

Manual do Usuário Linux

Kit de Middleware Universal Bit4id

Índice

- [1. introdução](#)
 - [1.1 Para quem é este documento?](#)
- [2. Antes de começar](#)
- [3. Instalação](#)
 - [3.1 Assistente de Instalação do Gerenciador PKI](#)
- [4. Problemas durante a instalação](#)
- [5. Configuração no Firefox](#)
- [6. Antes de começar a usar o Kit Bit4id](#)
- [7. Recursos](#)
 - [7.1 Tabela de recursos](#)
- [8. Perguntas frequentes](#)
- [9. Glossário](#)

1. introdução

Este manual serve como um guia para concluir com êxito o processo de instalação do Bit4id Kit para o uso de cartões criptográficos e o procedimento para acessar e usar o aplicativo de gerenciamento. O Kit Bit4id consiste nos seguintes componentes:

- **Bit4id Middleware:** bibliotecas que permitem que qualquer aplicativo do sistema operacional opere com cartões criptográficos.
- **Bit4id PIN Manager:** aplicativo para gerenciamento de cartões, que permite operações como alterar PIN ou PUK, desbloquear PIN, obter informações sobre o cartão, importar ou exportar certificados ...

Este manual o guiará de maneira simples no processo de instalação e uso do Kit Bit4id.

Para quem é este documento?

Usuários finais, que irão usar cartões com chip em ambientes Linux.

2. Antes de começar

Verifique se você tem:

- Um **leitor de cartão padrão** compatível com PC / SC que está conectado, instalado e configurado corretamente. Siga as instruções fornecidas pelo fabricante do leitor para verificar sua instalação e operação corretas.

- Tenha a **versão mais recente do Bit4id Kit** . Link para baixar a versão mais recente (<http://cdn.bit4id.com/es/middleware.htm>)
- Para poder instalar, é essencial ter **permissões de administrador** . Caso não os possua, a instalação será negada.

3. Instalação

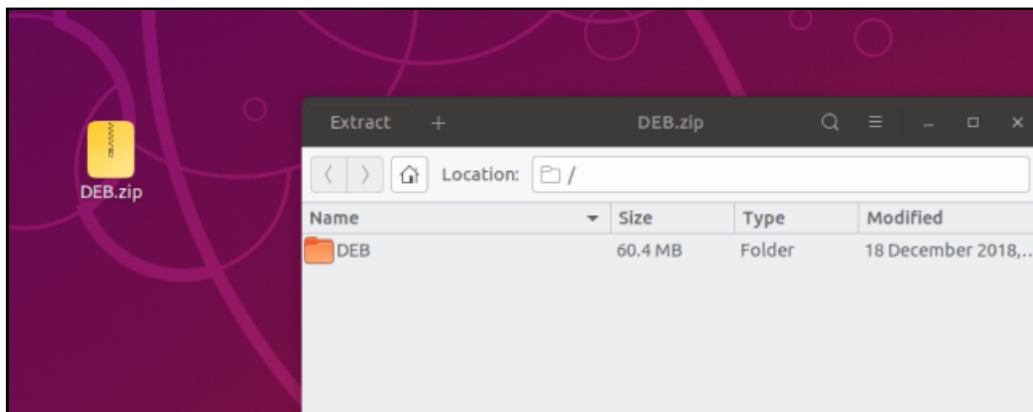
Se necessário, você deve baixar e instalar os drivers para que o seu computador reconheça o leitor que você comprou. Para fazer isso, vá para a página oficial do fabricante do leitor.

Siga as instruções fornecidas pelo fabricante do leitor para verificar sua instalação e operação corretas.

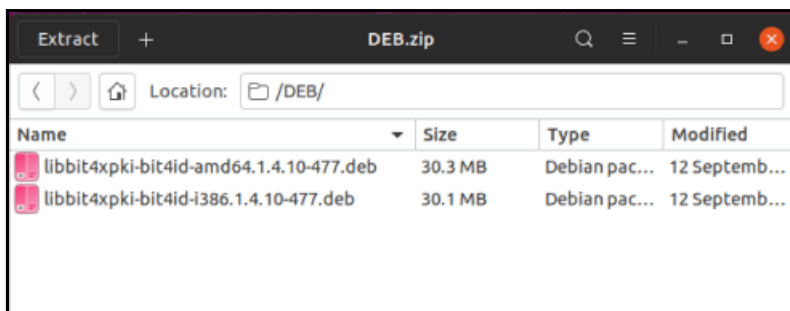
No caso de adquirir um leitor bit4id, se a sua versão do Linux tiver drivers PCSC instalados por padrão, não será necessário baixar nenhum driver. Caso contrário, devemos fazer o download dos drivers do leitor (<https://resources.bit4id.com/#/>).

3.1 Assistente de Instalação do Gerenciador PKI

1. Vá para a pasta em que você baixou o arquivo **DEB.zip**

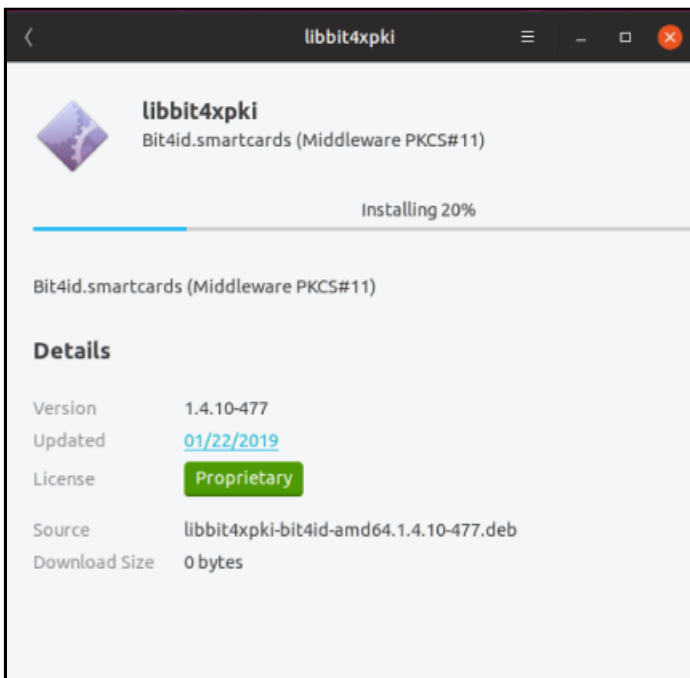
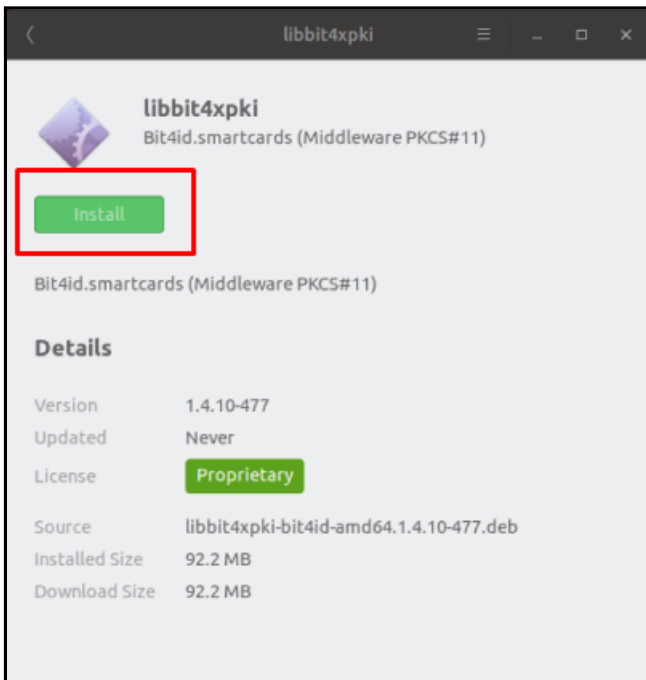


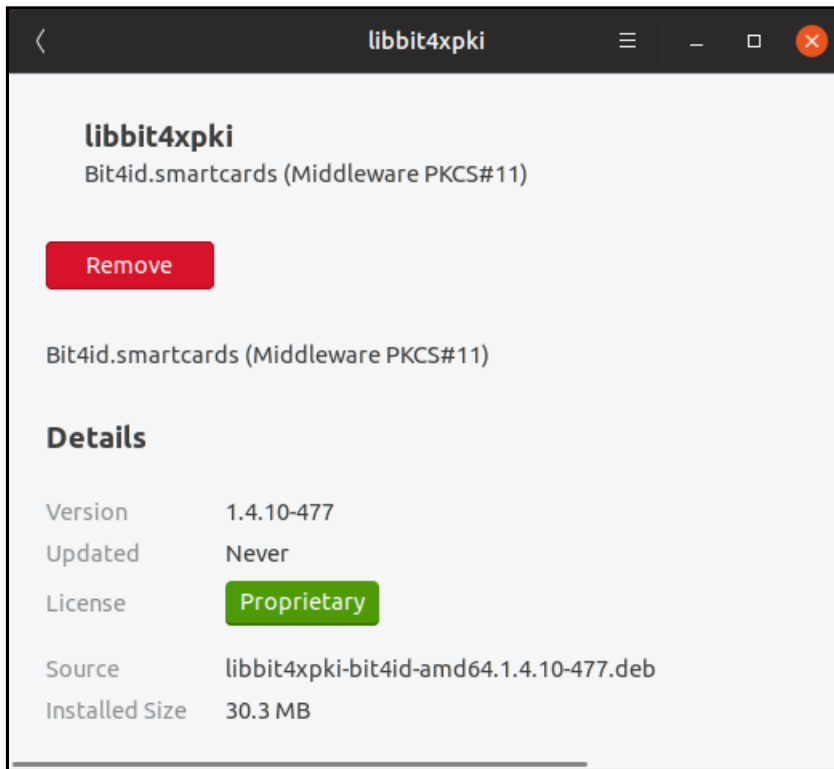
2. Descompacte a pasta. Dentro da pasta, 2 instaladores aparecerão.



- Se o seu sistema operacional for de **64 bits, você** deve executar: libbit4xpki-bit4id-amd64.1.4.10-477.deb
- Se o seu sistema operacional for **32 bits, você** deve executar: libbit4xpki-bit4id-i386.1.4.10-477.deb

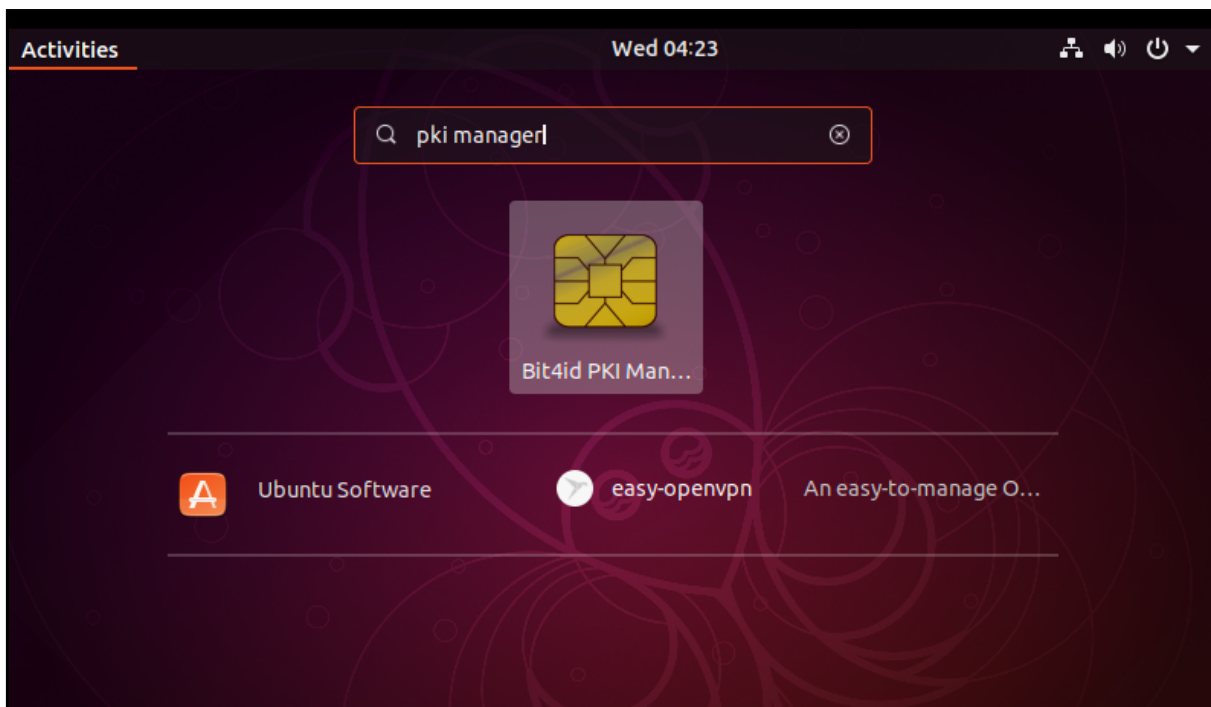
3. Siga as etapas do instalador.





4. Quando a instalação do PKI Manager estiver concluída, reiniciaremos o computador.

5. Una vez finalizado el reinicio, abrimos la aplicación.





6. Con la aplicación abierta, conectamos el lector en un puerto USB y seguidamente, insertamos la tarjeta. También podemos hacer este proceso, conectado el token en un puerto USB.



4. Problemas durante la instalación

Es posible que tenga versiones anteriores de la aplicación de Gestión de la tarjeta (Bit4id PKI 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.



¿Como desinstalar una versión anterior de PKI Manager?

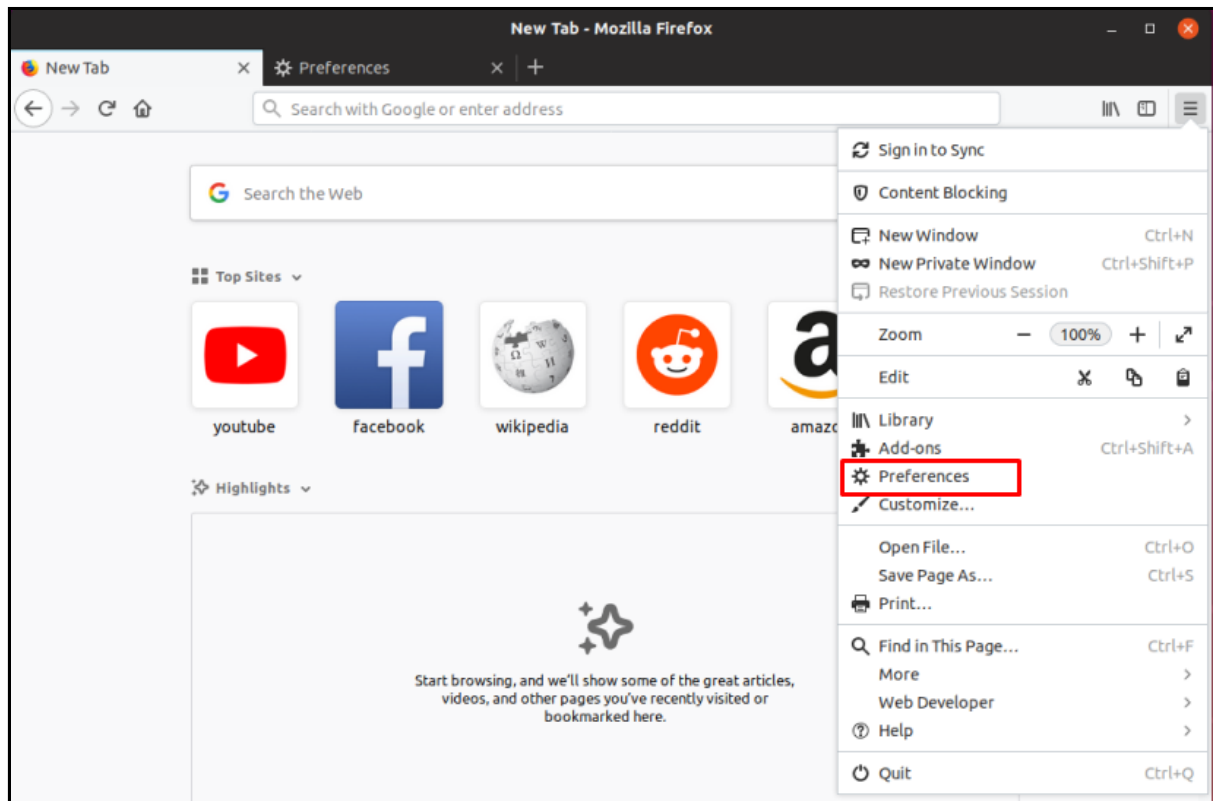
1. Ve al **Centro de Software / Gestor de Software**
2. Busca y selecciona la **pestaña de Instalados**
3. **Selecciona** el que quieras eliminar
4. Pulsa **desinstalar**
5. Si no, abre la **consola de comandos (Control + Alt + T)**
6. Escribe **`sudo apt-get --purge remove [nombre del programa]`**
7. Introduce tu contraseña y pulsa Enter


5. Configuración en Firefox

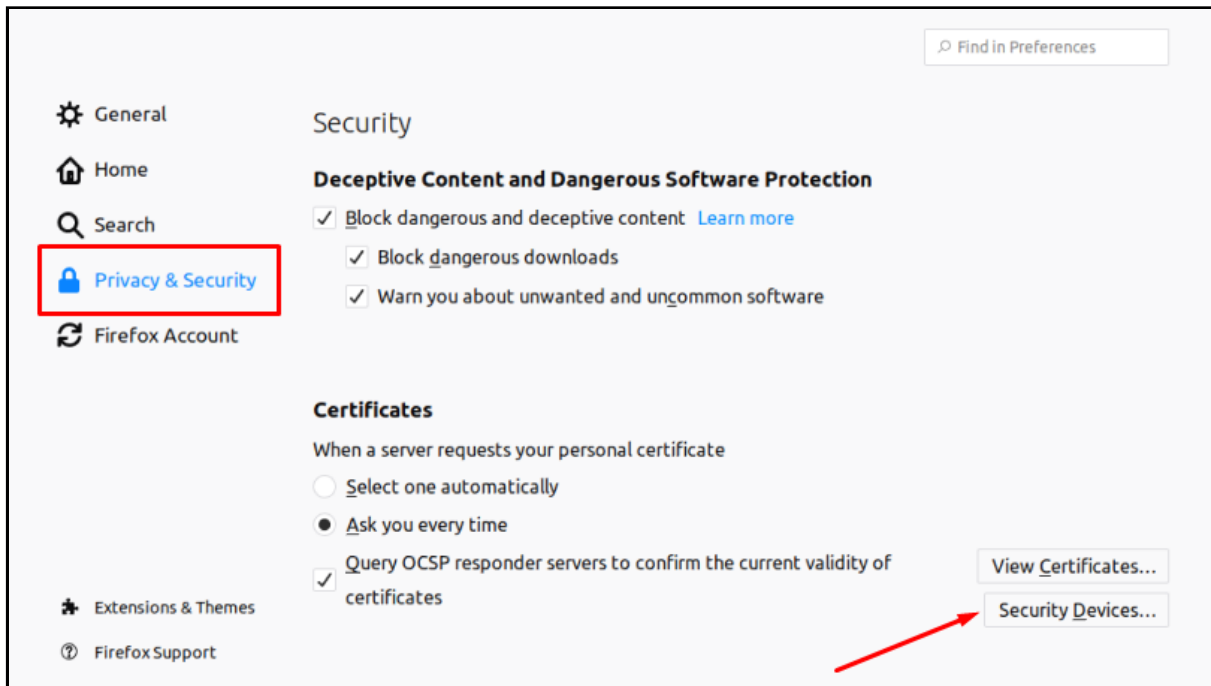
Para poder utilizar los certificados que contenga la tarjeta inteligente en el navegador Mozilla Firefox, es necesario incorporar unas librerías del Middleware Universal de Bit4id de forma manual.

La incorporación automatizada de dispositivos de seguridad en Firefox se deshabilitó desde la versión 3.5 como medida de seguridad.

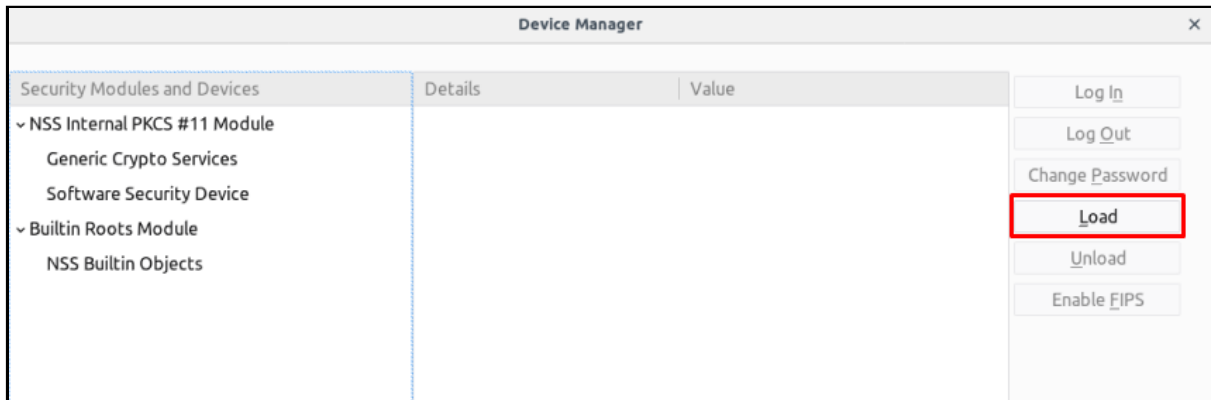
1. Abrimos Mozilla Firefox, nos dirigimos a  → Opciones ( Preferences)



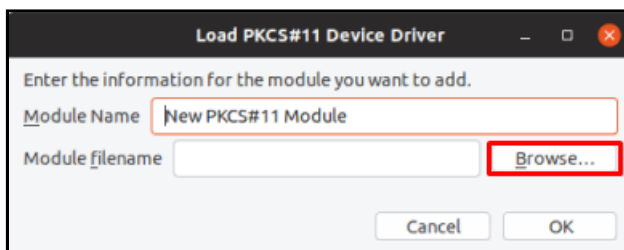
2. En el apartado de  Privacidad y Seguridad, buscamos el apartado de los certificados y clicamos en Dispositivos de Seguridad (Security Decives...)



3. Se nos abrirá el Administrador de dispositivos. Clicamos en Cargar (Load)

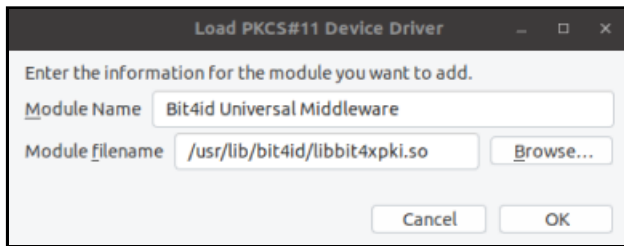


4. Cuando se abra esta ventana, debemos buscar el controlador del dispositivo PKCS#11. Clicamos en examinar (Browse...), para buscarlo en nuestro equipo.



En la anterior ventana, se debe introducir los siguientes datos:

- **Nombre del módulo (Module Name):** *Bit4id Universal Middleware*
- **Archivo del módulo (Module filename):** */usr/lib/bit4id/libbit4ipki.so*



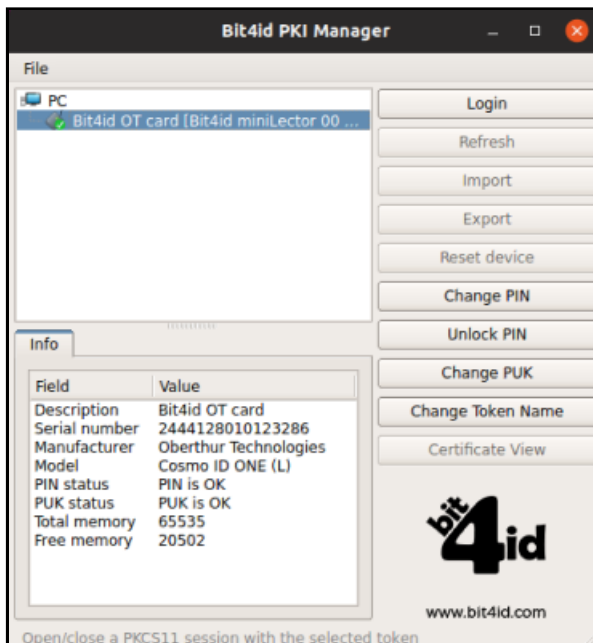
6. Antes de comenzar a usar el Kit Bit4id

Bit4id PIN Manager requiere un lector de tarjetas inteligentes estándar, compatible PC/SC, que se encuentre correctamente conectado, instalado y configurado antes de comenzar.

Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento.

7. Funcionalidades

La aplicación Bit4id PKI Manager dispone de múltiples funcionalidades disponibles desde la pantalla principal.



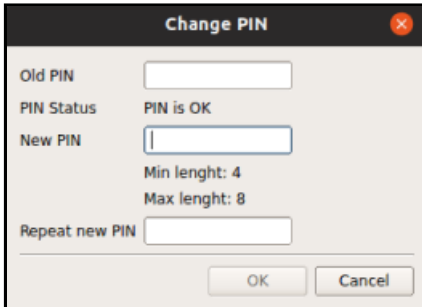
7.1. Tabla funcionalidades

Función	Descripción
Login	Petición de PIN para acceder al contenido de la tarjeta
Refresh	Actualiza el contenido del token para ver nuevos
Import/Export	Función para importar/exportar certificados sobre la tarjeta
Reset device	Función para dejar la tarjeta sin certificados ni claves
Change PIN	Función para cambiar el PIN de la tarjeta

Función	Descripción
Unlock PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma.
Change PUK	Función para cambiar el PUK de la tarjeta
Certificate View	Ventana emergente que muestra información sobre los certificados y su cadena de confianza
Info	Ventana que muestra información sobre la tarjeta (modelo, número de serie, identificación del fabricante y etiqueta)

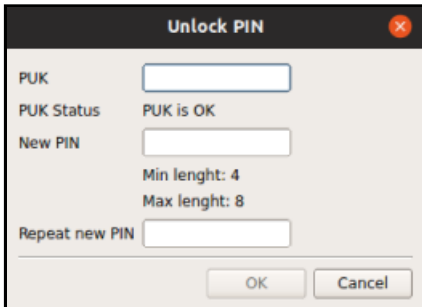
- **Cambiar el PIN (Change PIN)**

Para desbloquear el PIN, introduzca el PIN de la tarjeta e introducir el nuevo PIN. El nuevo PIN debe tener entre 4 y 8 dígitos alfanuméricos.



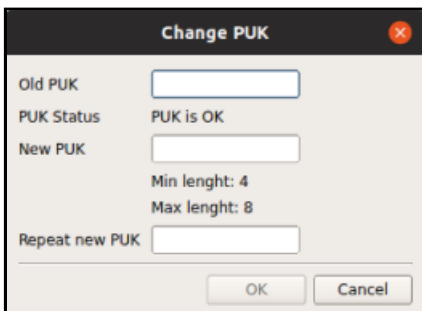
- **Desbloquear el PIN (Unlock PIN)**

Para desbloquear el PIN, introduzca el PUK de la tarjeta e introducir el nuevo PIN. El nuevo PIN debe tener entre 4 y 8 dígitos alfanuméricos.



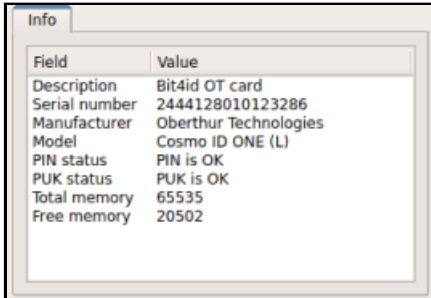
- **Cambiar el PUK (Change PUK)**

Introduzca el PUK antiguo de la tarjeta y el nuevo PUK. El nuevo PUK debe tener entre 4 y 8 dígitos alfanuméricos.



- **Información de la tarjeta (Info)**

Ofrece información detallada de la tarjeta: modelo, número de serie, fabricante y etiqueta. Es posible que soporte (soporte@bit4id.com) le solicite dicha información para conocer el tipo de tarjeta que está utilizando.



Field	Value
Description	Bit4id OT card
Serial number	2444128010123286
Manufacturer	Oberthur Technologies
Model	Cosmo ID ONE (L)
PIN status	PIN is OK
PUK status	PUK is OK
Total memory	65535
Free memory	20502

8. Preguntas frecuentes

¿Puedo combinar números y letras para el número PIN de la tarjeta?

Sí, no hay ningún problema, siempre que el nuevo PIN tenga entre 4 y 8 dígitos.

¿Existe un máximo de inserciones de PIN en el caso de que tenga alguna duda y no recuerde mi número PIN?

¿Cuándo puede quedar bloqueada la tarjeta?

Si inserta más de 3 veces el código PIN de forma errónea, este se bloquea. Póngase en contacto con Bit4id para desbloquearlo.

¿Existe un máximo de inserciones de PUK para intentar desbloquear el PIN? ¿Qué ocurre si la tarjeta queda bloqueada?

Si inserta más de 3 veces el código PUK de forma errónea, este se bloquea. Por razones de seguridad, la tarjeta se bloquea completamente. Póngase en contacto con Bit4id.

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 este 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.

Cartão inteligente: qualquer cartão com circuitos integrados que permitem a execução de certa lógica programada.