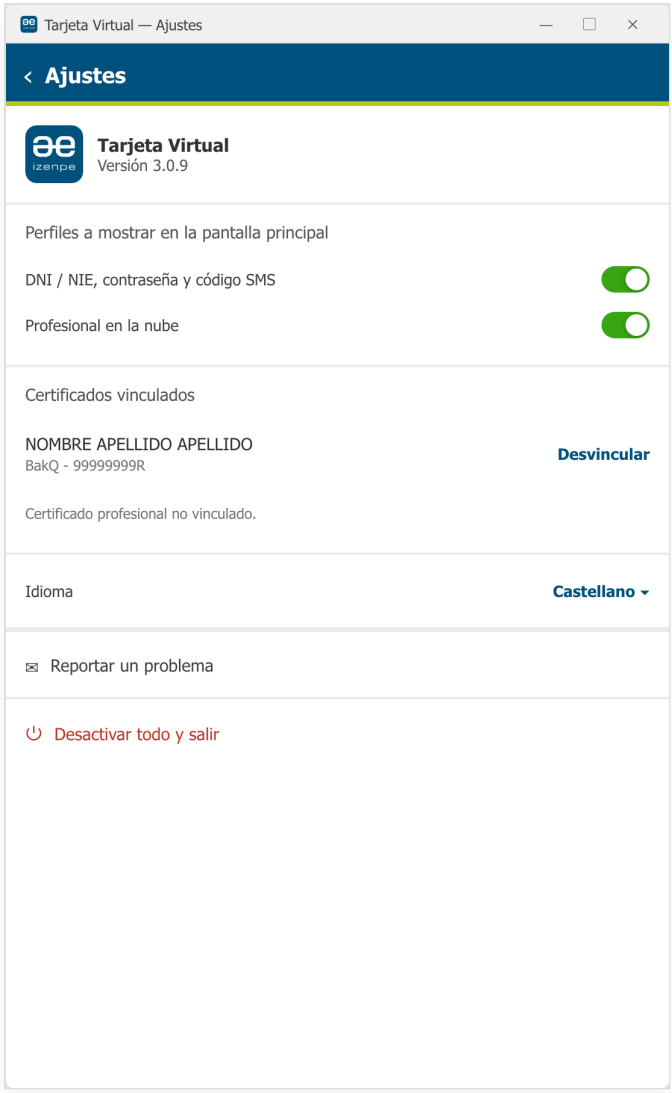


Figura 6 — Pantalla de Ajustes de la aplicación.

- **Perfiles a mostrar en la pantalla principal:** permite ocultar la tarjeta de Ciudadano (DNI/NIE), la de Profesional en la nube o ambas. Debe mantenerse siempre al menos un perfil visible.
- **Certificados vinculados:** muestra el detalle de los certificados ya vinculados y permite desvincularlos individualmente.
- **Idioma:** permite cambiar entre Castellano y Euskera. El cambio se aplica de manera inmediata, sin necesidad de reiniciar la aplicación.
- **Acciones:** enlaces a "Reportar un problema" y "Desactivar todo y salir".

5.7 Reportar un problema

Si el usuario detecta un problema usando la aplicación, puede notificarlo directamente al equipo de soporte de Izenpe desde la pantalla **Reportar un problema** (accesible desde Ajustes o desde Ayuda).

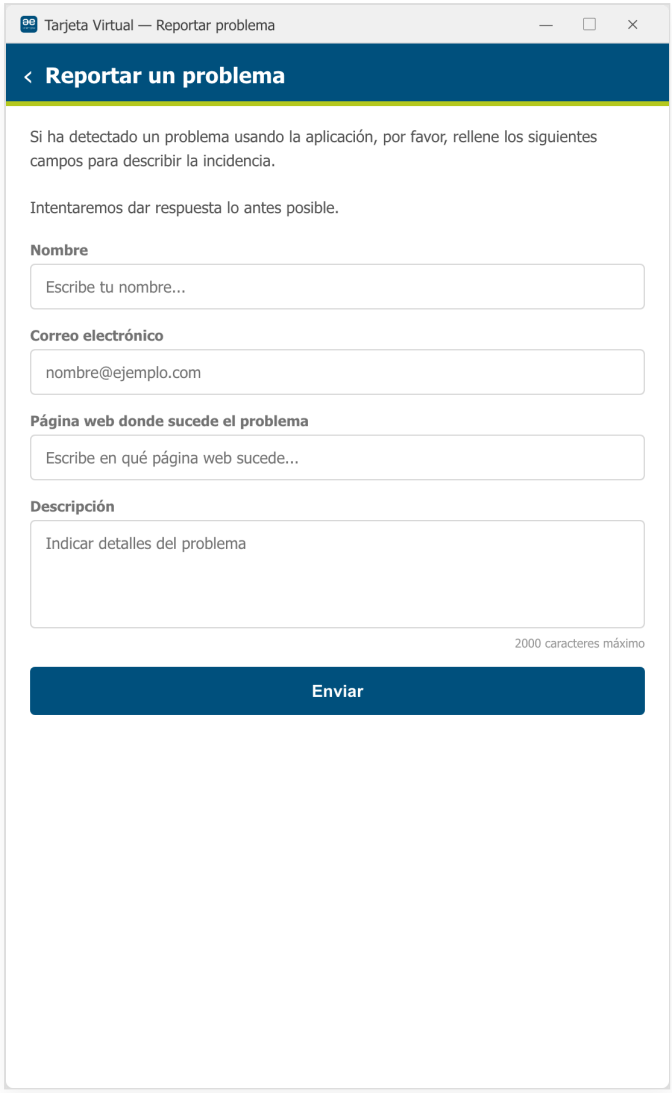


Figura 7 — Pantalla para reportar un problema al equipo de soporte.

El reporte se envía al sistema de tickets de Izenpe junto con metainformación técnica del entorno (versión de Windows, versión de la aplicación, identificador anónimo del equipo, etc.) que facilita el diagnóstico, sin incluir información personal sensible ni credenciales.

5.8 Salir de la aplicación

Para cerrar Tarjeta Virtual, el usuario dispone de varias alternativas:

- Pulsar la opción **Desactivar todo y salir** desde el pie de la ventana principal o desde la pantalla de Ajustes.
- Hacer clic con el botón derecho sobre el icono de la barra de tareas y seleccionar **Salir**.

Importante

Cerrar simplemente la ventana principal con el botón "X" (esquina superior derecha) NO cierra la aplicación: la oculta a la barra de tareas, manteniendo activos los certificados que estuvieran activados. Esto permite que las aplicaciones del equipo sigan utilizándolos sin necesidad de tener la ventana principal abierta. Para cerrar realmente la aplicación, debe utilizarse alguna de las dos vías anteriores.

6. Resolución de problemas

Este capítulo describe las situaciones más habituales que pueden encontrarse durante la instalación o el uso de la aplicación, y la forma de resolverlas.

6.1 El instalador indica que faltan permisos de administrador

El instalador realiza dos comprobaciones independientes: la API `IsAdmin()` de Windows y un test real de escritura en `C:\Windows\System32`. Si cualquiera de las dos falla, aborta la instalación con el mensaje "Permisos de administrador requeridos".

Solución: cierre el instalador, haga clic con el botón derecho sobre el fichero `TarjetaVirtual-Setup-4.1.0.exe` y seleccione "Ejecutar como administrador". Si el error persiste pese a usar una cuenta de administrador, contacte con el responsable de IT del equipo: es posible que existan políticas corporativas (AppLocker, restricciones de UAC) que impiden la elevación de privilegios.

6.2 El instalador no consigue copiar las DLLs a System32

Causa habitual: alguna aplicación (Chrome, Edge, Firefox, Adobe Reader, Microsoft Word, etc.) tiene una versión previa de `izenpe_ksp.dll` o `izenpe_sign_bridge.dll` cargada en memoria.

El propio instalador detecta esta situación y reintenta la copia de manera automática. Si tras varios reintentos no consigue completar la operación, muestra un diálogo con tres opciones: SÍ (reintentar), NO (continuar sin las DLLs, lo cual deja la instalación inservible) o CANCELAR (desinstalar).

Solución recomendada: pulse CANCELAR para desinstalar, cierre todos los navegadores y aplicaciones de Office y Adobe, reinicie el equipo y vuelva a ejecutar el instalador. En entornos con antivirus muy restrictivos, puede ser necesario añadir las DLLs de Izenpe a la lista de excepciones.

6.3 Los certificados no aparecen en Adobe Reader o Microsoft Office

Compruebe en orden los siguientes puntos:

1. Asegúrese de que la aplicación Tarjeta Virtual está en ejecución (verifique el icono de la barra de tareas).
2. Compruebe que el certificado a utilizar está activo (indicador verde) en la pantalla principal de la aplicación.
3. Cierre completamente la aplicación cliente (Adobe, Word, Excel, etc.) y vuelva a abrirla. Las aplicaciones cargan los KSP disponibles solo durante su arranque.

4. Si tras estas comprobaciones el certificado sigue sin aparecer, abra una consola de PowerShell como administrador y ejecute el siguiente comando para listar los certificados visibles en el almacén personal:

```
certutil -store -user My
```

Si la salida del comando no incluye los certificados de Tarjeta Virtual cuando éstos están activos, contacte con el equipo de soporte adjuntando un reporte mediante la opción descrita en el apartado 5.7.

6.4 Adobe Reader muestra "El emisor de este certificado no es de confianza"

Indica que la cadena de certificados intermedios CA no se ha desplegado correctamente. Esto puede ocurrir en equipos con políticas restrictivas que impiden el comando `certutil -addstore CA` durante la instalación.

Solución: ejecute el script `install_certificates.ps1` incluido en el directorio de instalación con privilegios de administrador:

```
powershell -ExecutionPolicy Bypass -File "C:\Program Files\Izenpe\Tarjeta
virtual\scripts\install_certificates.ps1"
```

6.5 Verificación manual del KSP

Para comprobar que el KSP de Izenpe está correctamente registrado en el sistema, abra una consola de PowerShell como administrador y ejecute:

```
Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Cryptography\Providers\Izenpe
KSP\UM\00010001"
```

El comando debe devolver una clave `Image` apuntando a `C:\Windows\System32\izenpe_ksp.dll`. Si no devuelve resultado o apunta a una ruta distinta, ejecute la herramienta `IzenpeKspConfig.exe -register` desde el directorio `C:\Program Files\Izenpe\Tarjeta virtual\tools` con permisos de administrador.

7. Notas de la versión 4.1.0

7.1 Cambios acumulados desde la versión 3.0.9

La rama 4.0.x consolida sobre la arquitectura CNG / KSP introducida en 3.x un conjunto de mejoras dirigidas a la operativa real en entornos corporativos. Este capítulo resume las que impactan al equipo IT que despliega y mantiene la aplicación.

7.1.1 ADOBE ACROBAT DC CON MODO PROTEGIDO ACTIVO (V4.0.3)

Se resuelve el bloqueo histórico entre el *sandbox* de Adobe (Protected Mode) y las claves entregadas por Key Storage Providers de terceros. En versiones anteriores era necesario desactivar el Modo Protegido desde las preferencias de Adobe para poder firmar PDFs con Tarjeta Virtual — algo que la mayoría de despliegues corporativos no permiten por política de seguridad (GPO). Desde la versión 4.0.3, la firma funciona con el Modo Protegido activado sin ningún cambio de configuración por parte del usuario o del departamento IT.

Detalle técnico: la propiedad `dwKeySpec` del `CRYPT_KEY_PROV_INFO` vinculado a cada certificado se fija a `AT_SIGNATURE`, permitiendo que Adobe entre por la ruta legacy *brokerizada* y termine en el KSP CNG a través del *broker* del propio Adobe. Chrome, Edge, Office, .NET, Cisco AnyConnect y demás consumidores modernos siguen rutando por CNG directo gracias a la propiedad `CERT_KEY_SPEC_PROP_ID = CERT_NCRYPT_KEY_SPEC` almacenada como propiedad independiente. La versión 4.0.3 incluye además una rutina de migración al arranque que reescribe la propiedad en certificados vinculados antes de la 4.0.3, sin necesidad de re-vinculación por parte del usuario.

7.1.2 FIRMA SILTRA / SHA-1 ACEPTADA POR EL *SIGN BRIDGE* (V4.0.4)

El envío de comunicaciones SILTRA (Sistema de Liquidación Directa de la Tesorería General de la Seguridad Social) firma con SHA-1, algoritmo que versiones anteriores del *sign bridge* de Windows descartaban antes de llegar al HSM. Desde la versión 4.0.4, el bridge acepta hashes SHA-1 (20 bytes crudos y 35 bytes en formato DigestInfo). El HSM de Izenpe autoriza la firma para este algoritmo en el marco del protocolo SILTRA.

El rechazo de firmas de handshake TLS legacy (36 bytes MD5+SHA1) se mantiene. La compatibilidad con firmas modernas (SHA-256, SHA-384, SHA-512) no se ve alterada.

7.1.3 PERSISTENCIA ROAMEABLE EN ENTORNOS VDI (V4.0.6)

Los credenciales de sesión OAuth y los *mappings thumbprint→sign_identity* gestionados por la aplicación se almacenan en el Windows Credential Manager con el flag `CRED_PERSIST_ENTERPRISE` (persistencia en el perfil roaming del usuario), en lugar de `CRED_PERSIST_LOCAL_MACHINE` (persistencia solo local).

Efecto en entornos VDI de tipo *Pooled Non-Persistent* (Citrix Virtual Apps and Desktops, Windows Server RDS, Windows 365 Cloud PC): los credenciales viajan con el perfil del usuario entre las VMs del pool via Citrix User Profile Management (UPM) o el perfil roaming corporativo. Como consecuencia, ambas fichas (Ciudadano y Profesional) permanecen coherentes entre sesiones. En estaciones de trabajo *standalone* sin perfil roaming, Windows degrada silenciosamente a persistencia local — sin cambio observable.

7.1.4 DISTRIBUCIÓN EN FORMATO MSI ADICIONAL (V4.0.X)

Además del instalador Inno Setup `.exe`, se distribuye un paquete `.msi` nativo generado con WiX Toolset. Este formato se integra directamente con las herramientas Microsoft (SCCM, Intune, GPO, Configuration Manager) sin necesidad de *bootstrapper*. Ambos formatos son funcionalmente equivalentes; ver § 4.3.2 para los comandos `msiexec` de instalación y desinstalación desatendida.

7.1.5 PARÁMETROS INFORMATIVOS EN EL FLUJO OAUTH (V4.0.5)

El *endpoint* `authorize` del flujo OAuth añade `app_version`, `app_platform` y `app_arch` como *query params* informativos, para permitir a Giltza (identity provider de Izenpe) el control de versiones y el diagnóstico de incidencias por versión de cliente. Sin PII adicional (los valores son metadatos del binario, no del usuario). Sin cambios en el token exchange ni el refresh. Transparente para el usuario final.

7.1.6 UNIFICACIÓN DEL NÚMERO DE VERSIÓN MULTI-PLATAFORMA (V4.0.8)

A partir de la versión 4.0.8, el número de versión de Windows se alinea con el de las ediciones iOS, macOS y Android publicadas en tienda. No supone ningún cambio funcional en la aplicación Windows respecto a la 4.0.6; únicamente el metadato de versión visible del ejecutable y del instalador.

7.1.7 SESIÓN ESTABLE CON LA APLICACIÓN MINIMIZADA (V4.1.0)

Tarjeta Virtual 4.1.0 corrige dos defectos encadenados que podían provocar que la sesión de un certificado vinculado se perdiera antes de lo esperado durante trámites largos con la ventana minimizada:

1. **Windows Efficiency Mode.** Windows 10 y Windows 11 aplican por defecto `PROCESS_POWER_THROTTLING_EXECUTION_SPEED` al proceso cuando la ventana no está visible, recortando los quantums de CPU y pausando el `Timer.periodic` interno de renovación OAuth. El token OAuth caducaba sin que nadie lo renovara. La versión 4.1.0 opta por no someterse a ese throttling al arrancar (`SetProcessInformation(…, ProcessPowerThrottling, {ControlMask=EXECUTION_SPEED, StateMask=0}, …)` , resuelta dinámicamente con `GetProcAddress` sobre `kernel32.dll` para que el binario siga compilando y arrancando también en Windows anteriores a la build 1809).
2. **Watchdog del flujo de renovación silenciosa.** Un fallo transitorio en la navegación interna del WebView durante la renovación silenciosa podía dejar el flujo colgado indefinidamente, bloqueando todos los refreshes posteriores con el error interno "already in progress". La nueva versión incorpora un watchdog de 60 segundos en el handler del refresh que libera el estado y resetea el flag si la renovación no completa a tiempo, permitiendo al siguiente ciclo operar normalmente. Un solo fallo transitorio ya no deja el sistema bloqueado.

Adicionalmente, el intervalo de reintentos de renovación OAuth se ajusta de 5 a 3 minutos (más margen frente a caídas puntuales del servidor de autenticación), y el umbral de desactivación por sesión antigua sube de 10 a 60 minutos, evitando desactivaciones prematuras ante fallos aislados cuando el token todavía es válido.

La capa criptográfica (KSP, *sign bridge*, cliente HSM, Credential Manager) es byte a byte idéntica a 4.0.9; el cambio se concentra en el ciclo de renovación OAuth del runner nativo y la lógica Dart asociada.

7.2 Compatibilidad con versiones anteriores

La versión 4.1.0 NO es compatible con Tarjeta Virtual 2.x. Si en el equipo existe una instalación previa de esa rama, se recomienda desinstalarla y reiniciar el equipo antes de instalar la nueva versión, para evitar conflictos entre el antiguo proveedor PKCS #11 (`p11rss.dll`) y el Key Storage Provider (`izenpe_ksp.dll`).

Las identidades de firma vinculadas en la rama 2.x deben volver a vincularse en 4.1.0 mediante el procedimiento descrito en el apartado 5.2, ya que el sistema de almacenamiento de tokens es diferente.

La actualización desde cualquier versión 3.0.x o 4.0.x se realiza in-place, sin desinstalar. Los certificados vinculados y la sesión OAuth se conservan. Los credenciales existentes en Credential Manager guardados con `CRED_PERSIST_LOCAL_MACHINE` siguen siendo legibles y se re-almacenan progresivamente con `CRED_PERSIST_ENTERPRISE` en cada operación de escritura (login OAuth, refresh, re-vinculación), sin pérdida de datos ni migración manual necesaria.

> *Soporte: para cualquier incidencia o consulta relacionada con esta aplicación, puede contactar con el Centro de Atención al Usuario de Izenpe a través del sitio web https://www.izenpe.eus o utilizar la opción "Reportar un problema" descrita en el apartado 5.7 de este manual.*

© 2026 Izenpe S.A. — Todos los derechos reservados.