TRUST SERVICES FORUM 8TH

Fabien Deboyser
OCTOBER 2022

SECURE CONNECTIONS FOR A SMARTER WORLD

Fabien Deboyser – Security certification expert @ NXP

- Common Criteria ISO17025 laboratory setup (Netherlands, UK)

- Standardization CEN/CENELEC ; patents

- Common Criteria EAL5+ (passports, Java Card platform, banking, HSM, tachograph, …)

- FIPS 140 security level 3 (HSM, PIV card) ; PCI; CAVP

NXP SEMICONDUCTORS WORLDWIDE

Together with our valued customers, we're not just advancing technology, we're advancing society.

60 years of combined experience and expertise

Operations in more than **30 countries** worldwide

Approximately **31,000 employees**

Headquarters in The Netherlands – **Eindhoven**

AUTOMOTIVE

Enabling carmakers to develop smarter solutions for complex autonomy, connectivity, and electrification challenges

Accelerating the shift to greater mobility

INDUSTRIAL

Reducing wasted time, money, and effort by helping business run more efficiently.

Enabling more efficient data processing

MOBILE

Giving wearable and mobile devices easier access to the services that make modern life more convenient without compromising security and safety.

Transforming how people and devices connect

SMART HOME

Solutions that listen, learn, and adapt into the places we call home for more comfort, affordability, safety, and convenience.

Powering the intelligence behind the technologies

SMART CITY

Simplifying how people access and interact with local services to achieve new standards of sustainability, efficiency, mobility, and economic growth.

Anticipating the demands of tomorrow

COMMUNICATION INFRASTRUCTURE

Powering insights and inspiring performance with hardware solutions for handling 5G connectivity across the emerging communications spectrum.

Delivering real-time responsiveness at the speed of 5G

SECURITY CERTIFICATION & STANDARDIZATION ACTIVITIES @ NXP

IT ISMS Services

- 99 ISO27001 certified sites

- 56 EAL6+ certified sites

- 4 GSMA certified sites

Product Certification

- 250+ product certifications

- Common Criteria, ID, Banking, SESIP, SESIP, eUICC, PSA, CAVP, FIPS 140

SDO participations

MOBILE

ENABLING SECURE TRANSACTIONS

VALUE PROPOSITION

Technology innovator

Leadership positions in NFC and embedded Secure Elements (eSE).

First in the industry to offer the full scope of mobile wallet development with mWallet 2GO.

Industry-first solution that combines UWB fine ranging, NFC, Secure Element, and embedded SIM (eSIM).

Driving secure applications
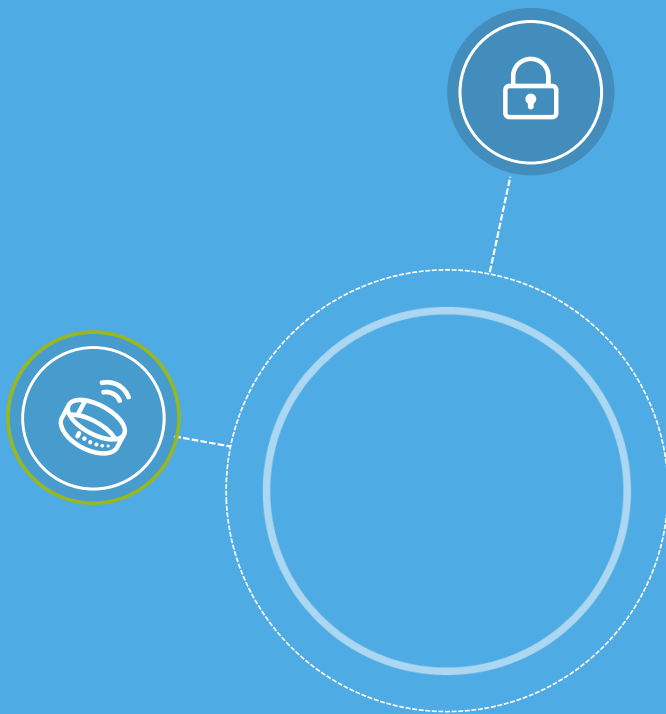
Payment | Transit | Access | Identification

Trusted partner across ecosystems

Mobile and wearable OEMs
Financial institutions
Governments
Public transit operators

NXP

MAIN CRITICAL ASPECTS

Only level High shall be allowed

- The EUID data needs to be trusted = by citizens (we protect) and from legal entities (we trust the data)
- The EUID will last for a long period = High offers enough security headroom to manage the evolution of the attacks, particularly scalable attacks
- Level High must be assessed according to measurable quantitative security assessments (e.g. Protection Profiles)

Offline mode shall be taken into account (for mobile phone & verifier)

- The use case where both the mobile phone and the verifier are offline must be considered
- The phone off use case must be foreseen (battery low[1] but wireless interface to secure element of mobile phone still operational)

Other important topics

- Timelines = All transitions or temporary dispositions in the Regulation must be specified according to a fixed well-defined timeline with hard limits
- Crypto agility = Migration + transition to PQC must be foreseen today
- UWB = Alternative technologies must be foreseen to improve the multi-modal multi-authentication solutions

[1]Low Battery Mode is also a mandatory requirement by CCC (Car Connectivity Consortium) for Digital Car Key Use case.

SECURE CONNECTIONS
FOR A SMARTER WORLD