

Co přijde po RFID kartách?

2N

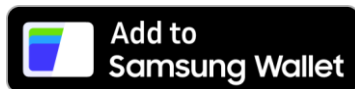
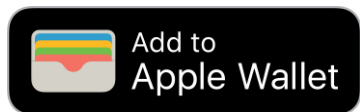


bastlíři SH
MacGyver
macgyver.siliconhill.cz

Adam Hořčica
Expert Engineer, 2N



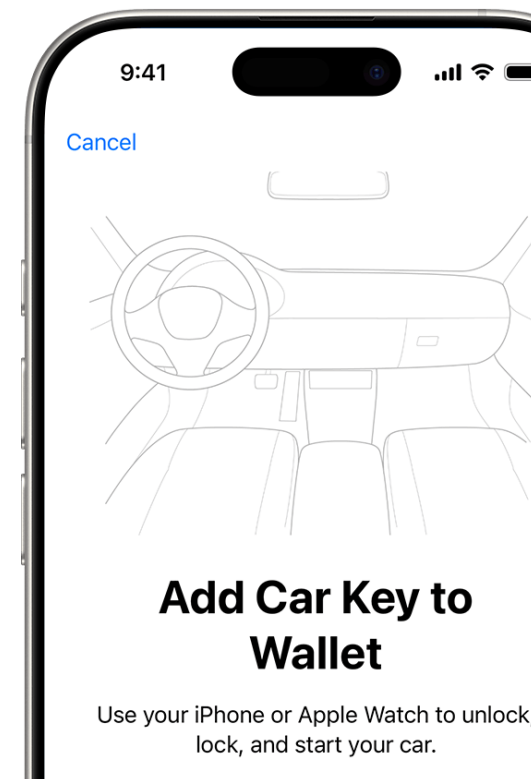
Klíč  který známe...



KASTLE



Google Wallet



... se mění

Adding a pass associates it with your Apple Account. Your device may share a device identifier with the pass provider for setup and management. [See how your data is managed...](#)

Dvě technologie



PHYSICAL CREDENTIALS



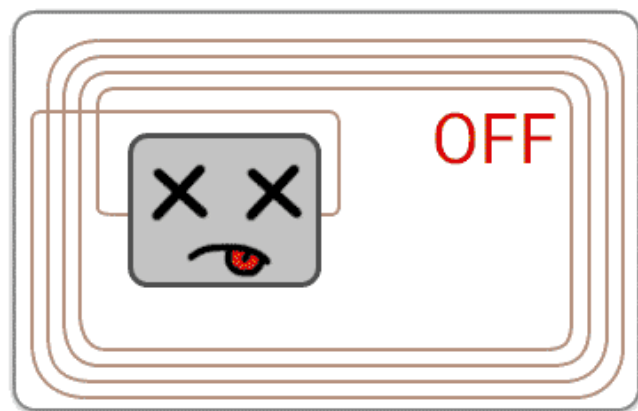
DIGITAL CREDENTIALS

Šifro... co? 🤔

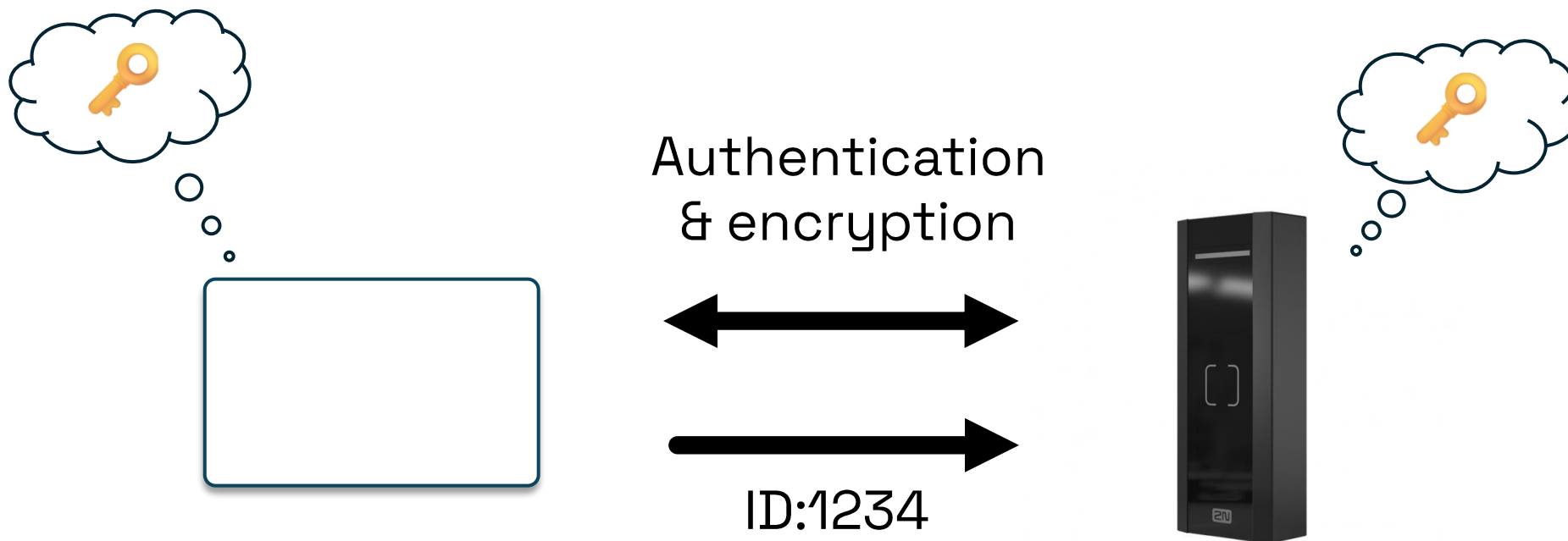


ID:1234

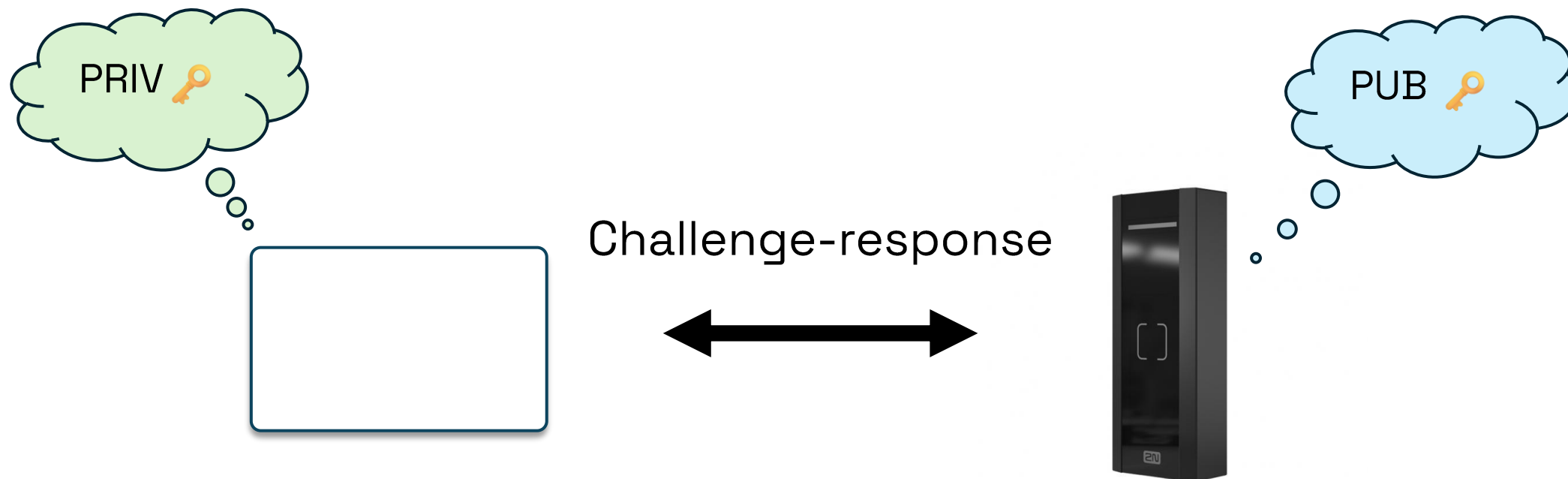




Symetrická cryptografie



Asymetrická kryptografie





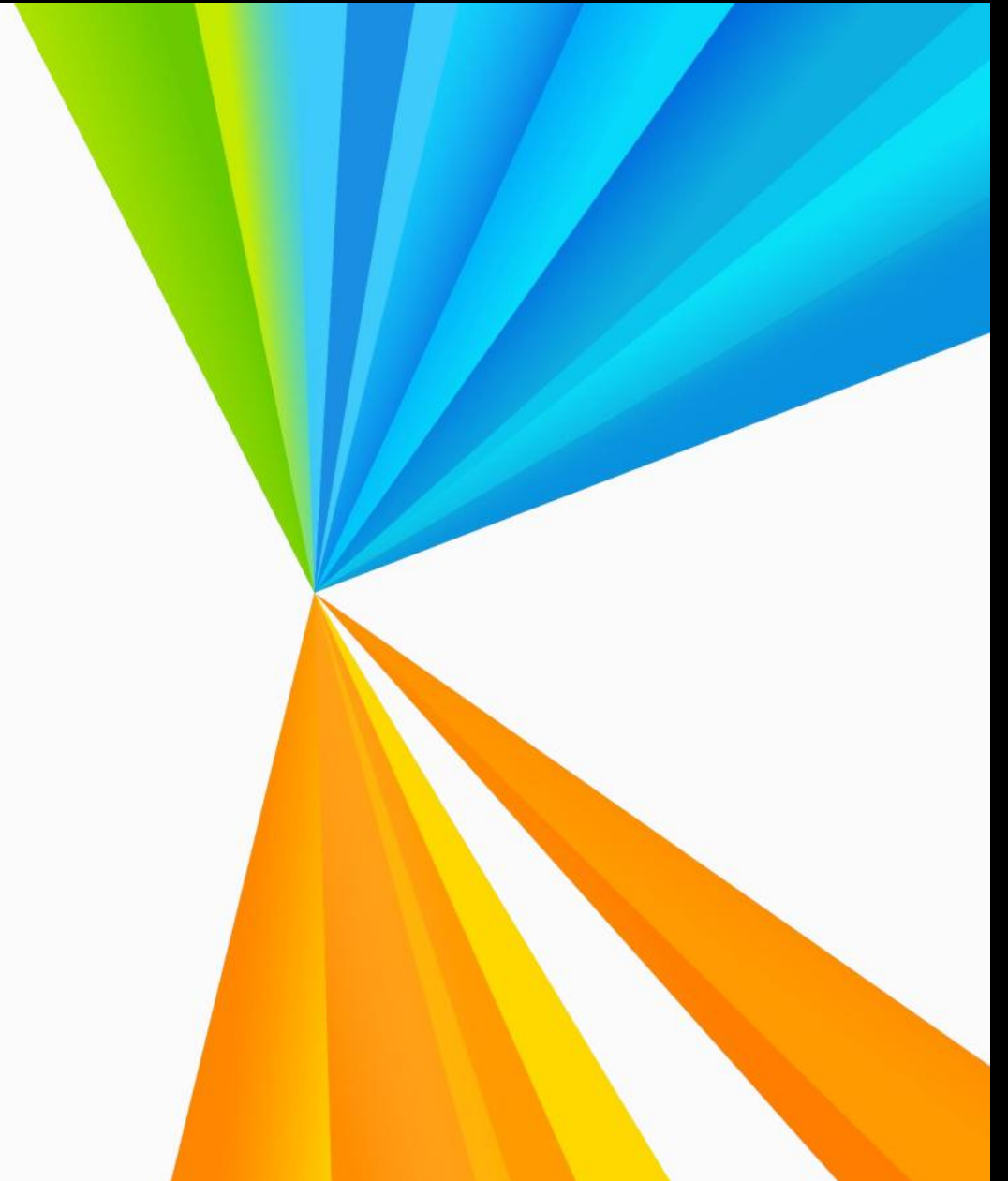
MIFARE DUOX® Simplifying Security in Smart City Applications

Sandra Hollerweger

Senior Product & Marketing Manager

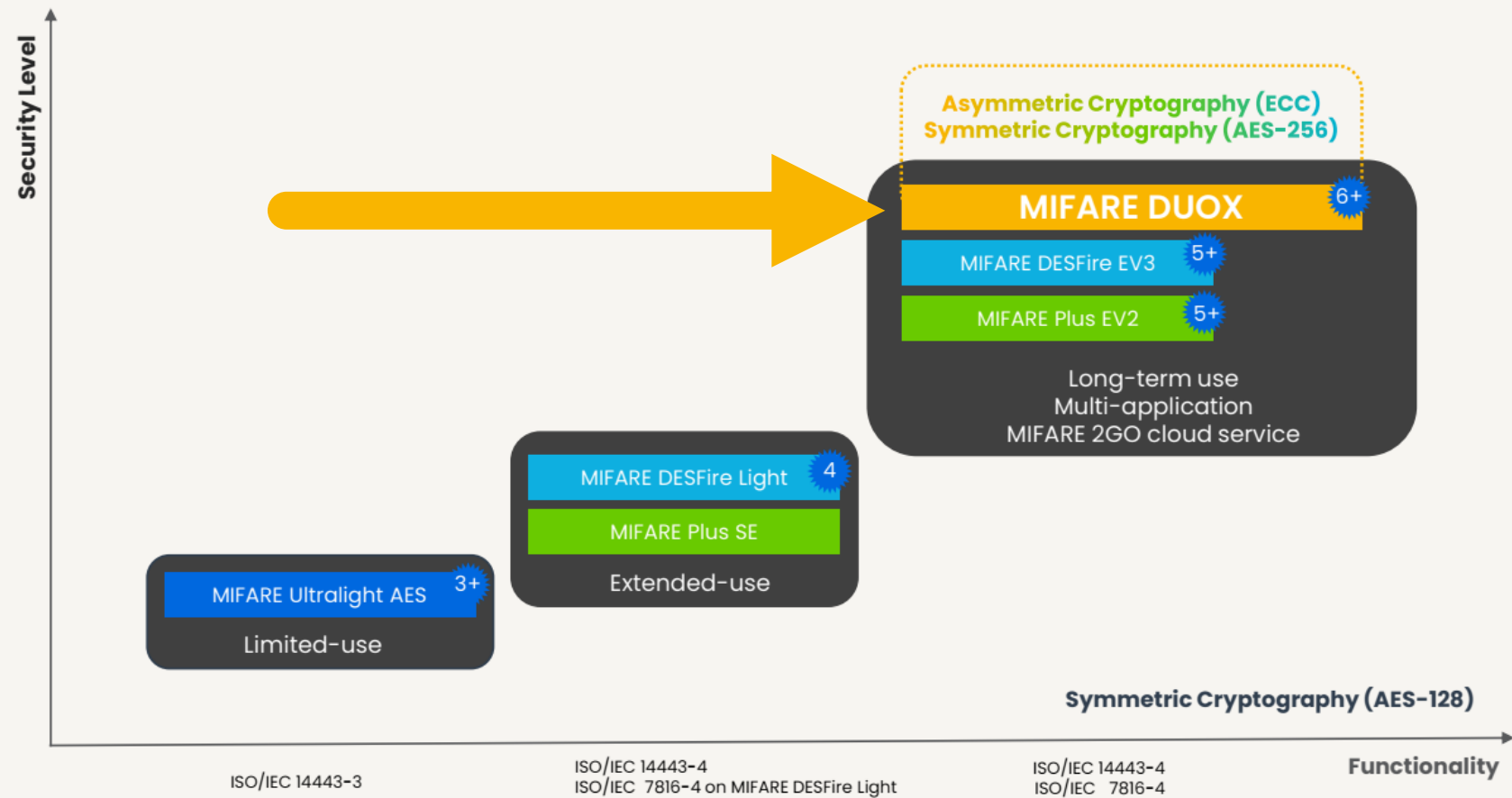
December 2024

| Public | NXP and the NXP logo are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2024 NXP B.V.



MIFARE DUOX enables high security NFC solutions

MIFARE portfolio ranges from cost-effective single-use product to multi-application high-end product





MIFARE DUOX is packed with innovative features and functionality

IC characteristics, memory & RF interface

Contactless interface per **ISO/IEC 14443 Type A**

13.56 MHz operating frequency

17pF and 70pF input capacitance versions for different form factors

High data rates support **up to 848 Kbit /s** and **VHBR**

2/4/8/16 KB user data memory

Data retention of **25 years**

Flexible file structure with **multi-application support** (>28 applications / 32 files)

Extended Operating **Temperature Range from -40°C to +105°C** on silicon level

Certification, norms & industry standards

Common Criteria certification with **CC EAL 6+** for HW and SW

ISO/IEC 14443 A levels 1-4

ISO/IEC 7816-4 commands and wrapped command format

NFC Forum Tag Type 4 certification

Product availability in **75µm** sawn bumped wafer and **MOA8** module

Automotive requirements compliance via automotive-like qual on silicon level incl. cold test, **ISO/SAE 21434** and **MISRA-C**

EV-Charging compliance to **VDE-DKE AR-E 2532-100**

Cryptography & security

Symmetric Crypto algorithm support with **AES-128** and **AES-256**

Asymmetric Crypto algorithm support with **ECC** with **NIST P-256** and **brainpoolP256r1**

Simplified key management and key distribution via **PKI** concept

Key management on card level: 2 pre-loaded asymmetric key pairs (including **NXP PICC Cert** and **NXP Originality Cert**) and 11 reserved slots for symmetric keys

Key management on application level: up to 5 certificates and up to 14 symmetric keys in up to 16 keysets

Flexibility, versatility & extended features

Proximity Check to detect relay attacks

Secure Unique NFC Message (SUN) to ensure security and integrity protected **NDEF** data reading

Transaction Timer to prevent **Man-in-the-Middle** attacks

Transaction MAC / Transaction Signature for generating a secure proof of executed transactions

Dynamic ECC-based Originality Check functionality to ensure originality and genuineness of the product

NXP

MIFARE DUOX

MIFARE DUOX is packed with features and functions

IC characteristics, memory & RF interface

Certification, norms & industry standards

Contactless interface per ISO 14443 Type A

13.56 MHz operating frequency

17pF and 70pF input capacitance versions for different form factors

High data rates support up to 848 Kbit/s and VHBR

2/4/8/16 KB user data memory

Data retention of 25 years

Flexible file structure with multi-application support (>28 applications / 32 files)

Extended Operating Temperature Range from -40°C to +105°C on silicon level

with CC EAL 6+ for HW and SW

ISO/IEC 14443 A levels 1-4

ISO/IEC 7816-4 commands and wrapped command format

NFC Forum Tag Type 4 certification

Product availability in 75µm sawn bumped wafer and MOA8 module

Automotive requirements compliance via automotive-like qual on silicon level incl. cold test ISO/SAE 21434 and MISRA-C

EV-Charging compliance to VDE-DKE AR-E 2532-100

Cryptography & security

Symmetric Crypto algorithm support with AES-128 and AES-256

Asymmetric Crypto algorithm support with ECC with NIST P-256 and brainpoolP256r1

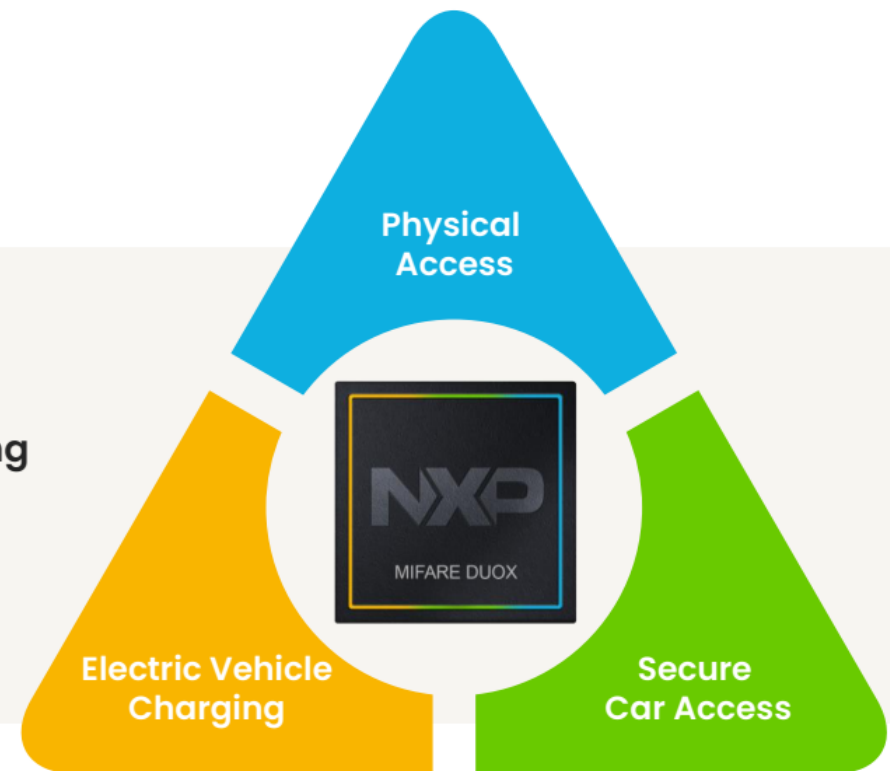
Simplified key management and key distribution via PKI concept

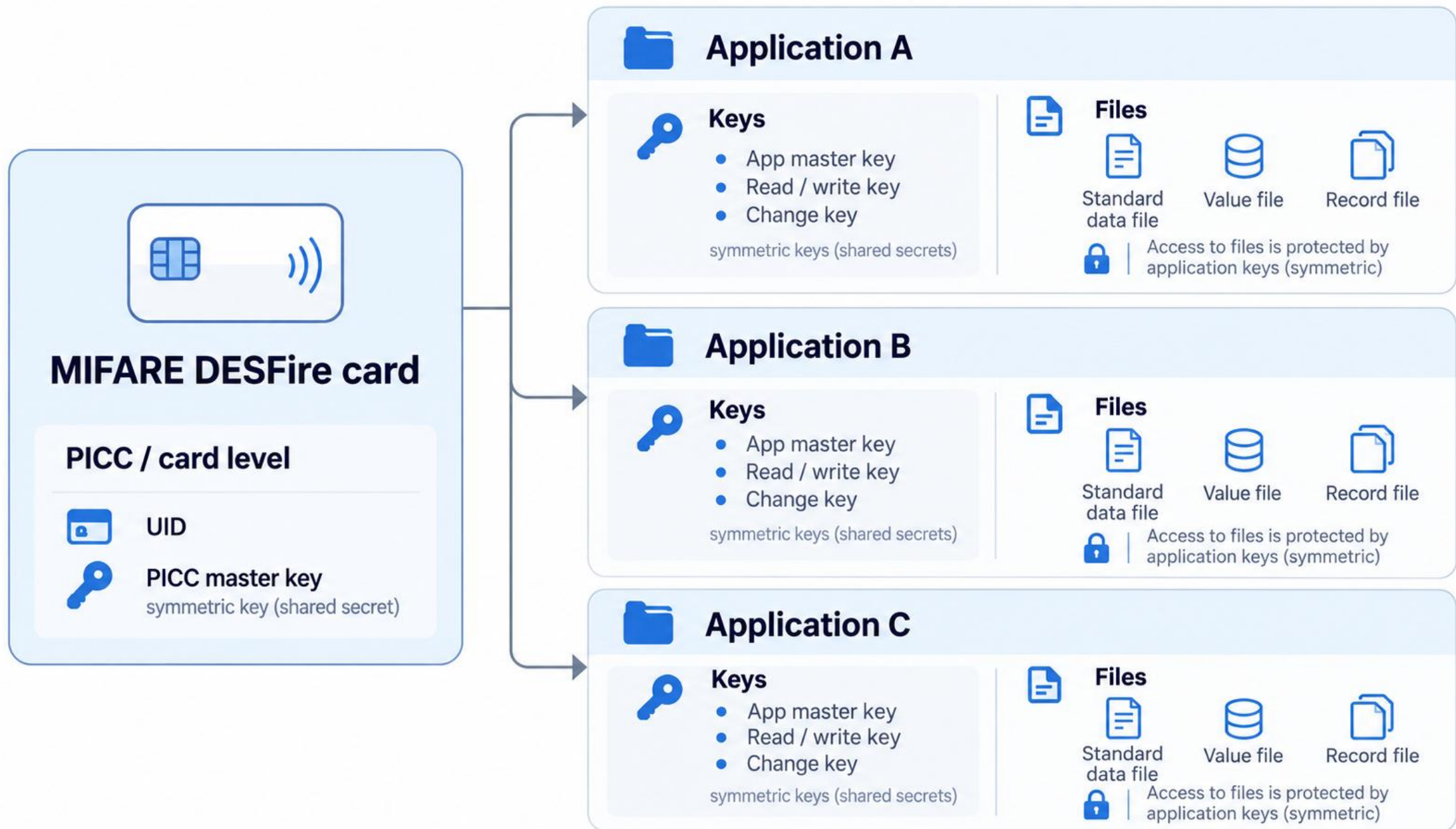
Key management on card level: 2 pre-loaded asymmetric key pairs (including NXP PICC Cert and NXP Originality Cert) and 11 reserved slots for symmetric keys

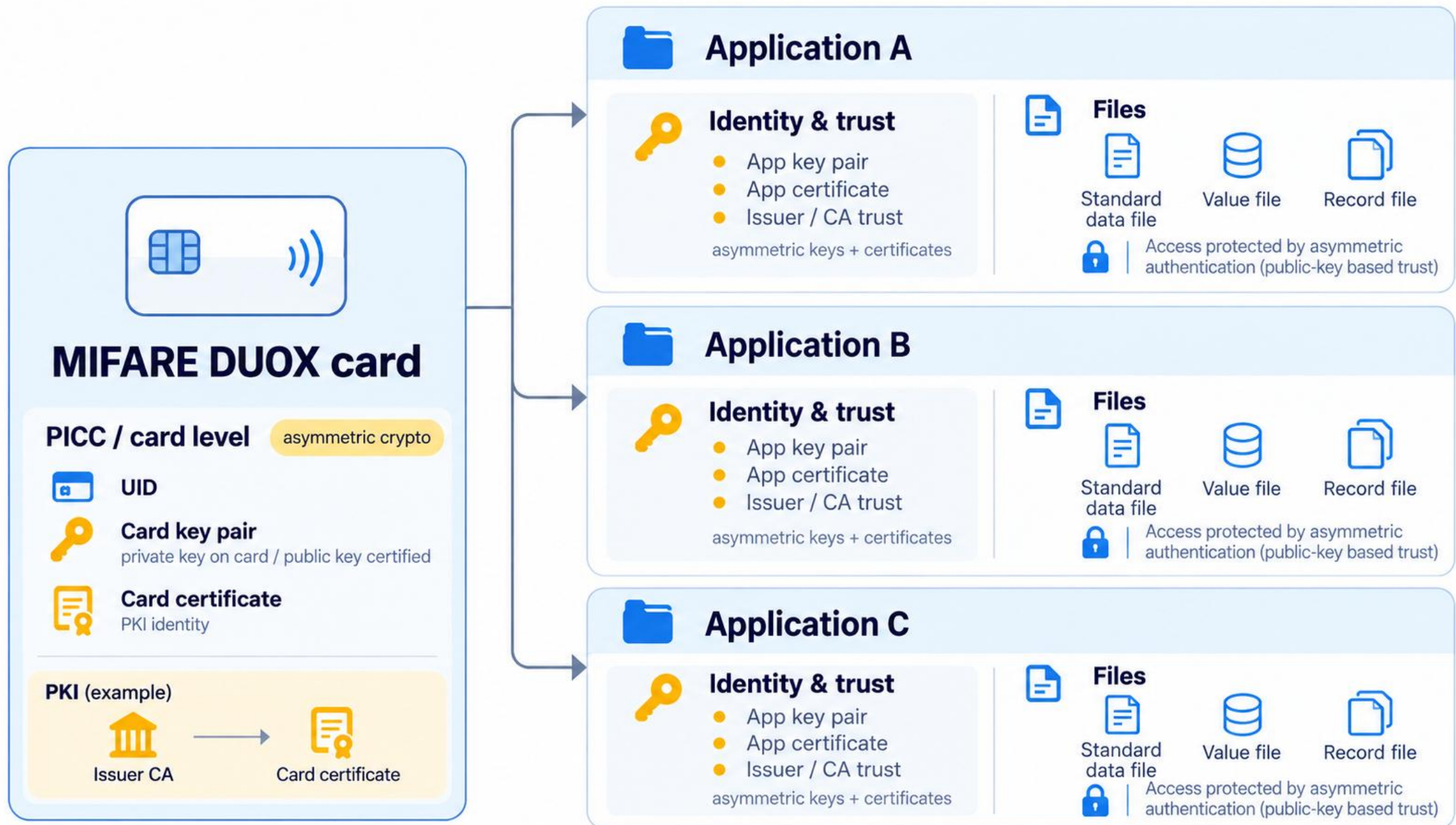
Key management on application level: up to 5 certificates and up to 14 symmetric keys in up to 16 keysets

Future proven secure contactless IC for applications demanding

flexibility, dynamic key provisioning and high security





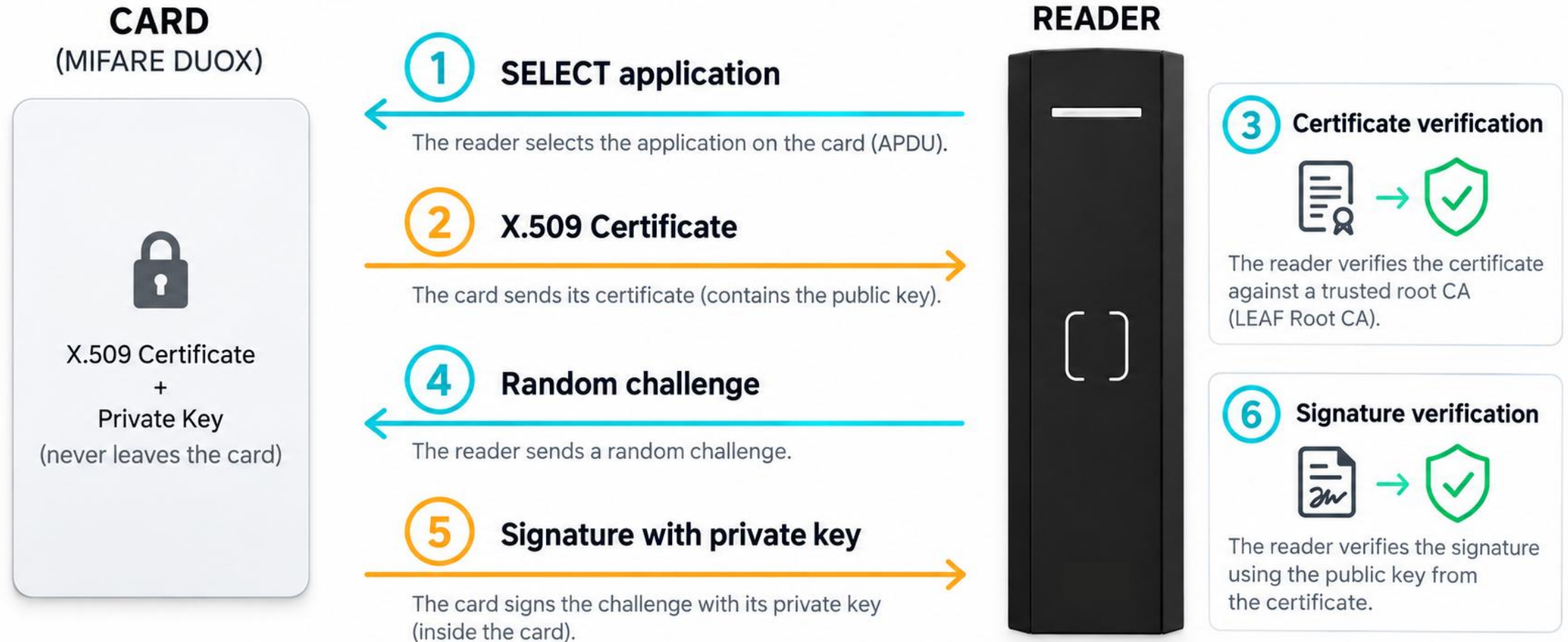


Access Control is Moving to Public Keys. Your Physical Credentials Should Too.

LEAF Verified brings modern cryptographic security to physical credentials, built on NXP's MIFARE DUOX® technology. The same public key foundation as Aliro™, with no shared secrets and no vendor lock-in. Designed for scale and open to everyone.

No LEAF membership required.





Secure User Identification and Authorization in **EV Charging Applications**





AN14223

MIFARE DUOX for EV charging use cases

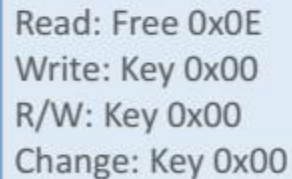
Rev. 1.0 — 10 July 2025

Application note

Application ID = 0xF61010

File No. 0x00

Contains the card
certificate(Data_{CARD})
and public key(PK_{CARD})



General purpose data
(1KB)

Read: Free (0x0E)
Write: Free (0x0E)
R/W: Free (0x0E)
Change: Free (0x0E)

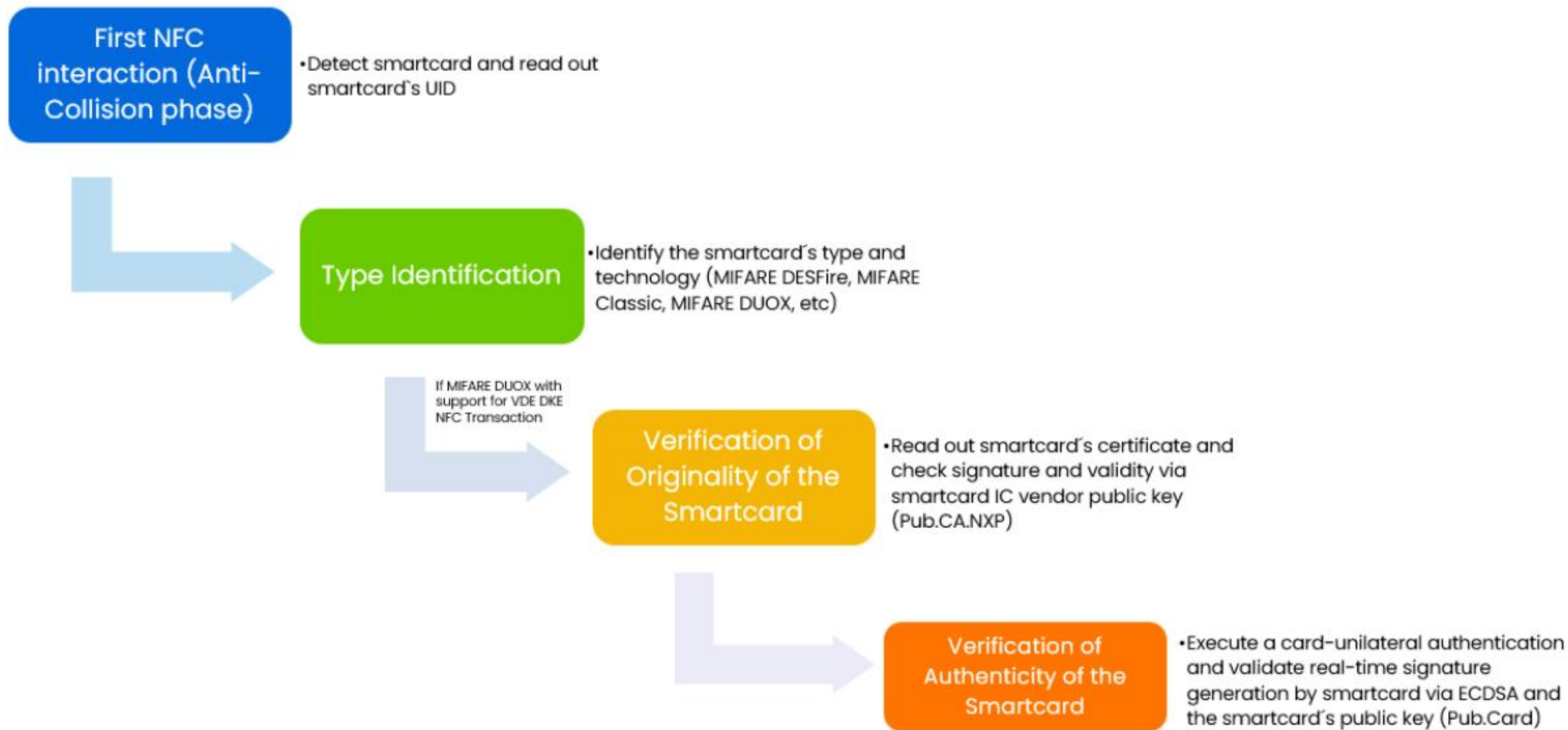


- 0x00 Application Masterkey
- 0x01 – 0x04: general purpose application keys initialized to 0000...0000

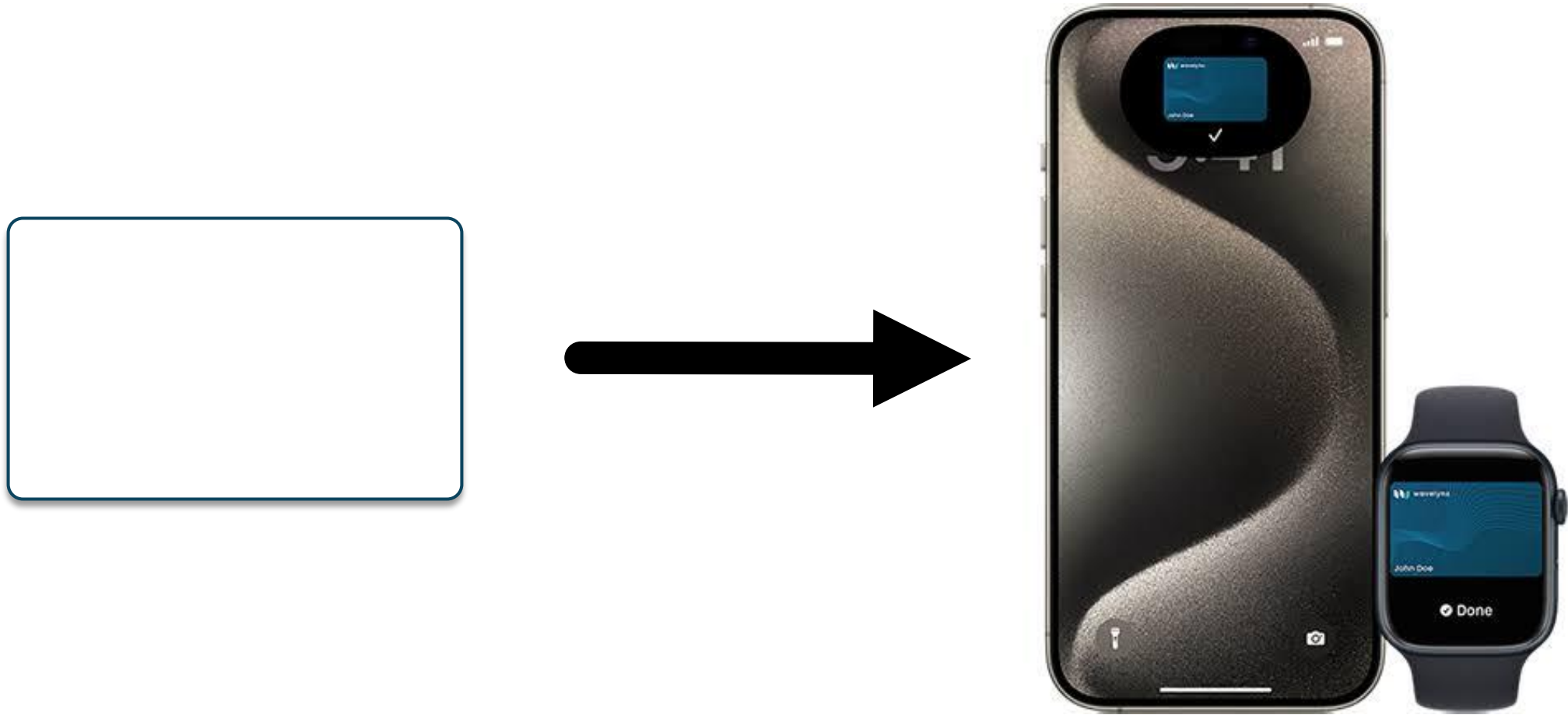
- 1 ECC private key (PK_{CARD}) generated on the card



VDE-AR-E 2532-100



EV Charging transaction elements



Co když credential přestane být jen karta?



QR

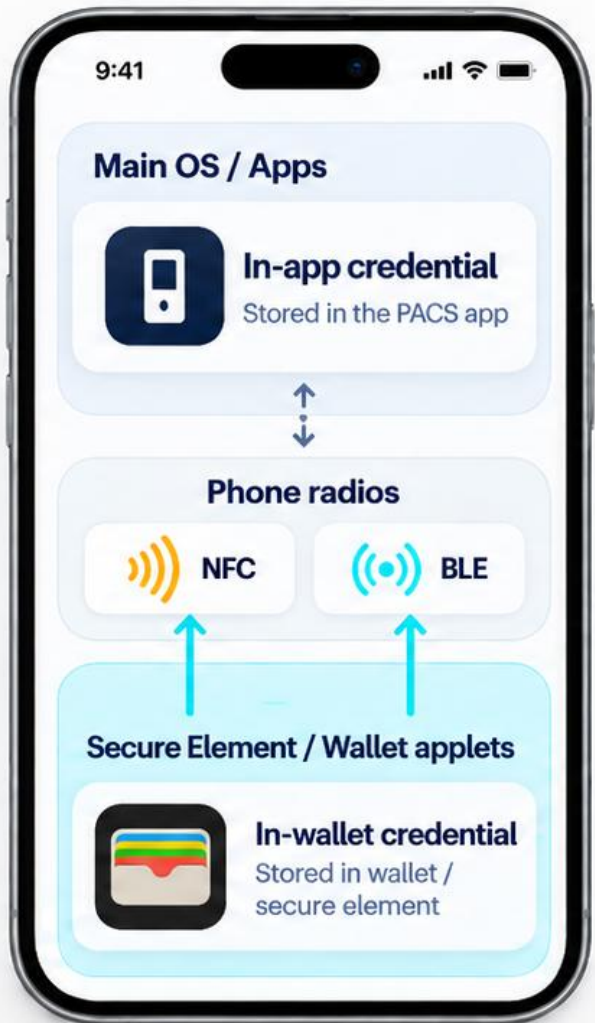


NFC



BLE

MOBILE PHONE



NFC

Tap / short range



BLE

Wireless / hands-free



UWB / CS

(future ranging)



READER



In-app vs in-wallet

Aliro



The Power of Open Access

- **Otevřený průmyslový standard** od Connectivity Standards Alliance (CSA)
- Veřejné od **únoru 2026**
- **Interoperabilita** napříč digitálními peněženkami, zařízeními a přístupovými čtečkami
- Bezpečné credentialy založené na **asymetrické kryptografii**
- Více způsobů použití: **NFC, BLE** a BLE + **UWB**

NFC

- Tap-to-access
- 13,56 MHz
- ISO 14443-4 / ISO 7816-4 / HCE
- Krátký dosah přirozeně určuje, u **kterých dveří** uživatel stojí

BLE

- **Hands-free / User-initiated access**
- **Bluetooth Low Energy**
- BLE zajišťuje **discovery + datovou komunikaci**
- Delší dosah → proximity nelze spolehlivě určit jen pomocí RSSI
 - UWB
- Aliro definuje vlastní **point-to-point aplikační protokol** nad BLE transportem

UWB — Ultra-Wideband

- 6–8,5 GHz
- **Velmi široké pásmo** — typicky kanály o šířce ≥ 500 MHz
- **Technologie pro přesné měření vzdálenosti** — typicky s přesností v řádu centimetrů
- Vzdálenost určuje pomocí **Time of Flight (ToF)**
 - Měří čas letu kryptograficky nepředvídatelného signálu.
- Poskytuje **informaci o vzdálenosti a poloze**, ne jen sílu signálu (AoA)
- Typicky funguje **společně s BLE** — BLE pro nalezení zařízení a komunikaci, UWB pro ranging
- Vyžaduje samostatný **UWB hardware** v telefonu i čtečce

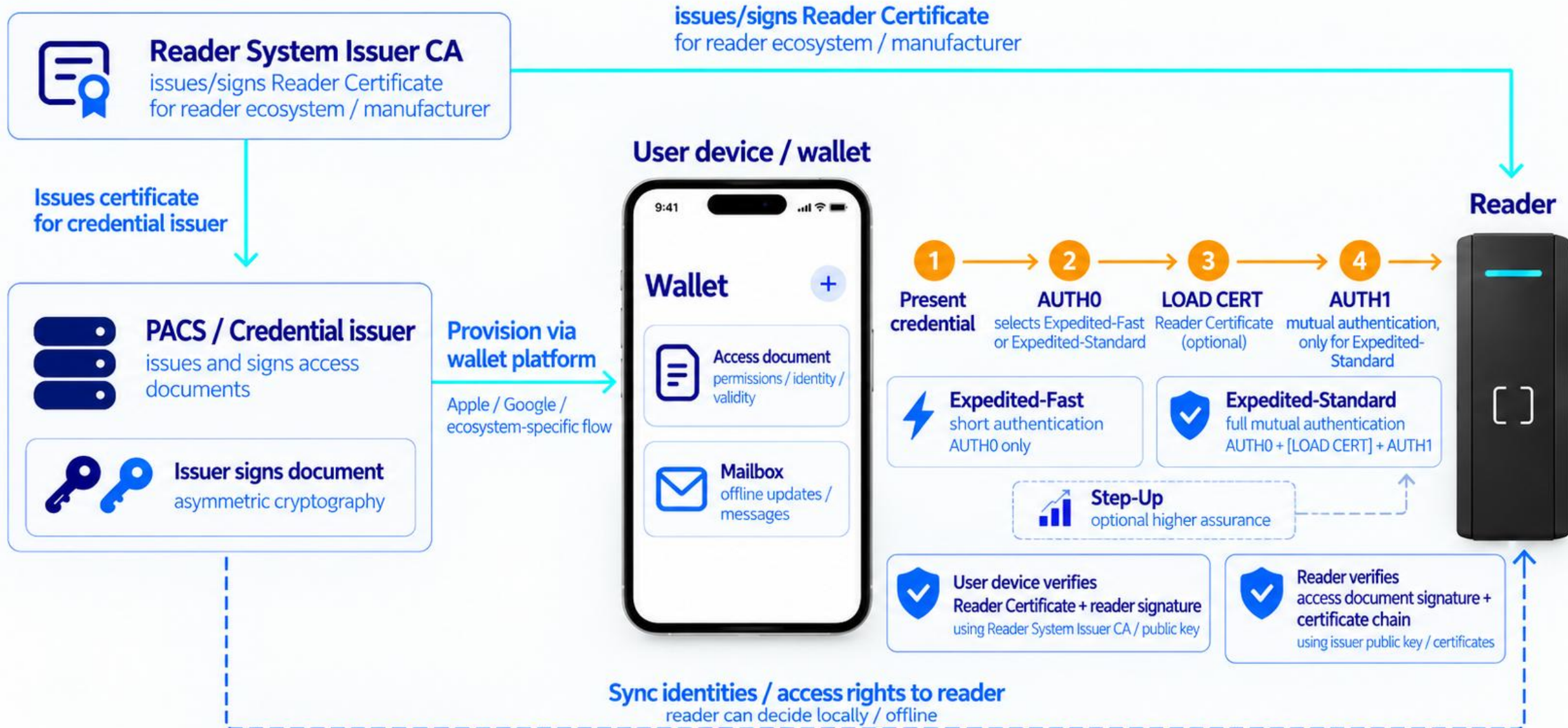
Bluetooth Channel Sounding

<Úkrok stranou>

- Nová ranging funkce v **Bluetooth Core 6.0**
- Používá existující **Bluetooth LE rádio** (ale ne každé to umí!)
- **PBR – Phase-Based Ranging** vzdálenost z rozdílu fáze na více frekvencích
- **RTT – Round-Trip Timing** doplňkové měření času, zejména pro bezpečnost / odolnost proti relay útokům

</Úkrok stranou>

Aliro: access document, trust model and authentication



ALIRO: open mobile access ecosystem

Outside Aliro / ecosystem-specific

backend integration, issuance workflows,
platform-specific APIs, smart-home ecosystem flows



Wallet provider / platform

Apple / Google / Samsung etc.



wallet APIs, wallet UX, device ecosystem



Issue / provision
credential



PACS / credential issuer

identity, permissions, lifecycle

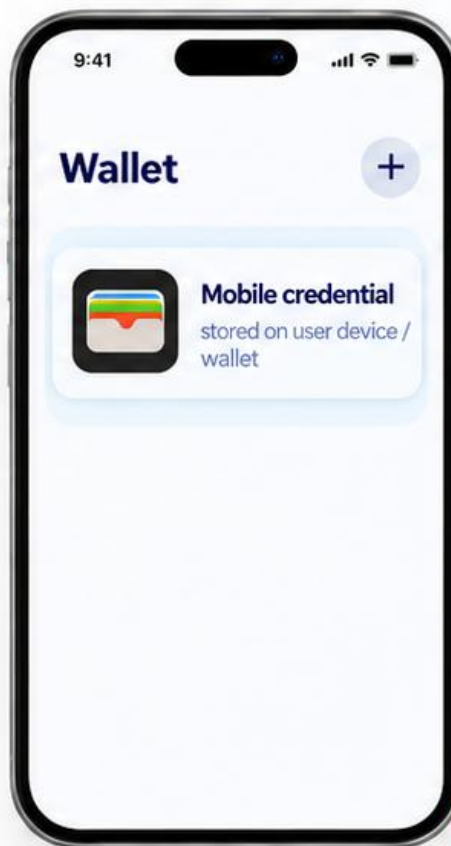


Matter ecosystem / controller

home setup, lock provisioning

Provision mobile
credential to device

User device (mobile phone)



Aliro specification

- common credential framework
- standardized reader ↔ user-device communication
- NFC / BLE access, optional UWB ranging

NFC

tap / short range



BLE

hands-free / wireless



UWB

precise ranging (used with BLE)

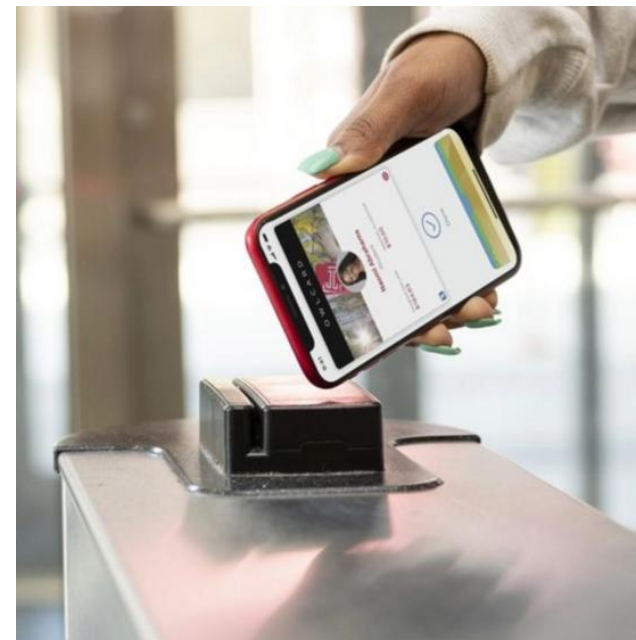


Reader



Provision Aliro config / credentials on lock

Dvě technologie, podobný posun





Credential
issuance

Wallet
integration

PKI /
Trust infrastructure

Key
management

Reader support
(HW / FW)

Provisioning

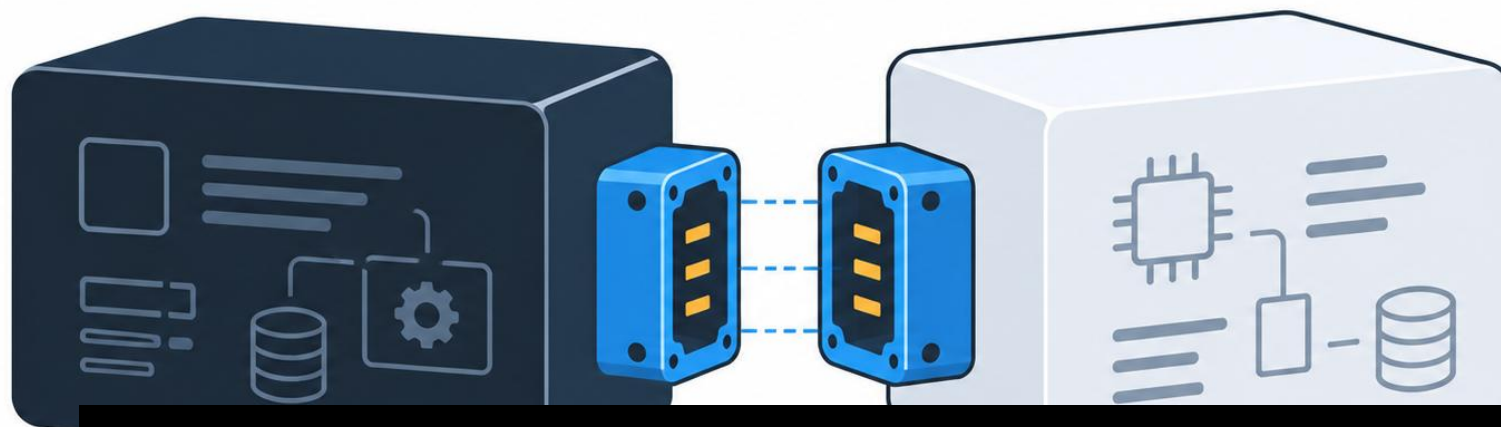
Lifecycle
management

PACS
integration

Security
& compliance

Operations
& monitoring

Open interfaces.
Independent implementations.



Otázky?

adam@horcica.cz | @horcicaa