Manual de usuario

Uanataca - PKI Manager

Contenido

1. Introducción

Este manual sirve de guía para llevar a cabo de manera exitosa el proceso de instalación del Middleware Uanataca - PKI Manager para el uso de tarjetas y tokens criptográficos, y el procedimiento para acceder y usar la aplicación de gestión. El middleware consta de los siguientes componentes:

- **Uanataca Middleware**: librerías criptográficas que permiten a cualquier aplicación del Sistema Operativo operar con los tokens y tarjetas criptográficas del fabricante Bit4id.
- **Uanataca PKI Manager**: aplicación para la gestión del token y tarjeta, que permite realizar operaciones como cambio de PIN o PUK, desbloqueo de PIN, importar certificados, etc.

Este manual le guiará de una manera sencilla en el proceso de instalación y uso del Middleware Uanataca - PKI Manager.

¿A quién va dirigido este documento?

A usuarios finales, que van a utilizar tarjetas y tokens criptográficos en entornos Windows.

2. Antes de comenzar

Asegúrese de disponer de:

- Un lector de tarjetas estándar, compatible PC/SC que se encuentre correctamente conectado, instalado y configurado. Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento.

- En el caso de disponer de un token criptográfico USB en vez de una tarjeta, este deberá ser compatible PC/SC.
- Para poder realizar la instalación, es indispensable poseer permisos de Administrador. En caso de no poseerlos la instalación será denegada.

3. Instalación

Descargue el instalador desde la página adecuada del Proveedor de Servicios de Certificación que le ha suministrado la tarjeta o token criptográfico y ejecútelo en su equipo. Si se le solicita, permita la ejecución de la aplicación.

Nota: En el caso de que no le solicite la ejecución de la aplicación vaya a la carpeta de descargas, busque el icono de Kit_Uanataca y ejecútelo desde allí.

Asistente de instalación

Bienvenido al Asistente de Instalación de Kit Uanataca. Haga clic en *Siguiente* para continuar.

Figura 1. Pantalla de instalación middleware

Revise los términos del acuerdo de licencia y haga clic en *Acepto* para continuar.

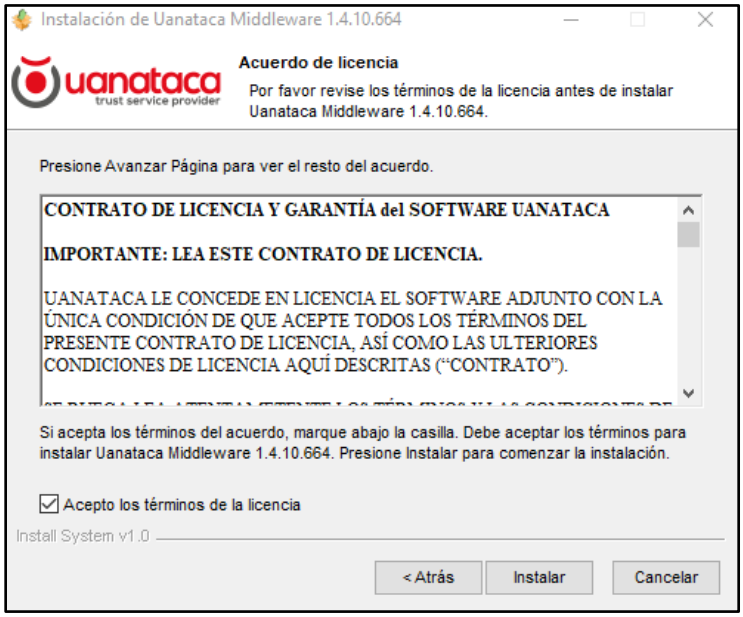

Figura 2. Aceptar términos de licencia

Automáticamente se instalarán todos los componentes del Kit Uanataca.

Una vez finalizado el proceso de instalación del Kit de Universal Middleware, cerrar la ventana presionando *Cerrar.*

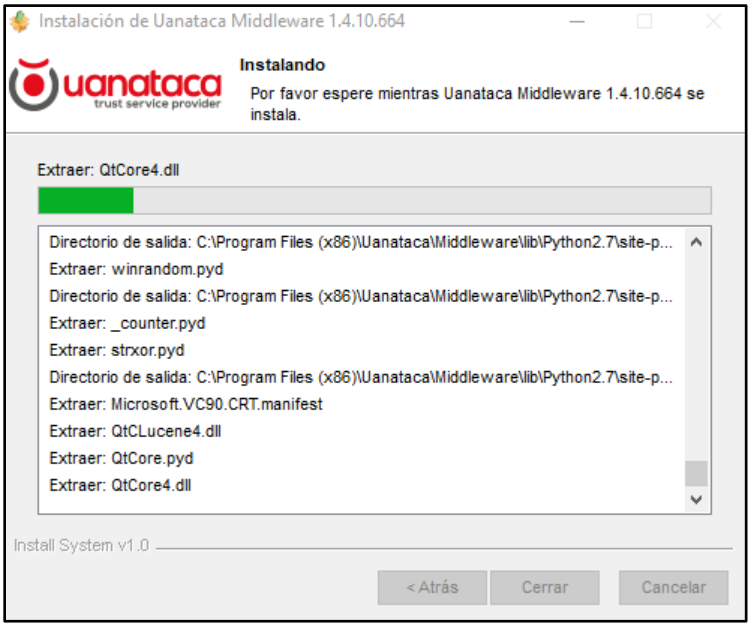

Figura 3. Finalizando instalación del kit

3.1. Instalación desatendida (para usuarios avanzados)

ATENCIÓN: este procedimiento es sólo para casos concretos en los que se le haya indicado explícitamente. La mayoría de los 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.

3.2. Problemas durante la instalación

Es posible que tenga versiones anteriores de la aplicación de Gestión de la tarjeta (Uanataca 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 Vista o 7, diríjase al menú Inicio > Panel de control > > Desinstalar un programa > Uanataca 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 > Uanataca PKI Manager x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

En Windows 10 diríjase a Menú de Inicio > Panel de Control > Programas y características.

3.3. Fin de la instalación

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

Figura 4. Icono gestor de certificados

Así mismo podrá acceder a la aplicación Uanataca - PKI Manager a través de la sección "Inicio" de Windows.

Figura 5. Acceso directo en menú de Windows al gestor de certificados

4. Funcionalidades

Uanataca PKI Manager (Gestión de la tarjeta) dispone de múltiples funcionalidades, accesibles desde la pantalla principal.

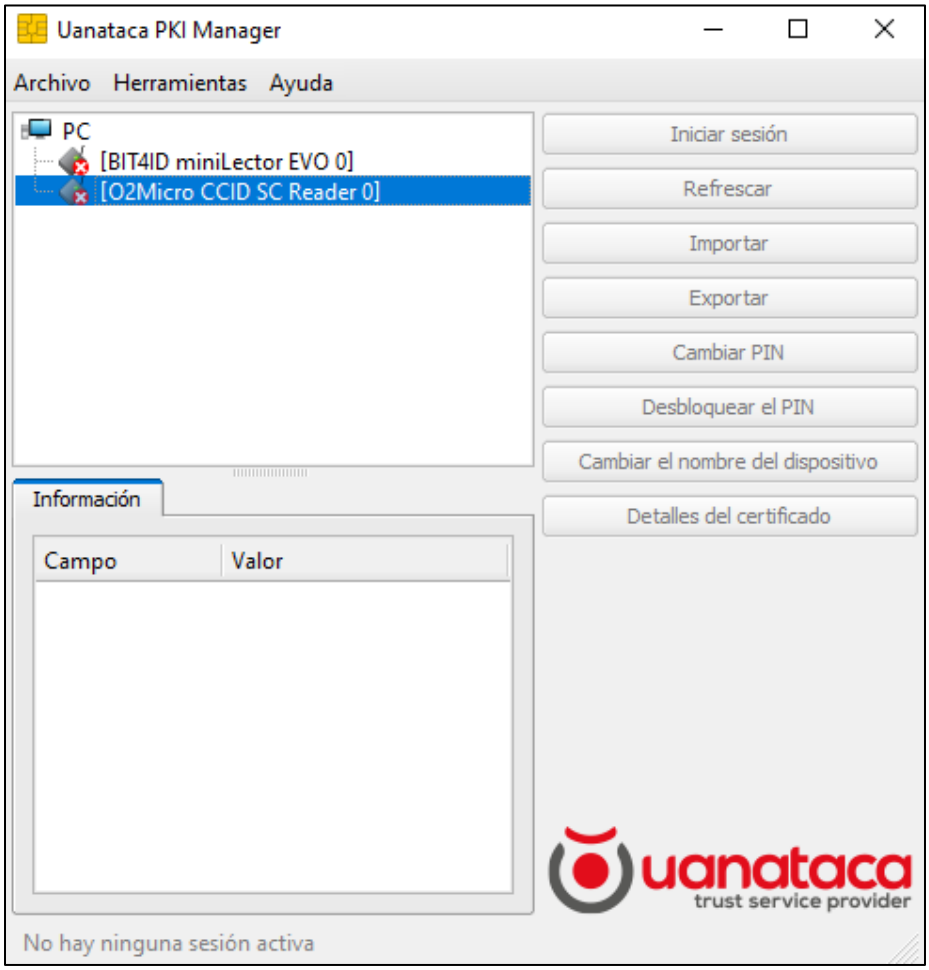

Figura 6. Pantalla principal del gestor de certificados

4.1. Tabla de funciones

Función	Descripción
Iniciar sesión	Solicitud de PIN para acceder al contenido de la tarjeta o del token (Imagen 1)
Actualizar	Función para actualizar nuevas tarjetas o tokens conectados
Importar/Exportar	Función para importar/exportar certificados (ver imagen 5)
Reiniciar dispositivo	Función para eliminar todos los certificados y claves de la tarjeta o token
Cambiar PIN/PUK	Función para cambiar el PIN y el PUK de la tarjeta o token (ver imagen 2 y 3)

Desbloquear PIN	Función para desbloquear el PIN de la tarjeta o token mediante el PUK de la misma (ver imagen 4)
Cambiar el nombre del dispositivo	Función para cambiar el nombre de la etiqueta de la tarjeta o del token
Detalles del certificado	Ventana emergente que muestra información sobre los certificados y su cadena de confianza
Copiar certificados	Copiar manualmente los certificados en el CSP de Windows

4.1.1. Acceder a funcionalidades del software

Antes de acceder a cualquier funcionalidad, es necesario iniciar sesión, introduciendo el PIN de la tarjeta o del token

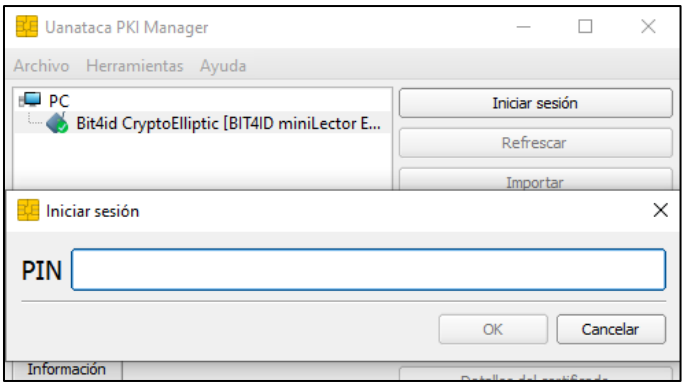

Figura 7. Inicio de sesión en Uanataca – PKI Manager

4.1.2. Cambiar PIN

Introduzca el PIN antiguo de la tarjeta o token y el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos, pudiendo ser alfanuméricos.

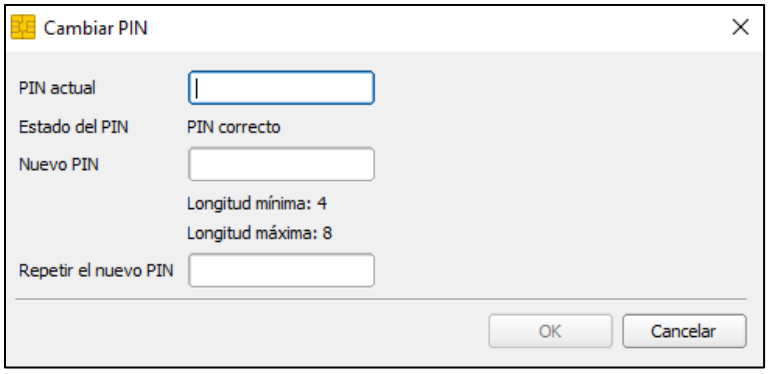

Figura 8. Cambio de PIN

4.1.3. Cambio de PUK

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

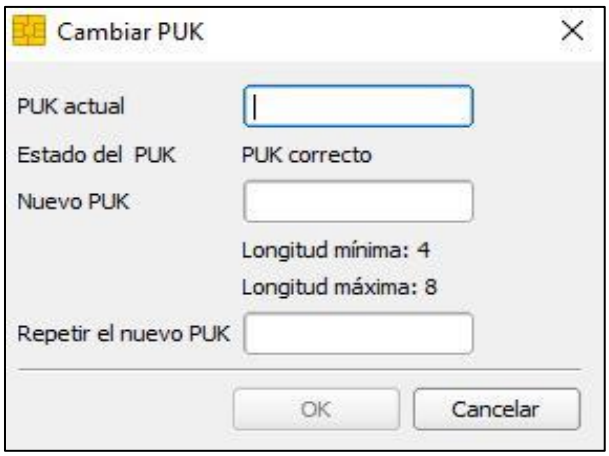

Figura 9. Cambio de PUK

4.1.4. Desbloqueo de PIN

Para desbloquear el PIN, introduzca el PUK de la tarjeta o token e introduzca el nuevo PIN. El nuevo PIN debe tener entre 6 y 8 dígitos.

Figura 10. Desbloqueo de PIN

4.1.5. Importación de certificado

Esta opción permite la importación de certificados en la tarjeta o token. 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:

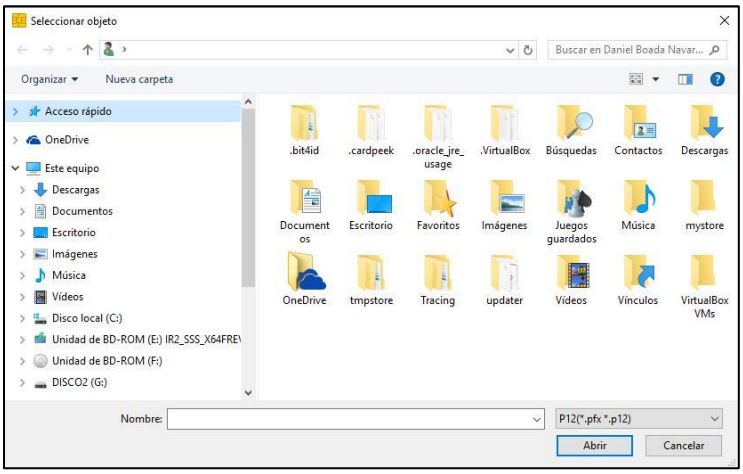

Figura 11. Explorador de archivos para buscar certificado

Una vez seleccionado el certificado, presione “Abrir”:

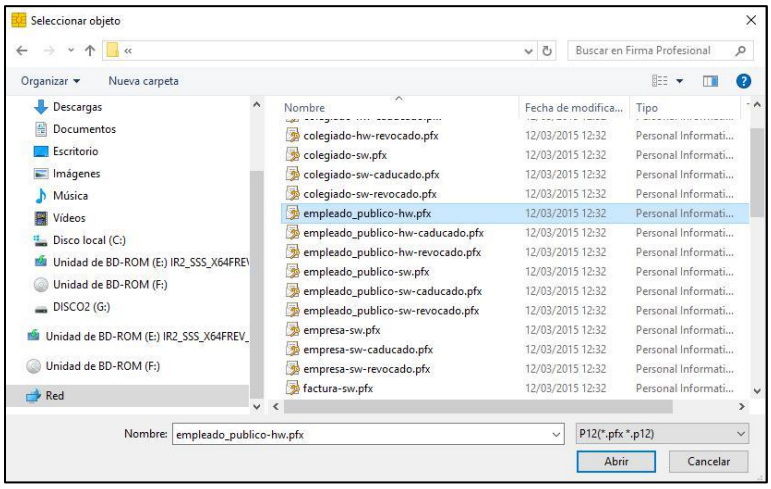

Figura 12. Seleccionamos certificado

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:

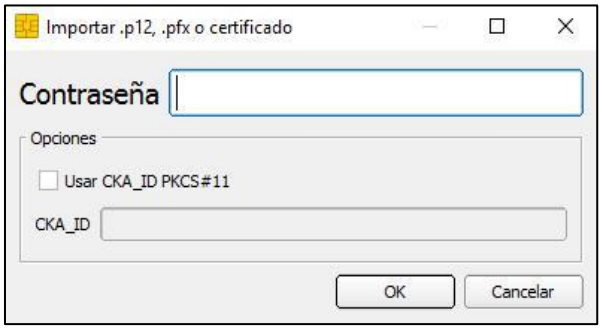

Figura 13. Introducimos contraseña del certificado

- ***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.

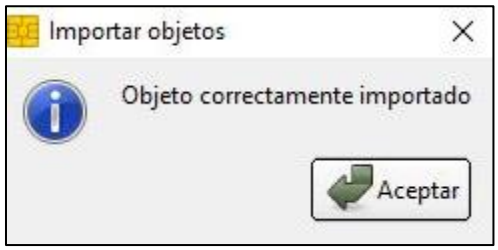

Figura 14. Importación completada

En el caso que se desee comprobar que el certificado ha sido correctamente importado, recuerde que puede revisar todos los certificados almacenados en la tarjeta o token a través de la opción “Ver” de Uanataca - PKI Manager.

4.1.6. Información de certificados

Para ver los certificados que se encuentran en la tarjeta o token, introduzca el PIN cuando le sea solicitado.

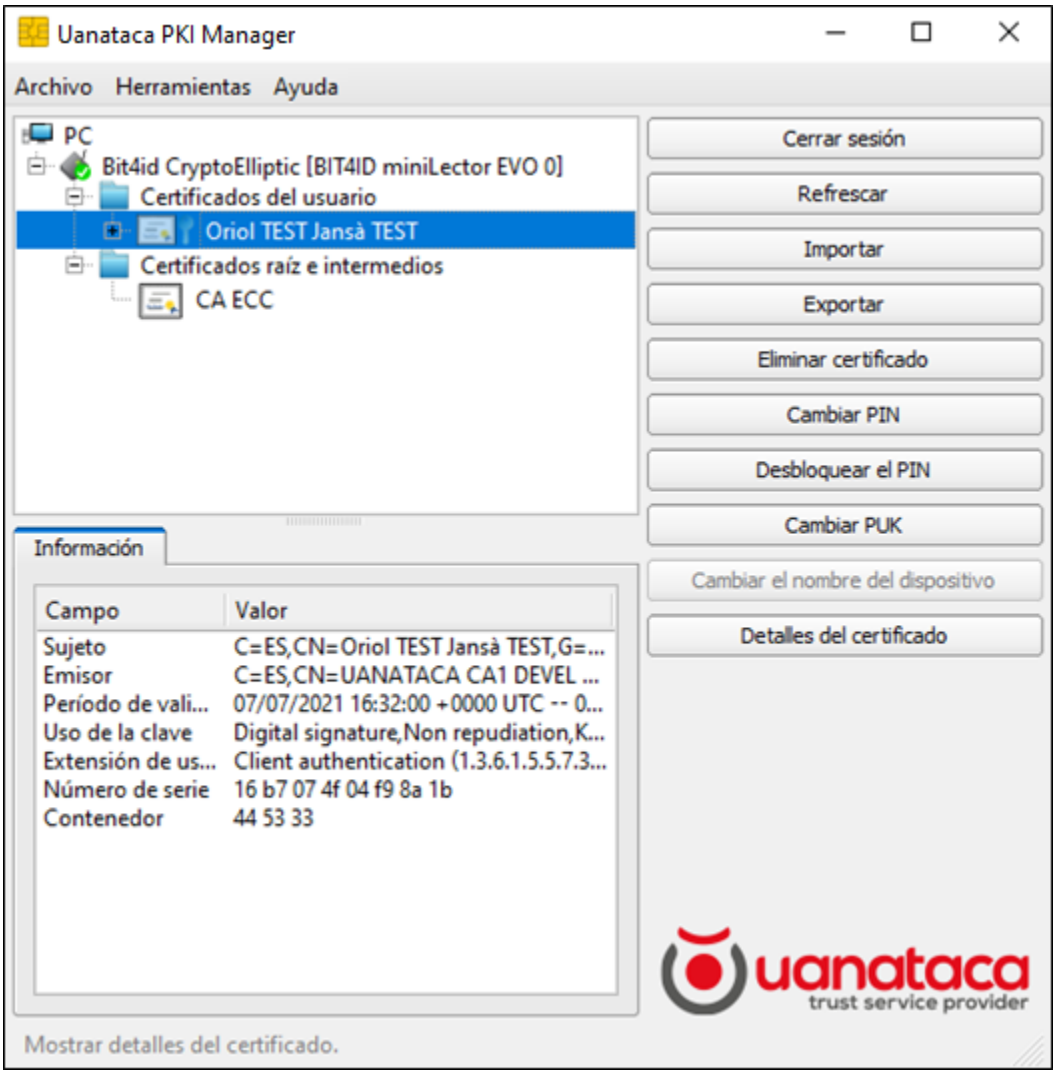

Figura 15. Información de certificados en la tarjeta

4.1.7. Información de la tarjeta

Ofrece información detallada de la tarjeta o token: modelo, número de serie, fabricante y etiqueta.

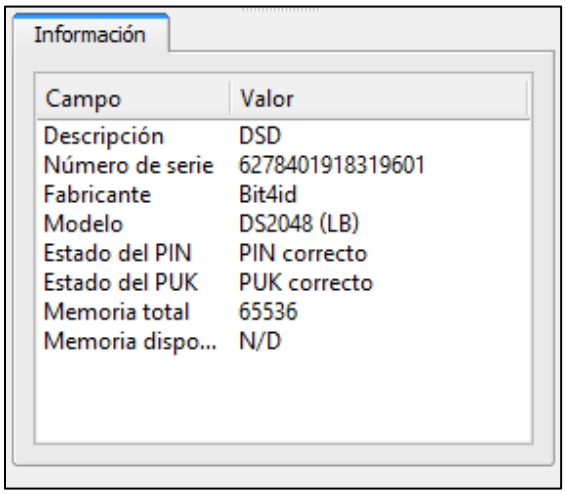

Figura 16. Información de la tarjeta que contiene un certificado

5. Comprobaciones adicionales frente a 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 esta.

Comprobación de carga de certificados en el almacén de Windows

Asegúrese de disponer de:

Tarjeta

- Lector de tarjetas conectado al PC
- Tarjeta inteligente insertada en el lector o identidad remota cargada en el sistema
- Al menos un certificado almacenado en la tarjeta

Token

- Token conectado al PC
- Al menos un certificado almacenado en el token

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 seguir los siguientes pasos:

- 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 > e introduzca *certmgr.msc*

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

Figura 17. Gestor de certificados de Windows (CSP)

Si los certificados de su tarjeta o token se muestran correctamente, la comprobación habrá finalizado satisfactoriamente.

Comprobación de carga de certificados en el almacén de Firefox

Si dispone del explorador Mozilla Firefox en su PC en cualquiera de sus versiones, realice también la siguiente comprobación:

- Abra el menú desplegable '*Herramientas*' del menú superior
- Seleccione opciones y vaya a la pestaña '*Avanzado*'
- Abra la pestaña '*Certificados*'

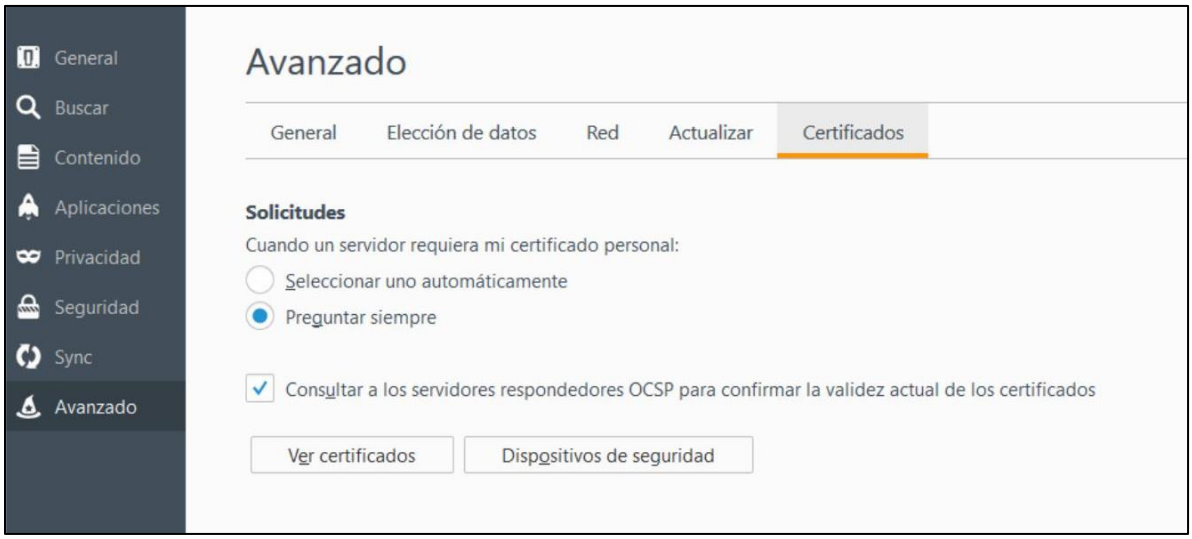

Figura 18. Pestaña de certificados en Firefox

- Seleccione la opción *Certificados* o *Ver certificados* (dependiendo de la versión del explorador)
- Introduzca el *PIN* de su tarjeta o token

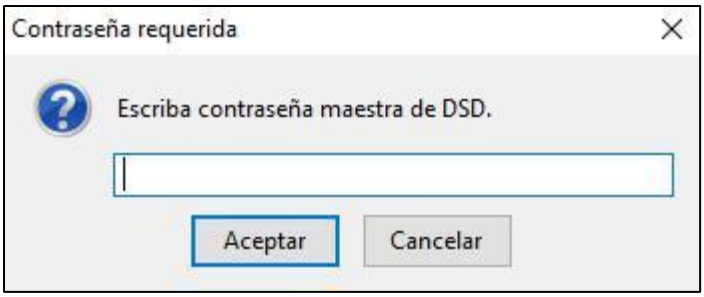

Figura 19. Contraseña de la tarjeta

Una introducido el PIN, vaya a la pestaña *Ver certificados* como muestra la siguiente imagen:

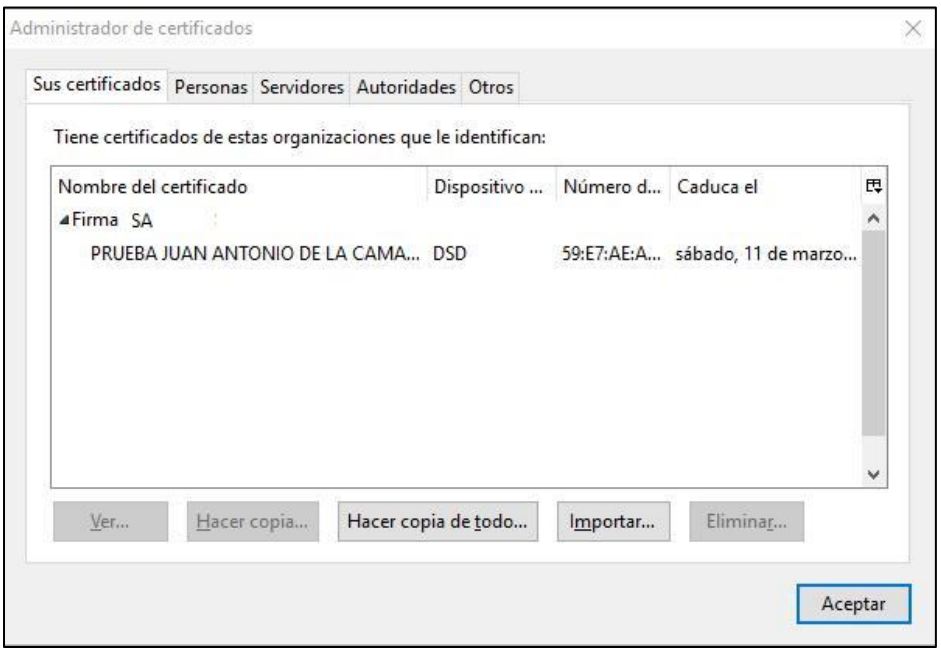

Figura 20. Certificado importado en el navegador

Si los certificados de su tarjeta o token se muestran correctamente, 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 Uanataca. 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 Uanataca?*

6. Preguntas frecuentes

¿Qué puede ocurrir si, usando PKI 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 PKI 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 perdura, 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, 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 bloqueará. Para desbloquearlo, podrá utilizar el código PUK.

¿Existe un máximo de inserciones de PUK para intentar desbloquear el PIN?

- Si inserta más de 3 veces el código PUK de forma errónea, este se bloqueará. Por razones de seguridad, la tarjeta se bloquea completamente, no pudiéndose recuperar.

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

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

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

7. 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.