



Instalación Kit Izenpe

Manual de usuario

 IZENPE
Beato Tomás de Zumarraga 71 - 1ª Planta
01008 Vitoria - Gasteiz
Tel.: 945 067 723
www.izenpe.com





Sumario

Glosario	3
Introducción	5
A quién va dirigido este documento	5
Antes de comenzar.....	5
Instalación	6
Instalación desatendida	8
Problemas durante la instalación.....	8
Fin de la instalación.....	9



Glosario

Autoridad de Certificación: Es la entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica. La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Caducidad del certificado digital: El certificado digital tiene un período de vigencia que consta en el mismo certificado. Generalmente es de 2 años, aunque por ley se permite una vigencia de hasta 5 años. Una vez el certificado haya caducado, no se podrán utilizar los servicios ofrecidos por la Administración que requieran firma electrónica, y cualquier firma electrónica que se haga a partir de ese momento no tendrá validez.

Certificado digital: Documento en soporte informático emitido y firmado por la Autoridad de Certificación, que garantiza la identidad de su propietario.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Firma electrónica: Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Existen 3 tipos de firma electrónica: firma electrónica simple, avanzada y reconocida.

Firma electrónica simple: Conjunto de datos, en forma electrónica, anejos a otros datos.

Firma electrónica avanzada: Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.



Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Listas de Revocación de Certificados o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

No repudio: El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de la clave privada que únicamente conoce él y que está obligado a custodiar. El no repudio permite, además, comprobar quién participó en una transacción.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero

Prestador de Servicios de Certificación o PSC: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Ver Autoridad de Certificación.

PIN: Secuencia de caracteres que permiten el acceso a los certificados. Número de Identificación Personal, en ocasiones llamado NIP.

PUK: Secuencia de caracteres que permiten el cambio o desbloqueo del PIN. Clave Personal de Desbloqueo.

Renovación: La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, antes de la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación: Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las claves. La revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Estas listas son públicas y deben estar siempre disponibles.

Tarjeta inteligente (smartcard): Cualquier tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.



Introducción

Este manual describe y sirve de guía para llevar a cabo de manera exitosa el proceso de instalación del Kit Izenpe para el uso de las tarjetas criptográficas Izenpe, y que consta de dos componentes:

- **Izenpe Middleware:** librerías que permiten a cualquier aplicación del Sistema Operativo operar con las tarjetas criptográficas mencionadas
- **Izenpe Card Manager:** aplicación para la gestión de la tarjeta, que permite realizar operaciones como cambio de PIN o PUK, desbloqueo de PIN, obtener información sobre la tarjeta,...

Las funcionalidades de esta aplicación vienen descritas con detalle en el manual de usuario de Izenpe Card Manager.

El asistente de instalación del Kit Izenpe le guiará de una manera sencilla en el proceso de instalación.

A quién va dirigido este documento

- *Usuarios finales*, que desean utilizar la tarjeta con chip de Izenpe

Antes de comenzar

Asegúrese de disponer de:

- Disponer de un lector de tarjetas estándar, compatible PC/SC que se encuentre correctamente conectado, instalado y configurado.
- Disponer de la última versión del Kit Izenpe
- Para poder realizar la instalación, es indispensable poseer permisos de Administrador. En caso de no poseerlos la instalación será denegada.



Instalación

La aplicación estará accesible a través de la web de Izenpe, a través del apartado “Gestiona tu certificado” > Puesta en marcha de un Certificado

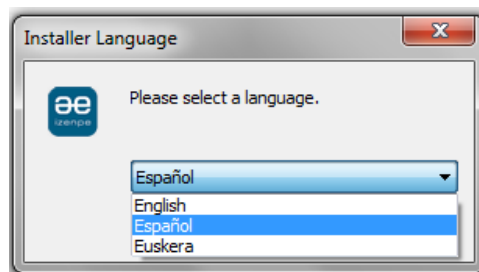


Descargue el instalador correspondiente a Windows, y ejecútelo en su equipo. Si se le solicita, permita la ejecución de la aplicación.

Selección del idioma

Una vez ejecutada la aplicación se solicita al usuario la selección del idioma en el que se va a instalar la aplicación. Idiomas disponibles:

- Español
- Euskera
- Ingles



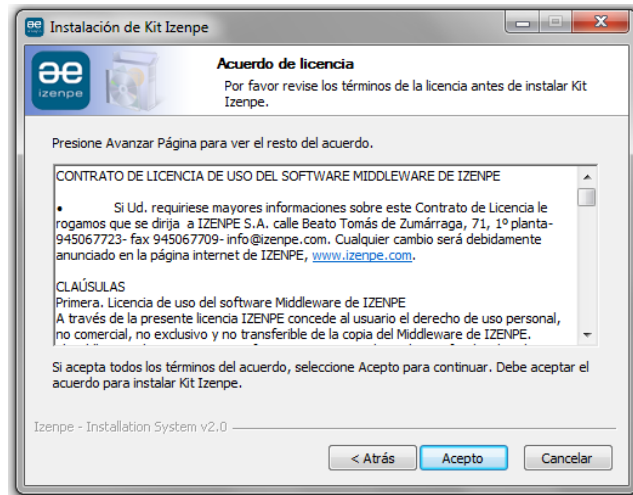
Seleccione el idioma y pulse OK. Se iniciará el Asistente de instalación que le guiará en el proceso. **Se recomienda cerrar cualquier otra aplicación antes de continuar con el proceso de instalación.**

Asistente de instalación

Bienvenido al Asistente de Instalación de Kit Izenpe. Haga click en Siguiente para continuar.



Revise los términos del acuerdo de licencia y haga click en Acepto para continuar



Automáticamente se instalaran todos los componentes del Kit Izenpe (Izenpe Middleware y Gestión de la Tarjeta).



Presione terminar para cerrar el asistente



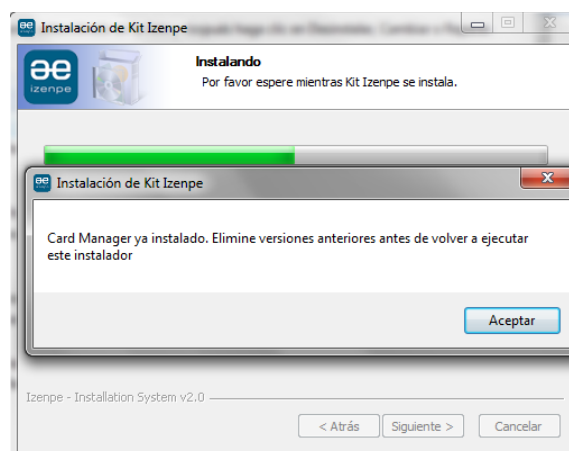
Instalación desatendida

Para poder realizar una instalación desatendida basta con introducir en el cuadro de comandos el instalador pasándole como parámetro “/S”.

ATENCIÓN: debido a las limitaciones de interacción de una instalación desatendida, es necesario eliminar versiones anteriores o incompatibles (SafeSign) antes de proceder. Así mismo, se debe forzar el reinicio de la máquina una vez concluida la instalación.

Problemas durante la instalación

Es posible que tenga versiones anteriores de la aplicación de Gestión de la tarjeta (Izenpe Card Manager) instaladas en su equipo, por lo que se le solicitará que elimine versiones anteriores antes de ejecutar el instalador. Elimine dichas versiones y ejecute de nuevo el instalador.





Fin de la instalación

Una vez finalizado el proceso de instalación se creará un acceso directo en el escritorio de la aplicación Izenpe Card Manager (Gestión de la tarjeta) que le permitirá realizar cualquier tipo de operación con la misma. Para mayor información, consulte el manual de uso de la aplicación.



Así mismo podrá acceder a la aplicación Izenpe Card Manager a través de:

Inicio > Programas > Izenpe > Izenpe Card Manager > Gestión de la tarjeta.

