

2N



2N[®] PICard

Spravujte zabezpečené RFID karty prostřednictvím
našeho uživatelsky přívětivého řešení

2N.com

K čemu potřebujeme zabezpečené karty?

Abychom mohli držet krok s nejnovějšími technologiemi a dokázali čelit aktuálním bezpečnostním hrozbám

I přes nástup moderních přístupových technologií zůstávají RFID karty nejpoužívanější metodou ověřování přístupových pověření: přesto se obrovské množství organizací stále spoléhá na **zastaralou technologii 125 kHz z 90. let minulého století**. Vzhledem k tomu, jak často dnes dochází k narušení bezpečnosti, je to znepokojující: **tyto staré karty nejsou zabezpečené a lze je velmi snadno naklonovat**.

Proč? Tyto staré karty obsahují pouze UID (CSN) identifikátor, který dokáže přečíst jakákoli čtečka. Představte si, že byste měli svá hesla zapsaná v obyčejném textovém dokumentu: každý, kdo si ho přečte, může zjistit úplně všechno!

Jaké je řešení? Vyberte si skutečně bezpečný standard technologie RFID navržený tak, aby tyto hrozby minimalizoval. Nejrozšířenějším standardem s perfektním poměrem rychlosti, výkonu a ekonomické efektivity je **MIFARE® DESFire®**, technologie vyvinutá společností NXP.

Tento vysoce zabezpečený standard RFID poskytuje **128bitové šifrování** a představuje „**multiaplikační produkt**“: to znamená, že různé subjekty mohou na čip **karty MIFARE® DESFire®** bezpečně nahrát požadované aplikace, aniž by došlo k narušení nebo ovlivnění jiných dat.

Poskytněte bezpečnost a flexibilitu s 2N[®] PICard

2N[®] PICard představuje jedinečné kryptografické řešení od společnosti 2N, které poskytuje zabezpečené identifikační přístupové údaje (Protected Identity Credentials - PIC) založené na multiaplikační technologii MIFARE[®] DESFire[®]. 2N[®] PICard:

1.



Přináší zcela bezpečné řešení pro přístupové systémy

2.



Propojuje vysokou úroveň zabezpečení s jednoduchým způsobem používání: pro spravování/vytváření klíčů nemusíte být odborníkem na problematiku formátování karet

3.



Nabízí flexibilitu pro správce objektů i systémové integrátory



Jak funguje 2N® PICard?



Jádrém celého řešení je **2N® PICard Commander** – softwarová aplikace, která umožňuje správcům vytvořit jedinečnou kryptografickou sadu klíčů pro každou lokalitu **1**. Sady klíčů jsou založeny na **hlavním šifrovacím klíči (MEK)**: od něj jsou odvozeny šifrovací klíče pro kódování pověření a klíče pro čtení.

- **Čtecí klíče** jsou exportovány a nahrány buď přímo do zařízení společnosti 2N nainstalovaných v dané lokalitě **2a**, nebo do programu **2N® Access Commander 2b**, který zajišťuje jejich následnou distribuci do připojených 2N IP interkomů a přístupových jednotek **3**. Nakódované karty mohou číst **pouze čtečky od společnosti 2N se správnou sadou čtecích klíčů 5**.
- **Šifrovací klíče** se používají k šifrování nových přístupových pověření na kartách prostřednictvím **2N USB čtečky 4**. Proces šifrování vypadá následovně:
 - 2N® PICard Commander nejprve vygeneruje pro každou kartu **jedinečné pověření**
 - Toto pověření je pak prostřednictvím digitálního podpisu propojeno s konkrétní kartou **MIFARE® DESFire®**, aby byla zajištěna její autentičnost
 - Následně je zašifrována, aby byla zajištěna její důvěrnost
 - Pověření je pak bezpečně uloženo na kartě

Vyberte si nastavení, které nejlépe vyhovuje vašim potřebám

Řešení **2N® PICard** nabízí flexibilitu všem, kteří jej využívají: koncovému uživateli, správci budovy i systémovému integrátorovi

2N® PICard Commander podporuje **tři způsoby šifrování karet**. Kódované pověření lze zapsat jak na prázdné karty určené pouze pro přístupový systém, tak na karty, které se již ve firmě používají pro jiné účely.



Vysoká kompatibilita: kartu lze použít nejen pro přístupový systém do společnosti 2N, ale i pro další místa, jako je kantýna nebo i pro kávovary a tiskárny. Přístupové údaje jsou šifrovány technologií 2N® PICard, ale původní nešifrované UID karty zůstává nezměněno a aplikace třetích stran jej mohou přečíst.

Vysoké zabezpečení: karta slouží výhradně jako přístupové pověření pro zařízení od společnosti 2N. UID původní nešifrované karty je pak randomizováno a při čtení čtečkou je vždy jiné. Není pak možné vystopovat uživatele, kterému karta patří.



Možnost přizpůsobení: zákazník již má a používá vlastní karty MIFARE® DESfire® s jinými aplikacemi třetích stran a potřebuje na ně zapsat přístupové údaje šifrované pomocí 2N® PICard. Tento režim to umožňuje.

Proč byste si měli pro svůj příští projekt vybrat řešení 2N® PICard?

Víceúrovňové zabezpečení

Minimalizujte riziko kopírování přístupových karet nebo neoprávněného zneužití přístupových údajů. Toto je možné díky **mnoha bezpečnostním opatřením**, mezi něž patří symetrické (AES-128) a asymetrické (ECDSA) šifrování, hlavní šifrovací klíč se nachází v rukou zákazníka, a navíc celý projekt je chráněn dalším heslem.

Flexibilita

Řešení je vhodné **jak pro facility managery spravující jednotlivé budovy, tak i pro systémové integrátory**, kteří mají na starost více lokalit. Systémoví integrátoři mohou také nabízet zabezpečenou správu karet jako službu: **software 2N® PICard Commander podporuje tři možnosti šifrování karet** v závislosti na způsobu jejich použití.

Funkčnost bez komplikací

Celé řešení je navrženo tak, aby **uživatel nemusel o technologii MIFARE® DESFire® nic vědět**, a přesto byl schopen nahrát na karty zabezpečené pověření. Řešení je kompatibilní s kartami EV2/EV3, které lze zakoupit přímo od společnosti 2N nebo od jiného dodavatele.



Technické specifikace a kompatibilita

Objednáací číslo	91379601
Operační systém	MS Windows 10 nebo novější
Licence	Jednorázová licence na připojenou externí USB čtečku (pro vygenerování nové licence je potřeba tzv. „klíč zařízení“ připojené USB čtečky)
Kompatibilní externí USB čtečky	9137421E Externí čtečka RFID karet 125 kHz + 13,56 MHz s NFC (USB) 9137424E Externí zabezpečená čtečka RFID karet 125kHz + 13,56 MHz s NFC (USB)
Bezpečnostní standardy a mechanismy	MIFARE® DESFire® EV2 zabezpečené zasílání zpráv

Šifrování AES-128	MIFARE® DESFire® EV2/EV3 11202601 2N karty 11202602 2N klíčenky
--------------------------	---

Poznámka: Pokud má být existující karta (tj. karta, kterou již uživatelé v zařízení používají) použita softwarem 2N® PICard Commander, musí být znám hlavní PICC klíč příslušné karty. Karta musí být také nastavena tak, aby vyžadovala zadání hlavního PICC klíče, aby na ni bylo možné zapsat aplikaci 2N® PICard.

Digitální podpis ECDSA	512B
-------------------------------	------

Minimální podporované verze FW a SW	2N® Access Commander 2.4 2N zařízení s 2N OS 2.37
--	--

Kompatibilní zařízení společnosti 2N

Pověření 2N® PICard dokážou přečíst následující zařízení společnosti 2N:

2N Access Unit 2.0	9160347 (-S) 9160346 (-S) 9160345 (-S) 9160342 (-S) 9160344 (-S)	2N® Access Unit 2.0 - Touch keypad, Bluetooth & (secured) RFID 2N® Access Unit 2.0 – Touch keypad & (secured) RFID 2N® Access Unit 2.0 – Bluetooth & (secured) RFID 2N® Access Unit 2.0 - RFID (secured) 13,56 MHz, NFC 2N® Access Unit 2.0 RFID - 125 kHz, (secured) 13,56 MHz, NFC
2N Access Unit M	9161121 9161141 9161151 9161161	2N® Access Unit M 13,56 MHz, NFC 2N® Access Unit M 125 kHz, 13,56 MHz, NFC 2N® Access Unit M Bluetooth & RFID - 125 kHz, 13,56 MHz, NFC 2N® Access Unit M Touch keypad & RFID - 125 kHz, 13,56 MHz, NFC

2N® IP Force čtečky	9151031 9151031S	2N® IP Force - RFID 13,56 MHz, NFC 2N® IP Force - secured RFID 13,56 MHz, NFC
----------------------------	---------------------	--

2N® IP Style	9157101 9157101-S	2N® IP Style main unit 2N® IP Style main unit, secured
---------------------	----------------------	---

2N® IP Verso moduly	91550946 (-S) 91550945 (-S) 9155042 9155086	2N® IP Verso – Touch keypad & (secured) RFID 2N® IP Verso – Bluetooth & (secured) RFID 2N® IP Verso - RFID 13,56 MHz 2N® IP Verso - secured RFID 13,56 MHz, NFC
----------------------------	--	--