NXP vision on Digital Identity & Agentic AI

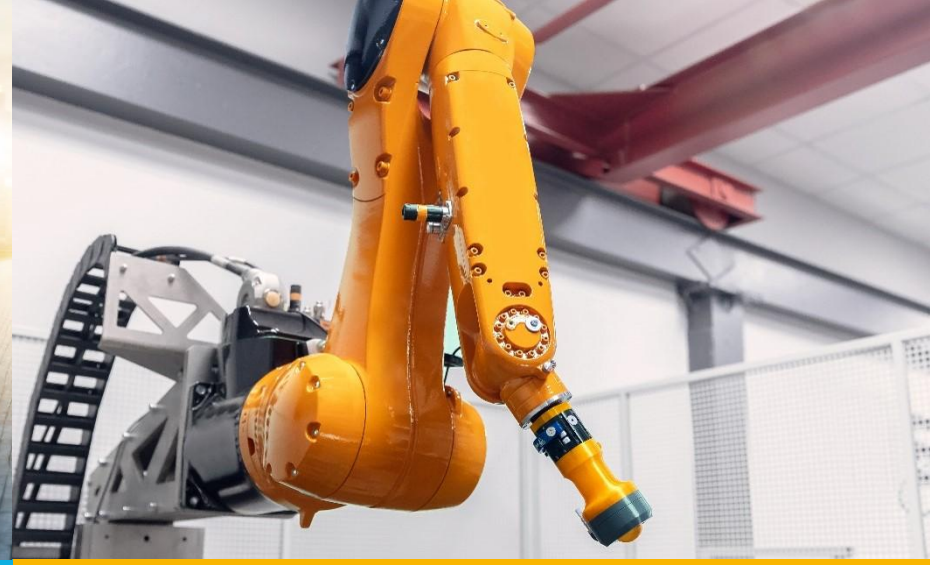
Fabien Deboyser
March 2026

NXP Corporate Overview

Together we accelerate the breakthroughs that advance our world

We design purpose-built, rigorously tested technologies that enable devices to sense, think, connect and act intelligently to improve people's daily lives.

Automotive



Industrial & IoT

Mobile

Communication Infrastructure

Examples of deployments leveraging Secure Element technology

Critical points for a trusted Digital Identity ecosystem

Assurance level high

EU regulation mandates strong assurance. Only HW-anchored trust can reliably meet this requirement

High attack potential resistant (AVA_VAN.5)

Tamper-resistant protection (passport-grade), ensuring long-term resilience against sophisticated attacks

Privacy-preserving architecture (GDPR)

Local credentials, ZKPs, and minimized data exposure, the wallet shall ensure privacy-by-design

Protection against large scale attacks

Local wallet ecosystems with distributed cryptographic trust significantly reduce systemic risks and avoid single centralized points of failure

Offline mode

Identity must remain usable at all time (airport, underground, rail stations, borders, rural areas, emergency situations etc.) or when the battery is off. This aligns with the emerging Digital Euro offline requirements

Enforced user consent

Every sensitive identity operation must be explicitly authorized by the user, cryptographically enforced and locally verified, a prerequisite for adoption and trust

Strong binding User ↔ Device ↔ Wallet

Trust relies on a cryptographically verifiable association between the citizen, the physical device, and the wallet instance. This prevents impersonation and enforces accountability

NXP SE technology offers

Security level high EAL4+ AVA_VAN.5
SEs are certified level high VAN.5

Root of Trust
Secure boot, signed firmware, secure logs, attestation

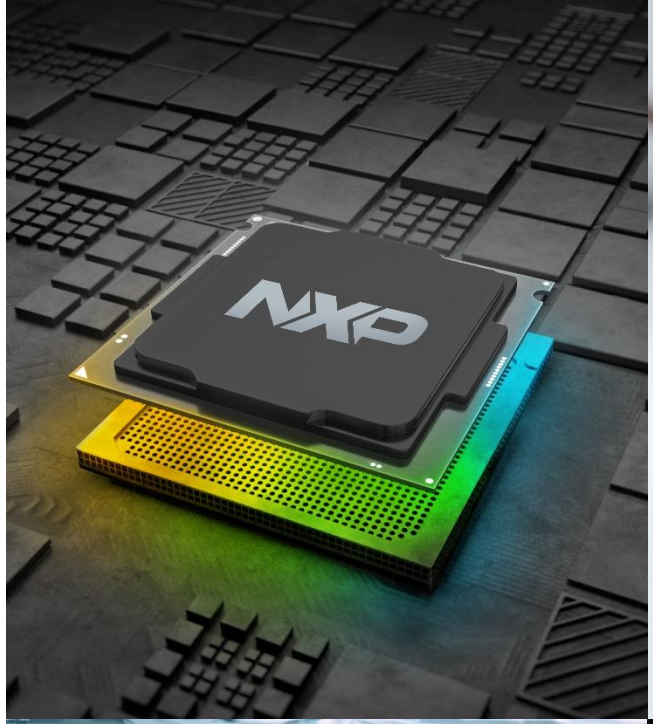
Enforce user consent
Keys never leave the SE enforcing sovereignty + trust

Battery-off
Ultra-low-power capabilities supporting battery-off

Offline mode
Secure execution of offline identity operations

Post-quantum resistant
Cryptographic engines supporting PQ-resistant algorithms

Privacy
Local processing and credential storage enable selective disclosure, unlinkability, and privacy-preserving flows (+ biometric)



Agentic AI security protected by SE

Agent Identity & Authentication

- Agentic AI must authenticate itself, maintain secure logs, and guarantee fresh, verified, and traceable actions
- This requires a hardware-anchored identity (stored in NVM) which secure enclaves typically cannot provide

SE-Anchored Binding Between Agent & Platform

The SE ensures that AI agents operate within a trusted boundary:

- binding the agent to the device
- binding the device to the wallet
- binding all actions to a high-assurance identity

VAN.5-Grade Protection of AI Credentials

- Model-access keys, signing keys, policy enforcement materials, and agent-decision signatures must be shielded from extraction or manipulation
- Only SEs provide adequate guarantees

Layered Flexibility & Future Evolution

- Secure Elements allow: applet updates / new crypto protocols / new policy engines / post-quantum transitions
- This flexibility is essential for evolving agentic capabilities and future regulation

backup

Top risks if SE-based architecture is not adopted

1. Fragmentation of Security Levels Across Devices & Regions

Low-end phones, older devices, or certain OS ecosystems cannot meet Level High without SEs

2. Vendor Lock-In via Proprietary Trust Layers

Device OS providers become de-facto trust authorities, undermining EU sovereignty

3. Inconsistent Enforcement of User Consent

Software-based (TEE) consent mechanisms can be bypassed or spoofed

4. Increased Attack Surface & Large-Scale Breach Scenarios

Centralized or cloud/TEE-based approaches reintroduce systemic risks

5. Inability to Support Battery-Off / Offline Identity Use Cases

Critical for Digital Euro, border control, mobility, emergency response

6. Weak Binding Between User, Device & Wallet

Identity impersonation and credential misuse become feasible

7. Exposure of Sensitive Keys & Credentials

Without tamper-resistance, side-channel, fault-attack, and physical attacks can extract secrets

8. Non-Compliance with eIDAS Level High Requirements

Software-trust models will have difficulties to match the level high security certification requirements

9. Unsafe Integration of Agentic AI

AI models manipulating identity actions without hardware-enforced boundaries opens unprecedented security & privacy dangers

nxp.com