Tarjeta Virtual

v.4.0.8

Manual de instalación y uso

Plataforma macOS

izenpe

CONTENIDO

1. Introducción

2. Casos de uso

    2.1 Publicación de certificados mediante CryptoTokenKit

        2.1.1 Firma de documentos y formularios

        2.1.2 Autenticación SSL/TLS

    2.2 Integración con aplicaciones

        2.2.1 Aplicaciones que usan el almacén del sistema

        2.2.2 Aplicaciones con almacén propio

3. Requisitos de sistema

    3.1 Sistema operativo

    3.2 Ubicación de la aplicación

    3.3 Permisos y privilegios

    3.4 Conectividad de red

    3.5 Navegadores y aplicaciones soportadas

4. Instalación y desinstalación

    4.1 Vías de distribución

    4.2 Instalación desde la Mac App Store

    4.3 Instalación desde el fichero DMG

    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 estado

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 4.0.8

Anexo A. Firefox, AutoFirma e Idazki Desktop (keychain-pkcs11)

1. Introducción

Tarjeta Virtual es una aplicación de escritorio que permite utilizar en un equipo Mac los certificados digitales del usuario custodiados en la nube de Izenpe (**BakQ** y **Profesional en la nube**), de modo que las aplicaciones del sistema puedan emplear dichos certificados y sus claves de firma como si estuvieran instalados localmente.

En la plataforma macOS, la integración con el sistema se realiza mediante **CryptoTokenKit (CTK)**, el mecanismo estándar de Apple para exponer tokens criptográficos al almacén de certificados del sistema. La aplicación incorpora una extensión CTK que publica el certificado de la sesión activa; a partir de ese momento el certificado es visible para Safari, Google Chrome, Adobe Acrobat y cualquier otra aplicación que consulte el Llavero del sistema. La clave privada no abandona en ningún momento la infraestructura de Izenpe: las operaciones de firma se delegan de forma remota.

Este manual describe los casos de uso, los requisitos del sistema, el procedimiento de instalación y desinstalación, la operativa habitual y la resolución de problemas de la aplicación en su versión 4.0.8 para macOS.

2. Casos de uso

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

2.1 Publicación de certificados mediante CryptoTokenKit

Con la aplicación instalada y un certificado activo, el certificado del usuario queda publicado en el almacén del sistema a través de la extensión *CryptoTokenKit* incluida en el paquete de la aplicación. macOS registra esa extensión al detectar la aplicación en la carpeta `/Aplicaciones`, y expone el certificado como un token del sistema.

Las consecuencias prácticas son:

- Los certificados aparecen automáticamente en el selector de certificados de los navegadores y de las aplicaciones de firma.
- Su ciclo de vida se controla desde la propia aplicación: aparecen al activar un certificado y desaparecen al desactivarlo, al caducar la sesión o al salir de la aplicación.
- La aplicación publica únicamente el certificado correspondiente a la sesión activa, evitando entradas duplicadas en el selector del sistema.

Importante

Los certificados gestionados por Tarjeta Virtual no pueden importarse ni eliminarse manualmente desde el Llavero de macOS. Son tokens virtuales publicados por la extensión CTK, y su ciclo de vida se controla exclusivamente desde la aplicación.

2.1.1 FIRMA DE DOCUMENTOS Y FORMULARIOS

Firma de documentos PDF mediante Adobe Acrobat y firma de formularios web desde Safari o Google Chrome. La operación criptográfica se realiza siempre de forma remota contra la infraestructura de Izenpe, sin que la clave privada abandone dicha infraestructura. Desde la versión 4.0.6 la aplicación utiliza padding RSA-PSS cuando el consumidor lo solicita, lo que habilita los escenarios de firma y autenticación de Safari.

2.1.2 AUTENTICACIÓN SSL/TLS

Acceso a sitios remotos que requieran autenticación TLS con certificado de cliente: sedes electrónicas, oficinas virtuales y servicios telemáticos. Al utilizar el almacén del sistema, tanto Safari como Google Chrome presentan el certificado publicado por Tarjeta Virtual en el diálogo de selección de certificado de cliente, sin configuración adicional.

2.2 Integración con aplicaciones

2.2.1 APLICACIONES QUE USAN EL ALMACÉN DEL SISTEMA

Las siguientes aplicaciones consultan el almacén de certificados de macOS y, por tanto, funcionan de manera transparente con Tarjeta Virtual:

- **Safari** — soportado desde la versión 4.0.6 de la aplicación.
- **Google Chrome** — autenticación TLS de cliente.
- **Adobe Acrobat** — firma de documentos PDF.
- Cualquier otra aplicación de macOS que resuelva identidades a través del Llavero del sistema.

2.2.2 APLICACIONES CON ALMACÉN PROPIO

Mozilla Firefox, **AutoFirma** e **Idazki Desktop** no utilizan el almacén de certificados de macOS: Firefox emplea su propio almacén NSS, y AutoFirma e Idazki Desktop se apoyan en el almacén de Java o en el de Firefox según su configuración. En estos casos, la integración requiere una librería puente PKCS #11 que traduzca las peticiones de dichas aplicaciones hacia el Llavero del sistema.

El procedimiento completo de instalación y configuración de esa librería se describe en el **Anexo A** de este manual.

3. Requisitos de sistema

Este capítulo describe los requisitos necesarios para instalar y ejecutar Tarjeta Virtual 4.0.8 en macOS.

3.1 Sistema operativo

Tarjeta Virtual 4.0.8 requiere **macOS 11.5 o posterior**. La aplicación se distribuye como binario universal y funciona tanto en equipos Mac con procesador Intel como en equipos con chip de Apple.

No se proporciona soporte para versiones anteriores de macOS.

3.2 Ubicación de la aplicación

> **Importante**
>
> La aplicación **debe residir en la carpeta** `/Aplicaciones`. macOS solo registra la extensión de CryptoTokenKit de una aplicación instalada en esa ubicación. Si la aplicación se ejecuta desde la imagen del DMG, desde la carpeta Descargas o desde cualquier otra ruta, la extensión CTK no se registra y **los certificados no se publican en el almacén del sistema**: no aparecerán en Safari, Chrome ni Adobe Acrobat, aunque en la propia aplicación el certificado figure como activo.

Esta es, con diferencia, la causa más frecuente de incidencias del tipo "la aplicación dice que el certificado está activo, pero el navegador no lo ve". La solución consiste en cerrar la aplicación, copiarla o moverla a `/Aplicaciones` y volver a abrirla desde allí.

3.3 Permisos y privilegios

La instalación de Tarjeta Virtual **no requiere permisos de administrador**: la aplicación se ejecuta en el contexto del usuario y no instala componentes en rutas del sistema ni extensiones de kernel. La extensión CTK se registra automáticamente a partir del propio paquete de la aplicación.

Los certificados se publican en el almacén del usuario que ejecuta la aplicación. En equipos compartidos, cada usuario debe vincular y activar sus propios certificados.

La librería puente `keychain-pkcs11` descrita en el Anexo A sí requiere privilegios de administrador, ya que su instalador escribe en `/usr/local/lib`. Se trata de un componente opcional y ajeno a Izenpe.

3.4 Conectividad de red

Tarjeta Virtual requiere **salida HTTPS hacia los servicios de Izenpe** para autenticar al usuario, mantener la sesión y ejecutar las operaciones de firma remota. Sin conectividad, la aplicación mostrará el estado "Desconectado" en la barra de estado y los certificados no podrán activarse.

Destino	Protocolo	Puerto
eidas.izenpe.com	HTTPS	443
eidas-prof.izenpe.eus	HTTPS	443
servicios.izenpe.com	HTTPS	443

Los dos primeros destinos son los que la aplicación utiliza para identificar al usuario y para firmar: **eidas.izenpe.com** para el certificado ciudadano (BakQ) y **eidas-prof.izenpe.eus** para el certificado profesional. Si alguno de ellos no es accesible, los certificados de ese tipo no podrán activarse. El tercero solo interviene en la comprobación de funcionamiento descrita más adelante.

La aplicación respeta la configuración de red y de proxy definida en el sistema. En entornos corporativos con cortafuegos o inspección TLS, el responsable de sistemas debe garantizar que el equipo del usuario alcance los servicios de Izenpe sin que la conexión sea interceptada por un certificado de inspección no confiable.

3.5 Navegadores y aplicaciones soportadas

Aplicación	Versiones soportadas	Notas
Safari	Últimas versiones	Almacén del sistema (desde 4.0.6)
Google Chrome	Últimas versiones	Almacén del sistema
Adobe Acrobat	DC y posteriores	Almacén del sistema, firma de PDF
Mozilla Firefox	Últimas versiones	Requiere keychain-pkcs11 (Anexo A)
AutoFirma	Últimas versiones	Requiere keychain-pkcs11 (Anexo A)
Idazki Desktop	Últimas versiones	Requiere keychain-pkcs11 (Anexo A)

4. Instalación y desinstalación

4.1 Vías de distribución

Tarjeta Virtual para macOS se distribuye por dos vías oficiales, funcionalmente equivalentes:

Vía	Origen	Uso recomendado
Mac App Store	Tienda de aplicaciones de Apple	Instalación y actualización automáticas por el usuario
Imagen de disco DMG	Sitio web de Izenpe	Equipos sin acceso a la App Store o despliegue controlado

Ambas distribuciones contienen la misma aplicación, firmada y notarizada, e incluyen la extensión de CryptoTokenKit. La diferencia está únicamente en el canal de entrega y en el mecanismo de actualización.

4.2 Instalación desde la Mac App Store

1. Abra la aplicación **App Store** en el Mac.
2. Busque **Tarjeta virtual** y verifique que el editor es **IZENPE S.A.**
3. Pulse **Obtener** y confirme la instalación.

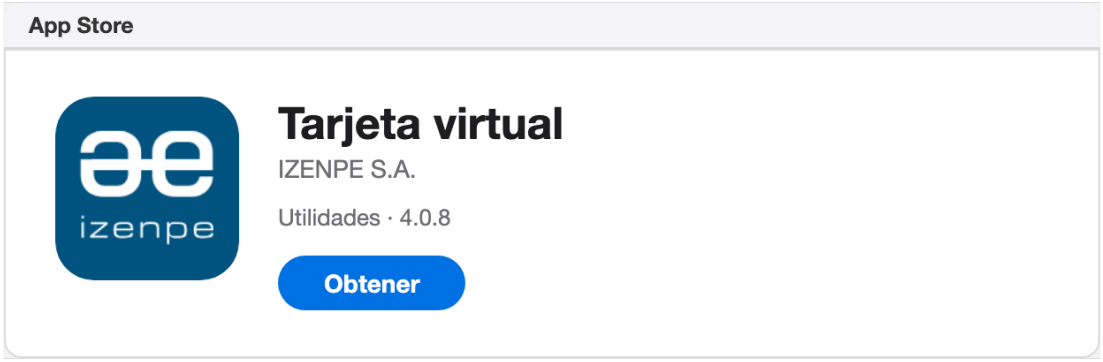


Figura 1 — Ficha de Tarjeta Virtual en la Mac App Store (versión 4.0.8, editor IZENPE S.A.).

La App Store instala siempre la aplicación en `/Aplicaciones`, por lo que el requisito de ubicación descrito en el apartado 3.2 se cumple de forma automática. Las actualizaciones se gestionan también desde la tienda.

4.3 Instalación desde el fichero DMG

La aplicación puede descargarse igualmente como imagen de disco (`.dmg`) desde el sitio web de Izenpe. El procedimiento es el siguiente:

1. Haga doble clic sobre el fichero `.dmg` descargado para montar la imagen.
2. **Arrastre el icono de Tarjeta Virtual sobre la carpeta Aplicaciones** que se muestra en la misma ventana.
3. Expulse la imagen de disco una vez finalizada la copia.
4. Abra la aplicación desde `/Aplicaciones` (Finder o Launchpad).

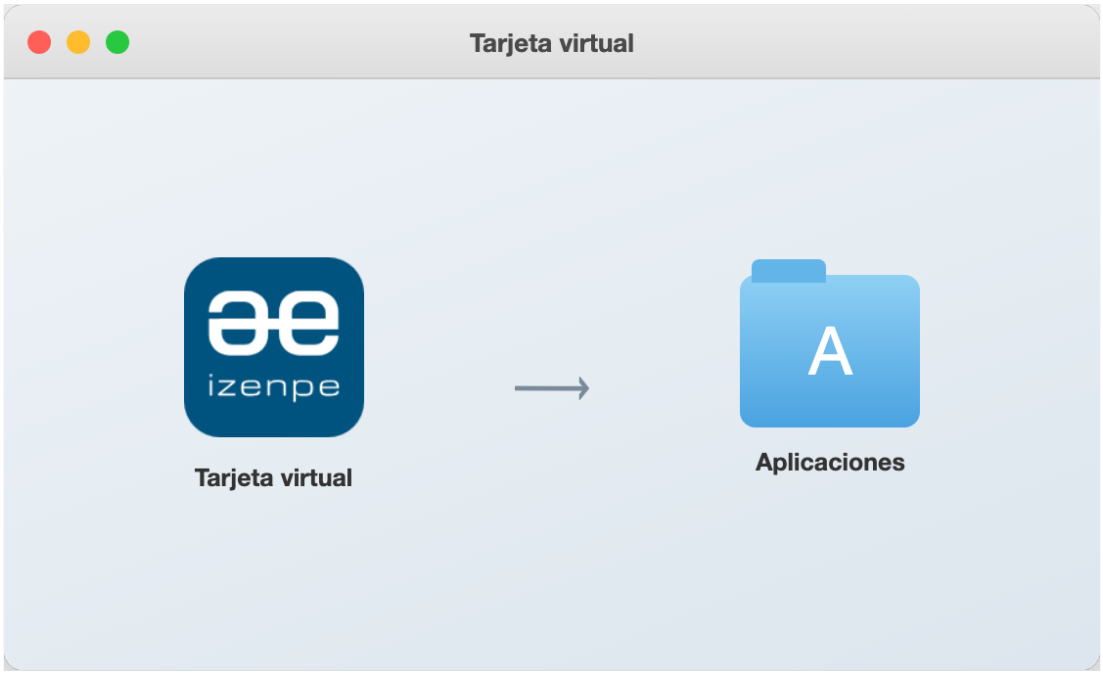


Figura 2 — Ventana del DMG: arrastrar la aplicación a la carpeta Aplicaciones.

Importante

No ejecute la aplicación desde la propia ventana del DMG ni desde la carpeta Descargas. En esas ubicaciones la extensión de CryptoTokenKit no se registra y los certificados no llegan a publicarse en el sistema. Copie siempre la aplicación a `/Aplicaciones` antes de abrirla.

Nota

La primera apertura de una aplicación descargada de Internet está sujeta a la verificación de Gatekeeper. El paquete DMG está firmado con el identificador de desarrollador de Izenpe y **notarizado por Apple**, por lo que macOS se limita a pedir una confirmación indicando que la aplicación no contiene software malicioso: basta con pulsar **Abrir**. No es necesario desactivar Gatekeeper ni autorizar la aplicación manualmente.

4.4 Desinstalación

Para desinstalar la aplicación:

- Arrastre **Tarjeta virtual** desde la carpeta `/Aplicaciones` a la **Papelera**.
- Si se instaló desde la Mac App Store, puede eliminarse también desde el **Launchpad**, manteniendo pulsado el icono y usando el aspa de borrado.

Al eliminarse la aplicación, macOS deja de registrar su extensión CTK y los certificados dejan de estar publicados en el almacén del sistema. Las identidades permanecen intactas en la nube de Izenpe y pueden volver a vincularse tras una reinstalación.

5. Uso

Este capítulo describe la operativa habitual con la aplicación, 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 la carpeta `/Aplicaciones` o desde el Launchpad. La ventana principal tiene un tamaño fijo — 500×680 píxeles mientras se muestra el mensaje de bienvenida y 500×500 una vez este desaparece — y **no es redimensionable ni minimizable**, en coherencia con el resto de plataformas.

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 estado. Bajo la franja se muestran las dos tarjetas de certificado disponibles, todavía sin vincular. En ejecuciones posteriores, la franja de bienvenida ya no se muestra.



Figura 3 — Pantalla principal en la primera ejecución, con la franja de bienvenida visible.

5.2 Vincular un certificado

Tarjeta Virtual permite vincular dos tipos de certificado:

- **DNI / NIE, contraseña y código SMS:** certificado de ciudadano, cuya identificación se realiza mediante **BakQ**.
- **Profesional en la nube:** certificado profesional asociado a una organización, para empleados públicos y profesionales colegiados o autónomos.

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

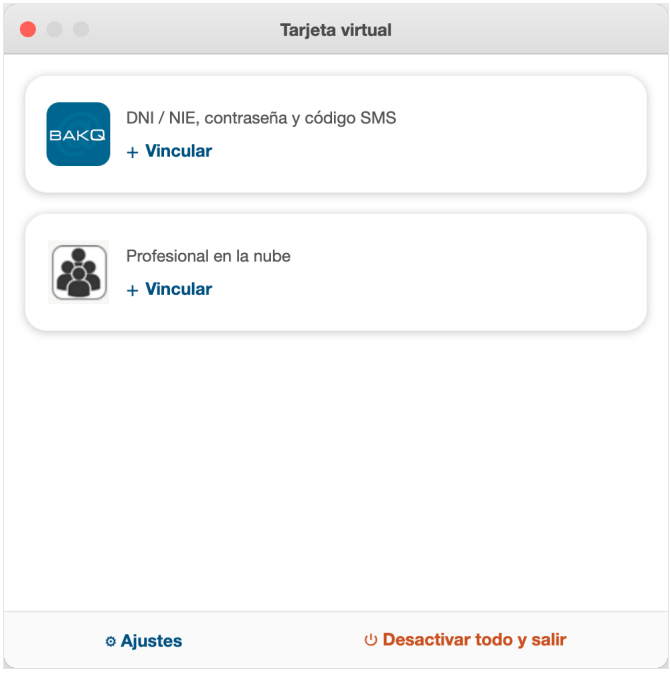


Figura 4 — Pantalla principal con ambos certificados sin vincular.

Al pulsar sobre la tarjeta correspondiente se abre, dentro de la propia aplicación, la ventana de identificación de Izenpe:

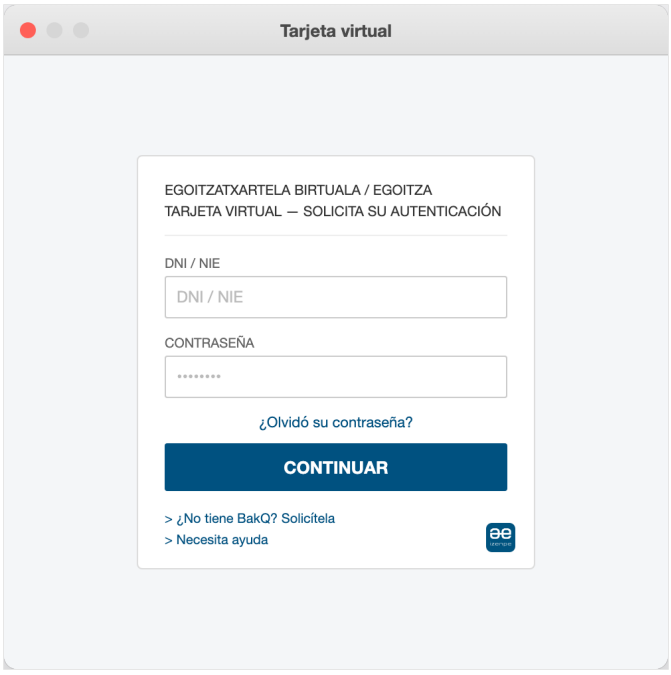


Figura 5 — Ventana de identificación de Izenpe (BakQ).

Una vez introducidas las credenciales y completado el proceso de identificación de doble factor (en BakQ, mediante código SMS), el certificado queda vinculado y aparece en la pantalla principal con su botón de encendido.

La vinculación se realiza una sola vez por certificado. Las credenciales no se almacenan localmente: la aplicación conserva únicamente las credenciales de sesión necesarias para renovar el acceso de forma transparente.

5.3 Activar y desactivar certificados

Una vez vinculado, la tarjeta del certificado muestra el nombre del titular, su identificador (DNI / NIE en el certificado de ciudadano, o el nombre de la organización en el profesional) y un **botón de encendido** circular que refleja el estado y permite conmutarlo:

- **Botón verde:** el certificado está activo. Ha sido publicado en el almacén del sistema mediante la extensión CTK y todas las aplicaciones del equipo pueden utilizarlo.
- **Botón gris:** el certificado está vinculado pero desactivado. No es visible para las aplicaciones del sistema y no puede emplearse para firmar ni autenticarse.



Figura 6 — Certificado de ciudadano (BakQ) vinculado y activo.

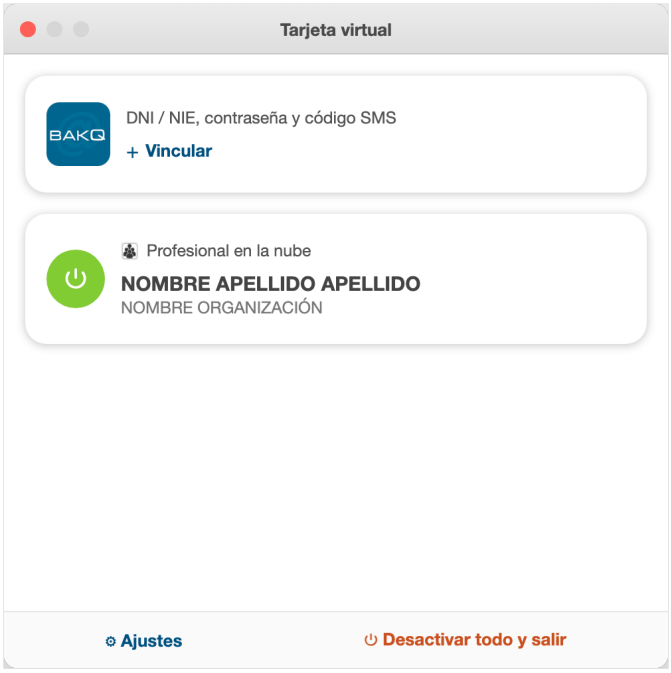


Figura 7 — Certificado profesional en la nube, vinculado y activo.



Figura 8 — Certificado vinculado pero desactivado (botón gris).

Nota

La sesión asociada a un certificado activo tiene una duración de **15 minutos**. Transcurrido ese tiempo, la sesión caduca, el certificado se retira del almacén del sistema y deja de estar disponible para las aplicaciones. Para reactivarlo basta con pulsar de nuevo el botón de encendido de su tarjeta.

Cuando el equipo despierta de un estado de suspensión, la aplicación renueva automáticamente la sesión de los certificados activos, sin intervención del usuario.

5.4 Acceso a sedes electrónicas

Con un certificado activo, el usuario puede acceder a cualquier sede electrónica desde su navegador habitual (Safari, Google Chrome…). Al solicitarse la autenticación TLS de cliente, el navegador presenta el certificado publicado por Tarjeta Virtual junto al resto de identidades del almacén del sistema.

No es necesario que la ventana principal esté visible; basta con que la aplicación se esté ejecutando, lo cual puede comprobarse mediante el icono de la barra de estado.

> **Nota**
>
> Para validar el funcionamiento de extremo a extremo, Izenpe proporciona una herramienta de prueba: acceda a https://servicios.izenpe.com/, entre en *Herramientas de certificados digitales* y seleccione *Probar identificación*.

5.5 Icono de la barra de estado

Mientras la aplicación está en ejecución se mantiene visible un icono en la barra de estado de macOS, en la esquina superior derecha de la pantalla. Al pulsar sobre él se despliega un menú que indica el estado actual:

- **Conectado:** existe al menos un certificado activo y la aplicación mantiene conexión con los servicios de Izenpe.
- **Desconectado:** no hay ningún certificado activo o no hay conexión con los servicios de Izenpe.
- **Verificando:** la aplicación está comprobando la conectividad o renovando la sesión.

El menú incluye además las acciones **Mostrar aplicación**, **Ocultar aplicación** y **Salir**.

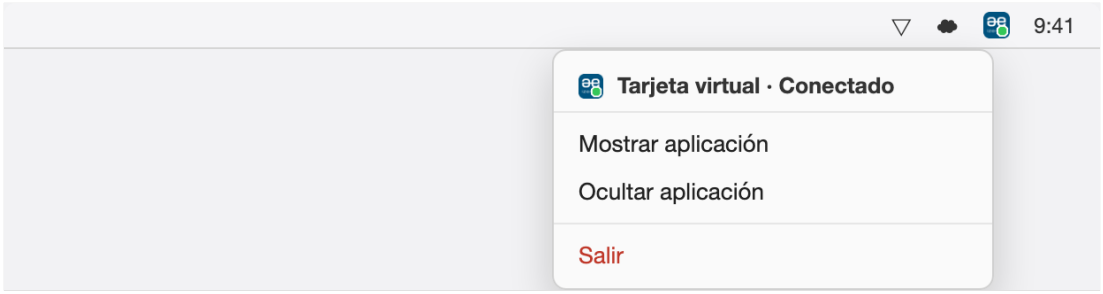


Figura 9 — Icono en la barra de estado de macOS y menú asociado.

5.6 Ajustes de la aplicación

La pantalla **Ajustes**, accesible desde el botón del mismo nombre situado en la parte 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.

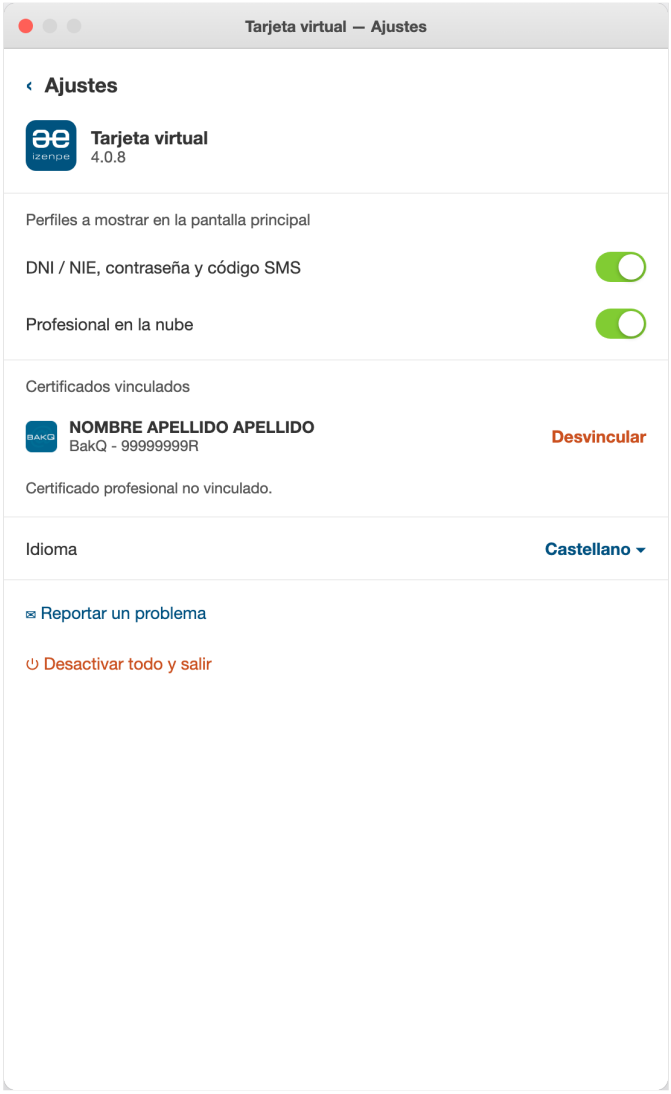


Figura 10 — Pantalla de Ajustes de la aplicación.

- **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 mediante la opción *Desvincular*.
- **Idioma:** permite conmutar entre Castellano y Euskera. El cambio se aplica de forma inmediata, sin 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 utilizando la aplicación, puede notificarlo directamente al equipo de soporte de Izenpe desde la pantalla **Reportar un problema**, accesible desde Ajustes.

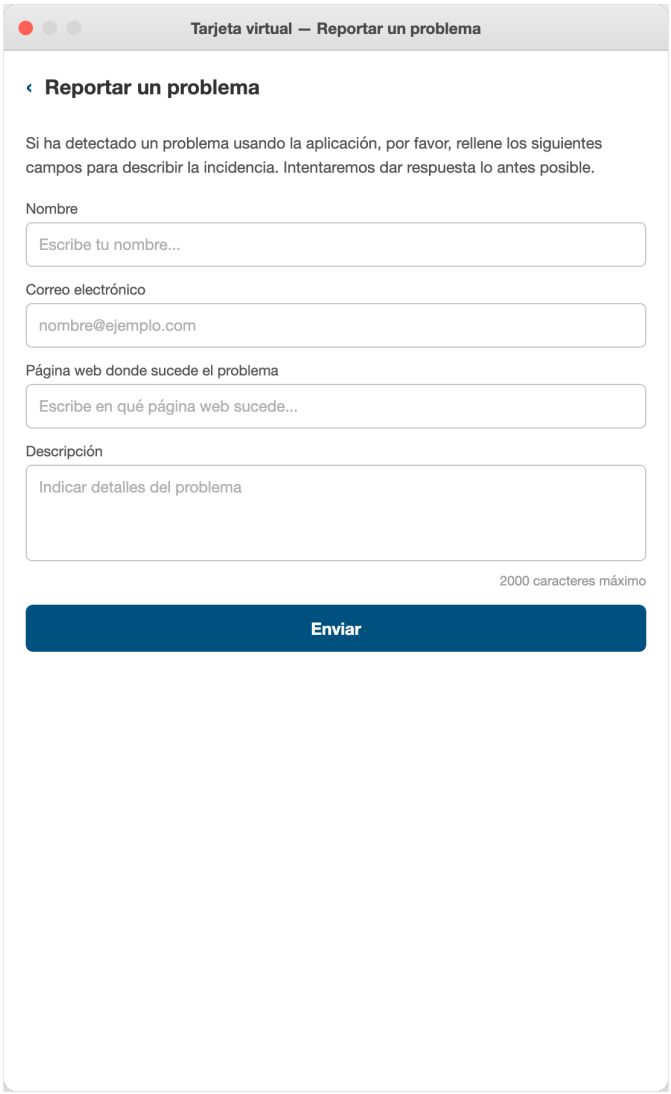


Figura 11 — Formulario para reportar un problema al equipo de soporte.

El reporte se envía al sistema de atención de Izenpe junto con metainformación técnica del entorno (versión de macOS, versión de la aplicación e identificador anónimo del equipo) 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 dos vías:

- Pulsar **Desactivar todo y salir**, disponible en el pie de la ventana principal y en la pantalla de Ajustes.

- Pulsar sobre el icono de la barra de estado y seleccionar **Salir**.

Importante

Cerrar la ventana principal con el botón rojo NO cierra la aplicación: la oculta, manteniendo activos los certificados que lo estuvieran y, por tanto, publicados en el almacén del sistema. Esto permite que el navegador y el resto de aplicaciones sigan utilizándolos sin tener la ventana abierta. Para finalizar realmente la aplicación debe emplearse alguna de las dos opciones anteriores.

6. Resolución de problemas

Este capítulo recoge las incidencias más habituales durante la instalación o el uso de la aplicación, y la forma de resolverlas.

6.1 Los certificados no aparecen en Safari, Chrome ni Adobe Acrobat

Causa más frecuente: la aplicación no está instalada en la carpeta `/Aplicaciones`. macOS solo registra la extensión de CryptoTokenKit de las aplicaciones ubicadas en esa carpeta; si la aplicación se ejecuta desde la imagen del DMG, desde Descargas o desde cualquier otra ruta, el certificado nunca llega a publicarse en el almacén del sistema, aunque la propia aplicación lo muestre como activo.

Solución:

1. Salga completamente de la aplicación (*Desactivar todo y salir*, o *Salir* desde el icono de la barra de estado).
2. Expulse la imagen del DMG si sigue montada.
3. Copie o mueva **Tarjeta virtual** a la carpeta `/Aplicaciones`.
4. Abra la aplicación desde `/Aplicaciones`, vincule o active de nuevo el certificado y reinicie el navegador o la aplicación de firma.

Si el problema persiste con la aplicación ya en `/Aplicaciones`, compruebe que el certificado figura como activo (botón verde) y que la sesión no ha caducado (apartado 6.2), y cierre y vuelva a abrir por completo la aplicación cliente: los navegadores y Adobe consultan el almacén del sistema al arrancar.

6.2 El certificado deja de funcionar al cabo de un rato

Causa: la sesión de un certificado activo tiene una duración de **15 minutos**. Al caducar, el certificado se retira del almacén del sistema y las aplicaciones dejan de verlo.

Solución: abra Tarjeta Virtual y pulse de nuevo el botón de encendido de la tarjeta del certificado para reactivarlo. Si el equipo ha estado suspendido, la aplicación renueva la sesión automáticamente al despertar; en ese caso no es necesaria ninguna acción.

6.3 Firefox, AutoFirma o Idazki Desktop no ven los certificados

Causa: estas aplicaciones no utilizan el almacén de certificados de macOS, sino almacenes propios (NSS en el caso de Firefox, y el almacén de Java o el de Firefox en AutoFirma e Idazki Desktop). Por tanto, no pueden consultar los tokens publicados por CryptoTokenKit.

Solución: instalar y configurar la librería puente PKCS #11 `keychain-pkcs11` según el procedimiento descrito en el **Anexo A** de este manual.

6.4 macOS impide abrir la aplicación descargada (Gatekeeper)

Causa: el fichero descargado ha perdido la firma o la notarización —por ejemplo, si se ha recomprimido o se ha transferido a través de un sistema que altera el contenido—, o bien el equipo no puede consultar el servicio de notarización de Apple.

Solución: descargue de nuevo el DMG desde la web de Izenpe sin manipularlo. Si aun así macOS impide abrir la aplicación, acceda a *Ajustes del Sistema* > *Privacidad y seguridad* (en macOS 12 y anteriores, *Preferencias del Sistema* > *Seguridad y privacidad*, pestaña *General*): aparecerá un mensaje indicando que se ha bloqueado la apertura de Tarjeta Virtual y un botón **Abrir igualmente**.

Si la aplicación se instala desde la Mac App Store, esta situación no se produce.

6.5 La aplicación muestra el estado "Desconectado"

Causa: la aplicación no consigue alcanzar los servicios de Izenpe. Suele deberse a falta de conectividad, a un proxy corporativo mal configurado o a un cortafuegos que bloquea la salida HTTPS.

Solución: verifique la conectividad general del equipo y compruebe con el responsable de sistemas que el acceso HTTPS (puerto 443) a los servicios de Izenpe está permitido, y que la conexión no está siendo interceptada por un proxy de inspección TLS con un certificado no confiable para el equipo.

7. Notas de la versión 4.0.8

7.1 Principales cambios

7.1.1 SOPORTE DE SAFARI (V4.0.6)

Desde la versión 4.0.6, los certificados publicados por Tarjeta Virtual son utilizables desde **Safari**, tanto para autenticación TLS de cliente como para firma. Esto se debe a la adopción del esquema de relleno RSA-PSS cuando el consumidor lo solicita, requisito de las APIs criptográficas empleadas por Safari. Las versiones anteriores de la aplicación no soportaban este navegador.

7.1.2 RENOVACIÓN DE SESIÓN TRAS LA SUSPENSIÓN (V4.0.6)

La aplicación detecta el despertar del equipo tras un estado de suspensión y renueva automáticamente la sesión de los certificados activos. Con ello se evita que el usuario tenga que reactivar el certificado manualmente cada vez que abre la tapa del portátil.

7.1.3 PUBLICACIÓN DE UN ÚNICO CERTIFICADO EN CTK (V4.0.6)

La extensión de CryptoTokenKit publica exclusivamente el certificado correspondiente a la sesión activa. Con ello se evita que el selector de certificados del sistema muestre varias entradas simultáneas y que el usuario elija una identidad que no corresponde a la sesión vigente.

7.1.4 DISTRIBUCIÓN EN LA MAC APP STORE (V4.0.8)

Además de la imagen DMG descargable desde el sitio web de Izenpe, la aplicación se distribuye a través de la **Mac App Store**. Este canal garantiza que la aplicación se instale siempre en `/Aplicaciones` y simplifica la gestión de actualizaciones.

7.2 Requisitos y compatibilidad

La versión 4.0.8 requiere macOS 11.5 o posterior. Es condición indispensable que la aplicación resida en la carpeta `/Aplicaciones` para que la extensión de CryptoTokenKit se registre y los certificados se publiquen en el almacén del sistema.

Las aplicaciones que emplean almacenes de certificados propios (Mozilla Firefox, AutoFirma e Idazki Desktop) requieren la configuración adicional descrita en el Anexo A.

Anexo A. Firefox, AutoFirma e Idazki Desktop (keychain-pkcs11)

Mozilla Firefox, AutoFirma e Idazki Desktop no consultan el almacén de certificados de macOS, por lo que no pueden ver directamente los certificados publicados por Tarjeta Virtual mediante CryptoTokenKit. Para utilizarlos desde estas aplicaciones es necesario instalar una **librería puente PKCS #11** llamada `keychain-pkcs11`, que traduce las peticiones PKCS #11 de dichas aplicaciones hacia el Llavero del sistema.

Importante

`keychain-pkcs11` es software desarrollado por un tercero, **ajeno a Izenpe**. Izenpe facilita el paquete de instalación por comodidad del usuario, pero no es el autor de la librería ni presta soporte sobre su código. Su instalación es opcional y solo necesaria si se van a utilizar Firefox, AutoFirma o Idazki Desktop.

A.1 Descarga e instalación del paquete

1. Acceda a la web de documentación técnica de Izenpe: https://www.izenpe.eus/soporte-y-documentacion-tecnica/webize01-cndoctecnica/es/
2. Localice y descargue el paquete **keychain-pkcs11** para macOS.
3. Ejecute el instalador descargado y siga los pasos del asistente. El proceso solicita credenciales de administrador, ya que la librería se copia en una ruta del sistema.
4. Al finalizar, verifique que existe el fichero:

```
/usr/local/lib/keychain-pkcs11.dylib
```

Tras la instalación, configure cada aplicación según los apartados siguientes.

A.2 Configuración de Mozilla Firefox

Firefox utiliza su propio almacén NSS y admite la carga de módulos PKCS #11 externos. Para registrar la librería puente:

1. Abra Firefox y acceda a *Preferencias* (o *Ajustes*, según la versión).
2. Entre en **Privacidad y seguridad**.

3. Desplácese hasta la sección **Certificados** y pulse **Dispositivos de seguridad**.
4. Pulse **Cargar**.
5. En *Nombre del módulo* escriba:

   ```
   Keychain PKCS11 Bridge
   ```

6. En *Nombre de archivo del módulo* indique la ruta de la librería:

   ```
   /usr/local/lib/keychain-pkcs11.dylib
   ```

7. Acepte. El módulo aparecerá en la lista de dispositivos de seguridad.

Con Tarjeta Virtual en ejecución y un certificado activo, los certificados serán visibles desde Firefox a través de este módulo.

Nota

Recuerde que el certificado debe estar **activo** en Tarjeta Virtual (botón verde) en el momento de utilizarlo desde Firefox. Si la sesión ha caducado (15 minutos), reactívelo desde la aplicación.

A.3 Configuración de AutoFirma

AutoFirma puede utilizar distintos almacenes de claves. Para trabajar con los certificados de Tarjeta Virtual a través de la librería puente, debe emplearse el almacén de Firefox, en el que previamente se ha registrado el módulo PKCS #11 según el apartado A.2.

1. Complete primero la configuración de Firefox descrita en el apartado A.2.
2. Abra AutoFirma.
3. En el momento de seleccionar el origen de los certificados, elija el **almacén de claves de Mozilla Firefox** en lugar del almacén del sistema.
4. Seleccione el certificado de Tarjeta Virtual en la lista que se muestre.

A.4 Configuración de Idazki Desktop

Idazki Desktop localiza los módulos PKCS #11 mediante un fichero de configuración incluido en su propio paquete de aplicación.

1. Instale previamente la librería puente según el apartado A.1.
2. Localice el fichero de configuración dentro del paquete de la aplicación, en la ruta:

```
Idazki Protocolo/Contents/Java/pcks11.properties
```

3. Verifique que dicho fichero hace referencia a la librería instalada en `/usr/local/lib/keychain-pkcs11.dylib`.
4. Reinicie Idazki Desktop para que la configuración surta efecto.

Si el fichero no recoge la ruta correcta o la aplicación sigue sin mostrar los certificados, contacte con el Centro de Atención al Usuario de Izenpe.

> *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.