2N PICard Commander

Installatiehandleiding

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

2N.com

Inhoudsopgave

Gebruikte symbolen en termen

In de handleiding worden de volgende symbolen en pictogrammen gebruikt:

GEVAAR
Altijd naleven deze instructies om het risico op letsel te voorkomen.

WAARSCHUWING
Altijd naleven deze instructies om schade aan het apparaat te voorkomen.

LET OP
Belangrijke waarschuwing. Als u de instructies niet opvolgt, kan het apparaat defect raken.

TIP
Bruikbare informatie voor eenvoudiger en sneller gebruik of installatie.

OPMERKING
Procedures en advies voor effectief gebruik van apparaatfuncties.

Productbeschrijving

2N PICard Commander is een softwareapplicatie voor het coderen van inloggegevens op toegangskaarten. De applicatie maakt projecten die een set coderings- en leessleutels genereren. Projectlezersleutels kunnen worden geïmporteerd in 2N-apparaten of in Access Commander, die vervolgens zorgt voor de distributie van leessleutels naar de aangesloten 2N-apparaten.

De 2N PICard technologie is ontworpen voor de codering van MIFARE DESFire EV2 en MIFARE DESFire EV3 kaarten.

In de toepassing **PICard Commander** kunnen de geüploade gegevens op de toegangskaarten worden verwijderd.

De functionaliteit van **PICard Commander** is afhankelijk van de aanschaf van een licentie.

Verwante producten

Bestelnummer: 91379601

2N PICard Commander Licence

De licentie wordt altijd uitgegeven voor een specifieke USB-kaartlezer op basis van de Device key van die lezer. De apparaatsleutel van de lezer kunt u vinden op **PICard Commander** voordat u de licentie uploadt. Ondersteunde USB-kaartlezers staan hieronder vermeld.

Bestelnummer: 9137421E

USB-lezer voor 13,56 MHz, 125 kHz RFID-kaarten en NFC/HCE-apparaten

Externe RFID-kaartlezer voor aansluiting op PC via USB-interface. Geschikt voor systeembeheer en het toevoegen van 13,56 MHz, 125 kHz kaarten en NFC/HCE-compatibele Android-apparaten met behulp van de 2N intercom webinterface of de **Access Commander app**. Geschikt voor het uploaden van MIFARE DESFire kaarten naar de coderingstoepassing **PICard Commander**[a]. Het leest dezelfde soorten kaarten en apparaten als de kaartlezers in 2N-intercoms:

Ondersteunde RFID-kaarten 125 kHZ:

- EM4x02
- HID Prox

Ondersteunde RFID-kaarten 13,56 MHz:

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

Bestelnummer: 9137424E

Secure USB 13,56 MHz, 125 kHz RFID kaartlezer en NFC/HCE apparaat

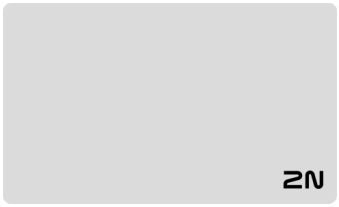
Externe beveiligde RFID-kaartlezer voor aansluiting op PC via USB-interface. Geschikt voor systeembeheer en het toevoegen van 13,56 MHz, 125 kHz kaarten en NFC/HCE-compatibele Android-apparaten met behulp van de 2N intercom webinterface of de **Access Commander app**. Geschikt voor het uploaden van MIFARE DESFire-kaarten naar de coderingstoepassing **2N PICard Commander**[a]. Het leest dezelfde soorten kaarten en apparaten als de kaartlezers in 2N-intercoms:

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)



Bestelnummer: 11202601

2N RFID-kaart MIFARE Desfire EV3 4K 13.56MH 10 stuks

pak van 10 stuks

MIFARE DESFire EV3 (ISO14443A)

Bestelnummer: 11202602

2N RFID fob MIFARE Desfire EV3 4K 13.56MHz 10 stuks

pak van 10 stuks

MIFARE DESFire EV3 (ISO14443A)

[a.] Technologie **2N PICard** is ontworpen voor het coderen van MIFARE DESFireEV2 en MIFARE DESFire EV3 kaarten.

Compatibele apparaten

PICard-lezen wordt ondersteund door alle 2N RFID-lezermodules die in februari 2023 of later op de markt zijn gebracht. De meeste interne lezers die na deze datum zijn geproduceerd, zijn ook compatibel, met uitzondering van de hieronder vermelde modellen.

De volgende modellen **zijn niet compatibel**:

- **2N IP-basis**: alle RFID-lezers
- **2N IP Force**: 9151011, 9151012, 9151016, 9151017, 9151019
- **2N IP Vario**: alle RFID-lezers
- **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

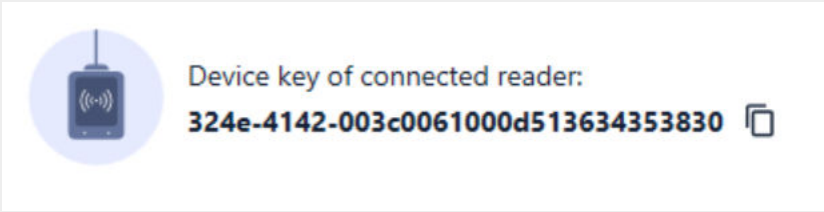
Voor de volgende modules is de compatibiliteit alleen gegarandeerd voor de eenheden die in de herfst van 2023 of later zijn vervaardigd:

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

De licentie installeren en laden

1. Installeer **PICard Commander** op de normale manier via het installatieprogramma.
2. Na het starten van de applicatie laadt u de licentie door te klikken op Load License in de oranje balk (of **onder Help > License**). Laad vervolgens het licentiebestand vanaf de schijf. De kaartlezer moet aangesloten zijn op de computer om de licentie met succes te kunnen uploaden.

OPMERKING
De licentie is gebonden aan een specifieke USB-kaartlezer. Om een licentie te verkrijgen, moet u daarom de apparaatsleutel van het leesapparaat opgeven, die u kunt vinden in de licentie-informatie in **PICard Commander** (**tab Help > Licentie**). De kaartlezer moet op de computer aangesloten zijn om de sleutel te kunnen bekijken.



Een andere lezer aansluiten

Als een andere lezer dan degene die gekoppeld is met de licentie die u gebruikt op uw computer is aangesloten, zal de toepassing **PICard Commander** u waarschuwen wanneer deze start. Onder **Help > License** kunt u een nieuwe licentie uploaden.

Project

Door individuele projecten op te zetten, kunt u groepen toegangskaarten in verschillende modi coderen. U kunt elk project speciaal instellen om de kaarten te gebruiken. Het project genereert een reeks coderings- en leessleutels. U kunt slechts de leessleutels van één project tegelijk uploaden naar het apparaat of naar Access Commander.

Een nieuw project opzetten

Zodra de toepassing geopend is, start u een nieuw project door te drukken op **Start new project**.

Alternatief pad: tab **Bestand > New project**

De wizard Nieuwe projectinstelling wordt geopend, volg dan Projectinstelling (p. 8).

Opening van het project

1. Klik op de knop Open project in de startinterface van de toepassing.
   Alternatief pad: **tabblad File > Open project**

Onlangs geopende projecten worden weergegeven in het onderste gedeelte van de startinterface van de toepassing.

Projectinstellingen

Wanneer u een project aanmaakt, moet u de parameters ervan instellen.

De instellingen kunnen later worden gewijzigd in de Projectconfiguratie in de begininterface van de toepassing (alternatieve pad: **tab Project > Change configuration**).

Basisinstellingen

- **Project name** - projectnaam
- **Project description** - ruimte om opmerkingen over het project te schrijven

Hoofdcoderingssleutel

Volgens de master encryptiesleutel (MEK) genereert **2N PICard Commander** een reeks encryptiesleutels. De sleutel moet dus uniek en voldoende veilig zijn. De sleutelset is gebaseerd op de master-encryptiesleutel, dus projecten met dezelfde master-encryptiesleutel genereren dezelfde sleutelsets. Als een project verloren gaat, kan een nieuw project met dezelfde mastercoderingssleutel aangemaakt worden en de codering voortzetten.

WAARSCHUWING
De mastercoderingssleutel kan later niet worden **bekeken of gewijzigd**.

TIP
Voor maximale beveiliging is het belangrijk om zowel het projectbestand zelf als de master encryption key (MEK) op te slaan. In het ideale geval wordt de master encryptiesleutel (MEK) veilig opgeslagen buiten de online omgeving, bijv. in een kluis, een kluis, enz.

Coderingsmodus (Kaartmodus)

U kunt kiezen uit de volgende kaartcoderingsmodi:

- **Card may be used for other applications later on (best compatibility)** - Kaarten zullen voornamelijk door 2N-systemen worden gebruikt. De gegevens op de kaart worden versleuteld, maar de UID blijft leesbaar voor toepassingen van derden. De kaarten kunnen opnieuw geformatteerd worden naar hun oorspronkelijke staat.
- **Card will be used only for access control with 2N devices (best privacy)** - Kaarten worden uitsluitend gebruikt in 2N-systemen. De kaartparameters worden permanent gereset. Wanneer de kaart gecodeerd is, wordt de functie Random ID op de kaart geactiveerd.
- **Card is already used for other applications (advance settings)** - Toepassingen van derden zijn al op de kaarten geladen. In de volgende stap kunt u geselecteerde parameters instellen voor de MIFARE DES-Fire kaarten waarvan de toegangsgegevens moeten worden versleuteld door de 2N PICard technologie in het project.

> **OPMERKING**
> Het selecteren van de modus **Card is already used for other applications** is onomkeerbaar.

In de volgende stap kunt u invullen:

- **Application ID (AID)** - de code waaronder de toepassing 2N PICard op de kaart wordt geïdentificeerd. AID is vooraf ingesteld op 53324E.
- **PICC master key type** - het type PICC-mastersleutel dat op de kaarten is ingesteld om door de toepassing 2N Picard te worden versleuteld.
- **PICC master key type** - waarde van de PICC-mastersleutel van de kaarten die door de toepassing 2N Picard moeten worden versleuteld.
- **Enable randomisation of readable card ID** inschakelen - Random ID inschakelen zorgt ervoor dat de UID van de kaart elke keer dat deze gelezen wordt, willekeurig veranderd wordt. Daarom kan een onbevoegd persoon de kaart niet misbruiken om de kaarthouder te identificeren.
- **Encrypt cards in factory default state (change default PICC master key)** - optie om de opgegeven PICC-mastersleutel te uploaden naar andere lege kaarten wanneer u ze in het project codeert. Als deze optie niet geselecteerd is, zal **PICard Commander** weigeren de lege kaart te coderen.

> **WAARSCHUWING**
>
> - Na het kaartcoderingsproces onder de nieuwe AID moet u de leessleutels opnieuw exporteren. Eerder gecodeerde kaarten met de oude AID zullen onleesbaar worden voor het 2N-apparaat.
> - Door de PICC-mastersleutel te wijzigen in een project met reeds versleutelde kaarten, is het onmogelijk om deze kaarten verder in het project te wijzigen en hun gegevens te wissen. De geldigheid van de verificatiekaarten in het 2N-apparaat wordt niet beïnvloed door de wijziging.
> - Het inschakelen van de functie Willekeurige ID-kaart is onomkeerbaar. De oorspronkelijke UID van de kaart blijft onleesbaar, zelfs na het formatteren van de kaart.

Opslag op schijf

Het projectbestand wordt op schijf opgeslagen als *Projectnaam*.picprj.

Als u het selectievakje **Protect project file with password** inschakelt, kunt u een beschermend wachtwoord instellen om het project te openen. Het wachtwoord kan later worden gewijzigd in **onder Project > Change protection password**.

WAARSCHUWING
Vergeten wachtwoorden kunnen later niet worden bekeken of opgehaald .

Codering en kaartlezen

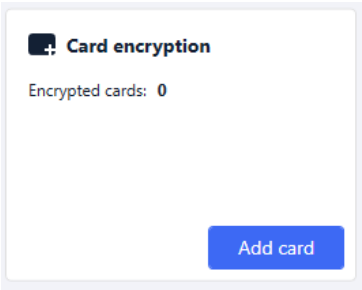
Hier vindt u een overzicht van wat u in het hoofdstuk zult vinden:

Kaartcodering

Het kaartcoderingsproces in **PICard Commander** kent aan elke kaart een unieke 128-bits identificatie toe, die vervolgens wordt gecodeerd met behulp van de coderingssleutels van het bijbehorende project. Het is mogelijk om de kaart in het project uit te lezen en de toegewezen identificator te achterhalen, of andere informatie over de kaart en of deze gecodeerd kan worden in het project.

Coderingsproces

1. Klik in de begininterface van de toepassing op **Aad card** onder **Card encryption**.
   Alternatief pad: tab **Project > Nieuwe kaart coderen**



   Credential ID for new card - nieuwe identificatiecode voor geüploade kaart
2. Plaats de kaart op de lezer. Als u op de knop **Encrypt** drukt, worden toegangsgegevens aan de kaart toegewezen, die tegelijkertijd gecodeerd worden.

> **TIP**
> Door het vakje rechts aan te vinken, kunt u de automatische versleuteling van andere aangesloten kaarten starten zonder dat u opnieuw op de knop **Encrypt** hoeft te drukken.

3. De toepassing informeert over de succesvolle codering van de kaart.

Als de kaart niet gecodeerd kon worden, informeert de toepassing u over de reden:

- **Card cannot be encrypted** - **PICard Commander** toepassing heeft geen toegang tot de PICC-masters-leutel van de kaart. Als u kaarten wilt coderen met een vooraf ingestelde PICC-hoofdsleutel, moet u de juiste coderingsmodus selecteren in Projectinstellingen (p. 8).
- **Not enough free space on card** - niet genoeg vrije ruimte op kaart om technologie te laden **2N PICard**. Het minimaal vereiste geheugen is 512 B.
- **Unsupported card** - de toepassing ondersteunt dit type kaart niet. Technologie **2N PICard** is ontworpen om MIFARE DESFire EV2 en EV3 kaarten te coderen.
- **Only MIFARE DESFire EV2 or EV3 are supported** - de applicatie ondersteunt dit type kaart niet. De geladen kaart is MIFARE DESFire EV1.
- **Communication failure with card** - de lezer heeft de kaart niet geladen. Bevestig de kaart aan de lezer en verwijder deze niet voordat het coderingsproces is voltooid.

TIP
In het onderste gedeelte van het venster staat een vervolgkeuzelijst met gecodeerde kaartidentifiers. Als u de lijst wilt bewaren, kopieert u deze voordat u het venster sluit. Als u het venster sluit, wordt de lijst verwijderd. Later kunt u de identificaties alleen voor individuele kaarten bekijken.

Lezersleutels exporteren

Om 2N-apparaten toegang te geven tot de gegevens op gecodeerde kaarten, moeten ze de leessleutels van het project kennen. Vanuit de toepassing **PICard Commander** kunnen de leessleutels worden geëxporteerd naar een 2N-apparaat of naar de **Access Commander**, die voor distributie naar alle aangesloten 2N-apparaten zorgt. Zodra de leessleutels naar het apparaat zijn geüpload, kunnen de apparaten kaarten lezen die in het project werden gecodeerd nadat de leessleutels werden geüpload.

1. Klik in de begininterface van de toepassing op Export in de sectie Lezersleutels exporteren (alternatief pad: **tab Project > Export reader keys**).
2. U kunt projectsleutels op twee manieren exporteren:

   - Sleutels exporteren naar bestand (p. 12)
   - Upload keys to Access Commander (p. 12)

LET OP
Als u een uitbreidingsmodule voor RFID-kaartlezers aansluit op het 2N apparaat met een VBUS-kabel, moet u deze module koppelen met het apparaat. Het koppelen van de lezeruitbreidingsmodule kan via de webinterface van het apparaat op **Access > Modules**.

Sleutels exporteren naar bestand

De toepassing genereert een sleutelbestand en slaat dit op schijf op. Het bestand moet dan worden geïmporteerd in de 2N apparaatinstellingen of **Access Commander** via hun webinterfaces. In de volgende stap van het exporteren kunt u het beveiligingswachtwoord van het opgeslagen bestand instellen.

- **Importeren in Access Commander** via de webinterface: **Instellingen > Authenticatie > tabblad PICard-sleutels >** Importeren
- **Importeren naar het 2N-apparaat** via de webinterface: **Toegang > Beveiligde kaarten > PICard-sleutel**

Upload keys to Access Commander

De toepassing **PICard Commander** uploadt de gelezen sleutels rechtstreeks naar de Access Commander, die vervolgens zorgt voor de distributie naar de aangesloten 2N-apparaten. De volgende stap is het invoeren van de inloggegevens van de beheerder voor de licentie Access Commander.

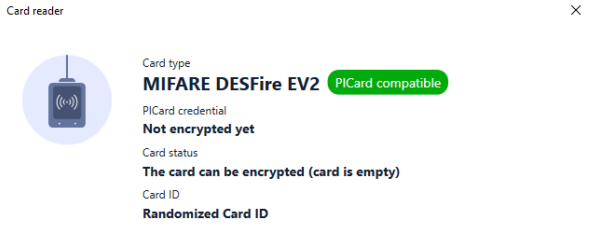
Address - HTTP-adres van de webinterface van Access Commander

Login name - inlognaam van de beheerdersaccount in Access Commander

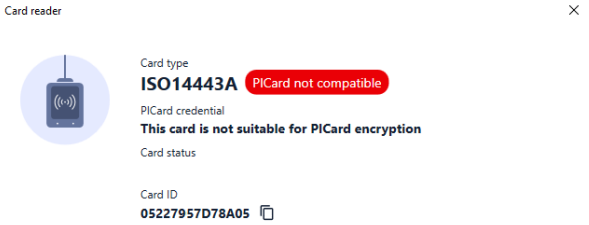
Password- het aanmeldwachtwoord voor deze account in Access Commander

Kaartinformatie lezen

De toegewezen kaartidentificatie en andere informatie over de kaart en de coderingsopties kunnen worden bekeken onder **Project > Read card**. De informatie wordt gelezen wanneer de kaart in de lezer wordt gestoken.



Deze kaart kan in de toepassing gecodeerd worden.



Dit type kaart kan niet gecodeerd worden in de toepassing.

PICard credential haalt de kaartidentificatiecode op die tijdens het coderingsproces is toegewezen. Als de kaart geen identificatiecode heeft, verschijnt er informatie over de opties om er een toe te wijzen:

- **Not encryptable** - het kaarttype is compatibel met 2N PICard-technologie, maar het project heeft geen toegang tot zijn PICC-mastersleutel.
- **This card is not suitable for PICard encryption** - de toepassing ondersteunt dit kaarttype niet. Technologie 2N PICard is ontworpen voor het coderen van MIFARE DESFire EV2 en EV3 kaarten.
- **Not encrypted yet** - de kaart kan gecodeerd worden.
- **Unknown** - de kaart is versleuteld in een ander project onder een andere mastercoderingssleutel. De kaart kan ook beschadigd zijn.

Card Status geeft de coderingsstatus of -opties van de kaart weer:

- **Valid PICard credential** - de kaart is gecodeerd in dit project.
- **The card can be encrypted (card is empty)** - de kaart is niet gecodeerd. Het tabblad toont de fabrieksinstellingen.
- **The card can be encrypted** - de kaart is niet gecodeerd. De PICC-mastersleutel die compatibel is met dit project is op de kaart ingesteld.
- **Different PICC Master Key detected. De huidige PICC Master Key van de kaart is vereist voor codering** - de kaart kan in dit project niet gecodeerd worden. De ingestelde PICC-hoofdsleutel is anders.
- **PICard application created in a different project, so cannot be read in this project** - de kaart is gecodeerd in een ander project.
- **Only MIFARE DESFire EV2 or EV3 are supported** - de kaart kan niet worden gecodeerd. De toepassing ondersteunt dit type kaart niet. De geladen kaart is MIFARE DESFire EV1.
- **INVALID CREDENTIAL (there's a problem with the digital signature)** - gecodeerde kaarttoegangsgegevens kunnen niet worden weergegeven. Bevestiging van hun echtheid is mislukt. De digitale handtekening is ongeldig.

Card ID geeft de UUID van de kaart weer of informeert u dat de functie Random ID is ingeschakeld.

Gegevens op de kaart verwijderen

Met de toepassing **PICard Commander** kunt u kaarten formatteren of hun gecodeerde toegangsgegevens wissen. Kaarten kunnen alleen gewist en geformatteerd worden in het project waarin ze gecodeerd zijn.

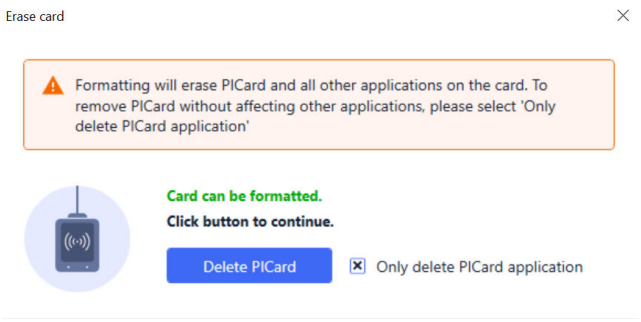
De kaart formatteren

WAARSCHUWING
Formatteren van de kaart verwijdert alle gegevens op de kaart, inclusief gegevens van derden.

1. Open het tabblad **Project > Format Card**.
2. Bevestig de kaart aan de lezer. Druk op de knop Format card om de kaart te formatteren.

> **OPMERKING**
> Als de Random ID-functie op de kaart is ingeschakeld, zal het formatteren van de kaart de leesbaarheid van de oorspronkelijke UID niet herstellen.

Toegangsgegevens verwijderen



1. Open het tabblad **Project > Format Card**.
2. Schakel het selectievakje **Only delete PICard application** in.
3. Bevestig de kaart aan de lezer.
4. Druk op de knop Delete PICard om de gecodeerde toegangsgegevens van de kaart te verwijderen.

Licenties van derden

Zie **Help > About** voor een volledige lijst van gebruikte bibliotheeklicenties van derden.

2N PICard Commander – Installatiehandleiding

2N.com