

Manual do Usuário para Windows

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. Instalação autônoma \(para usuários avançados\)](#)
- [5. Problemas durante a instalação](#)
- [6. Fim da instalação](#)
- [7. Acesso ao aplicativo](#)
- [8. Recursos](#)
 - [8.1 Tabela de recursos](#)
- [9. Verificações adicionais contra mau funcionamento](#)
 - [9.1 Verificação de upload de certificado na Windows Store](#)
 - [9.2 Verificação de upload de certificado na Firefox Store](#)
- [10. Perguntas freqüentes](#)
- [11. 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.

1.1 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.

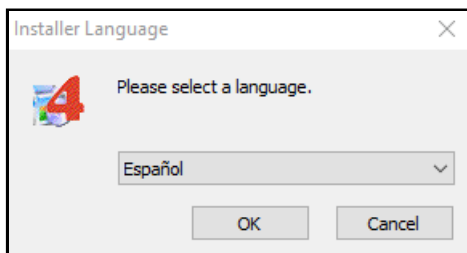
Siga as instruções fornecidas pelo fabricante do leitor para verificar sua instalação e operação corretas.

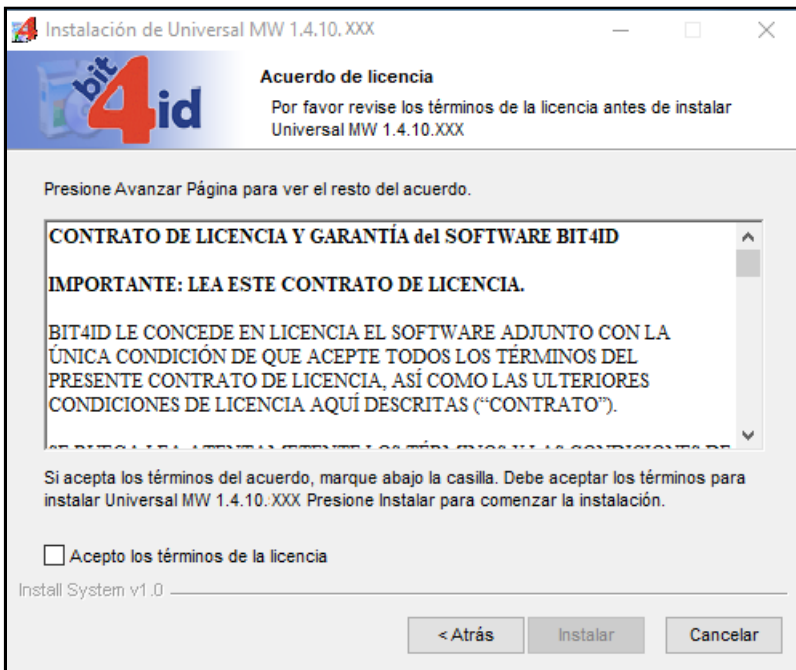
No caso de adquirir um leitor bit4id, se a sua versão do Windows for igual ou superior ao Windows 7, não será necessário instalar nenhum driver.

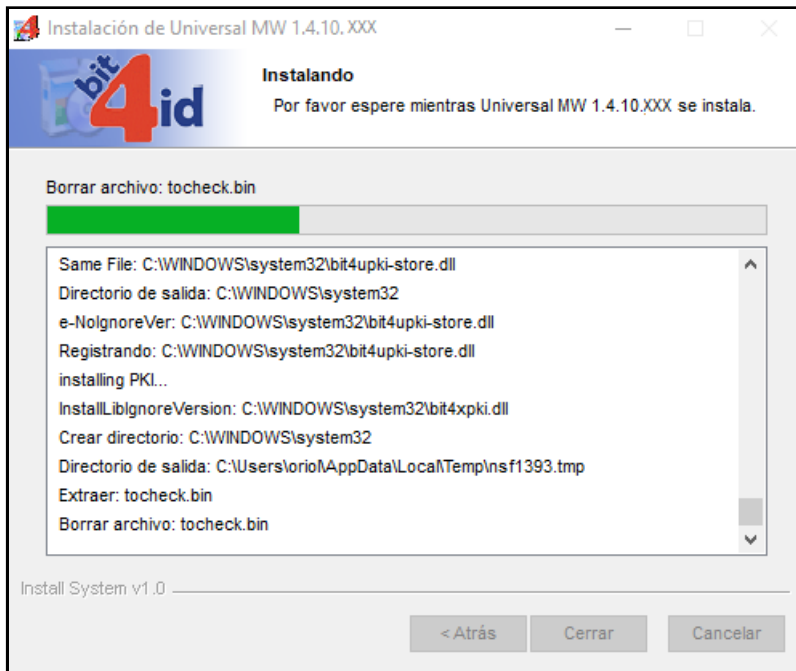
Caso nosso sistema operacional não reconheça o leitor, precisamos fazer o download dos drivers do leitor (<https://resources.bit4id.com/#/>).

3.1 Assistente de Instalação do Gerenciador PKI

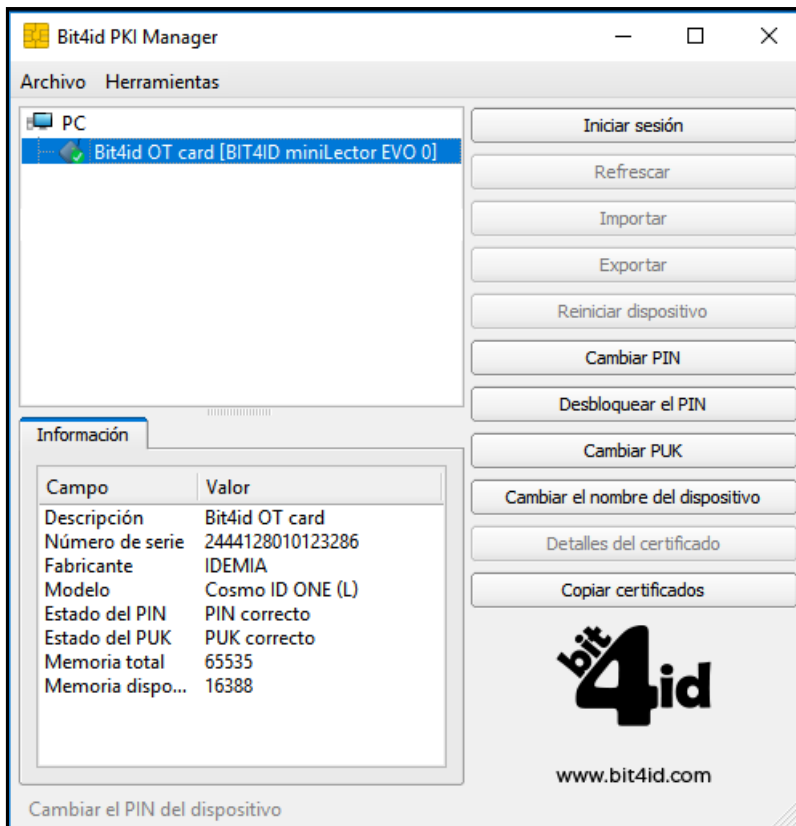
1. Vá para a pasta em que você baixou o arquivo e execute-o.
2. Siga as etapas do instalador.







3. Quando a instalação do PKI Manager estiver concluída, reiniciaremos o computador.
4. Finalizado el reinicio, abrimos la aplicación.
5. 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. Instalación desatendida (para usuario avanzados)

ATENCIÓN: este procedimiento es sólo para casos concretos en los que se le haya indicado explícitamente. La mayoría de usuarios no deberían realizar una 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 antes de proceder. Así mismo, se debe forzar el reinicio de la máquina una vez concluida la instalación.

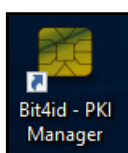
5. Problemas durante la instalación

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.

- Para eliminar versiones anteriores en **Windows XP**, diríjase al menú Inicio > Panel de control > Agregar o quitar programas > Bit4id PKI Manager x.x.x.x (dónde x.x.x.x representa el número de versión instalada)
- Para eliminar versiones anteriores en **Windows Vista o 7**, diríjase al menú Inicio > Panel de control > Desinstalar un programa > Bit4id PKI Manager x.x.x.x (dónde x.x.x.x representa el número de versión instalada)
- Para eliminar versiones anteriores en **Windows 8**, diríjase al menú lateral derecho > Configuración > Panel de control > Desinstalar un programa > Bit4id PKI Manager x.x.x.x (dónde x.x.x.x representa el número de versión instalada)
- Para eliminar versiones anteriores en **Windows 10** diríjase a Menú de Inicio > Panel de Control > Programas y características > Bit4id - Universal MW x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

6. Fin de la instalación

Una vez finalizado el proceso de instalación se creará un acceso directo de la aplicación Bit4id PKI Manager (Gestión de la tarjeta) en el escritorio que le permitirá realizar cualquier tipo de operación con la misma.

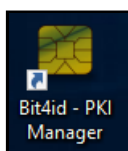


Así mismo podrá acceder a la aplicación Bit4id PKI Manager a través de la sección Inicio



7. Acceso a la aplicación

La aplicación Bit4id PKI Manager es accesible desde el escritorio, haciendo click sobre:



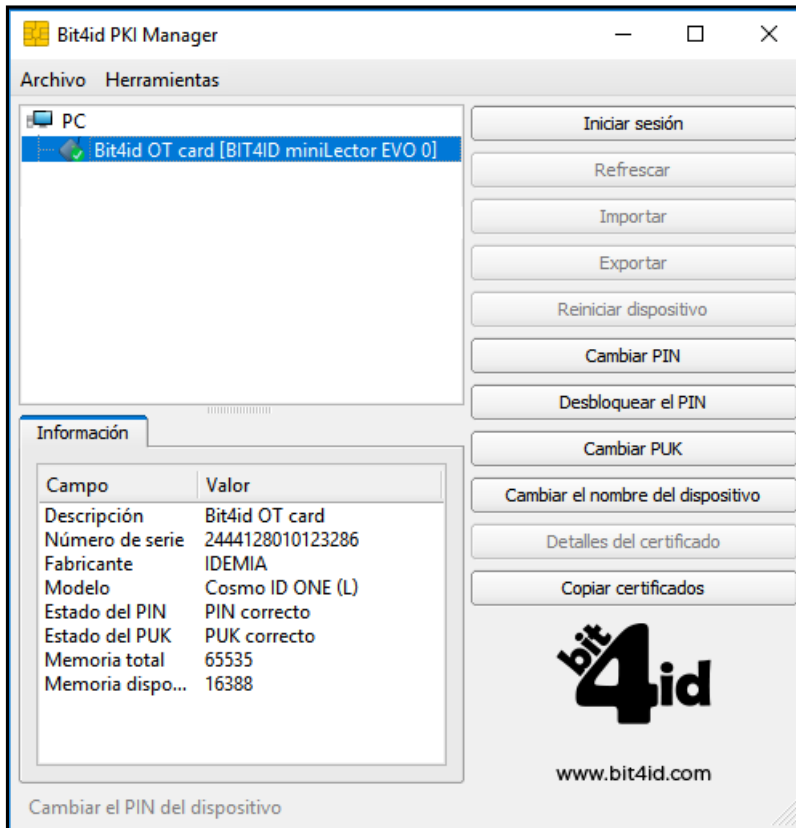
Así mismo se puede acceder a la aplicación Gestión de Tarjeta a través de:

- en **Windows XP**, dirijase al menú Inicio > Programas > Bit4id > Bit4id PKI Manager
- en **Windows Vista o 7**, dirijase al menú Inicio > Todos los programas > Bit4id > Bit4id PKI Manager
- en **Windows 8 o 10**, dirijase al menú Inicio > Todas las aplicaciones > Bit4id PKI Manager

8. Funcionalidades

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

IMPORTANTE: Bit4id PKI Manager viene por defecto con la versión de usuario. Para poder disponer de todas sus funcionalidades, se debe pasar a la versión de administrador mediante el comando: **Ctrl+A**



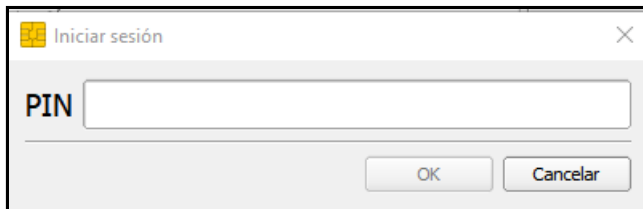
8.1. Tabla funcionalidades

Funcion	Descripción
Iniciar sesión	Petición de PIN para acceder al contenido de la tarjeta
Refrescar	Actualiza el contenido del token/tarjeta para ver nuevos certificados
Importar/Exportar	Función para importar/exportar certificados sobre la tarjeta
Reiniciar dispositivo	Función para dejar la tarjeta sin certificados ni claves
Cambiar PIN/PUK	Función para cambiar el PIN/PUK de la tarjeta

Funcion	Descripción
Desbloquear PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma
Cambiar el nombre del dispositivo	Definir el nombre con el que aparece el dispositivo
Detalles del certificado	Ventana emergente que muestra información sobre los certificados y su cadena de confianza
Información	Ventana situada en la parte inferior de la aplicación que muestra información sobre la tarjeta (modelo, número de serie, identificación del fabricante y etiqueta)
Copiar certificados	Copiar los certificados en el CSP de Windows

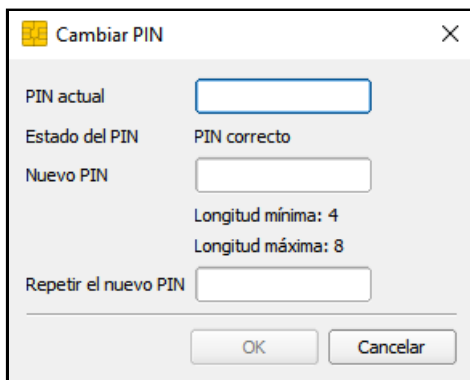
- **Iniciar sesión**

Para acceder a cualquier funcionalidad que ofrece el software, hay que introducir el PIN de la tarjeta



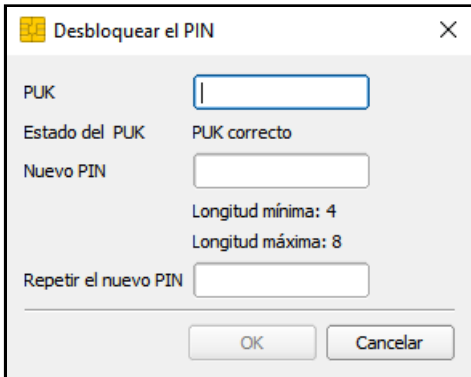
- **Cambiar el PIN**

Para cambiar 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**

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.



Desbloquear el PIN

PUK

Estado del PUK PUK correcto

Nuevo PIN

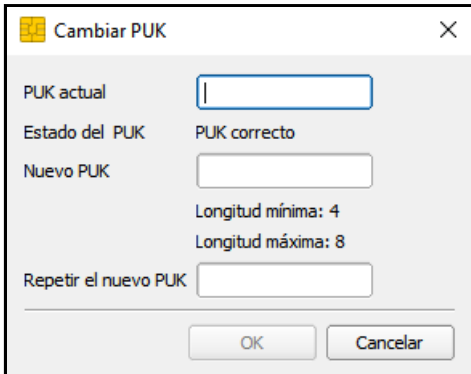
Longitud mínima: 4
Longitud máxima: 8

Repetir el nuevo PIN

OK Cancelar

- **Cambiar el PUK**

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



Cambiar PUK

PUK actual

Estado del PUK PUK correcto

Nuevo PUK

Longitud mínima: 4
Longitud máxima: 8

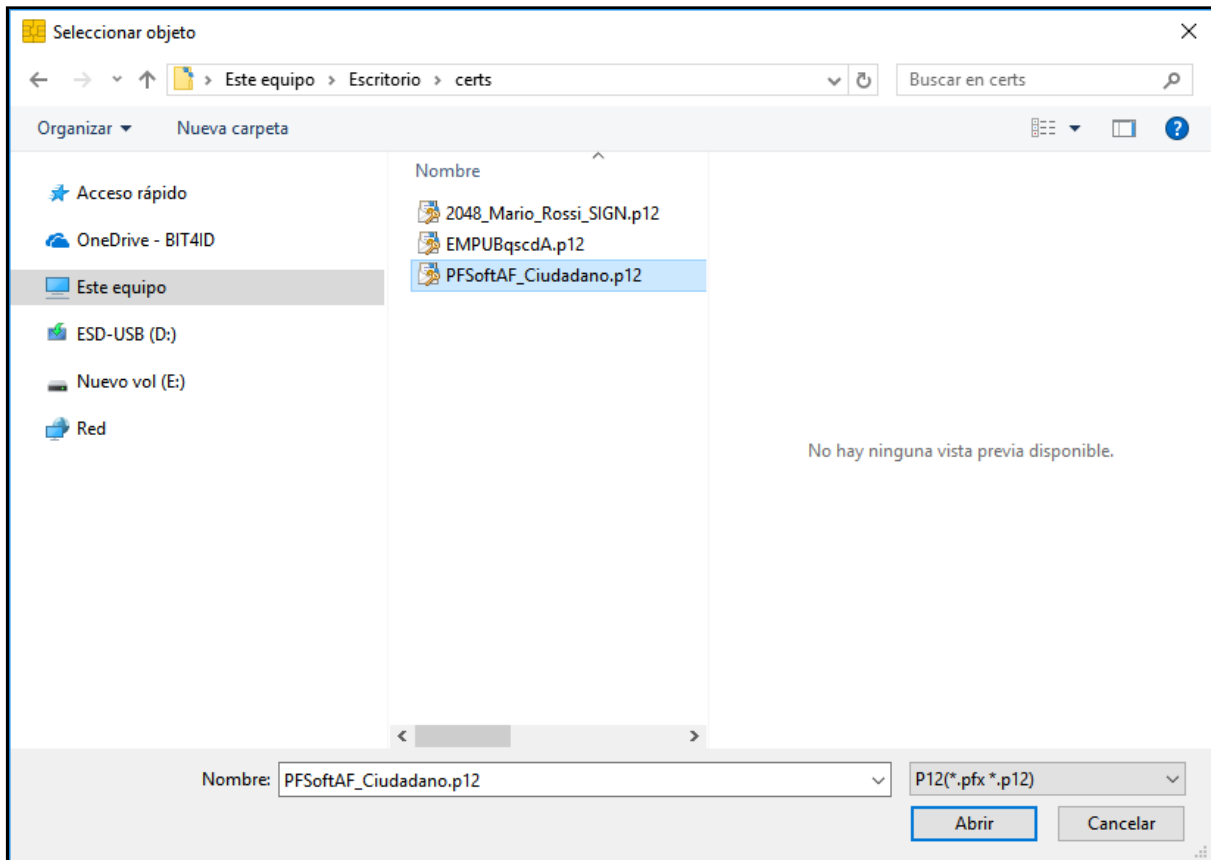
Repetir el nuevo PUK

OK Cancelar

- **Importación**

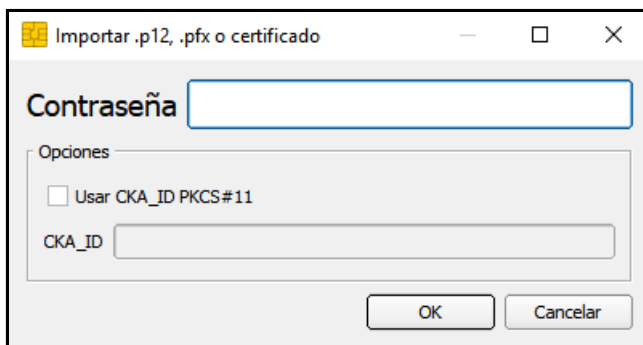
Esta opción permite la importación de certificados en la tarjeta. Los formatos aceptados para la importación de certificados en tarjeta .p12 o .pfx ya que dichos formatos incluyen la clave privada del certificado, imprescindible para realizar operaciones criptográficas.

Para iniciar la importación, antes seleccione el certificado desde su ubicación, tal y como se muestra en la siguiente imagen:



Una vez seleccionado el certificado, presione “Abrir”:

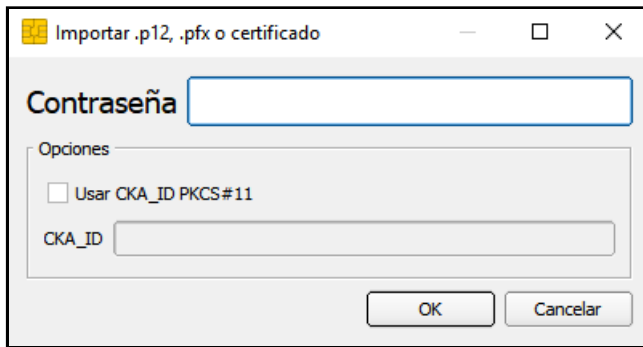
El sistema le pedirá la contraseña del archivo PFX o P12 (certificado y clave privada del mismo) que desea importar, y que contiene su certificado y par de claves. Insértela y complete según su conveniencia las opciones de importación, donde:



– Importar certificados sin par de claves asociado: permite importar toda la jerarquía de certificación incluida en el fichero PFX o P12. Recomendamos NO MARCAR esta opción.

– Definir CKA_ID de PKCS#11: identificador que determinadas aplicaciones utilizan a la hora de mostrar el certificado. Recomendamos introducir un valor identificativo útil, por ejemplo pedro_firma, pedro_acceso, pedro_cifrado, etc.

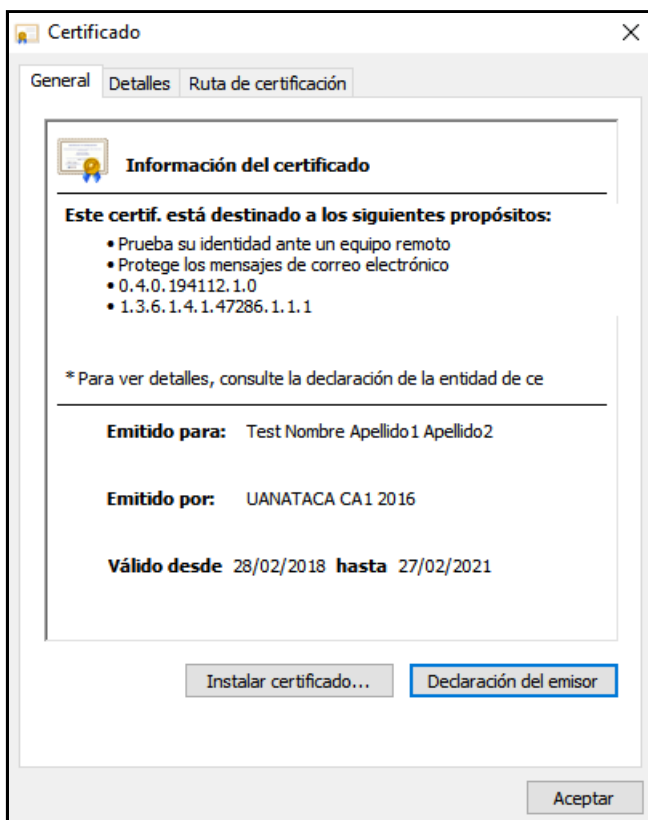
Y la importación del certificado se habrá completado:



En el caso que se desee comprobar que el certificado ha sido correctamente guardado, recuerde que puede revisar todos los certificados almacenados en la tarjeta a través de la opción "Ver" de Bit4id PKI Manager.

• Detalles del certificado

Una vez se introduce el PIN de la tarjeta, podemos ver los certificados que se encuentra dentro de ella. En la ventana emergente que muestra la aplicación, podemos ver informaci



• Información de la tarjeta

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.

Campo	Valor
Sujeto	C=ES,Serial Number=IDCES-L12345678...
Emisor	C=ES,CN=UANATACA CA1 2016,L=Bar...
Período de vali...	28/02/2018 20:16:16 +0000 UTC -- 27/0...
Uso de la clave	Digital signature,Non repudiation,Key ...
Extensión de us...	Client authentication (1.3.6.1.5.5.7.3.2),...
Número de serie	6c 0b b5 d5 a8 92 57 a3
Contenedor	66 09 2b 65

9. Comprobaciones adicionales frente al mal funcionamiento

Los resultados de las siguientes comprobaciones son necesarias para la resolución de cualquier tipo de incidencia. Dichos resultados se deben reportar al departamento técnico ante cualquier incidencia relacionada con el uso de sus certificados almacenados en sus tarjetas. De esta forma se reducirá el tiempo de resolución de la misma.

9.1. Comprobación de carga de certificados en el almacén de Windows

Asegúrese de disponer de:

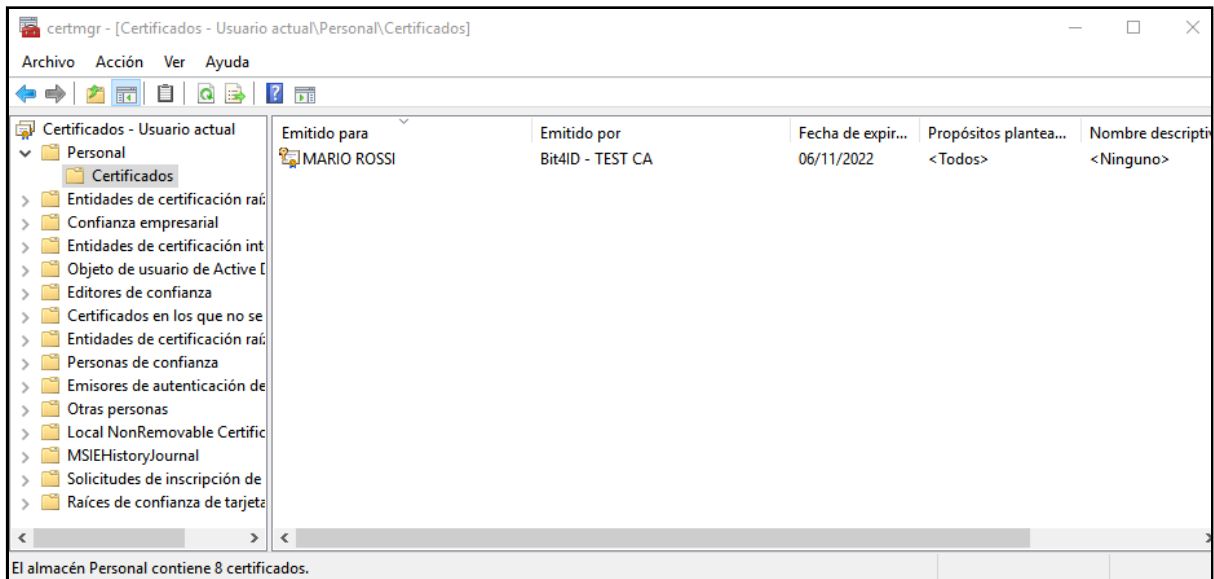
- Lector de tarjetas conectada a la máquina
- Tarjeta inteligente insertada en el lector
- Al menos un certificado almacenado en la tarjeta

Esta prueba pretende comprobar la correcta carga de los certificados de la tarjeta en el almacén de certificados de Windows, lo cual es imprescindible para el uso de nuestros certificados en aplicaciones de Microsoft.

Para ello debemos abrir dicho almacén:

- en Windows XP, diríjase al menú Inicio > Ejecutar e introduzca "certmgr.msc"
- en Windows Vista o 7, diríjase al menú Inicio > Buscar programar y archivos > Introduzca "certmgr.msc"
- en Windows 8 o 10, diríjase al menú Inicio > introduzca certmgr.msc




Una vez ejecutada la ventana, abra la carpeta Personal y seguidamente la carpeta Certificados tal y como muestra la siguiente imagen:



Si se le muestra información referente a los certificados de su tarjeta la comprobación habrá finalizado satisfactoriamente.

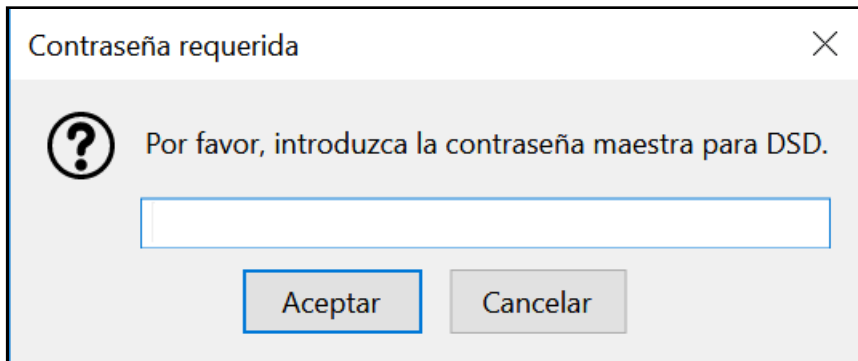
9.2. Comprobación de carga de certificados en el almacén de Firefox

Si dispone en su máquina del explorador Mozilla Firefox en cualquiera de sus versiones realice también la siguiente prueba:

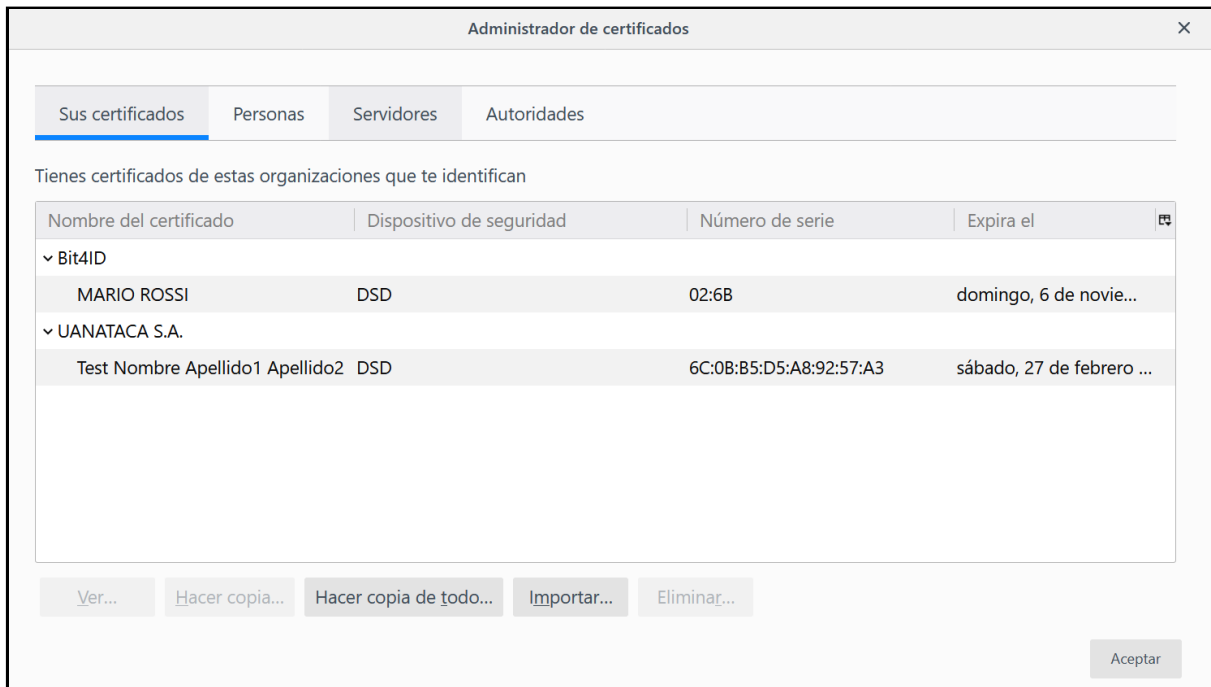
1. Abrimos Mozilla Firefox, nos dirigimos a  -> Opciones  Preferences
2. En el apartado de  Privacidad y Seguridad, buscamos el apartado de los certificados y clicamos en Ver certificados...



3. Introduzca el PIN de su tarjeta



4. Una introducido el PIN, vaya a la pestaña Ver certificados como se muestra a continuación



Si se le muestra información referente a los certificados de su tarjeta la comprobación habrá finalizado satisfactoriamente.

NOTA: Además de los resultados de las comprobaciones expuestas en este apartado, indique al departamento técnico la versión del Kit Bit4id. Para conocer la versión de su kit siga las instrucciones expuestas en el siguiente apartado Preguntas Frecuentes, concretamente en la respuesta de la pregunta ¿Cómo puedo comprobar que dispongo de las últimas versiones del Kit Bit4id?

10. Preguntas frecuentes

¿Qué puede ocurrir si, usando Card Manager, me aparece el mensaje de error "C_OpenSession debido al error 0x1"?

Consulte con el proveedor de la tarjeta (Autoridad de Certificación) sobre el estado de la misma, indicando todos los pasos que ha llevado a cabo.

¿Qué puede ocurrir si, usando Card Manager, me aparece el mensaje de error "C_Login debido al error 0x5"?

Es posible que el código PIN de su tarjeta se encuentre en un estado inconsistente. Pruebe a cambiarlo. Si el error permanece, consulte con el proveedor de la tarjeta (Autoridad de Certificación) sobre el estado de la misma, indicando todos los pasos que ha llevado a cabo.

¿Qué puede ocurrir si al intentar cambiar el PIN de la tarjeta le aparece me el mensaje de error “C_SetPIN debido al error 0x6”?

Compruebe que el nuevo PIN tiene entre 6 y 8 dígitos alfanuméricos.

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

Sí, no hay ningún problema, siempre que el nuevo PIN tenga entre 6 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.

¿Cómo puedo comprobar que dispongo de las últimas versiones del Kit Bit4id?

- Para comprobar la versión instalada de forma sencilla en Windows XP, diríjase al menú Inicio > Panel de control > Agregar o quitar programas > Bit4id PKI Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)
- En Windows Vista o 7, diríjase al menú Inicio > Panel de control > > Desinstalar un programa > Bit4id PKI Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)
- En Windows 8 o 10, diríjase al menú lateral derecho > Configuración > Panel de control > Desinstalar un programa > Bit4id PKI Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

¿Qué puede ocurrir si al ejecutar el instalador del Kit Bit4id tengo una versión anterior instalada en el ordenador?

Siempre es recomendable eliminar versiones anteriores antes de instalar. No obstante, el instalador está diseñado para detectarlo automáticamente y eliminar versiones anteriores. Siga atentamente las instrucciones por pantalla.

11. 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.

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