



2N PICard Commander

Benutzerhandbuch



Inhaltsverzeichnis

| | |
|--|-----------|
| Verwendete Symbole und Begriffe | 3 |
| Produktbeschreibung | 4 |
| Verwandte Produkte | 5 |
| Kompatible Geräte | 6 |
| Installation und Laden der Lizenz | 8 |
| Anschließen eines anderen Lesers | 8 |
| Projekt | 9 |
| Erstellen eines neuen Projekts | 9 |
| Projekt öffnen | 9 |
| Projekt Einstellungen | 9 |
| Grundeinstellungen (Basic settings) | 9 |
| Hauptverschlüsselungsschlüssel (Main Encryption Key) | 9 |
| Verschlüsselungsmodus (Card mode) | 10 |
| Auf Festplatte speichern | 11 |
| Verschlüsselung und Kartenlesen | 12 |
| Kartenverschlüsselung | 12 |
| Export von Leseschlüsseln | 13 |
| Schlüssel in eine Datei exportieren | 13 |
| Laden Sie Schlüssel hoch Access Commander | 14 |
| Karteninformationen lesen | 14 |
| Löschen der Daten auf der Karte | 15 |
| Lizenzen Dritter | 17 |

Verwendete Symbole und Begriffe

Im Handbuch werden folgende Symbole und Piktogramme verwendet:



GEFAHR

Halten Sie sich stets daran Beachten Sie diese Hinweise, um Verletzungsgefahren zu vermeiden.



WARNUNG

Halten Sie sich stets daran Beachten Sie diese Hinweise, um Schäden am Gerät zu vermeiden.



ACHTUNG

Wichtige Warnung. Die Nichtbeachtung der Anweisungen kann zu Fehlfunktionen des Geräts führen.



TIPP

Nützliche Informationen für eine einfachere und schnellere Verwendung oder Einrichtung.



ANMERKUNG

Verfahren und Ratschläge zur effektiven Nutzung der Gerätefunktionen.

Produktbeschreibung

2N PICard Commander ist eine Softwareanwendung zum Verschlüsseln von Zugangsdaten auf Zugangskarten. Die Anwendung erstellt Projekte, die eine Reihe von Verschlüsselungs- und Leseschlüsseln generieren. Projektleiterschlüssel können in 2N-Geräte oder importiert werden Access Commander, der anschließend die Verteilung der Leseschlüssel an die angeschlossenen 2N-Geräte gewährleistet.

Technologie 2N PICard ist für die Kartenverschlüsselung vorgesehen MIFARE® DESFire® EV2 Und MIFARE® DESFire® EV3.

In der App PICard Commander Es besteht die Möglichkeit, die aufgezeichneten Daten auf den Zutrittskarten zu löschen.

Anwendungsfunktionen PICard Commander ist an den Erwerb einer Lizenz gebunden.

Verwandte Produkte

Bestellnummer: 91379601

2N PICard Commander-Lizenz

Die Lizenz wird immer für einen bestimmten USB-Kartenleser basierend auf dem Geräteschlüssel des jeweiligen Lesers ausgestellt. Geräteschlüsselleser können vor dem Hochladen der Lizenz gefunden werden PICard Commander. Die unterstützten USB-Kartenleser sind unten aufgeführt.



Bestellnummer: 9137421E

USB-Leser für 13,56 MHz, 125 kHz RFID-Karten und NFC/HCE-Geräte

Externer RFID-Kartenleser zum Anschluss an den PC über USB-Schnittstelle. Geeignet für die Systemverwaltung und das Hinzufügen von 13,56-MHz-, 125-kHz-Karten und Android-Geräten mit NFC/HCE-Unterstützung über die Webschnittstelle oder App der 2N IP-Gegensprechanlage Access Commander. Geeignet zum Hochladen von MIFARE DESFire-Karten in eine Verschlüsselungsanwendung PICard Commander^a. Es liest die gleichen Karten- und Gerätetypen wie die Kartenleser in den 2N IP-Gegensprechanlagen:

Unterstützte RFID-Karten 125 kHz:

- EM4x02
- NXP HiTag2

Unterstützte RFID-Karten 13,56 MHz:

- **ISO14443A** (nur MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **Mobile Key**



Bestellnummer: 9137424E

Gesichert USB-Leser für 13,56 MHz, 125 kHz RFID-Karten und NFC/HCE-Geräte

Externer sicherer RFID-Kartenleser zum Anschluss an den PC über USB-Schnittstelle. Geeignet für die Systemverwaltung und das Hinzufügen von 13,56-MHz-, 125-kHz-Karten und Android-Geräten mit NFC/HCE-Unterstützung über die Webschnittstelle oder App der 2N IP-Gegensprechanlage Access Commander. Geeignet zum Hochladen von MIFARE DESFire-Karten in eine Verschlüsselungsanwendung 2N PICard-CommanderJahr^a. Es liest die gleichen Karten- und Gerätetypen wie die Kartenleser in den 2N IP-Gegensprechanlagen:

125 kHz

- EM4xxx
- HID Prox

13,56 MHz

- ISO14443A (MIFARE DESFire)

- PicoPass (HID iClass)
- FeliCa
- ST SR(IX)
- 2N Mobile Key
- HID SE (Seos, iClass SE, MIFARE SE)



Bestellnummer: 11202601

2N RFID-Karte MIFARE Desfire EV3 4K 13,56 MH 10 Stk

Packung mit 10 Stück

MIFARE DESFire EV3 (ISO14443A)

Bestellnummer: 11202602

2N RFID-Anhänger MIFARE Desfire EV3 4K 13,56 MHz 10 Stk

Packung mit 10 Stück

MIFARE DESFire EV3 (ISO14443A)



^aTechnologie 2N PICard ist für die Verschlüsselung von MIFARE DESFireEV2- und MIFARE DESFire EV3-Karten vorgesehen.

Kompatible Geräte

Karten mit PICard-Technologie können auf folgenden Geräten gelesen werden:

2N IP Style

- 2N IP Style main unit
(Bestell-Nr. 9157101)
- 2N IP Style main unit, secured
(Bestell-Nr. 9157101-S)

2N IP Verso

- 2N IP Verso – 13.56MHz secured card reader, NFC, reads UID + PACS ID
(Bestell-Nr. 9155086/9155042)
- 2N IP Verso Bluetooth & RFID reader 125kHz, 13.56MHz, NFC
(Bestell-Nr. 91550945)
- 2N IP Verso Bluetooth & RFID reader 125kHz, secured 13.56MHz, NFC
(Bestell-Nr. 91550945-S)
- 2N IP Verso Touch keypad & RFID reader 125kHz, 13.56MHz, NFC
(Bestell-Nr. 91550946)
- 2N IP Verso Touch keypad & RFID reader 125kHz, secured 13.56MHz, NFC
(Bestell-Nr. 91550946-S)

2N Access Unit

- 2N Access Unit 2.0 13.56 MHz, NFC
(Bestell-Nr. 9160342)
- 2N Access Unit 2.0 secured 13.56 MHz, NFC
(Bestell-Nr. 9160342-S)
- 2N Access Unit 2.0 125kHz, 13.56MHz, NFC
(Bestell-Nr. 9160344)
- 2N Access Unit 2.0 125kHz, secured 13.56MHz, NFC
(Bestell-Nr. 9160344-S)
- 2N Access Unit 2.0 Bluetooth & RFID – 125kHz, 13.56MHz, NFC
(Bestell-Nr. 9160345)

Produktbeschreibung

- 2N Access Unit 2.0 Bluetooth & RFID – 125kHz, secured 13.56MHz, NFC
(Bestell-Nr. 9160345-S)
- 2N Access Unit 2.0 Touch keypad & RFID – 125kHz, 13.56MHz, NFC
(Bestell-Nr. 9160346)
- 2N Access Unit 2.0 Touch keypad & RFID – 125kHz, secured 13.56MHz, NFC
(Bestell-Nr. 9160346-S)

2N Access unit M

- 2N Access Unit M 13.56 MHz, NFC ready
(Bestell-Nr. 916112)
- 2N Access Unit M RFID – 125kHz, 13.56MHz, NFC
(Bestell-Nr. 916114)
- 2N Access Unit M Bluetooth & RFID – 125kHz, 13.56MHz, NFC
(Bestell-Nr. 916115)
- 2N Access Unit M Touch keypad & RFID – 125kHz, 13.56MHz, NFC
(Bestell-Nr. 916116)

2N IP Force

- 2N IP Force 13.56MHz card reader, NFC ready, reads UID
(Bestell-Nr. 9151031)
- 2N IP Force 13.56MHz card reader, NFC ready, reads UID + PACS ID
(Bestell-Nr. 9151031S)

Installation und Laden der Lizenz

1. Es installieren PICard Commander wie gewohnt über das Installationsprogramm.
2. Nachdem Sie die Anwendung gestartet haben, laden Sie die Lizenz hoch, indem Sie auf klicken **Load License** in der orangefarbenen Leiste (oder im Reiter Hilfe > Lizenz). Laden Sie dann die Lizenzdatei von der Diskette. Um die Lizenz erfolgreich hochzuladen, muss der Kartenleser mit dem Computer verbunden sein.



ANMERKUNG

Die Lizenz ist an einen bestimmten USB-Kartenleser gebunden. Um eine Lizenz zu erhalten, ist daher die Eingabe des Geräteschlüssels des Lesegeräts erforderlich, der in den Lizenzinformationen in zu finden ist PICard Commander (Help > License). Zur Anzeige des Schlüssels muss der Kartenleser an den Computer angeschlossen sein.



Device key of connected reader:

324e-4142-003c0061000d513634353830 

Anschließen eines anderen Lesers

Wenn ein anderes als das mit der verwendeten Lizenz gekoppelte Lesegerät mit dem Computer verbunden ist, wird die App PICard Commander Es wird Sie nach dem Start benachrichtigen. Sie können eine neue Lizenz auf der Registerkarte Hilfe > Lizenz hochladen.

Projekt

Durch das Erstellen einzelner Projekte können Gruppen von Zugangskarten in verschiedenen Modi verschlüsselt werden. Sie können jedes Projekt gezielt für den Verwendungszweck der Karten einrichten. Das Projekt generiert eine Reihe von Verschlüsselungs- und Leseschlüsseln. Zum Gerät oder zum Access Commander Sie können jeweils nur die Leseschlüssel eines Projekts hochladen.

Erstellen eines neuen Projekts

Klicken Sie nach dem Öffnen der Anwendung auf die Schaltfläche, um ein neues Projekt zu erstellen **Start new project**.

Alternativer Weg: Lesezeichen *File > New project*

Ein neuer Projekt-Setup-Assistent wird geöffnet. Führen Sie die folgenden Schritte aus [Projekt Einstellungen \[9\]](#).

Projekt öffnen

1. Klicken Sie in der ersten Benutzeroberfläche der Anwendung auf die Schaltfläche **Open project**.

Alternativer Weg: Lesezeichen *File > Open project*

Die zuletzt geöffneten Projekte werden im unteren Bereich der ersten Benutzeroberfläche der Anwendung angezeigt.

Projekt Einstellungen

Beim Starten eines Projekts ist es notwendig, dessen Parameter festzulegen.

Die Einstellungen können später in der Projektkonfiguration in der Startoberfläche der Anwendung geändert werden (alternativer Pfad: Registerkarte Project > Change configuration).

Grundeinstellungen (Basic settings)

- **Project name** - Name des Projekts
- **Project description** – Platz für die Eingabe von Notizen zum Projekt

Hauptverschlüsselungsschlüssel (Main Encryption Key)

Entsprechend wird der Hauptverschlüsselungsschlüssel (MEK) von der Anwendung generiert PICard Commander eine Reihe von Schlüsseln zur Verschlüsselung der Kartenzugangsdaten. Der Schlüssel sollte daher eindeutig und ausreichend sicher sein. Der Schlüsselsatz basiert auf dem Hauptverschlüsselungsschlüssel, sodass Projekte mit demselben Hauptverschlüsselungsschlüssel dieselben Schlüsselsätze generieren. Wenn ein Projekt verloren geht, besteht die Möglichkeit, ein neues Projekt mit demselben Hauptverschlüsselungsschlüssel zu erstellen und mit der Verschlüsselung anderer Karten fortzufahren. Leseschlüssel des verlorenen Projekts, die bereits auf das 2N-Gerät hochgeladen wurden, gelten auch für die neu verschlüsselten Karten.



WARNUNG

Der Hauptverschlüsselungsschlüssel darf nicht später sein **ansehen oder ändern**.



TIPP

Für maximale Sicherheit ist es wichtig, sowohl die Projektdatei selbst als auch den Master Encryption Key (MEK) zu speichern. Es ist ideal, den Hauptverschlüsselungsschlüssel (MEK) sicher außerhalb der Online-Umgebung aufzubewahren, z. B. in einem Safe, Bankschließfach usw.

Verschlüsselungsmodus (Card mode)

Es besteht die Möglichkeit, zwischen folgenden Kartenverschlüsselungsmodi zu wählen:

- **Card may be used for other applications later on (best compatibility)** – Die Karten werden hauptsächlich von 2N-Systemen verwendet. Die Daten auf der Karte werden verschlüsselt, ihre UID bleibt jedoch für Anwendungen Dritter lesbar. Karten können in ihren ursprünglichen Zustand zurückformatiert werden..
- **Card will be used only for access control with 2N devices (best privacy)** – Karten werden ausschließlich in 2N-Systemen verwendet. Die Kartenparameter werden dauerhaft zurückgesetzt. Bei Verschlüsselung wird die Random-ID-Funktion auf der Karte aktiviert.
- **Card is already used for other applications (advance settings)** – Anwendungen von Drittanbietern sind bereits auf den Karten geladen. Im nächsten Schritt können Sie ausgewählte Parameter der MIFARE DESFire-Karten einstellen, über deren Zugangsdaten die Technologie verfügt 2N PICard im Projekt zu verschlüsseln.



ANMERKUNG

Modusauswahl **Card is already used for other applications** ist irreversibel.

Im nächsten Schritt können Sie Folgendes ausfüllen:

- **Application ID (AID)** – der Code, unter dem die Bewerbung erfolgen wird 2N PICard auf der Karte gekennzeichnet. AID ist auf 53324E voreingestellt.
- **PICC master key type** – der Typ des PICC-Hauptschlüssels, der auf den Karten festgelegt ist, über die die Anwendung verfügt 2N Picard Verschlüsseln.
- **PICC master key** – der Wert der PICC-Master-Schlüsselkarten, über die die Anwendung verfügt 2N Picard Verschlüsseln.
- **Enable randomisation of readable card ID** – Durch das Einschalten der Random-ID-Funktion wird sichergestellt, dass sich die UID der Karte bei jedem Laden zufällig ändert. Daher kann ein Unbefugter die Karte nicht zur Identifizierung des Inhabers missbrauchen.
- **Encrypt cards in factory default state (change default PICC master key)** – Option zum Hochladen des angegebenen PICC-Hauptschlüssels auf andere leere Karten, wenn diese im Projekt verschlüsselt werden. Wenn diese Option nicht ausgewählt ist, PICard Commander weigert sich, eine leere Karte zu verschlüsseln.



WARNUNG

- Nach der Verschlüsselung der Karten mit der neuen AID müssen die Leserschlüssel erneut exportiert werden. Zuvor verschlüsselte Karten mit alter AID werden für 2N-Geräte nicht mehr lesbar.
- Eine Änderung des PICC-Masterschlüssels in einem Projekt mit bereits verschlüsselten Karten macht es unmöglich, diese Karten im Projekt weiter zu verändern und ihre Daten zu löschen. Die Gültigkeit von Karten zur Authentifizierung in 2N-Geräten wird durch die Änderung nicht beeinträchtigt.
- Das Einschalten der Random-ID-Kartenfunktion kann nicht rückgängig gemacht werden. Die ursprüngliche UID der Karte bleibt auch nach der Formatierung der Karte unlesbar.

Auf Festplatte speichern

Die Projektdatei wird auf der Festplatte gespeichert als *Name des Projekts.picprj*.

Aktivieren Sie das Kontrollkästchen **Protect project file with password** ermöglicht Ihnen, ein Passwort zum Öffnen des Projekts festzulegen. Das Passwort kann später im Reiter Project > Change protection password.



WARNUNG

Sie können Ihr Passwort später nicht vergessen **ansehen oder wiederherstellen**.

Verschlüsselung und Kartenlesen

Hier ist eine Übersicht über den Inhalt des Kapitels:

- [Kartenverschlüsselung \[12\]](#)
- [Export von Leseschlüsseln \[13\]](#)
- [Karteninformationen lesen \[14\]](#)
- [Löschen der Daten auf der Karte \[15\]](#)

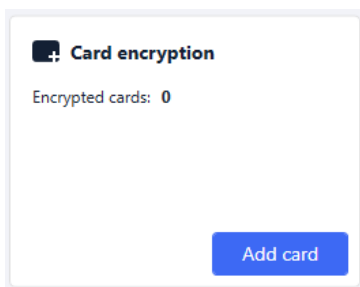
Kartenverschlüsselung

Der Prozess der Verschlüsselung von Karten PICard Commander weist jeder Karte eine eindeutige 128-Bit-Kennung zu, die dann mit den Verschlüsselungsschlüsseln des jeweiligen Projekts verschlüsselt wird. Im Projekt ist es möglich, die Karte zu laden und so ihre zugewiesene Kennung, ggf. weitere Informationen zur Karte und ob eine Verschlüsselung im Projekt möglich ist, herauszufinden.

Verschlüsselungsprozess

1. Klicken Sie in der ersten Benutzeroberfläche der Anwendung auf **Add Card** im Bereich **Card encryption**.

Alternativer Weg: Lesezeichen *Project > Encrypt New Card*



Credential ID for new card – neue Kennung der hochgeladenen Karte

2. Legen Sie die Karte auf das Lesegerät. Durch Drücken der Taste **Encrypt** Der Karte werden Zugangsdaten zugeordnet, die gleichzeitig verschlüsselt werden.



TIPP

Durch Ankreuzen des Kästchens rechts können Sie die automatische Verschlüsselung weiterer angeschlossener Karten starten, ohne den Button erneut drücken zu müssen **Encrypt**.

Die Anwendung informiert über die erfolgreiche Verschlüsselung der Karte.

Wenn die Karte nicht verschlüsselt werden konnte, teilt die Anwendung den Grund mit:

- **Card cannot be encrypted** – Anwendung PICard Commander keinen Zugriff auf die PICC-Masterschlüsselkarte hat. Wenn Sie Karten mit einem voreingestellten PICC-Hauptschlüssel verschlüsseln möchten, müssen Sie den entsprechenden Verschlüsselungsmodus auswählen [Projekt Einstellungen \[9\]](#).
- **Not enough free space on card** – Auf der Karte ist nicht genügend Speicherplatz zum Hochladen der Technologie vorhanden 2N PICard. Der minimal erforderliche Speicher beträgt 512 B.
- **Unsupported card** – Die Anwendung unterstützt diesen Kartentyp nicht. Technologie 2N PICard ist für die Verschlüsselung von MIFARE DESFire EV2- und EV3-Karten konzipiert.
- **Only MIFARE DESFire EV2 or EV3 are supported** – Die Anwendung unterstützt diesen Kartentyp nicht. Die geladene Karte ist MIFARE DESFire EV1.

- **Communication failure with card** – Das Lesegerät konnte die Karte nicht lesen. Legen Sie die Karte an das Lesegerät und entfernen Sie sie erst, wenn der Verschlüsselungsvorgang abgeschlossen ist.



TIPP

Im unteren Bereich des Fensters befindet sich eine Dropdown-Liste mit verschlüsselten Kartenkennungen. Wenn Sie die Liste speichern möchten, kopieren Sie sie, bevor Sie das Fenster schließen. Durch Schließen des Fensters wird die Liste gelöscht. Später können Identifikatoren nur noch für einzelne Karten angezeigt werden.

Export von Leseschlüsseln

Damit 2N-Geräte auf Daten auf verschlüsselten Karten zugreifen können, müssen sie die Leseschlüssel des Projekts kennen. Aus der App PICard Commander Können gelesene Schlüssel auf ein 2N-Gerät exportiert werden oder auf Access Commander, das die Verteilung an alle angeschlossenen 2N-Geräte ermöglicht. Sobald die Leseschlüssel auf das Gerät hochgeladen wurden, können die Geräte Karten lesen, die im jeweiligen Projekt nach dem Hochladen der Leseschlüssel verschlüsselt wurden.

1. Klicken Sie in der ersten Benutzeroberfläche der Anwendung auf **Export** im Abschnitt Leseschlüssel exportieren (alternativer Pfad: Registerkarte Project > Export reader keys).
2. Sie können Projektleserschlüssel auf zwei Arten exportieren:
 - [Schlüssel in eine Datei exportieren \[13\]](#)
 - [Laden Sie Schlüssel hoch Access Commander \[14\]](#)



ACHTUNG

Wenn Sie das RFID-Kartenleser-Erweiterungsmodul neu mit einem VBUS-Kabel an das 2N-Gerät anschließen, in das die Leseschlüssel geladen sind, muss dieses Modul mit dem Gerät gekoppelt werden. Sie können das Leser-Erweiterungsmodul über die Weboberfläche des Geräts im Abschnitt „Hardware“ im Menü „Erweiterungsmodule“ koppeln.

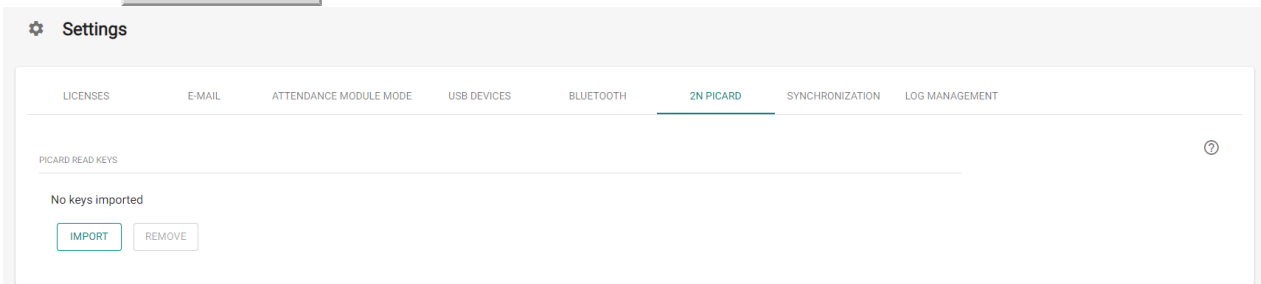



Schlüssel in eine Datei exportieren

Die Anwendung generiert eine Schlüsseldatei und speichert sie auf der Festplatte. Die Datei muss dann in die 2N-Geräteeinstellungen oder in importiert werden Access Commander über ihre Webschnittstellen. Im nächsten Schritt des Exports besteht die Möglichkeit, ein Passwort für die gespeicherte Datei festzulegen.

- **Import in Access Commander (Version 3.00 und höher)** über die Weboberfläche: Einstellungen > Zugriff > Registerkarte PICard > **Importieren**

- In **Access Commander importieren** über die Weboberfläche: Systemeinstellungen > 2N PICARD > Abschnitt **IMPORTIEREN**



- **Auf 2N-Gerät importieren** über die Weboberfläche: Abschnitt „Dienste“ > Menü „Zugriffskontrolle“ > Registerkarte „PICard“ > 

Laden Sie Schlüssel hoch Access Commander

Anwendung PICard Commander lädt Leseschlüssel direkt hoch Access Commander, was die anschließende Verteilung an angeschlossene 2N-Geräte gewährleistet. Im nächsten Schritt ist die Eingabe der Administrator-Anmeldedaten für die Lizenz erforderlich Access Commander.

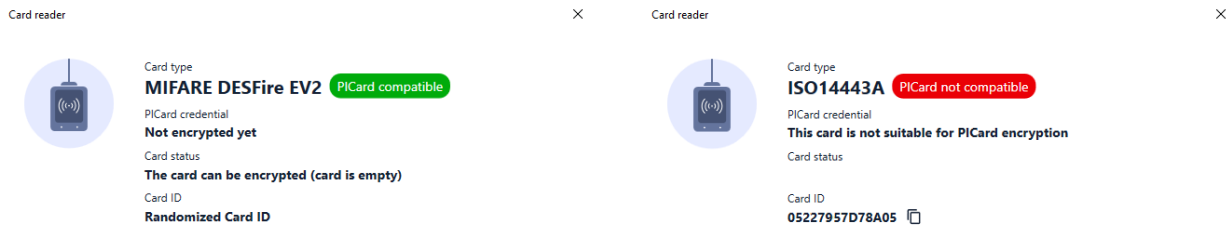
Address – HTTP-Adresse der Weboberfläche Access Commander

Login name – Anmeldenname des Administratorkontos v Access Commander

Password – Login-Passwort für das angegebene Konto Access Commander

Karteninformationen lesen

In der Registerkarte können die zugewiesene Kartenkennung und weitere Informationen zur Karte und ihren Verschlüsselungsoptionen eingesehen werden *Project > Read Card*. Die Informationen werden gelesen, wenn die Karte an das Lesegerät angelegt wird.



Diese Karte kann in der Anwendung verschlüsselt werden.

Dieser Kartentyp kann in der Anwendung nicht verschlüsselt werden.

PICard credential ruft die während des Verschlüsselungsprozesses zugewiesene Kartenkennung ab. Verfügt die Karte über keine Kennung, werden Informationen zu den Vergabemöglichkeiten angezeigt:

- **Not encryptable** – Der Kartentyp ist mit der Technologie kompatibel 2N PICard, aber das Projekt hat keinen Zugriff auf ihren PICC-Hauptschlüssel.
- **This card is not suitable for PICard encryption** – Die Anwendung unterstützt diesen Kartentyp nicht. Technologie 2N PICard ist für die Verschlüsselung von MIFARE DESFire EV2- und EV3-Karten vorgesehen.
- **Not encrypted yet** – Die Karte kann verschlüsselt werden.
- **Unknown** – Die Karte wird in einem anderen Projekt mit einem anderen Hauptverschlüsselungsschlüssel verschlüsselt. Möglicherweise ist auch die Karte beschädigt.

Card Status zeigt den Status oder die Verschlüsselungsoptionen der angegebenen Karte an:

- **Valid PICard credential** – Die Karte ist in diesem Projekt verschlüsselt.
- **The card can be encrypted (card is empty)** – Die Karte ist nicht verschlüsselt. Auf der Karte sind Werkseinstellungen vorhanden.
- **The card can be encrypted** – Die Karte ist nicht verschlüsselt. Auf der Karte ist ein mit diesem Projekt kompatibler PICC-Hauptschlüssel festgelegt.
- **Different PICC Master Key detected. Card's current PICC Master Key required for encryption** – Die Karte kann in diesem Projekt nicht verschlüsselt werden. Der eingestellte PICC-Masterschlüssel ist unterschiedlich.
- **PICard application created in a different project, so cannot be read in this project** – Die Karte ist in einem anderen Projekt verschlüsselt.
- **Only MIFARE DESFire EV2 or EV3 are supported** – Die Karte kann nicht verschlüsselt werden. Die Anwendung unterstützt diesen Kartentyp nicht. Die geladene Karte ist MIFARE DESFire EV1.
- **INVALID CREDENTIAL (there's a problem with the digital signature)** – Verschlüsselte Zugangsdaten der Karte können nicht angezeigt werden. Ihre Echtheit konnte nicht bestätigt werden. Die digitale Signatur ist ungültig.

Card ID zeigt die UUID der Karte an oder meldet, dass die Random-ID-Funktion aktiviert ist.

Löschen der Daten auf der Karte

Anwendung PICard Commander ermöglicht es Ihnen, Karten zu formatieren oder deren verschlüsselte Zugangsdaten zu löschen. Karten können nur in dem Projekt gelöscht und formatiert werden, in dem sie verschlüsselt sind.

Formatieren der Karte



WARNUNG

Durch das Formatieren der Karte werden alle Daten auf der Karte gelöscht, auch Daten von Drittanbietern.

1. Öffnen Sie die Registerkarte **Project** > **Format card**. Legen Sie die Karte an das Lesegerät. Durch Drücken der Taste **Format card** Die Karte wird formatiert.



ANMERKUNG

Wenn die Funktion „Random ID“ auf der Karte aktiviert ist, wird durch das Formatieren der Karte die Lesbarkeit der ursprünglichen UID nicht wiederhergestellt.

Zugangsdaten löschen

Erase card



Formatting will erase PICard and all other applications on the card. To remove PICard without affecting other applications, please select 'Only delete PICard application'



Card can be formatted.
Click button to continue.

Delete PICard

Only delete PICard application

1. Öffnen Sie die Registerkarte **Project** > **Format Card**.

2. Aktivieren Sie das Kontrollkästchen **Only delete PICard application**.
3. Legen Sie die Karte an das Lesegerät.
4. Durch Drücken der Taste **Delete PICard** Die verschlüsselten Zugangsdaten der Karte werden gelöscht.

Lizenzen Dritter

Eine vollständige Liste der verwendeten Bibliothekslizenzen von Drittanbietern finden Sie auf der Registerkarte [Help > About](#).

2N



wiki.2n.com

2N PICard Commander – Benutzerhandbuch

© 2N Telekomunikace a. s., 2024

[2N.com](https://2n.com)