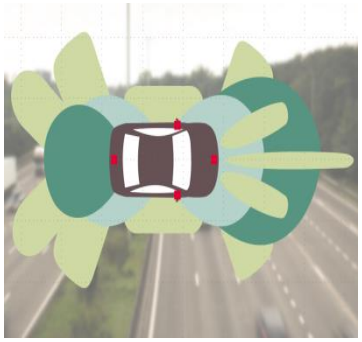
Cyber security of automated vehicles

B. Steurich
Infineon Technologies

AMAA 2017 Conference Sep. 2017, Berlin

Infineon

Building blocks of automated driving: Cooperation of multiple system and disciplines



Data Processing and Decision Making

Sensing

Vehicle Dynamics and Control

Making
HMI

Vehicle Sensors
Radar, Ultrasonic, Camera, Lidar, GPS, Maps

Fusion
Sensor Data Central Computing

Connectivity
DSRC, Wi-Fi Cellular

spension

Transmission

Braking

Steering

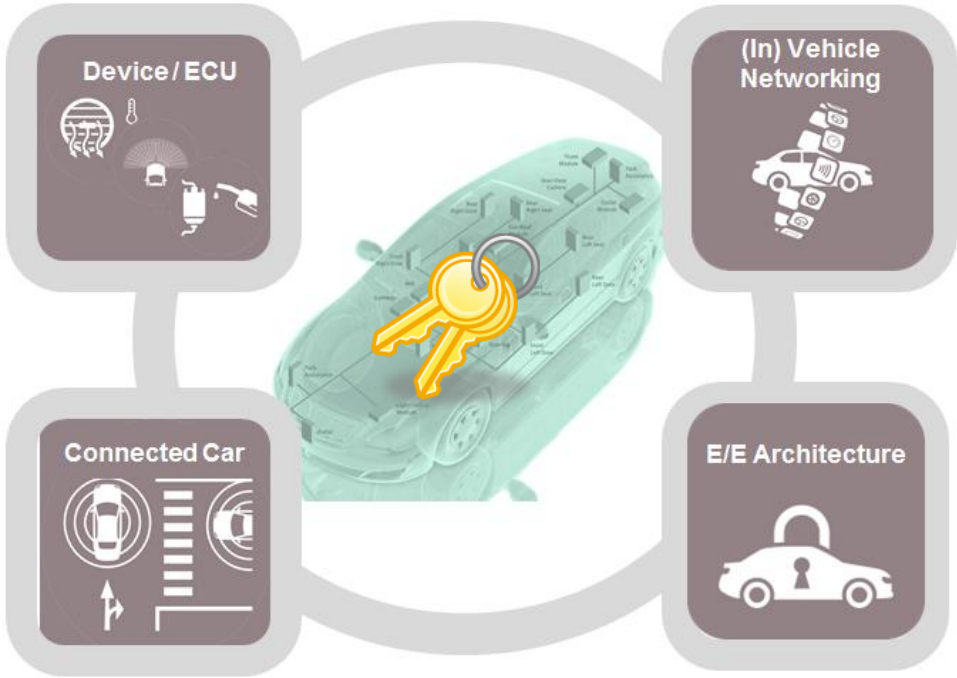
Engine

IT security is built on three cornerstones

Automotive security needs more…

Overall automotive security goals

- Enable functional safety
- Protect business & IP
- Meet customers quality expectation
- Fulfill privacy & regulation requirements



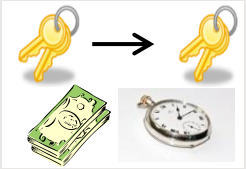
Secret keys are the basic prerequisite of any secured vehicle operation

Secret keys must be protected

Key integrity is essential for system security

- Compromised keys = no security

- Revocation of keys is expensive and takes time



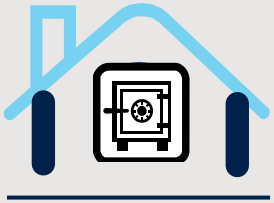
- Key handling must be secured through the whole lifecycle

Hardware trust anchors

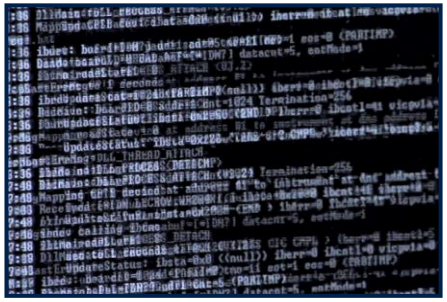
Provide protected execution environments & tamper resistance for high-security demands

› Key storage & related crypto operation

› Key management and deployment in insecure environment

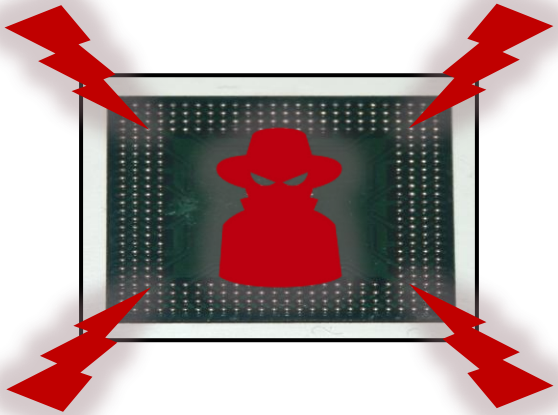


Standard microchips can be attacked by various means



Logical attack
e.g. protocol fuzzing

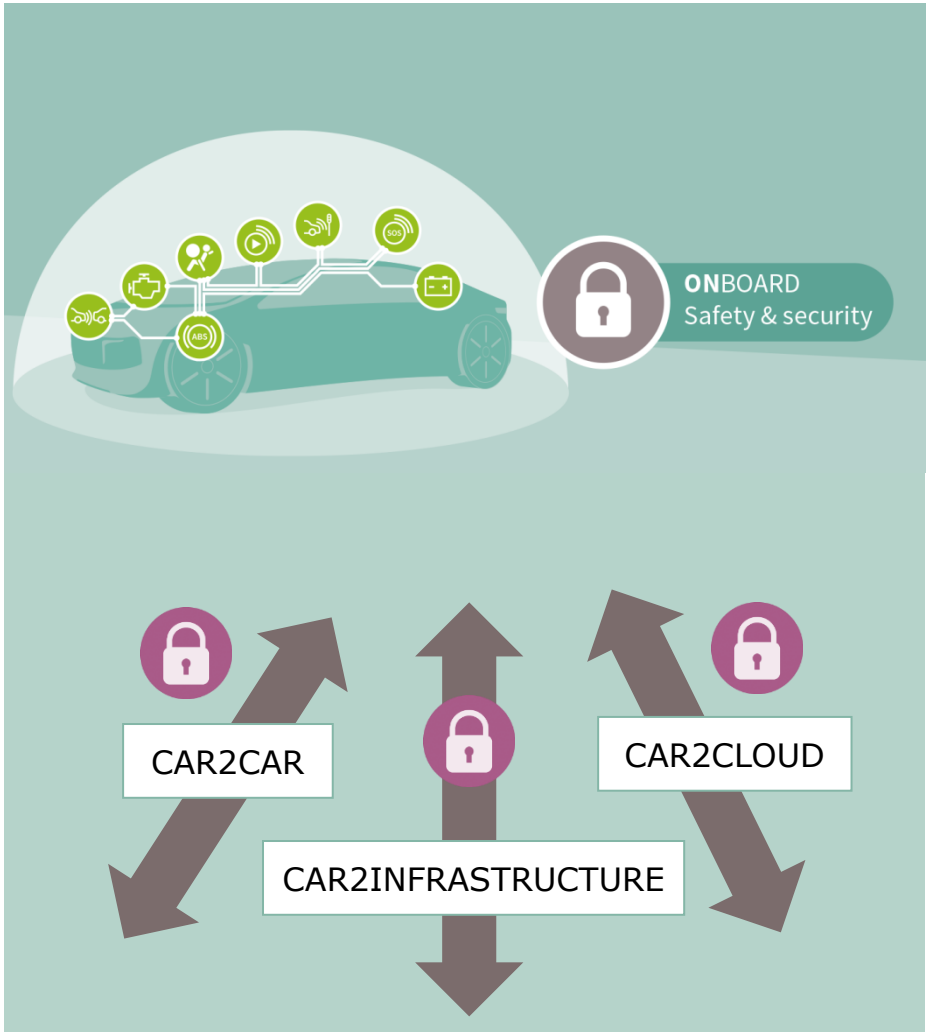
Observative attack
e.g. power analysis



Manipulative attack
e.g. probing

Semi-invasive attack
e.g. laser fault injection

Features of trust anchors
for automotive security



Integrated on MCU (HSM)

- Onboard security
- Protected com. & debug interfaces
- High-speed / real-time critical tasks

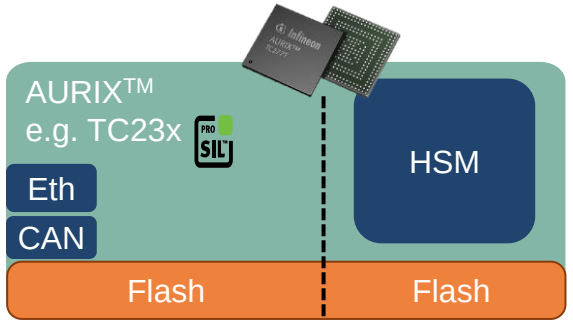
Discrete Security Controller

- Protected external communication
- Certified hardware security
- Protecting critical keys & certificates

Hardware security module (HSM) and Trusted platform module (TPM) - Overview

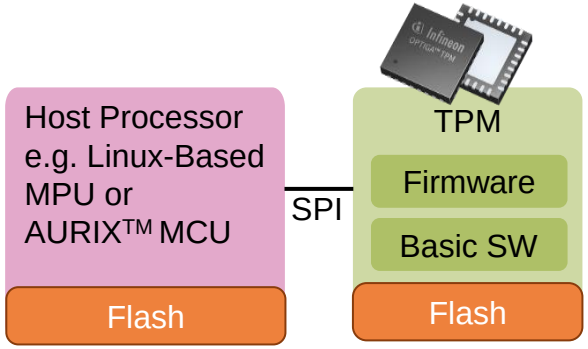
HSM - Integrated on MCU

- **Integrated security hardware** incl.
  - Protected key & program storage, internal firewall, debug protection, crypto accelerators (AES-128/ECC256/SHA-2), AIS31 compliant True Random Number Generator (TRNG) for key generation, 32bit CPU…
- **High performance, real-time** capable
- Full Automotive temperature range and quality (AEC Q-100 Grade 0+, DFR), AUTOSAR compliant



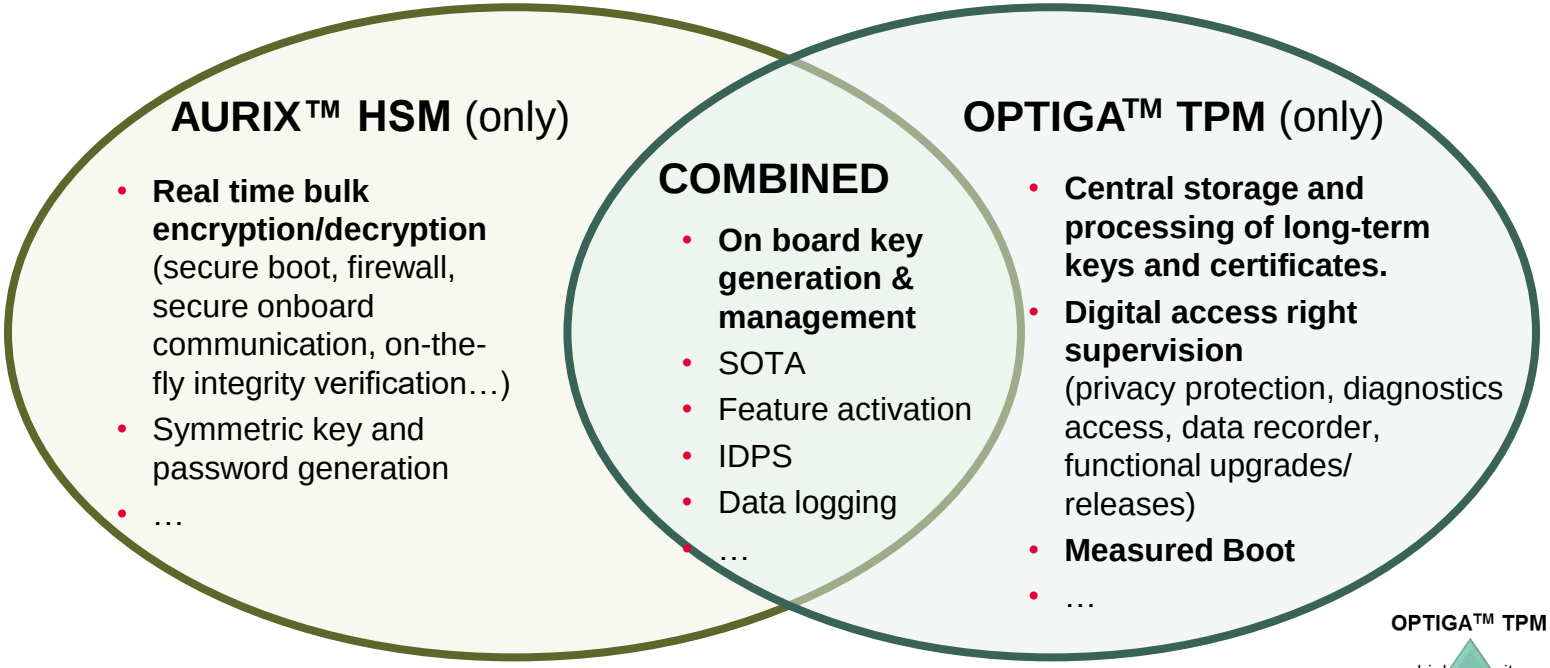
TPM – Discrete security hardware

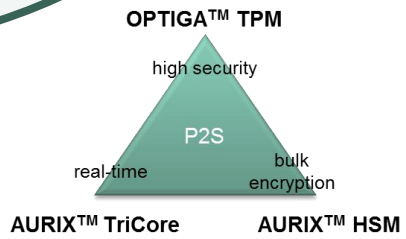
- **EAL 4+ high** security certified hardware & software (high tamper resistance)
- Ca. **100 standardized crypto functions**
- Supports multiple crypto schemes (incl. AES-256/ECC512/RSA2028)
- AEC-Q100 Grade 2 compatible
- AIS31 compliant (TRNG) for key generation



A selection of security use cases in conjunction with automated vehicles

We propose three use case classes (AURIX™ & TPM):





Remark:

- Some use cases can be implemented with both AURIX or TPM.
- The security architecture requirements of the OEM are decisive.
- There is a need to maximize security level and minimize overall cost

Connectivity and security in the context of automated driving

- **Self-driving cars need to know their precise location and what's around them** to maneuver safely.
- **Sensors have their limits**, and self-driving cars need the ability to see "around corners" and into the distance in advance.
- **Date integrity** (accuracy & authenticity of data) must be ensured.

5GAA Automotive Association

V2X - 5GAA – Configuration A
Multiple use cases in parallel

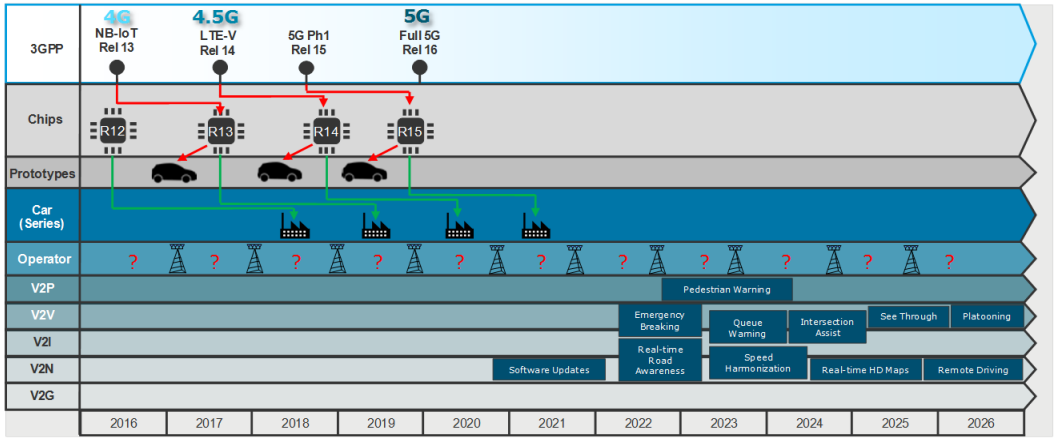
Real-time

- See-through scenarios
- Sensor sharing
- Intersection movement assist
- Real time situational awareness & high definition maps
- Cooperative lane change (automated driving merging assist)
- Vulnerable road user (incl. V2P)/ collision avoidance
- Queue warning incl. congestion
- Speed harmonization
- Road-side unit (RSU) assisted safety/ platooning
- Tele operated driving
- …

Not real-time

- Firmware & software update

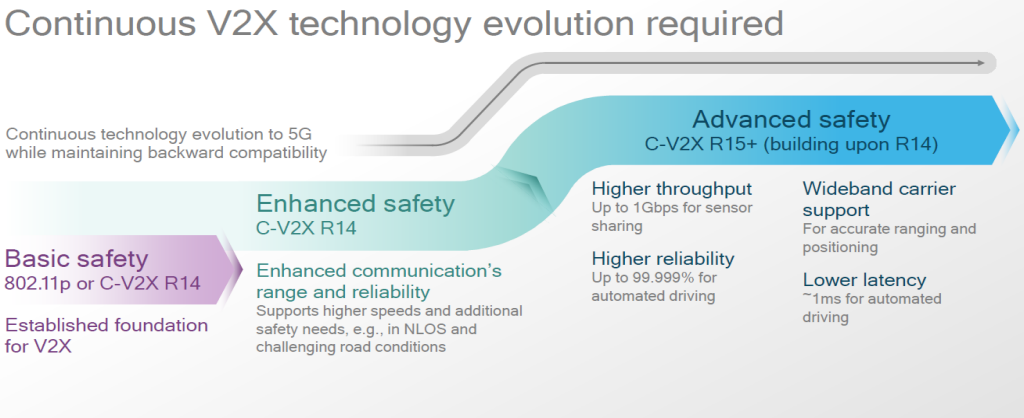
5G V2X Timeline (5GAA Vision)



- Vehicles are getting prepared for **heterogeneous com. configuration** (incl. LTE/5G, BT and DSRC)
- Automotive Ethernet will be used as communication backbone (**up to 20Gbit/s**)

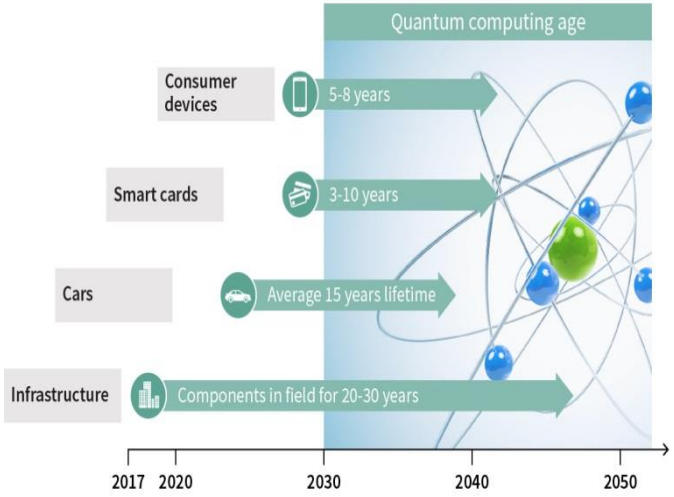
Holistic security concept

- Access control to in-vehicle network (IVN)
- Secure on-board communication
- Data usage policies
- Anomaly detection and defense etc.



Source: 5GAA & OEM discussion

Quantum computers – food for thought



Quantum Computers

- Powerful machine that can be used for crypto analysis and more
- Idea: Use quantum mechanical effects for computation
- Different from classical computers with quantum bits (qubits), quantum gates and some restrictions (no cloning, reversibility)
- Universal quantum computers expected in 15 – 20 years
  - Goal to increase the number of stable qubits
  - 2016: 5-qubit computer by IBM
  - 2017: 17-qubit computer by IBM

Possible other specialized application of quantum computers

- Optimization problems
- Quantum chemistry

IBM's quantum cloud computer goes commercial
http://www.nature.com/news/ibm-s-quantum-cloud-computer-goes-commercial-1.21585

European Commission will launch €1 billion quantum technologies flagship
https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-quantum-technologies-flagship

The threat of quantum computers to cryptography

Quantum cryptanalysis on an universal quantum computer

Currently used **asymmetric** cryptosystems (RSA/ECC) breakable by using **Shor's algorithm**

- Classical world (currently): ECC-256 has 128-bit of security
- Quantum world (in 15-20 years): ECC-256 has almost 0-bit of security

Bit-security level for **symmetric** cryptography is halved by **Grover's algorithm**

- Classical world (currently): AES-128 has 128-bit of security
- Quantum world (in 15-20 years): AES-128 has only 64-bit of security

Quantum world (in 15-20 years)

Heavily affected:
RSA, ECDSA, ECDH

Considered safe:
AES-256, SHA512, SHA3-512

Affected:
AES-128, 3DES

Post-quantum cryptography and quantum cryptography

Post-Quantum Cryptography and Quantum Cryptography are not the same

Post-Quantum Cryptography

- Conventional cryptography deployable without quantum computers (i.e. on a classical computer)
- Requires new mathematical hardness assumptions for public-key-crypto
- Mainly 5 families of crypto schemes being researched (widely vary in the key length and applicability)

Quantum Cryptography

- Mainly Quantum Key Distribution (QKD) to secure communication using quantum mechanics
- Security relies on quantum mechanics not computational assumptions
- Physical requirements like fiber-optical cable between communication parties

As the leading provider of security solutions, Infineon is actively pursuing intensive research on **post-quantum cryptography**

www.infineon.com/post-quantum-crypto

Demonstrator of post-quantum cryptography

› Demonstrator of post-quantum cryptography on a smart card chip

Infineon's contactless smart card (SLE 78)

Infineon succeeded to implement a variant of New Hope on an Infineon contactless smart card microcontroller (SLE 78)

› This chip family is used in numerous high-security applications like electronic passports

› In smart cards, computing and memory resources are limited

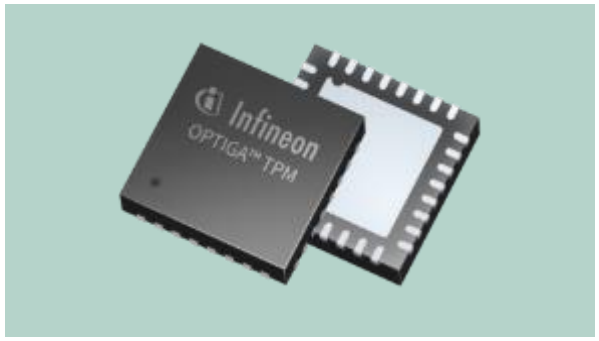
The New Hope key-exchange protects the communication between the smart card and the reader

› Required for electronic passports but also when smart card or secure element establishes a secure channel with the cloud (e.g. in case of IoT)

Summary

Connected cars offer cost saving potentials, convenience gains and new business opportunities. Trust anchors are indispensable in the context.

Infineon investigates solutions to provide security by a combination of ***AURIX™ and OPTIGA™ TPM*** as well as solutions to match future challenges of connectivity and crypto agility.



Infineon's scalable portfolio of hardware trust anchors can achieve ***Digital Resilience and Survivability*** in a cost efficient manner through the supply chain