2N® PICard

Manage secured RFID cards
using our user-friendly solution

2N.com

Why do we need secured cards?

To keep up with technological advancements & outmatch modern security threats

Despite the rise of modern access technologies, RFID cards remain the most widely used authentication method: however, a vast number of organizations are still relying on **outdated 125 kHz technology from the 1990s.** Given the frequency of security breaches nowadays, that's worrying: **these old cards are not secured and are very easy to clone.**

Why? These old cards have only a UID (CSN) identifier, which can be read by any reader. Think of it as having your passwords stored in a plaintext document: anyone who reads it can see everything!

The solution? Choose a truly secure RFID standard designed to minimize these threats. The most widespread one with the perfect balance of speed, performance, and cost-efficiency is **MIFARE® DESFire®,** a technology developed by NXP.

This high-security RFID standard provides **128-bit encryption** and is a **"multi-application product":** meaning that different entities can upload their needed applications securely to the MIFARE® DESFire® card's chip without impairing/touching the other data.

Provide safety and flexibility with 2N® PICard

2N® PICard is 2N's unique cryptographic solution, providing **Protected Identity Credentials (PIC)** built on the multi-application MIFARE® DESFire® technology. 2N® PICard:

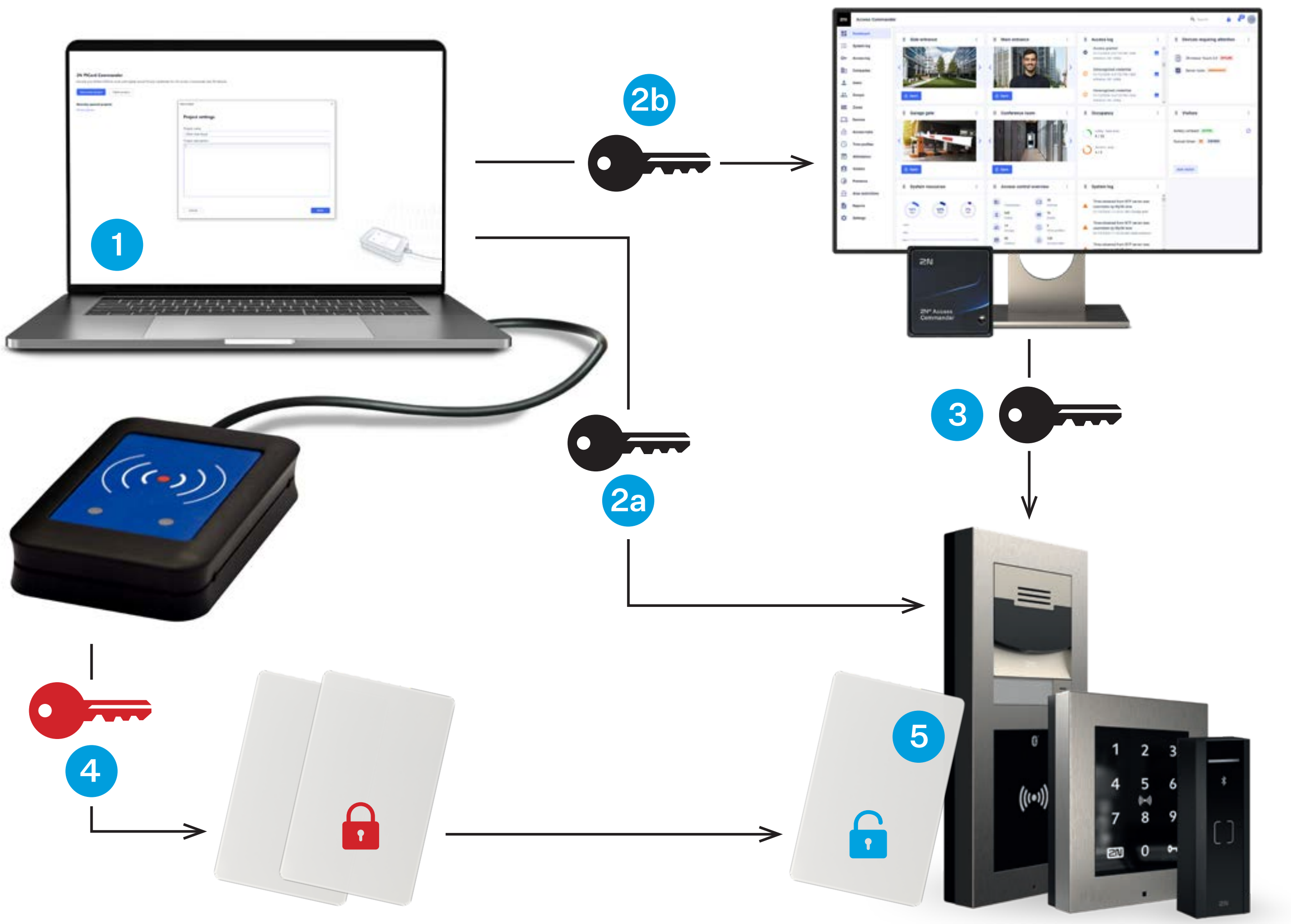
1. Delivers a completely **secure access control** solution

2. Combines a **high level of security** with a **simple workflow:** you don't need to be a card format expert to manage/create keys

3. Offers flexibility for both **facility managers** and **system integrators**

Card encryption
Card successfully encrypted.
Remove the card and place another one card on the reader.

How does 2N® PICard work?



The heart of the entire solution is **2N® PICard Commander** – a software application that allows administrators to create a unique cryptographic keyset for every site ①. Keysets are based on the **main encryption key (MEK):** from which encryption keys for encoding credentials and reading keys are derived.

- **Reading keys** are exported and uploaded either directly to the 2N devices installed onsite 2a or to **2N® Access Commander** 2b that subsequently distributes them to connected 2N IP intercoms and Access Units ③.

- **Encryption keys** are used to encrypt new credentials on cards via a **2N USB reader** ④**.** The encryption process looks like this:
  - 2N® PICard Commander first generates a unique credential for every card
  - This credential is then tied to a specific MIFARE® DESFire® card via a digital signature to provide authenticity
  - It then gets encrypted to provide confidentiality
  - The credential is consequently stored securely on the card

Only 2N readers with the right reading keyset can read the encoded cards ⑤.

Choose the settings that best fit your needs

The 2N® PICard solution brings flexibility to everyone using it: end user, facility manager or system integrator

2N® PICard Commander supports **three ways of card encryption.** Encoded credentials can be written both on blank cards intended only for the access system, and on cards already used in the company for other applications.

High compatibility: card may be used not **only for 2N access control, but also for other things** such as the cafeteria, coffee machines or printers. The access credentials are encrypted by 2N® PICard, but the original unencrypted card's UID stays unchanged and will be readable by third party applications.

High security: card is used **exclusively as an access credential for 2N devices.** The original unencrypted card's UID is then randomized and is always different when read by a reader. It is then impossible to trace the user to whom the card belongs.

Customisability: the customer already has and uses their own MIFARE® DESFire® cards with other third-party applications and they need to write access credentials encrypted by 2N® PICard on them. With this mode, it is possible.

Why should you choose the 2N® PICard solution for your next project?

Multi-level security
Minimize the possibility of access card copying or access credentials eavesdropping. Possible thanks to the **many security measures** including symmetric (AES-128) and asymmetric (ECDSA) encryption, the master encryption key being in the hands of the customer, the entire project protected by an additional password, and more.

Flexibility
The solution is suitable for both **facility managers** managing single buildings and **system integrators** managing multiple sites. Integrators can also offer secure card management as a service: the **2N® PICard Commander software supports three options for encrypting cards** according to their use.

Capability without complexity
The entire solution is designed so that **the user doesn't need to know anything about MIFARE® DESFire® technology** and is still able to upload secure credentials onto the cards. The solution is compatible with EV2/EV3 cards purchased both directly from 2N and from another supplier.

Technical specifications & compatibility

Ordering number	02722-001
Operating system	MS Windows 10 or newer
License	One-time license per connected external USB reader (device key of the connected USB reader is needed in order to generate a new license)
Compatible external USB readers	01400-001 External RFID Card Reader 125 kHz + 13,56 MHz with NFC (USB) 01527-001 External Secured RFID Card Reader 125 kHz + 13,56 MHz with NFC (USB)
Security standards and mechanisms	MIFARE® DESFire® EV2 Secure messaging AES-128 encryption ECDSA digital signature

Compatible RFID cards and keyfobs	MIFARE® DESFire® EV2/EV3 02787-001 2N Card 02788-001 2N Keyfob Note: If an existing card (i.e. a card that is already being used by users in a facility) is supposed to be used with the 2N® PICard Commander, a PICC master key of the respective card must be known. The card must be also set in a way that it requires the PICC master key to be entered to write a 2N® PICard application on it.
Minimum free card capacity	512B
Minimum supported SW & FW	2N® Access Commander 2.4 2N devices with 2N OS 2.37

Compatible 2N devices

PICard credentials can be read by following 2N devices:

2N Access Unit 2.0	02777-001	2N® Access Unit 2.0 - Touch keypad, Bluetooth & secured RFID
	02775-001	2N® Access Unit 2.0 - Touch keypad & secured RFID
	02773-001	2N® Access Unit 2.0 - Bluetooth & secured RFID
	02142-001	2N® Access Unit 2.0 - RFID secured 13,56 MHz, NFC
	02146-001	2N® Access Unit 2.0 RFID - 125 kHz, secured 13,56 MHz, NFC
2N Access Unit M	02393-001	2N® Access Unit M 13,56 MHz, NFC
	02394-001	2N® Access Unit M 125 kHz, 13,56 MHz, NFC
	02395-001	2N® Access Unit M Bluetooth & RFID - 125 kHz, 13,56 MHz, NFC
	02396-001	2N® Access Unit M Touch keypad & RFID - 125 kHz, 13,56 MHz, NFC
2N® IP Force readers	01730-001	2N® IP Force - secured RFID 13,56 MHz, NFC
2N® IP Style	02407-001	2N® IP Style, secured
	02719-001	2N® IP Style AntiBac, secured
2N® IP Verso modules	02443-001	2N® IP Verso - Touch keypad & secured RFID
	02444-001	2N® IP Verso - Bluetooth & secured RFID
	02141-001	2N® IP Verso - secured RFID 13,56 MHz, NFC