centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1006

Procedimiento de Empleo Seguro
Yubikey 5 CCN Series



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 3
4 FASE PREVIA A LA INSTALACIÓN 4
4.1 ENTREGA SEGURA DEL PRODUCTO 4
4.1.1 SOFTWARE DE APOYO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 6
5 FASE DE INSTALACIÓN 7
6 FASE DE CONFIGURACIÓN 8
6.1 MODO DE OPERACIÓN SEGURO 8
6.2 AUTENTICACIÓN 8
6.2.1 AUTENTICACIÓN DE USUARIOS 8
6.2.2 AUTENTICACIÓN CON COMPONENTES EXTERNOS 8
6.3 ADMINISTRACIÓN DEL PRODUCTO 9
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 9
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 9
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 13
6.5 GESTIÓN DE CERTIFICADOS 14
6.6 SERVIDORES DE AUTENTICACIÓN 15
6.7 SINCRONIZACIÓN 15
6.8 ACTUALIZACIONES 15
6.9 BACKUP 16
7 REFERENCIAS 17
8 ABREVIATURAS 18

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Ejemplo de embalaje original 4
Ilustración 2. Pantalla de configruación de Passkeys 10
Ilustración 3. Creación de un nuevo PIN 10
Ilustración 4. Pantalla de cambio de PIN 12
Ilustración 5. Pantalla de cambio de PUK 12
Ilustración 6. Actualización de Management Key 13
Ilustración 7. Página Home, remarcado *Toggle applications* 13
Ilustración 8. Configurando protocolos disponibles y métodos de comunicación (remarcado) 14

1 INTRODUCCIÓN

La serie YubiKey 5 CCN está compuesta por un conjunto de dispositivos físicos diseñados para reforzar la seguridad en los procesos de autenticación de usuarios. Se presenta en forma de llave hardware compacta que puede conectarse a distintos equipos mediante interfaces habituales como USB o tecnologías inalámbricas de corto alcance como NFC, facilitando su uso en diferentes entornos y dispositivos.

El objetivo principal del producto es proporcionar un mecanismo adicional de verificación de identidad, reduciendo la dependencia de contraseñas tradicionales y mejorando la protección frente a accesos no autorizados. Para ello, permite al usuario autenticarse de manera segura en aplicaciones, sistemas y servicios digitales, tanto en entornos corporativos como en servicios en línea.

La YubiKey 5 CCN puede utilizarse en distintos escenarios de autenticación, actuando como token de seguridad o como dispositivo equivalente a una tarjeta inteligente. Esto la convierte en un elemento versátil que puede integrarse tanto en arquitecturas modernas de autenticación como en infraestructuras existentes basadas en certificados y credenciales tradicionales.

Desde el punto de vista físico y operativo, se trata de un dispositivo robusto, sin partes móviles ni necesidad de batería, lo que simplifica su uso y mantenimiento. Está diseñado para ser utilizado directamente por el usuario final, sin requerir instalaciones complejas, más allá de una configuración inicial básica para su puesta en funcionamiento segura.

En conjunto, la YubiKey 5 CCN constituye un elemento de seguridad que complementa los sistemas de autenticación existentes, proporcionando un mecanismo adicional basado en hardware para mejorar el control de acceso y la protección de identidades digitales.

2 OBJETO Y ALCANCE

El presente documento se desarrolla para la serie de dispositivos YubiKey 5 CCN, un conjunto de dispositivos hardware de autenticación que comparten una misma base funcional y de seguridad.

En concreto las YubiKey cualificadas en CPSTIC corresponden a:

- **YubiKey 5 NFC CCN:** con interfaces físicas USB-A y NFC.
- **YubiKey 5C NFC CCN:** con interfaces físicas USB-C y NFC.

El producto YubiKey 5 CCN Series ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF1].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Cuando el usuario reciba la YubiKey, deberá realizar una serie de comprobaciones para verificar que el dispositivo no ha sido manipulado durante el transporte y que corresponde con el producto solicitado. Estas comprobaciones forman parte del proceso de aceptación segura del producto [REF2].

Las YubiKey se suministran en embalajes diseñados para evidenciar cualquier intento de manipulación, ver Ilustración 1, distribuyéndose en embalaje tipo "blister" (carcasa de plástico sellada) o en la caja con pestaña perforada de apertura. Estos embalajes están diseñados para que cualquier manipulación deje marcas visibles.

- **Embalaje tipo Blíster:** Consiste en una carcasa de plástico sellada. La parte trasera del cartón tiene una línea de puntos perforada para facilitar su apertura.
- **Embalaje en Caja:** Algunas YubiKeys se distribuyen en una caja de cartón con una pestaña perforada para su apertura.

Al recibir su YubiKey, inspeccione cuidadosamente los siguientes elementos del embalaje:

- **Sello del Blíster:** Verifique que el sello de la carcasa de plástico esté intacto y no presente signos de haber sido abierto o dañado.
- **Parte Trasera de Cartón:** Asegúrese de que la zona perforada en la parte trasera del embalaje de cartón no esté rota o dañada antes de que usted la abra.
- **Pestaña de la Caja:** Si su YubiKey viene en una caja, compruebe que la pestaña perforada de apertura esté intacta.
- **Embalaje no Oficial:** Asegúrese de que el embalaje se corresponde con el oficial de Yubico y no ha sido sustituido por otro no aprobado.



Ilustración 1. Ejemplo de embalaje original

4.1.1 SOFTWARE DE APOYO

Aunque el producto se puede configurar a través de protocolos estándar a través de software de terceras partes, se recomienda utilizar las herramientas software proporcionadas por Yubico. Estas herramientas son *YubiKey Manager*, *Yubico Authenticator* y *YubiKey Minidriver*.

Los productos **YubiKey Manager**, **Yubico Authenticator** y **YubiKey Minidriver** se distribuyen como software descargable a través del sitio web oficial del fabricante en la sección *Resources → Downloads*. Para garantizar la integridad y autenticidad del software antes de su instalación, el usuario deberá seguir el procedimiento descrito a continuación.

a) El usuario deberá acceder exclusivamente al sitio web oficial del fabricante mediante la URL:

   `https://www.yubico.com`

b) A continuación, deberá navegar hasta la sección **Resources → Downloads**, donde se encuentran disponibles las versiones oficiales de **YubiKey Manager** y **Yubico Authenticator**.

c) Antes de proceder a la descarga, el usuario deberá comprobar que:

   - La URL pertenece al dominio oficial yubico.com.
   - No existen redirecciones sospechosas a dominios no relacionados.
   - La URL utiliza el protocolo seguro HTTPS (https://).

d) El usuario deberá comprobar el certificado digital presentado por el sitio web, asegurándose de que:

   - El certificado ha sido emitido para el dominio `yubico.com`.
   - El certificado es válido y no está caducado.
   - La cadena de confianza del certificado es correcta (emitido por una Autoridad de Certificación reconocida).

e) Una vez verificadas la URL y el certificado, el usuario podrá proceder a la descarga del software correspondiente (instalador o paquete binario).

El producto YubiKey Minidriver permite la interacción directa de la YubiKey 5 CCN Series con las interfaces del Sistema Operativo Windows para gestionar tarjetas inteligentes (modo PIV).

La YubiKey 5 CCN Series es común que sea usado mediante protocolos estándar utilizando software de terceras partes, el uso de dicho software queda fuera del control del fabricante. En estos casos, es responsabilidad del administrador del sistema evaluar la idoneidad del software utilizado, así como verificar su integridad, autenticidad y correcto funcionamiento dentro del entorno operativo.

4.2 ENTORNO DE INSTALACIÓN SEGURO

La YubiKey se utiliza conectándola directamente a un equipo cliente (ordenador o dispositivo móvil) mediante interfaces USB o NFC.

No obstante, desde el punto de vista de seguridad operacional, los sistemas con los que interactúa la YubiKey (por ejemplo, estaciones de trabajo, sistemas operativos o

navegadores) deben considerarse plataformas de confianza y estar bajo el control de personal autorizado.

4.3 REGISTRO Y LICENCIAS

YubiKey 5 CCN Series es un dispositivo hardware que incorpora en su firmware todas las funcionalidades de seguridad necesarias, por lo que su uso no está condicionado a la activación de licencias adicionales tras la adquisición.

Tanto *YubiKey Manager* como *Yubico Authenticator* son herramientas de código abierto con licenciamiento *BSD-2* y *Apache License 2.0* respectivamente, por lo que pueden ser utilizadas sin restricciones.

4.4 CONSIDERACIONES PREVIAS

Si fuese necesaria una configuración adicional **relativa a la seguridad, previa a iniciar la instalación y configuración** del producto, deben indicarse **paso a paso en este documento** aquellos aspectos que se deban tener en cuenta, puesto que influirán en la forma de configurarlo de forma segura.

Por ejemplo: preparación de otros componentes necesarios (token de entropía, almacén de claves criptográficas, plataformas hardware, etc.), decisión sobre aspectos de arquitectura física (por ejemplo, alta disponibilidad), o lógica (por ejemplo, métodos de autenticación).

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El dispositivo requiere un ordenador o dispositivo móvil que disponga de un puerto USB (tipo A o C, según el modelo de YubiKey) o de un lector NFC para poder interactuar con él.

Adicionalmente, dependiendo de la funcionalidad que se vaya a utilizar, se necesita el siguiente software:

- **Para la autenticación FIDO2:** Es necesario un navegador web compatible con el estándar FIDO (y W3C WebAuthn), como Google Chrome, Mozilla Firefox, Safari o Microsoft Edge.
- **Para el uso como tarjeta inteligente (PIV):** Se requiere un sistema operativo o una aplicación (como OpenSC) que sea compatible con el estándar PIV y que pueda comunicarse con el dispositivo a través de CCID (Chip Card Interface Device).

5 FASE DE INSTALACIÓN

El producto, la YubiKey 5 CCN Series, es un dispositivo de hardware que se entrega al usuario con el *firmware* ya instalado y listo para su uso. Por lo tanto, no requiere un proceso de instalación de *firmware* por parte del usuario final. La interacción principal se realiza a través de las interfaces nativas del sistema operativo para PIV y de los navegadores web para FIDO, sin necesidad de instalar software adicional para su funcionamiento básico.

Para la gestión y configuración segura del dispositivo, se utiliza la aplicación Yubico Authenticator. Esta aplicación se ejecuta en plataformas de escritorio y permite al usuario configurar los parámetros de seguridad del dispositivo.

La instalación de las aplicaciones de escritorio para distintos sistemas operativos se encuentra en:

- La sección “install the App” de [REF3] para Yubico Authenticator.
- La sección “Installation” de [REF4] para YubiKey Manager.
- La sección “YubiKey Minidriver Installation” de [REF5] para YubiKey Minidriver.

Los procesos de instalación son directos y no requieren configuraciones adicionales que puedan impactar en la seguridad del producto. En particular, las aplicaciones se instalan siguiendo los procedimientos estándar del sistema operativo correspondiente, sin necesidad de modificar parámetros críticos, dependencias de seguridad ni realizar integraciones complejas.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Para que el producto opere en el modo de cumplimiento definido en la cualificación, no es necesario que el usuario active una configuración específica adicional sobre la YubiKey. En este caso, el requisito esencial consiste en utilizar desde el inicio una unidad perteneciente a la serie **YubiKey 5 CCN**, ya que esta variante limita el modo de operación de la versión genérica al modo cualificado.

6.2 AUTENTICACIÓN

A continuación, se describen los mecanismos de autenticación que utiliza el producto YubiKey 5 CCN Series.

El producto utiliza dos protocolos de autenticación dentro del alcance de la cualificación: FIDO2 y PIV. Para utilizar dichos protocolos el usuario se tiene que autenticar contra la YubiKey, así mismo la YubiKey se autentica con componentes externos. A continuación, se muestran los distintos tipos de autenticaciones.

6.2.1 AUTENTICACIÓN DE USUARIOS

La autenticación del usuario final para poder utilizar las funciones del dispositivo se realiza mediante credenciales locales gestionadas por el propio YubiKey. El usuario se autentica directamente en el dispositivo utilizando un PIN/PUK.

- **Para FIDO2:** Se utiliza un PIN para proteger el acceso a las credenciales almacenadas (passkeys). El dispositivo se bloquea tras 8 intentos fallidos.
- **Para PIV:** Se utiliza un PIN para acceder a los certificados y claves almacenados para operaciones como la firma digital o la autenticación. Dispone de un mecanismo de protección con un PUK (Personal Unblocking Key) que se requiere tras 3 intentos fallidos de PIN.

6.2.2 AUTENTICACIÓN CON COMPONENTES EXTERNOS

La autenticación del dispositivo YubiKey con servicios, servidores o aplicaciones externas se basa en criptografía de clave pública, donde la clave privada nunca abandona el dispositivo. Los mecanismos criptográficos utilizados por las funcionalidades FIDO2 y PIV permiten el empleo de algoritmos y longitudes de clave conformes con los requisitos de fortaleza criptográfica establecidos en la guía CCN-STIC 807.

- **Para FIDO2:** Para la autenticación en servicios web (Relying Parties), el YubiKey utiliza el protocolo FIDO2. Este proceso consta de dos fases:
  - **Registro:** El dispositivo genera un par de claves único para el servicio. La clave pública se envía al servidor, mientras que la privada permanece segura en el YubiKey.
  - **Autenticación:** El servicio envía un desafío al dispositivo, que lo firma con la clave privada y lo devuelve para su validación. Este mecanismo es resistente a ataques de phishing y man-in-the-middle.
- **Para PIV:** En su modo PIV, la YubiKey funciona como una tarjeta inteligente (Smart Card) que almacena certificados digitales y sus claves privadas asociadas. Permite

realizar operaciones criptográficas como la firma de desafíos para autenticarse en sistemas compatibles con PKI (Infraestructura de Clave Pública), como el inicio de sesión en sistemas operativos o el acceso a aplicaciones corporativas.

Para más información sobre el proceso de autenticación consultar los estándares [REF6] y [REF7] para FIDO y PIV respectivamente.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración del dispositivo se realiza a través de aplicaciones cliente ejecutadas en el equipo anfitrión, principalmente mediante la aplicación Yubico Authenticator [REF3] y herramientas compatibles con el estándar PIV (por ejemplo, OpenSC), que actúan como interfaz de gestión del dispositivo. Estas aplicaciones se comunican con la YubiKey a través de las interfaces USB o NFC.

La interacción se lleva a cabo utilizando software cliente que se comunica con la YubiKey a través de:

- **GUI (Interfaz Gráfica de Usuario):** La aplicación Yubico Authenticator es la herramienta principal recomendada para la configuración y gestión del dispositivo. Permite gestionar las aplicaciones FIDO2 y PIV, establecer los PINs, y cambiar la clave de gestión.
- **CLI (Interfaz de Línea de Comandos):** Para una gestión más avanzada, especialmente para la funcionalidad PIV, se pueden utilizar herramientas como OpenSC o la herramienta YubiKey Manager [REF4], que ofrecen una interfaz de línea de comandos. Estas herramientas interactúan con el dispositivo a través de la interfaz CCID (Chip Card Interface Device).

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

El YubiKey 5 CCN Series es un dispositivo de autenticación personal. El propietario del dispositivo actúa como el único administrador del mismo, siendo responsable de su gestión. No existen roles de administración delegada; el control se ejerce mediante el conocimiento de las credenciales de seguridad (PIN, PUK y Clave de Gestión).

La herramienta principal para la configuración del producto es la aplicación Yubico Authenticator, disponible para sistemas de escritorio y móviles. La documentación de referencia del fabricante se encuentra en [REF3].

Los mecanismos de bloqueo contra ataques de fuerza bruta están integrados en el firmware del dispositivo y no son configurables por el usuario. Es fundamental conocer su funcionamiento:

- **FIDO:** El dispositivo se bloquea tras **ocho (8) intentos** fallidos del PIN. Este bloqueo requiere un reseteo de la aplicación FIDO, eliminando todas las *Passkeys* almacenadas.
- **PIV**: El PIN se bloquea tras **tres (3)** intentos fallidos. Se puede desbloquear usando el PUK. Si el PUK falla **tres (3)** veces, la aplicación PIV se bloquea permanentemente, perdiéndose todos los certificados y claves PIV.

6.3.2.1 CONFIGURACIÓN DEL PIN DE FIDO2 (PARA PASSKEYS)

El PIN de FIDO2 es una credencial local que protege el acceso y la creación de *Passkeys* (credenciales sin contraseña) en el dispositivo. Actúa como un factor de verificación del usuario (`User Verification`), asegurando que solo el propietario legítimo pueda autorizar operaciones de autenticación. Es fundamental establecer un PIN robusto desde el inicio para proteger las credenciales FIDO2 almacenadas contra el uso no autorizado.

Existen tres métodos principales para configurar o modificar el PIN de FIDO2. En cualquiera de los tres métodos de deben seguir la siguiente política de contraseñas:

Longitud mínima: Doce (12) caracteres.

Composición: Mezcla de mayúsculas, minúsculas, números y símbolos.

Configuración del PIN a través de la aplicación Yubico Authenticator

En Yubico Authenticator, navegue a la pestaña `Passkeys`.

Haga clic en la opción `Set PIN` (Establecer PIN), ver Ilustración 2.

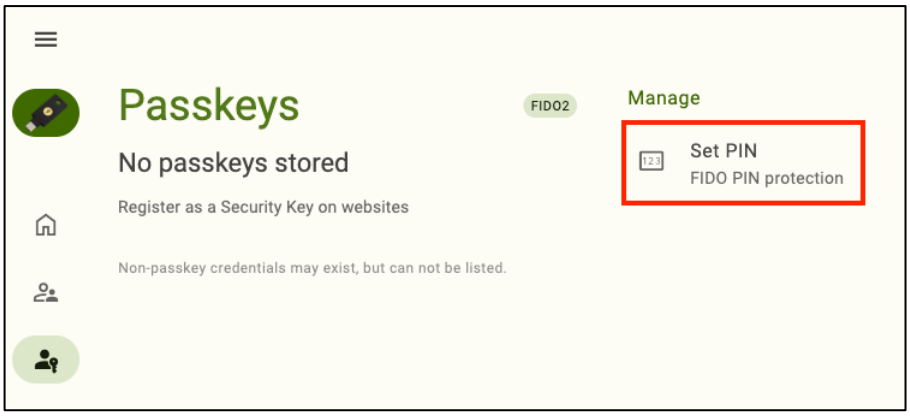


Ilustración 2. Pantalla de configuración de Passkeys

Introduzca un PIN seguro en el campo `New PIN`.

Confirme el nuevo PIN y guárdelo, ver Ilustración 3.

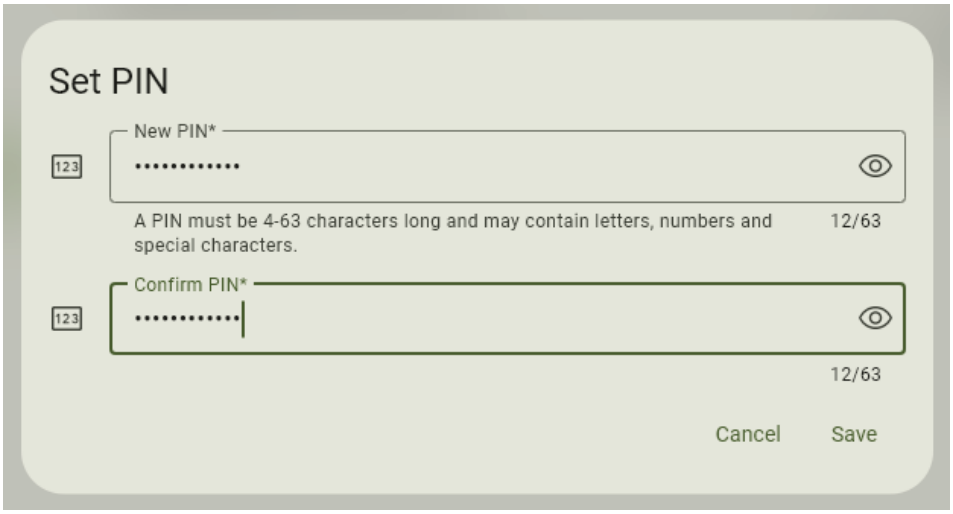


Ilustración 3. Creación de un nuevo PIN

Configuración del PIN a través de la configuración del Sistema Operativo Windows

a) En Windows vaya a **Configuración > Cuentas > Opciones de inicio de sesión.**

b) Seleccione Llave de seguridad y haga clic en Administrar.

c) Inserte su YubiKey y siga las instrucciones en pantalla para establecer o cambiar el PIN.

Configuración del PIN a través del Navegador Web Google Chorme

Este método es especialmente útil en sistemas operativos como macOS o Linux, donde la integración nativa puede ser menos directa.

a) Abra el navegador Google Chrome.

b) Haga clic en el icono de los tres puntos situado en la esquina superior derecha de la ventana.

c) Seleccione la opción `Configuración`.

d) En el menú lateral, acceda a `Privacidad y seguridad`.

e) Seleccione la opción `Seguridad`.

f) Desplácese hasta la sección de configuración avanzada y haga clic en `Gestionar claves de seguridad`.

g) Conecte la llave de seguridad al equipo, en caso de que no esté ya conectada.

h) Seleccione la opción `Crear un PIN`.

i) Introduzca el PIN deseado y vuelva a introducirlo para confirmarlo, siguiendo las instrucciones mostradas en pantalla.

6.3.2.2 CONFIGURACIÓN DE CREDENCIALES PIV (PIN, PUK Y CLAVE DE GESTIÓN)

La funcionalidad PIV (Verificación de Identidad Personal) del dispositivo está protegida por tres credenciales distintas: el PIN, el PUK y la Clave de Gestión. El PIN se utiliza para las operaciones diarias de autenticación y firma; el PUK sirve para desbloquear el PIN en caso de bloqueo; y la Clave de Gestión es necesaria para administrar los certificados. Cambiar estas tres credenciales de sus valores de fábrica es el paso de seguridad más importante para proteger la infraestructura de clave pública (PKI) que alberga el dispositivo.

En Yubico Authenticator, navegue a la pestaña `Certificates (PIV)`

El panel de `Manage` (Administrar) mostrará advertencias sobre el uso de credenciales por defecto. Proceda a cambiarlas:

- **Cambiar PIN:** Haga clic en `Change PIN`. Introduzca el PIN por defecto (`123456`) y, a continuación, el nuevo PIN de ocho (8) caracteres compuestos por letras y números. Ver Ilustración 4.

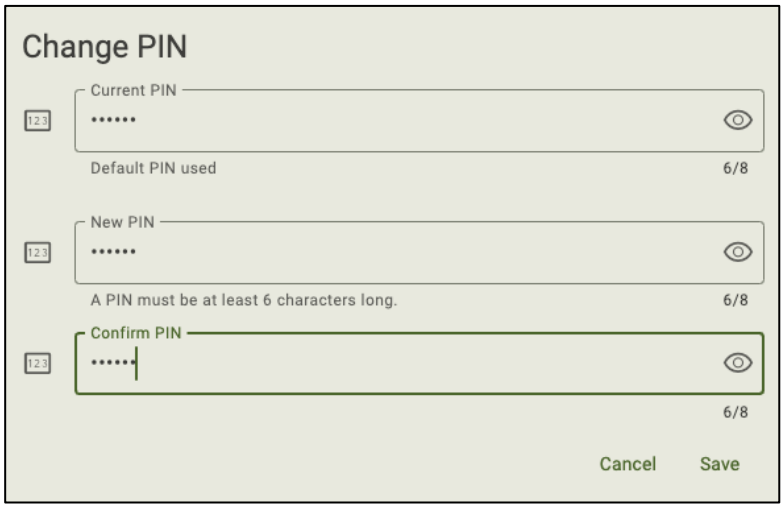


Ilustración 4. Pantalla de cambio de PIN

- **Cambiar PUK:** Haga clic en `Change PUK`. Introduzca el PUK por defecto (`12345678`) y, a continuación, el nuevo PUK de ocho (8) caracteres compuestos por letras y números. Ver Ilustración 5.

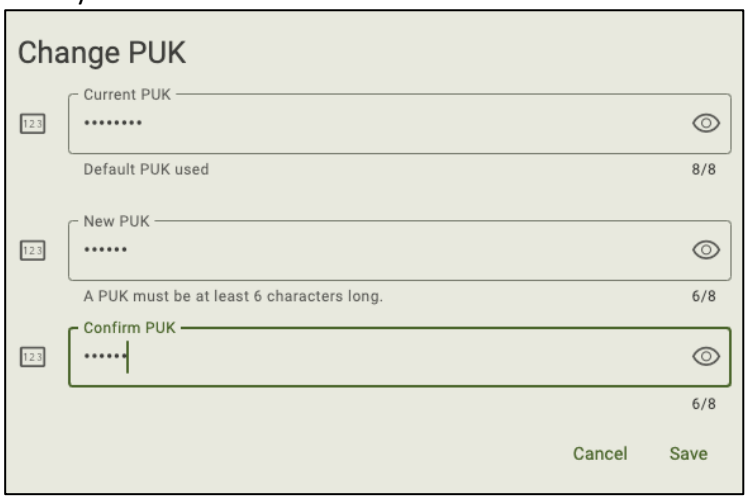


Ilustración 5. Pantalla de cambio de PUK

- **Cambiar Clave de Gestión (`Management Key`):** Haga clic en `Management Key`. Introduzca la clave por defecto y establezca una nueva clave segura. Se recomienda que la aplicación genere una para máxima seguridad. Importante: Guarde una copia de esta clave en un lugar seguro (gestor de contraseñas), ya que es necesaria para futuras tareas de administración de certificados. Para mayor protección se puede proteger con PIN mediante AES 256. Ver Ilustración 6.

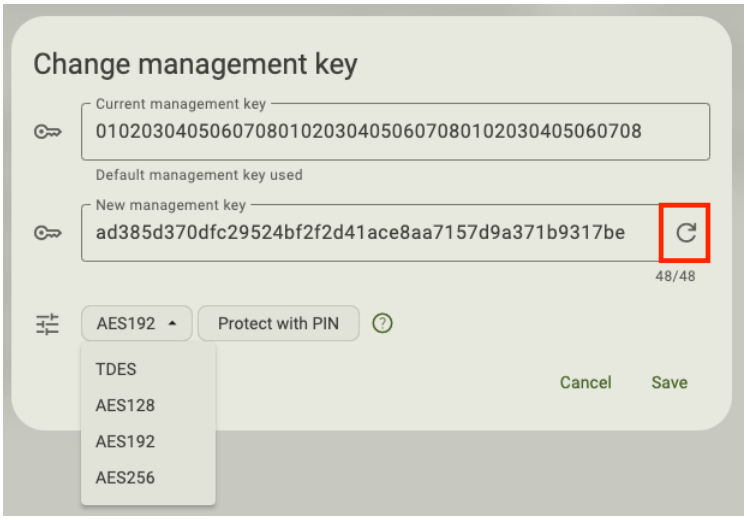


Ilustración 6. Actualización de Management Key

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

En la YubiKey 5 CCN, la configuración segura de interfaces consiste en reducir la superficie de exposición del dispositivo dejando habilitadas únicamente las funcionalidades necesarias para el uso seguro. De acuerdo con la configuración segura definida para el producto, deben dejarse activadas solo las aplicaciones **PIV**, **FIDO2** o ambas, según las funcionalidades requeridas, en los transportes **USB** y **NFC**, deshabilitando el resto de las aplicaciones no requeridas. Esta medida evita que aplicaciones fuera del alcance de la configuración cualificada puedan interactuar con equipos externos a través de la llave.

La aplicación Yubico Authenticator [REF3] se utilizará para esta configuración. Siga los siguientes pasos:

a) Conecte la YubiKey al equipo.

b) Utilizando Yubico Authenticator, En la página `Home`, haga clic en `Device → Toggle applications`. Ver Ilustración 7.



Ilustración 7. Página Home, remarcado *Toggle applications*

c) Deje seleccionadas únicamente las aplicaciones **PIV y FIDO2** para los métodos de comunicación **USB y NFC**. Haga clic en “Save”. Ver Ilustración 8.

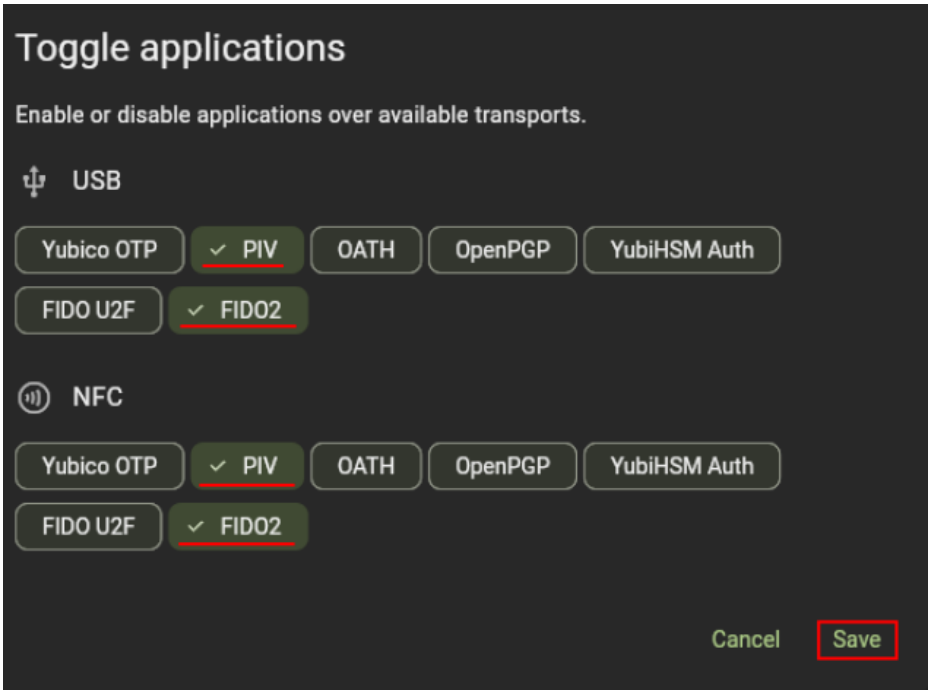


Ilustración 8. Configurando protocolos disponibles y métodos de comunicación (remarcado)

6.5 GESTIÓN DE CERTIFICADOS

La gestión explícita de certificados únicamente aplica a la funcionalidad PIV del dispositivo. En el caso de FIDO2, la creación y utilización de las credenciales criptográficas se realiza de forma transparente para el usuario y para los servicios compatibles con WebAuthn/FIDO2, sin que sea necesaria la generación de solicitudes de certificado (CSR), la emisión o importación de certificados digitales ni la gestión de Autoridades de Certificación.

Por el contrario, cuando se utiliza la funcionalidad PIV, el usuario o administrador debe gestionar de forma explícita los certificados digitales y claves asociadas, tal y como se describe a continuación.

En modo PIV, la generación de claves criptográficas, la solicitud de certificados (CSR), la importación de certificados de usuario y la importación de certificados de Autoridades de Certificación (CA) se realizan mediante la funcionalidad PIV del dispositivo. Estas operaciones pueden realizarse utilizando herramientas compatibles con PIV, como YubiKey Manager [REF4], Yubico Authenticator [REF3] u otras herramientas compatibles con tarjetas inteligentes (por ejemplo, OpenSC).

De forma general, el procedimiento para la gestión de certificados es el siguiente:

a) **Generación del par de claves en la YubiKey:** Se genera el par de claves RSA-3072 o ECC P-256/P-384 directamente dentro del dispositivo mediante la funcionalidad PIV, de forma que la clave privada nunca abandona el dispositivo.

b) **Solicitud de certificado (CSR):** Se genera una solicitud de certificado (CSR) asociada a la clave generada en la YubiKey mediante YubiKey Manager o herramientas PIV compatibles. Alternativamente, esta gestión puede realizarse con un CMS (Certificate Management System) o utilizando las herramientas nativas de certificados de Windows dentro de un entorno de Directorio Activo de Microsoft.

c) **Firma del certificado por la Autoridad de Certificación:** La CSR se envía a la Autoridad de Certificación correspondiente para la emisión del certificado digital, ya sea a través de procesos manuales o integrados en un CMS o infraestructura de Active Directory.

d) **Importación del certificado en la YubiKey:** Una vez emitido el certificado, este se importa en el slot correspondiente del contenedor PIV de la YubiKey.

e) **Importación de certificados de Autoridades de Certificación (CA):** Los certificados de las Autoridades de Certificación raíz o intermedias pueden importarse en el sistema operativo o en la aplicación que vaya a utilizar la YubiKey para permitir la validación de la cadena de certificación, incluyendo su distribución automática mediante políticas de grupo (GPO) en entornos Active Directory cuando aplique.

Si ya se dispone de un certificado y su clave privada correspondiente, estos se pueden introducir en la YubiKey siguiendo las indicaciones de la sección `Certificates: PIV -> Add and manage certificate` en [REF3].

Toda la gestión criptográfica se realiza dentro del entorno seguro del dispositivo, y las claves privadas generadas o importadas están marcadas como **no exportables**, garantizando su protección conforme a los requisitos de seguridad del ENS.

6.6 SERVIDORES DE AUTENTICACIÓN

La YubiKey 5 CCN Series no utiliza directamente servidores de autenticación externos como RADIUS, LDAP, SAML o Kerberos. La YubiKey es un dispositivo de autenticación del lado del cliente que funciona como un segundo factor (2FA).

6.7 SINCRONIZACIÓN

El producto no dispone de reloj interno ni realiza sincronización de tiempo de forma autónoma. La sincronización horaria es responsabilidad del sistema operativo o de los sistemas y servicios externos con los que se integra el producto (por ejemplo, sistemas de autenticación, servidores de identidad, servidores de certificados, etc.), que son los que utilizan la información temporal para la validación de certificados, autenticaciones, registros de eventos y otros procesos de seguridad.

Por este motivo, se recomienda que los sistemas en los que se utilice el producto estén sincronizados con una fuente de tiempo fiable mediante el protocolo NTP (Network Time Protocol), preferiblemente con servidores NTP internos de la organización o, en su defecto, con servidores NTP públicos de confianza.

6.8 ACTUALIZACIONES

Las actualizaciones de firmware de la serie YubiKey 5 CCN no son realizadas por el usuario final. Estos dispositivos están diseñados como elementos de seguridad de hardware y su firmware se programa durante la fabricación en entornos controlados para garantizar su integridad.

Por tanto, el administrador no dispone de mecanismos para instalar, modificar o actualizar el firmware del dispositivo.

6.9 BACKUP

En el caso del producto YubiKey 5 CCN Series, las copias de seguridad no se realizan sobre el propio dispositivo, ya que las claves privadas y el material criptográfico almacenado en la YubiKey están diseñados para ser **no exportables**, por lo que no es posible realizar copias de seguridad directas de dicho material. Este diseño forma parte de las medidas de seguridad del producto para evitar la clonación del dispositivo o la extracción de claves criptográficas.

No obstante, deben realizarse copias de seguridad de los elementos externos asociados al uso del dispositivo, que son necesarios para la recuperación del servicio en caso de pérdida, robo o fallo del dispositivo. En concreto, se recomienda realizar copias de seguridad de los siguientes componentes:

- Certificados digitales y claves privadas generadas fuera de la YubiKey antes de su importación al dispositivo.
- Autoridades de certificación (CA) y cadenas de certificados asociadas.
- Configuración de los servicios donde la YubiKey está registrada como segundo factor.
- Documentación de configuración del dispositivo (PIN policy, PIV configuration, etc.).
- Copias de seguridad de los sistemas o servicios donde se utilicen los certificados almacenados en la YubiKey.

Se recomienda realizar copias de seguridad de forma periódica de todos los elementos indicados anteriormente, especialmente de certificados, configuraciones y códigos de recuperación de servicios FIDO2. Asimismo, se recomienda disponer de **dispositivos YubiKey de respaldo** previamente configurados, de forma que, en caso de pérdida o fallo del dispositivo principal, se pueda mantener el acceso a los sistemas sin necesidad de realizar procedimientos de recuperación de emergencia.

7 REFERENCIAS

[REF1] Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

[REF2] YubiKey packaging
https://www.yubico.com/support/shipping-and-buying-information/packaging/

[REF3] Yubico Authenticator User Guide
https://docs.yubico.com/software/yubikey/tools/authenticator/auth-guide/index.html

[REF4] YubiKey Manager (ykman) CLI User Guide
https://docs.yubico.com/software/yubikey/tools/ykman/

[REF5] YubiKey Minidriver User Guide
https://docs.yubico.com/software/yubikey/tools/minidriver/

[REF6] FIDO 2.0: Key Attestation Format
https://www.w3.org/submissions/2015/SUBM-fido-key-attestation-20151120/

[REF7] FIPS 201-3 - Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022
https://csrc.nist.gov/pubs/fips/201-3/final

8 ABREVIATURAS

2FA	Two Factor Authentication
AES	Advanced Encryption Standard
CA	Certification Authority
CCID	Chip Card Interface Device
CLI	Command Line Interface
CSR	Certificate Signing Request
ECC	Elliptic Curve Cryptography
ENS	Esquema Nacional de Seguridad.
FIDO	Fast Identity Online
FIDO2	Fast Identity Online 2
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
NFC	Near Field Communication
NTP	Network Time Protocol
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
RADIUS	Remote Authentication Dial In User Service
RSA	Rivest Shamir Adleman
SAML	Security Assertion Markup Language
URL	Uniform Resource Locator
USB	Universal Serial Bus
W3C	World Wide Web Consortium