2N PICard Commander

Manual de instalación

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Tabla de contenidos

Símbolos y términos utilizados.

Los siguientes símbolos y pictogramas se utilizan en el manual:

PELIGRO
Siga siempre las recomendaciones aquí descritas para evitar daños personales.

AVISO
Siga siempre las recomendaciones aquí descritas para evitar daños en los dispositivos.

ATENCIÓN
Información importante para el correcto funcionamiento del sistema.

SUGERENCIA
Información útil para la funcionalidad rápida y eficiente.

NOTA
Procedimientos y consejos para el uso efectivo de las funciones del dispositivo.

Descripción del Producto

2N PICard Commander es una aplicación de software para cifrar credenciales en tarjetas de acceso. La aplicación crea proyectos que generan un conjunto de claves de cifrado y lectura. Las claves del lector de proyectos se pueden importar a dispositivos 2N o a **Access Commander**, que posteriormente garantiza la distribución de claves de lectura a los dispositivos 2N conectados.

Tecnología 2N PICard está destinado al cifrado de tarjetas MIFARE DESFire EV2 y MIFARE DESFire EV3.

en la aplicación **PICard Commander** es posible borrar los datos registrados en las tarjetas de acceso.

Características de la aplicación **PICard Commander** está sujeto a la compra de una licencia.

Productos relacionados

2N Nº de referencia: 91379601

Axis Nº de referencia 02722-001

Licencia 2N PICard Commander

La licencia siempre se emite para un lector de tarjetas USB específico según la clave de dispositivo del lector determinado. Los lectores de claves del dispositivo se pueden encontrar antes de cargar la licencia en **PICard Commander**. Los lectores de tarjetas USB compatibles se enumeran a continuación.

2N Nº de referencia: 9137421E

Axis Nº de referencia 01400-001

Lector USB de tarjetas RFID de 13,56 MHz, 125 kHz y dispositivos NFC/HCE

Lector de tarjetas RFID externo para conexión a PC mediante interfaz USB. Adecuado para la gestión del sistema y la adición de tarjetas de 13,56 MHz, 125 kHz y dispositivos Android con soporte NFC/HCE a través de la interfaz web o la aplicación del intercomunicador IP 2N **Access Commander**. Adecuado para cargar tarjetas MIFARE DESFire a una aplicación de cifrado **PICard Commander**[a]. Lee los mismos tipos de tarjetas y dispositivos que los lectores de tarjetas de los intercomunicadores IP 2N:

Tarjetas RFID compatibles 125 kHz:

- EM4x02
- HID Prox

Tarjetas RFID compatibles 13,56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**

2N Nº de referencia: 9137424E

Axis Nº de referencia 01527-001

asegurado Lector USB de tarjetas RFID de 13,56 MHz, 125 kHz y dispositivos NFC/HCE

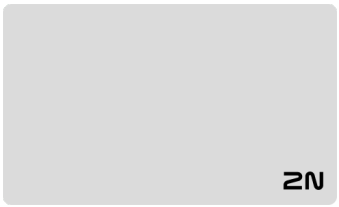
Lector de tarjetas RFID externo seguro para conexión a PC mediante interfaz USB. Adecuado para la gestión del sistema y la adición de tarjetas de 13,56 MHz, 125 kHz y dispositivos Android con soporte NFC/HCE a través de la interfaz web o la aplicación del intercomunicador IP 2N **Access Commander**. Adecuado para cargar tarjetas MIFARE DESFire a una aplicación de cifrado **Comando 2N PICard**año[a.]. Lee los mismos tipos de tarjetas y dispositivos que los lectores de tarjetas de los intercomunicadores IP 2N:

125 kHz

- EM4xxx
- HID Prox

13.56 MHz

- ISO14443A (MIFARE DESFire)
- PicoPass (HID iClass)
- FeliCa
- ST SR(IX)
- My2N
- HID SE (Seos, iClass SE, MIFARE SE)



2N Nº de referencia: 11202601

Axis Nº de referencia 02787-001

Tarjeta RFID 2N MIFARE Desfire EV3 4K 13.56MH 10uds

paquete de 10 piezas

MIFARE DESFire EV3 (ISO14443A)

2N Nº de referencia: 11202602

Axis Nº de referencia 02788-001

Llavero RFID 2N MIFARE Desfire EV3 4K 13.56MHz 10 piezas

paquete de 10 piezas

MIFARE DESFire EV3 (ISO14443A)

[a.] Tecnología **2N PICard** está destinado al cifrado de tarjetas MIFARE DESFireEV2 y MIFARE DESFire EV3.

Dispositivos compatibles

La lectura de PICard es compatible con todos los módulos lectores RFID 2N lanzados en febrero de 2023 o después. La mayoría de los lectores internos fabricados después de esta fecha también son compatibles, excepto los modelos que se indican a continuación.

Los siguientes modelos **no son compatibles**:

- **2N IP Base**: todos los lectores RFID
- **2N IP Force**: 9151011, 9151012, 9151016, 9151017, 9151019
- **2N IP Vario**: todos los lectores RFID
- **2N IP Verso**: 915503x, 915504x, 915508x
- **2N Access Unit M**: 91611x
- **2N Access Unit 1.0**: 916008, 916009, 916010, 916011, 916013, 916016, 916019
- **2N Access Unit 2.0**: 916033x

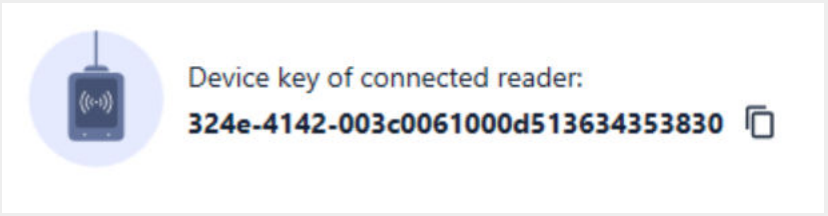
Para los siguientes módulos, la compatibilidad sólo está garantizada para las unidades fabricadas en otoño de 2023 o después:

- **2N IP Force**: 9151031, 9151031S

Instalación y carga de licencias.

1. Instalarlo **PICard Commander** de la forma habitual a través del instalador.
2. Tras iniciar la aplicación, cargue la licencia haciendo clic en la Load License de la barra naranja (o en **Help > License**). A continuación, cargue el archivo de licencia desde el disco. El lector de tarjetas debe estar conectado al ordenador para cargar correctamente la licencia.

NOTA
La licencia está vinculada a un lector de tarjetas USB específico. Por lo tanto, para obtener una licencia, es necesario ingresar la clave del dispositivo del dispositivo lector, que se puede encontrar en la información de la licencia en **PICard Commander** (**Help > License**). Para mostrar la clave, el lector de tarjetas debe estar conectado a la computadora.



Conectando otro lector

Si se conecta a la computadora un lector distinto al emparejado con la licencia en uso, la aplicación **PICard Commander** Te notificará después de comenzar. Puede cargar una nueva licencia en la pestaña **Help > License**.

Proyecto

La creación de proyectos individuales permite cifrar grupos de tarjetas de acceso en diferentes modos. Puede configurar cada proyecto específicamente para utilizar las tarjetas. El proyecto genera una serie de claves de cifrado y lectura. Al dispositivo o al Access Commander puedes cargar las claves de lectura de un solo proyecto a la vez.

Creando un nuevo proyecto

Después de abrir la aplicación, presione el botón para crear un nuevo proyecto **Start new project**.

Ruta alternativa: pestaña **File > New project**

Se abrirá un asistente de configuración de nuevo proyecto, siga los pasos a continuación Configuración del proyecto (p. 9).

Abriendo el proyecto

1. En la interfaz inicial de la aplicación, haga clic en el botón Open project.
   Ruta alternativa: pestaña **File > Open project**

Los proyectos abiertos más recientemente se muestran en la sección inferior de la interfaz inicial de la aplicación.

Configuración del proyecto

Al iniciar un proyecto, es necesario configurar sus parámetros.

La configuración se puede cambiar más adelante en la configuración del Proyecto en la interfaz inicial de la aplicación (ruta alternativa: pestaña **Project > Change configuration**).

Configuraciones básicas (Basic settings)

- **Project name** – nombre del proyecto
- **Project description** – espacio para ingresar notas sobre el proyecto

Clave de cifrado principal (Main Encryption Key)

En función de la clave maestra de cifrado (MEK), **2N PICard Commander** genera un conjunto de claves de cifrado. Por lo tanto, la clave debe ser única y suficientemente segura. El conjunto de claves se basa en la clave de cifrado maestra, por lo que los proyectos con la misma clave de cifrado maestra generan los mismos conjuntos de claves. Si se pierde un proyecto, se puede crear uno nuevo con la misma clave maestra de encriptación y continuar con la encriptación.

AVISO
La clave de cifrado maestra no puede ser posterior **ver o cambiar**.

SUGERENCIA
Para máxima seguridad, es importante guardar tanto el archivo del proyecto como la clave de cifrado maestra (MEK). Es ideal almacenar la clave de cifrado maestra (MEK) de forma segura lejos del entorno en línea, por ejemplo, en una caja fuerte, caja de seguridad, etc.

Modo de cifrado (Card mode)

Es posible elegir entre los siguientes modos de cifrado de tarjetas:

- **Card may be used for other applications later on (best compatibility)** – Las tarjetas serán utilizadas principalmente por sistemas 2N. Los datos de la tarjeta se cifrarán, pero su UID seguirá siendo legible para aplicaciones de terceros. Las tarjetas se pueden reformatear a su estado original.
- **Card will be used only for access control with 2N devices (best privacy)** – Las tarjetas se utilizarán exclusivamente en sistemas 2N. Los parámetros de la tarjeta se restablecerán permanentemente. Cuando está cifrada, la función de identificación aleatoria se activa en la tarjeta.
- **Card is already used for other applications (advance settings)** – Las aplicaciones de terceros ya están cargadas en las tarjetas. En el siguiente paso, puede configurar los parámetros seleccionados de las tarjetas MIFARE DESFire cuyos datos de acceso tiene la tecnología. 2N PICard para cifrar en el proyecto.

NOTA
Selección de modo **Card is already used for other applications** es irreversible.

En el siguiente paso, puede completar:

- **Application ID (AID)** – el código bajo el cual se realizará la solicitud 2N PICard identificado en la tarjeta. La AID está preestablecida en 53324E.
- **PICC master key type** – el tipo de clave maestra PICC configurada en las tarjetas que tiene la aplicación 2N Picard cifrar.
- **PICC master key** – el valor de las tarjetas de llave maestra PICC que tiene la aplicación 2N Picard cifrar.
- **Enable randomisation of readable card ID** – activar la función ID aleatoria garantiza que el UID de la tarjeta cambie aleatoriamente cada vez que se carga. Por tanto, una persona no autorizada no puede hacer un uso indebido de la tarjeta para identificar a su titular.
- **Cifrar tarjetas en el estado predeterminado de fábrica (cambiar la clave maestra PICC predeterminada)** – opción para cargar la clave maestra PICC especificada en otras tarjetas en blanco al cifrarlas en el proyecto. Si esta opción no está seleccionada, **PICard Commander** se negará a cifrar una tarjeta vacía.

AVISO

- Tras el proceso de cifrado de tarjetas con el nuevo AID, deberá volver a exportar las claves de lectura. Las tarjetas previamente encriptadas con el antiguo AID se volverán ilegibles para el dispositivo 2N.
- Al cambiar la clave maestra PICC en un proyecto con tarjetas ya encriptadas, será imposible modificar estas tarjetas más adelante en el proyecto y borrar sus datos. La validez de las tarjetas de autenticación en el dispositivo 2N no se verá afectada.
- Activar la función de tarjeta de identificación aleatoria es irreversible. El UID original de la tarjeta permanece ilegible incluso después de formatear la tarjeta.

Guardar en el disco

El archivo del proyecto se guarda en el disco como *Nombre del proyecto*.picprj.

Marcando la casilla **Protect project file with password** le permite establecer una contraseña para abrir el proyecto. La contraseña se puede cambiar más adelante en la pestaña **Project > Change protection password**.

AVISO
No podrás olvidar tu contraseña más tarde **ver o restaurar**.

Cifrado y lectura de tarjetas.

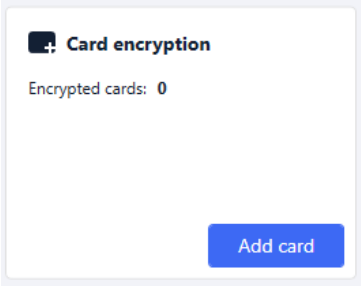
A continuación se ofrece una descripción general de lo que encontrará en el capítulo:

Card encryption

El proceso de cifrado de tarjetas en **PICard Commander** asigna a cada tarjeta un identificador único de 128 bits, que luego se cifra utilizando las claves de cifrado del proyecto respectivo. En el proyecto es posible cargar la tarjeta y así conocer su identificador asignado, posiblemente otra información sobre la tarjeta y si es posible cifrarla en el proyecto.

Proceso de cifrado

1. En la interfaz inicial de la aplicación, haga clic en **Add card** en la sección **Card encryption**.
   Ruta alternativa: pestaña **Project > Encrypt New Card**



   Credential ID for new card – nuevo identificador de la tarjeta cargada
2. Coloque la tarjeta en el lector. Al presionar el botón **Encrypt** A la tarjeta se asignan datos de acceso que al mismo tiempo están cifrados.

> **SUGERENCIA**
> Al marcar la casilla de la derecha, puede iniciar el cifrado automático de otras tarjetas adjuntas sin tener que presionar el botón nuevamente **Encrypt**.

3. La aplicación informa sobre el cifrado exitoso de la tarjeta.

Si no se pudo cifrar la tarjeta, la aplicación informa el motivo:

- **Card cannot be encrypted** – solicitud **PICard Commander** no tiene acceso a la tarjeta de llave maestra PICC. Si desea cifrar tarjetas con una clave maestra PICC preestablecida, debe seleccionar el modo de cifrado apropiado en Configuración del proyecto (p. 9).
- **Not enough free space on card** – no hay suficiente espacio en la tarjeta para cargar la tecnología **2N PICard**. La memoria mínima requerida es 512 B.
- **Unsupported card** – la aplicación no soporta este tipo de tarjeta. Tecnología **2N PICard** está diseñado para cifrar tarjetas MIFARE DESFire EV2 y EV3.
- **Only MIFARE DESFire EV2 or EV3 are supported** – la aplicación no soporta este tipo de tarjeta. La tarjeta cargada es MIFARE DESFire EV1.
- **Communication failure with card** – el lector no pudo leer la tarjeta. Coloque la tarjeta contra el lector y no la retire hasta que se complete el proceso de cifrado.

SUGERENCIA
En la sección inferior de la ventana hay una lista desplegable de identificadores de tarjetas cifradas. Si desea guardar la lista, cópiela antes de cerrar la ventana. Al cerrar la ventana se elimina la lista. Posteriormente, los identificadores sólo se podrán mostrar para tarjetas individuales.

Exportación de claves de lectura

Para que los dispositivos 2N puedan acceder a los datos de las tarjetas cifradas, necesitan conocer las claves de lectura del proyecto. Desde el **PICard Commander**, las claves de lectura pueden exportarse a un dispositivo 2N o al **Access Commander**, que se encarga de distribuirlas a todos los dispositivos 2N conectados. Una vez cargadas las claves de lectura en los dispositivos, éstos también podrán leer las tarjetas que se hayan cifrado en el proyecto después de cargar las claves de lectura.

1. Haga clic en Export en la sección Exportación de claves de lectura de la interfaz de inicio de la aplicación (ruta alternativa: **Project > Export reader keys**).
2. Puede exportar claves del lector de proyectos de dos maneras:

   - Exportar claves a un archivo (p. 13)
   - Subir claves a Access Commander (p. 13)

ATENCIÓN
Si acaba de conectar un módulo de ampliación del lector de tarjetas RFID al dispositivo 2N mediante un cable VBUS, deberá emparejar este módulo con el dispositivo. El emparejamiento del módulo de ampliación del lector puede realizarse a través de la interfaz web del dispositivo en **Acceso > Módulos**.

Exportar claves a un archivo

La aplicación genera un archivo clave y lo guarda en el disco. Luego, el archivo debe importarse a la configuración del dispositivo 2N o a **Access Commander** a través de sus interfaces web. En el siguiente paso de exportación, es posible establecer una contraseña para el archivo guardado.

- **Importar a Access Commander** a través de la interfaz web: **Configuración del sistema > 2N PICARD > sección** IMPORTAR
- **Importación al dispositivo 2N** a través de la interfaz web: **Access > Secure Cards > PICard Key**

Subir claves a Access Commander

Solicitud **PICard Commander** carga claves de lectura directamente a Access Commander, que garantiza la distribución posterior a los dispositivos 2N conectados. En el siguiente paso, es necesario ingresar los datos de inicio de sesión del administrador para la licencia. Access Commander.

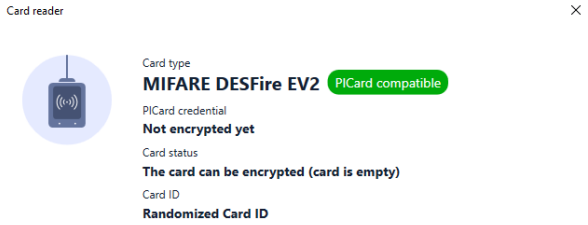
Address – Dirección HTTP de la interfaz web Access Commander

Login name – nombre de inicio de sesión de la cuenta de administrador v Access Commander

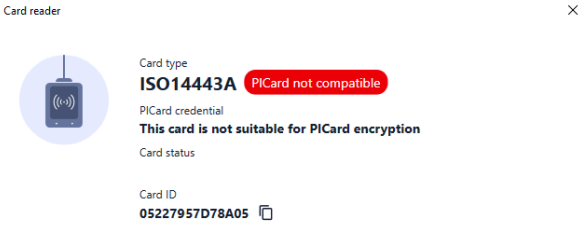
Password– contraseña de inicio de sesión para la cuenta dada v Access Commander

Leer información de la tarjeta

El identificador de tarjeta asignado y otra información sobre la tarjeta y sus opciones de cifrado se pueden ver en la pestaña **Project > Read card**. La información se lee cuando la tarjeta se aplica al lector.



Esta tarjeta se puede cifrar en la aplicación.



Este tipo de tarjeta no se puede cifrar en la aplicación.

PICard credential ecupera el identificador de la tarjeta asignado durante el proceso de cifrado. Si la tarjeta no tiene identificador aparecerá información sobre sus opciones de asignación:

- **Not encryptable** – el tipo de tarjeta es compatible con la tecnología 2N PICard, pero el proyecto no tiene acceso a su clave maestra PICC.
- **This card is not suitable for PICard encryption** – la aplicación no soporta este tipo de tarjeta. Tecnología 2N PICard está destinado al cifrado de tarjetas MIFARE DESFire EV2 y EV3.
- **Not encrypted yet** – la tarjeta se puede cifrar.
- **Unknown** – la tarjeta está cifrada en otro proyecto con una clave de cifrado maestra diferente. La tarjeta también podría estar dañada.

Card Status muestra el estado o las opciones de cifrado de la tarjeta dada:

- **Valid PICard credential** – la tarjeta está cifrada en este proyecto.
- **The card can be encrypted (card is empty)** – la tarjeta no está cifrada. Hay configuraciones de fábrica en la tarjeta.
- **The card can be encrypted** – la tarjeta no está cifrada. En la tarjeta se establece una clave maestra PICC compatible con este proyecto.
- **Different PICC Master Key detected. Card's current PICC Master Key required for encryption** – la tarjeta no se puede cifrar en este proyecto. La clave maestra PICC configurada es diferente.
- **PICard application created in a different project, so cannot be read in this project** – la tarjeta está cifrada en otro proyecto.
- **Only MIFARE DESFire EV2 or EV3 are supported** – la tarjeta no se puede cifrar. La aplicación no soporta este tipo de tarjeta. La tarjeta cargada es MIFARE DESFire EV1.
- **INVALID CREDENTIAL (there's a problem with the digital signature)** – no se pueden visualizar los datos de acceso cifrados de la tarjeta. No se pudo confirmar su autenticidad. La firma digital no es válida.

Card ID muestra el UUID de la tarjeta o informa que la función de ID aleatoria está activada.

Borrar los datos de la tarjeta

Solicitud **PICard Commander** le permite formatear tarjetas o borrar sus datos de acceso cifrados. Las tarjetas sólo se pueden eliminar y formatear en el proyecto en el que están cifradas.

Formatear la tarjeta

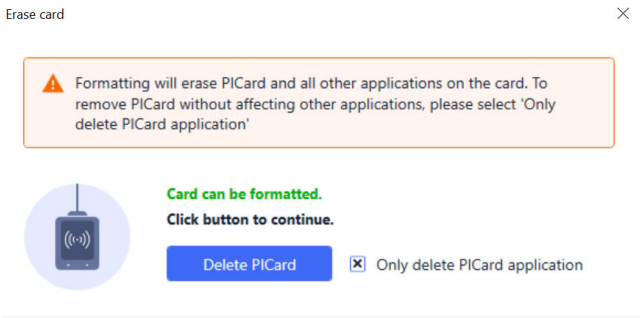
AVISO
Al formatear la tarjeta se borrarán todos los datos de la misma, incluidos los datos de terceros.

1. Abra la pestaña Project > Format card.

2. Coloque la tarjeta en el lector. Pulse el botón Format card para formatear la tarjeta.

> **NOTA**
> Si la función de ID aleatoria está habilitada en la tarjeta, formatear la tarjeta no restaurará la legibilidad del UID original.

Eliminación de datos de acceso



1. Abra la pestaña Project > Format card.
2. Revisa la caja **Only delete PICard application**.
3. Coloque la tarjeta contra el lector.
4. Al presionar el botón Delete PICard Se eliminarán los datos de acceso cifrados de la tarjeta.

Licencias de terceros

Para obtener una lista completa de las licencias de bibliotecas de terceros utilizadas, consulte **Help > About**.

2N PICard Commander – Manual de instalación

2N.com