



# Izenpe PIN Manager

## Manual de usuario – Mac OS X



## Sumario

Glosario .....	3
Introducción .....	5
A quién va dirigido este documento .....	5
Antes de comenzar.....	5
Funcionalidades .....	6
Tabla de funciones .....	6

#

## 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 el uso de la aplicación Izenpe PIN Manager (Gestión de la tarjeta), que permite realizar una serie de funciones sobre los dispositivos criptográficos soportados por las librerías contenidas dentro del Izenpe Middleware.

## A quién va dirigido este documento

- *Usuarios finales*, que desean gestionar su tarjeta, cambiar el PIN, importar certificados, ...

## Antes de comenzar

Asegúrese de disponer de la última versión de

- **Izenpe PIN Manager**
- **Izenpe Middleware**

Por lo general ambos componentes se suministran dentro de un Kit único.

Izenpe PIN Manager requiere un lector de tarjetas estándar, compatible PC/SC, que se encuentre correctamente conectado, instalado y configurado antes de comenzar.

## Funcionalidades

Izenpe PIN Manager dispone de múltiples funcionalidades, accesibles desde la pantalla principal:



[Imagen 1]

### Tabla de funciones

La siguiente tabla resume las funciones expuestas en la pantalla principal de Izenpe PIN Manager.

Función	Descripción
Cambiar PIN	Función para cambiar el PIN de la tarjeta (ver imagen 2)
Cambiar PUK	Función para cambiar el PUK de la tarjeta (ver imagen 3)
Desbloquear PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma (ver imagen 4)
Información de la tarjeta	Ventana que muestra información sobre la tarjeta (modelo, número de serie, identificación del fabricante y etiqueta) (ver imagen 5)

### ***Cambiar PIN***

Introduzca el PIN antiguo de la tarjeta y el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.



The screenshot shows a window titled "PIN Manager" with the "ae izenpe" logo and a SIM card icon. The "Cambiar PIN" tab is selected. It contains three input fields: "PIN actual:", "Nuevo PIN:", and "Repetir nuevo PIN:". Below the fields are three buttons: "Información", "Vaciar", and "Cambiar".

[Imagen 2]

### ***Cambiar PUK***

Introduzca el PUK antiguo de la tarjeta y el nuevo PUK. El nuevo PUK tiene que tener entre 6 y 8 dígitos alfanuméricos.



The screenshot shows the same "PIN Manager" window, but with the "Cambiar PUK" tab selected. It contains three input fields: "PUK actual:", "Nuevo PUK:", and "Repetir nuevo PUK:". Below the fields are three buttons: "Información", "Vaciar", and "Cambiar".

[Imagen 3]

### **Desbloquear PIN**

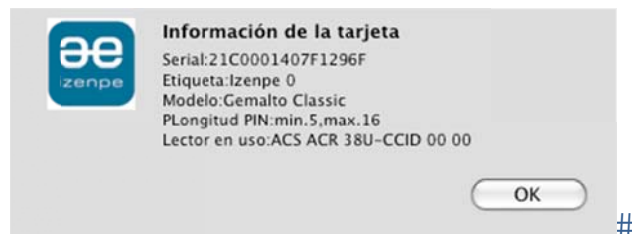
Para desbloquear el PIN, introduzca el PUK de la tarjeta e introducir el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.



[Imagen 4]

### **Información de la tarjeta**

Ofrece información detallada de la tarjeta: modelo, número de serie, fabricante y etiqueta. Es posible que el CAU le solicite dicha información para conocer el tipo de tarjeta que está utilizando.



[Imagen 5]