escrypt GmbH – Embedded Security
Systemhaus für eingebettete Sicherheit

Designing Secure Automotive Hardware for Enhancing Traffic Safety – The EVITA Project

Marko Wolf, escrypt GmbH – Embedded Security

CAST Workshop Mobile Security for Intelligent Cars

Darmstadt, Germany, August 27th, 2009

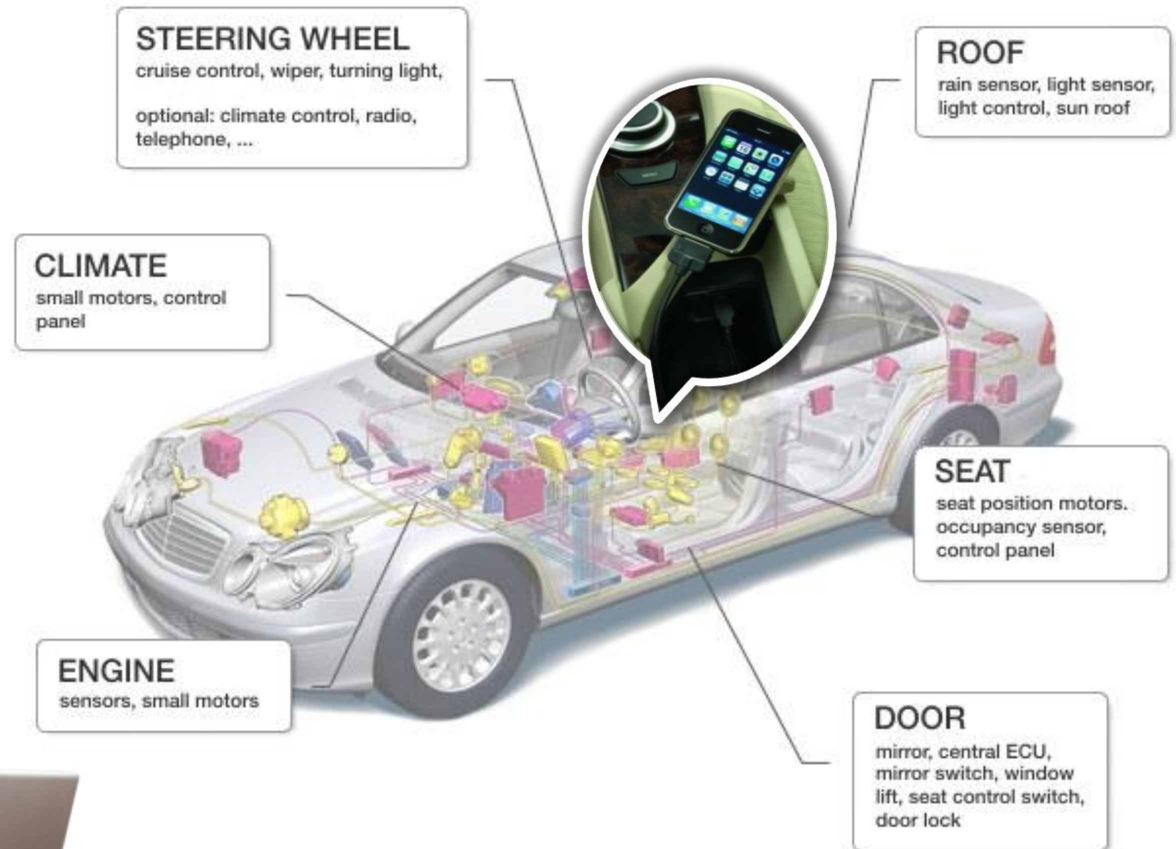
escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

info@escrypt.com
phone: +49(0)234 43 870 209
fax: +49(0)234 43 870 211

SEVENTH FRAMEWORK PROGRAMME

Motivation

The need for ***in-vehicle*** security



➲ You already know this…

The need for in-vehicle security
Possible attacks & attack intentions for vehicles

- **Steal** the vehicle or a valuable component
- **Circumvent** restrictions in hardware or software functionality (e.g., speed locks, feature activation, software updates)
- **Manipulate** financially, legally, or warranty relevant vehicular components (e.g., toll devices, digital tachograph, chip tuning)
- **Spy on** manufacturer's expertise and intellectual property (e.g., counterfeits, industrial espionage)
- **Violate** privacy issues (e.g., contacts, last trips)
- **Impersonate** (e.g., electronic license plate)
- **Misuse** external communications (e.g., disturb, misuse, harm)
- **Harm** passengers, destroy OEM’s reputation (e.g., safety attacks)

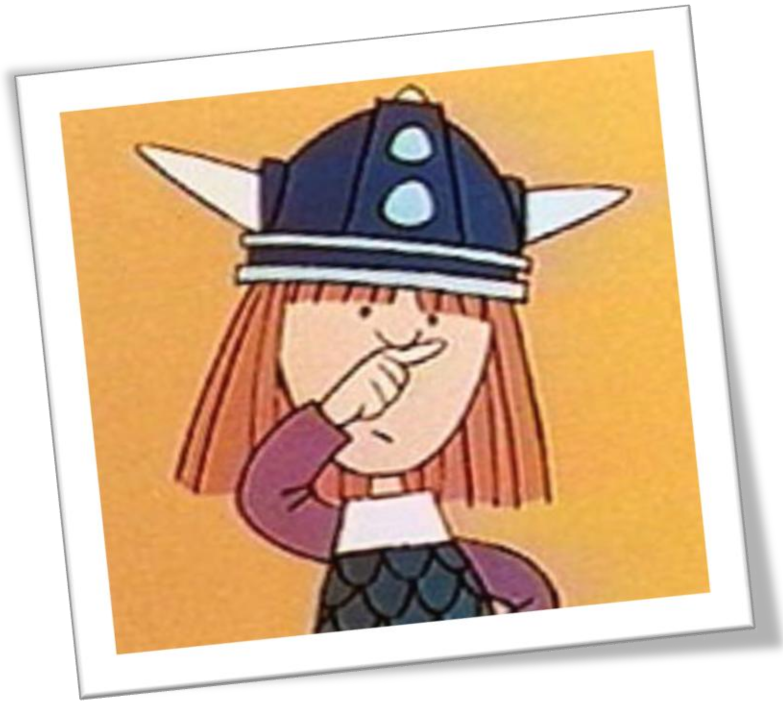
➲ Strong need for reliable security mechanisms!

info@escrypt.com

The security of vehicular security mechanisms

Why just applying standard (non-vehicle) solutions won't work

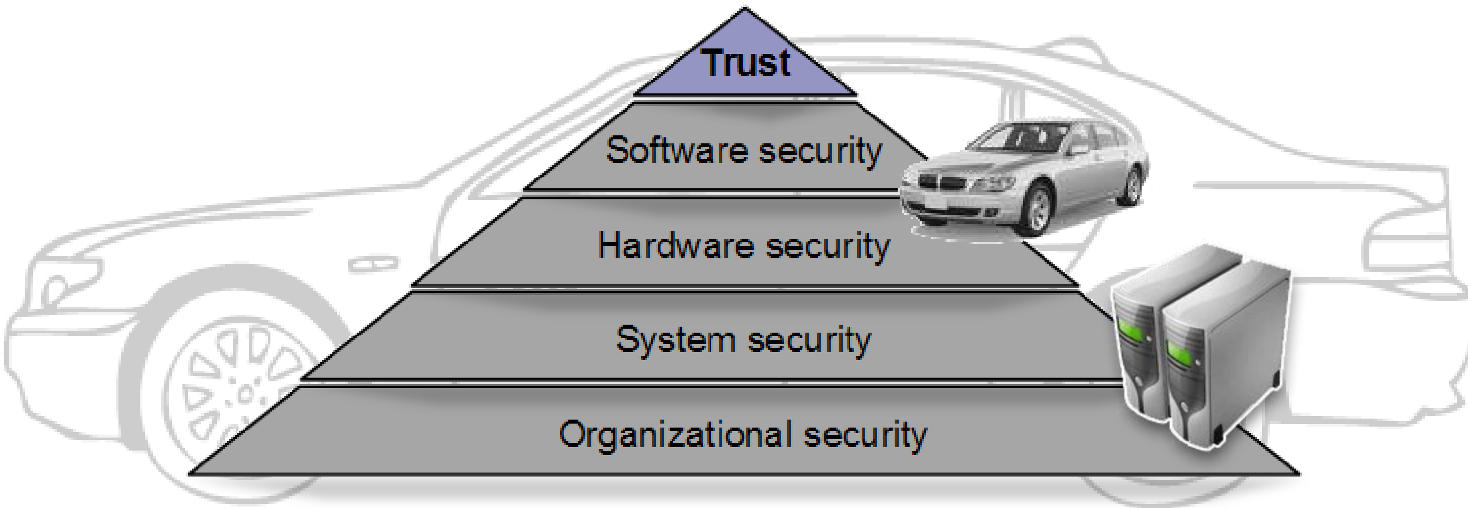
- **Beyond "standard attacks" ..**
  - **Insider attacks**
  - **Offline attacks**
  - **Physical attacks**
- **Many different attackers and attacking incentives**
- **Many different attack points**
- **Vehicular IT is client/server, embedded and mobile world**



➲ Standard (non-vehicle) security solutions won't work!

info@escrypt.com

The security of vehicular security mechanisms
The security pyramid of a dependable IT system



- **Organizational security** *against* **organization attacks** (e.g., social engineering) by well-thought *security processes, secure infrastructures and organizational security policies*
- **System security** *against* **logical attacks** (e.g., cryptographic weaknesses or weak APIs) by a *secure well-thought security system design and adequate security protocols*
- **Hardware security** *against* **hardware attacks** (e.g., security artifacts manipulations or read-out, physical locks, side-channels etc.) by *hardware tamper-protection measures*
- **Software security** *against* **software attacks** (e.g., weak OS mechanisms or malware) by reliable *software security mechanisms* (e.g., secure init, secure RTE) and *hardware security mechanisms that protect and enforce security of software mechanisms*

Vehicular Security Hardware
What security hardware can help

- **Protects** software security mechanisms by
  - ➲ Providing a trustworthy *security anchor* for upper SW layers
  - ➲ *Secure generation, secure storage, and secure processing* of security-critical material shielded from all pot. malicious SW
- **Prevents** hardware tampering attacks by
  - ➲ Applying *tamper-protection* measures
- **Accelerates** security mechanisms by
  - ➲ Applying *cryptographic accelerators*
- **Reduces** security costs on high volumes by
  - ➲ Applying highly optimized special circuitry instead of general purpose hardware

Vehicular Security Hardware
What is the current situation?

- **Proprietary** and **single-purpose** hardware security solutions in vehicular environments, for example:
  - Immobilizer
  - Digital tachograph
  - Toll Collect OBU

VDO digital tachograph

- General-purpose hardware security modules for **non-automotive** environments , for example:
  - IBM cryptographic coprocessor
  - Cryptographic smartcards
  - Trusted Platform Module
  - Mobile Trusted Module

IBM 4758 cryptographic coprocessor

➲ **Are where any solutions for vehicular security HW?**

E-safety Vehicle Intrusion proTected Application (EVITA)

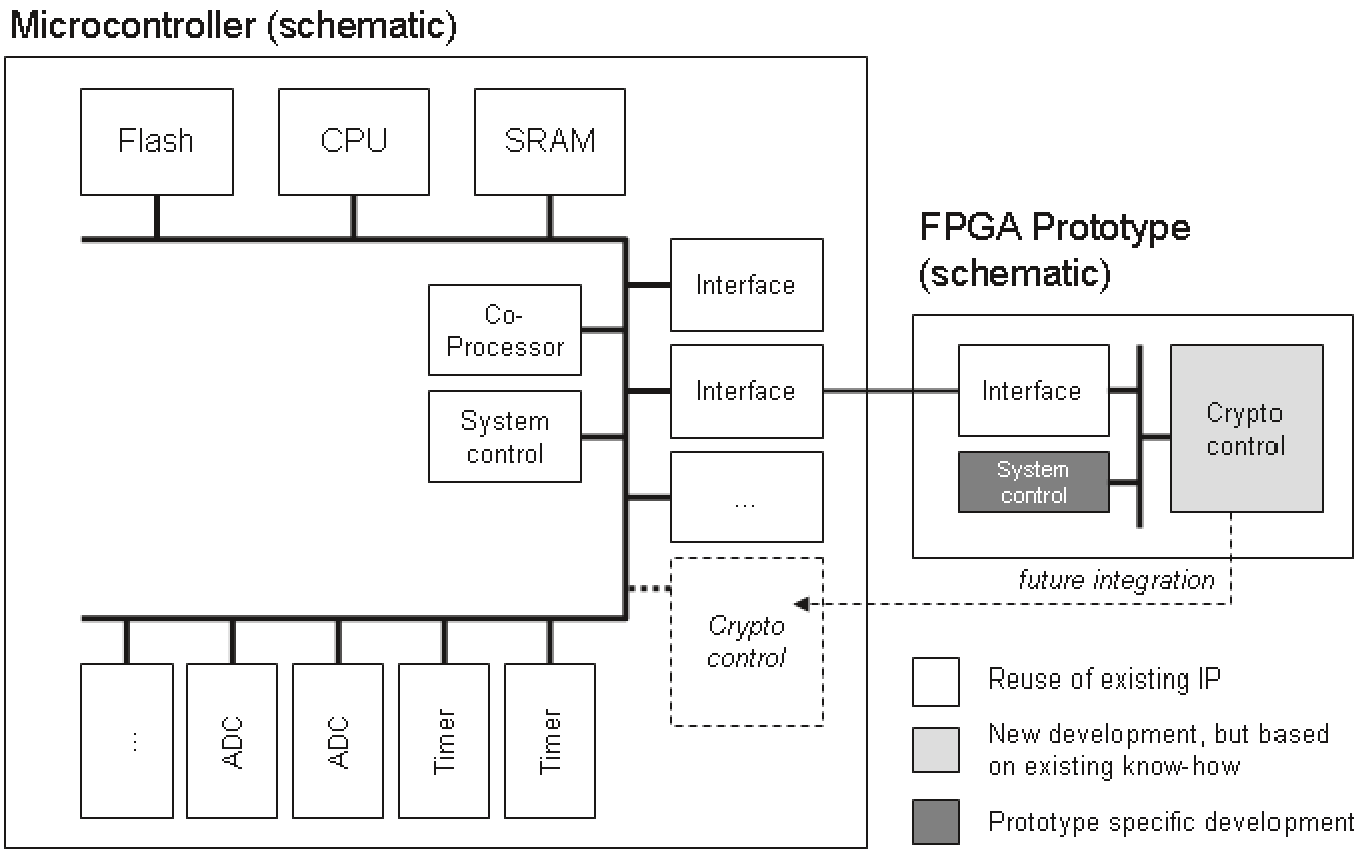
Project objectives

- **Powerful ECU security hardware extension** that: *".. aims at designing, verifying, and prototyping an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise."*
- **Prevent** or at least detect **malicious malfunction** of in-vehicle e-safety applications
- **Detect** manipulated information from **external entities**
- **Design** and **verify** a **ECU security architecture**, including
  - ECU hardware security extension
  - ECU software security components
  - corresponding (e-safety) security protocols
- **Implement** , **demonstrate** and **validate** ECU security architecture for practicability

EVITA Project
Background information

- **Objective:** Automotive capable security hardware (“automotive TPM”) for enabling a vehicular security architecture protecting e-safety V2X communications (e.g., emergency break, eCall)
- **Program**: FP7-ICT-2007 of the European Community (EC)
- **Partners**: BMW, Bosch, Continental, escrypt, EURECOM, Fraunhofer, Fujitsu, Infineon, Institute TELECOM, KU Leuven, MIRA, TRIALOG from Belgium, France, Germany, Sweden, UK
- **Duration**: 36 months (July 2008 – June 2011)
- **Total cost**: 6 million €
- **Further information**: *www.evita-project.org*

EVITA General Approach
Microcontroller security extension



EVITA General Approach
ECU security architecture

- E-safety application layer (security protocols)
- AUTOSAR / Linux (*MobLin*) RTE
- Basic software layer including security software and EVITA drivers
- Microcontroller abstraction layer (MCAL)
- Microcontroller hardware layer
  - Security hardware

EVITA Project Status
Current work plan / milestones

- Work plan
  - 2008: Security requirements analysis
  - **2009: Secure on-board architecture design**
  - 2010: Reference implementation in SW & HW
  - 2010: Prototyped-based demonstration (lab car)
  - 2011: Publication as open specification

EVITA Project Status
What has been done I

- Identification of e-safety relevant use-cases (D2.1)
  - V2V: Traffic information, local danger warning, active break..
  - V2I: POI, e-Call, e-Tolling, “remote vehicle function control”..
  - CE Integration: User/Third Party applications, secure isolation/integration..
  - Aftermarket: Feature activation, ECU replacement..
  - Diagnosis: remote diagnosis, “remote repair”..

EVITA Project Status
What has been done II

- Identification and evaluation of possible dark-side scenarios (D2.3/B)
  - Attack motivations (harm driver, gain driver information, gain hacker reputation, personal gain, financial gain, harm OEM, terrorism..)
  - Possible attacks (tamper with warning messages, tamper e-traffic control, attack e-Tolling, attack e-Call, safety attacks..)
  - Threat and risk analysis based on CC attack potential taxonomy

EVITA Project Status
What has been done III

- Specification of relevant security requirements (D2.3)
  - Security requirements regarding data confidentiality, authenticity, freshness, access control, privacy, availability

Requirement reference: Authenticity_29
Informal description: Whenever a firmware is installed to the car, it shall be authentically programmed by the manu-facturer.
Semi-formal description: *authentic(program(Manufacturer,Firmware),install(car,Firmware),car)* *authentic(program(Manufacturer,Firmware),install(car,Firmware),Manufacturer(car))*
Use case references: 17, 18
Notes: This property is related to a different system model, outside the runtime component-model of the car.

  - Basic security requirements prioritization

➲ EVITA security extension in every ECU?

EVITA Overall Hardware Architecture
Deployment architecture I

➲ EVITA security extension in every ECU?

- Appropriate hardware security levels to meet:
  - different cost constraints
  - different security protection requirements
  - different (security) functional requirements
- By applying EVITA modules enables:
  - Protection of all security-critical ECUs for a holistic security architecture
  - All modules are capable to interact securely with each other
  - Efficiently meet cost, security, and functional requirements

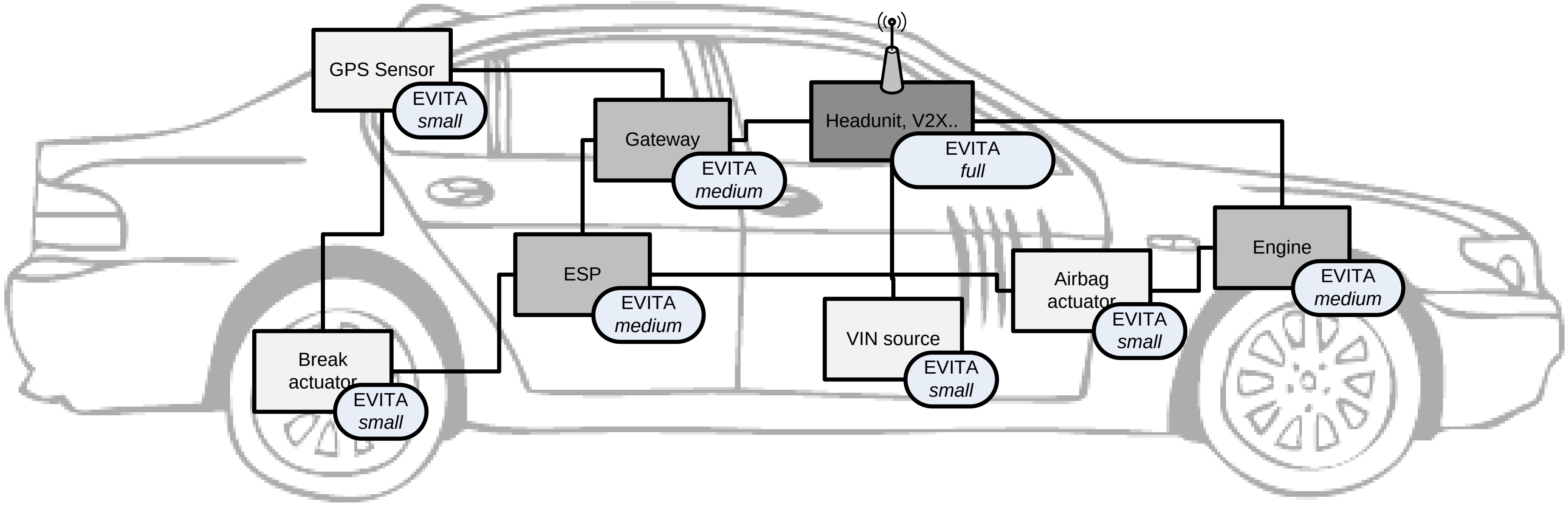
➲ Cost-effective, flexible, and holistic vehicular security architecture

info@escrypt.com

EVITA Overall Hardware Architecture
Deployment architecture II

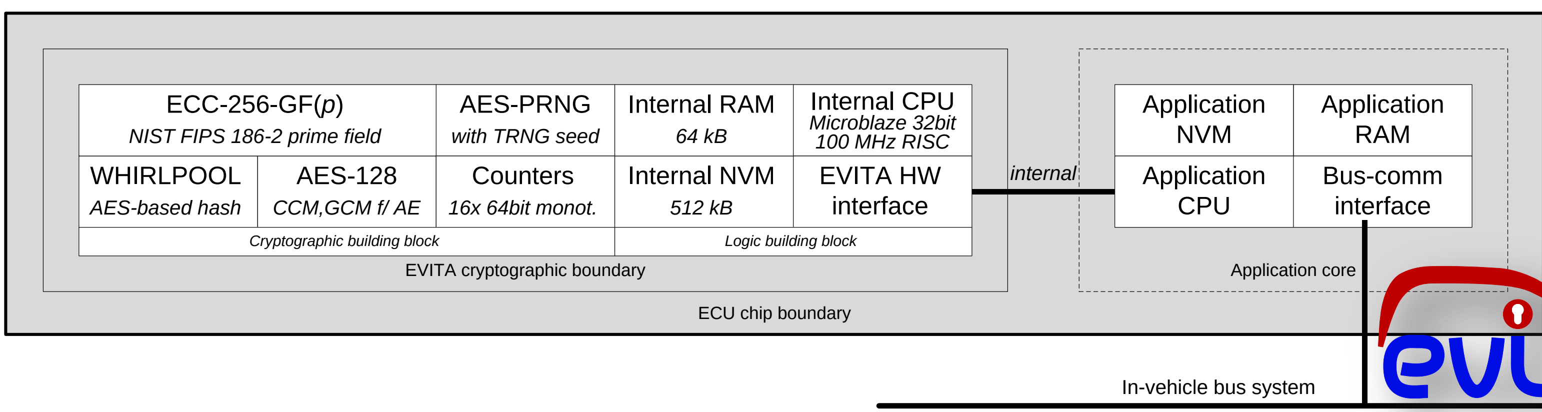
- EVITA *full* module in 1 – 2 high-performance comm. ECUs
  - V2X communication unit
  - Central gateway (possibly)
- EVITA *medium* module in 2 - 4 central multi-purpose ECUs
  - Engine control
  - Front/rear module
  - Immobilizer
- EVITA *small* in less, but security-critical client ECUs
  - Critical sensors: e.g., wheel, acceleration, pedal sensors
  - Critical actuator: e.g., breaks, door locks, turn signal indicator
  - Critical small ECU: e.g., GPS module, lighting, clock

EVITA Overall Hardware Architecture
Deployment architecture III



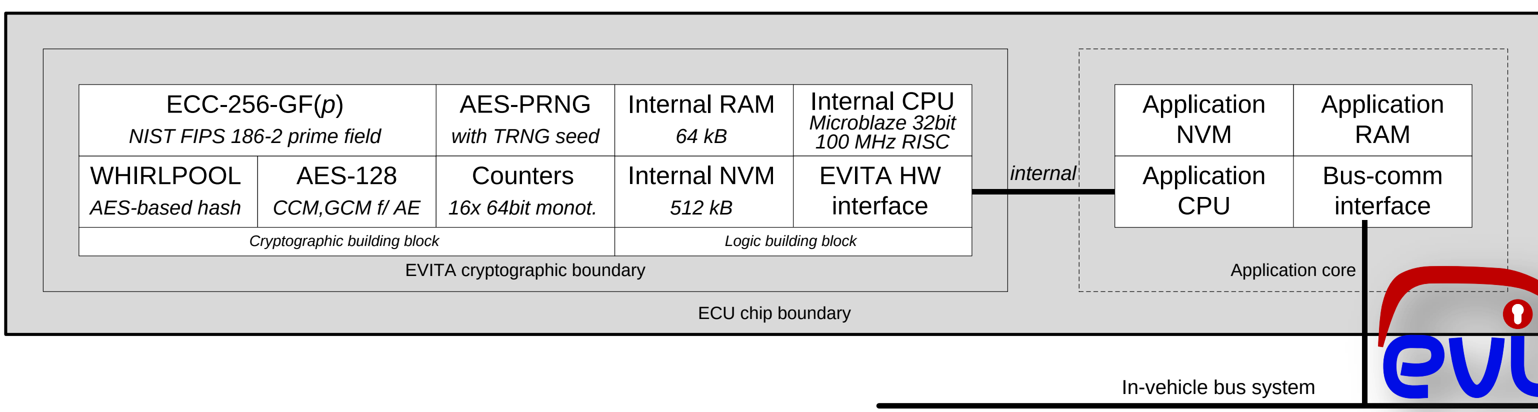
EVITA Hardware Security Modules
Full size version (draft!)

- **ECC-256-GF(p)**: High-performance 256-bit **NIST standard** elliptic curve arithmetic that can generate and verify ≈ **250 signatures/s**
- **WHIRLPOOL**: Generic hash function (allows ASIC w/ **SHA-3**) actually using AES-based **NIST standardized** hash function with ≈ **1 Gbit/s** throughput
- **AES-128**: Symmetric **NIST standard** ECB/CBC block encryption/decryption but also advanced **AE modes** e.g. GCM/CCM with ≈ **1 Gbit/s** throughput
- **AES-PRNG**: PRNG using a **true random seed** based an internal AES engine according to **BSI-AIS20 standard** with ≈ **500 Mbit/s** throughput
- **COUNTER**: 16 x 64-bit monotonic counters at 1 Hz to act as **"secure clock"**



EVITA Hardware Security Modules
Full size version (draft!)

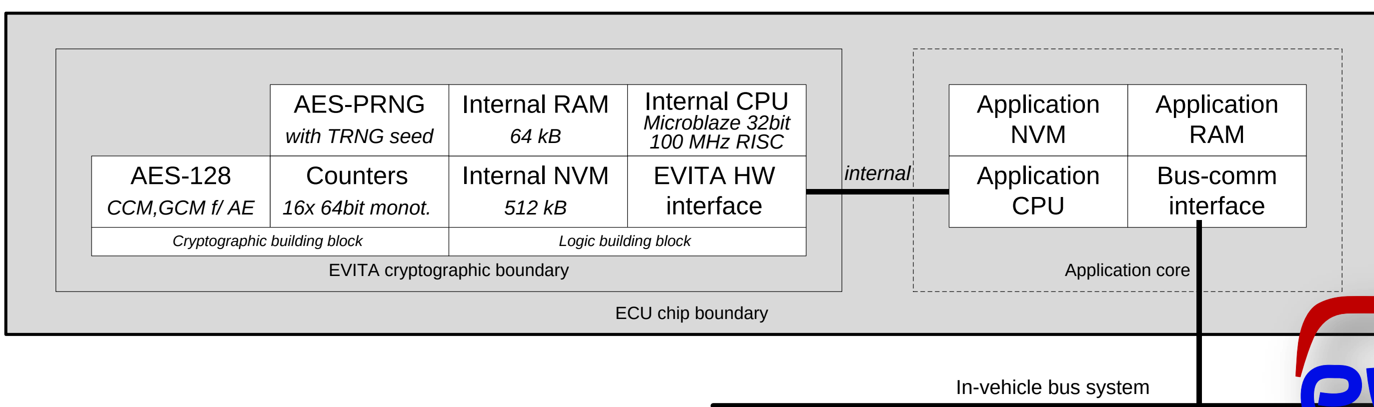
- **Internal-CPU**: Internal **32-bit RISC** microprocessor to handle all logics and non-time-critical cryptographic functionality that operates at ≈ **100 MHz**
- **Internal-RAM**: Small volatile memory to store for instance runtime values and variables with a capacity of ≈> **64 kByte**
- **Internal-NVM**: Small non-volatile memory to store for instance internal keys and security certificates with a capacity of ≈> **512 kByte**
- **HW-API**: EVITA hardware interface to enforces a well-defined access to the EVITA hardware security functionality for the application CPU and software (e.g., provides message pre-/post-processing, session management/control)



escrypt Embedded Security

EVITA Hardware Security Modules
Medium size version (draft!)

- Designed to **suit both**: stringent **security** requirements and significant **cost pressures** of powerful multi-functions ECUs
- Virtually identical to the EVITA *full* version except in that it has **no dedicated ECC hardware** and **no dedicated hash hardware**
- Very fast symmetric cryptography in hardware, but rather slow – but nonetheless practicable – asymmetric cryptography
- Meets **all in-vehicle security** use cases, but not suitable for V2X

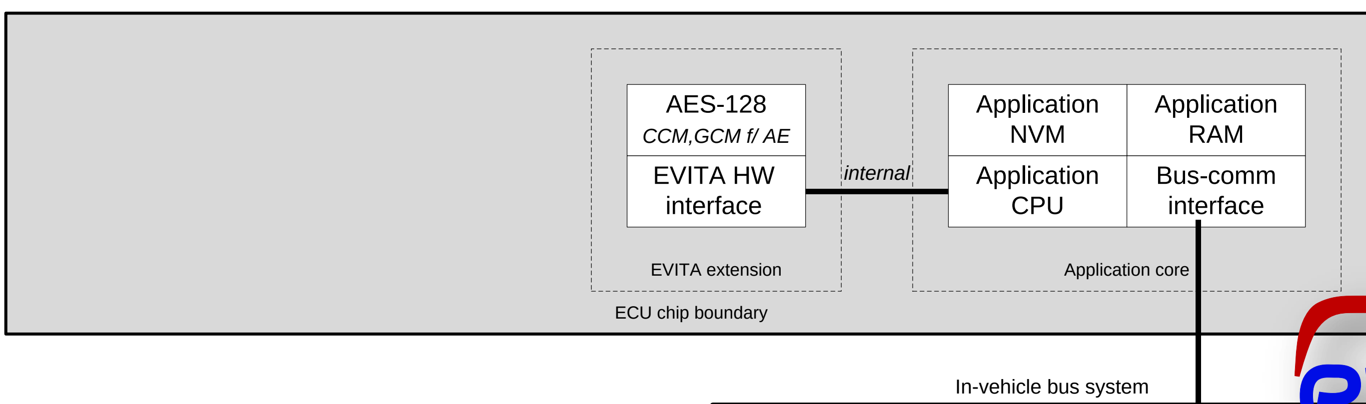


info@escrypt.com

escrypt Embedded Security

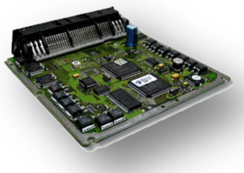
EVITA Hardware Security Modules
Small size version (draft!)

- **Integrates** and protects **small ECUs**, **sensors** and **actuators** that provide or process security critical information
- Reduced to a single very **cost-optimized symmetric AES hardware** accelerator (i.e., all security credentials are handled by the application processor)
- Cannot provide any hardware-based security, but enables sensors and actuators to **efficiently process and generate protected information**

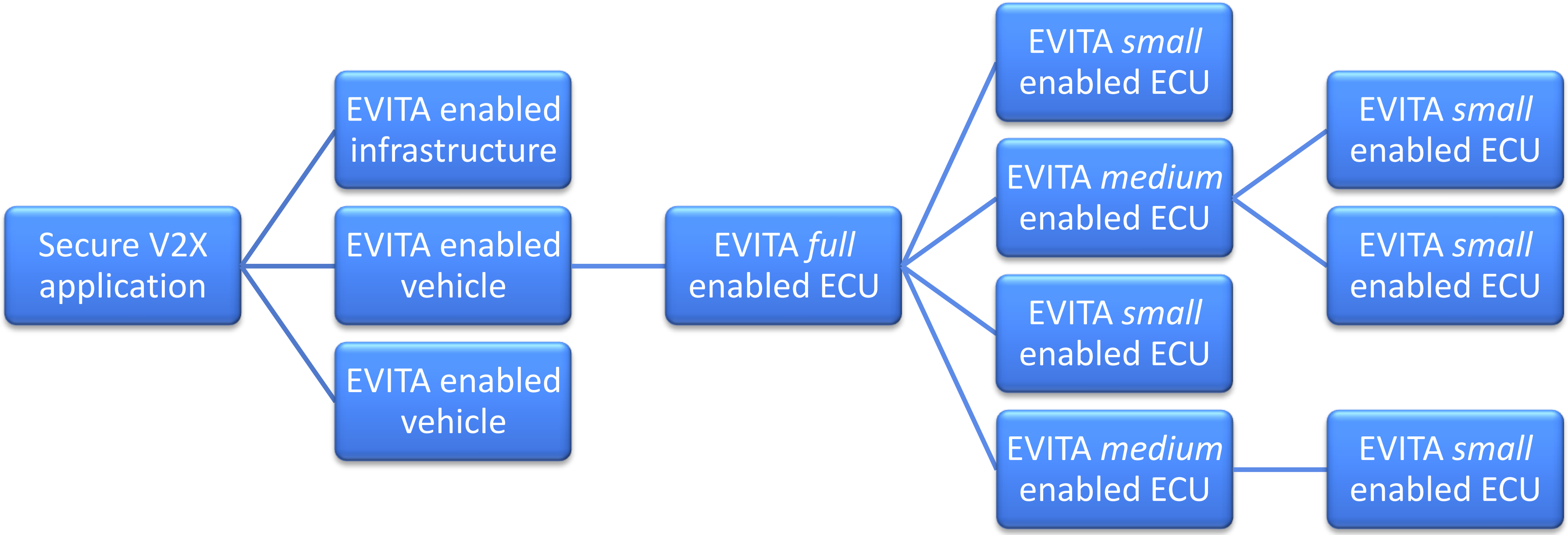


Dependable Vehicular Security Architectures

Continuous security chain from ITS to sensors



Vehicular applications → Cars & infrastructures → V2X Head unit → Standard ECU → Sensors/Actuators

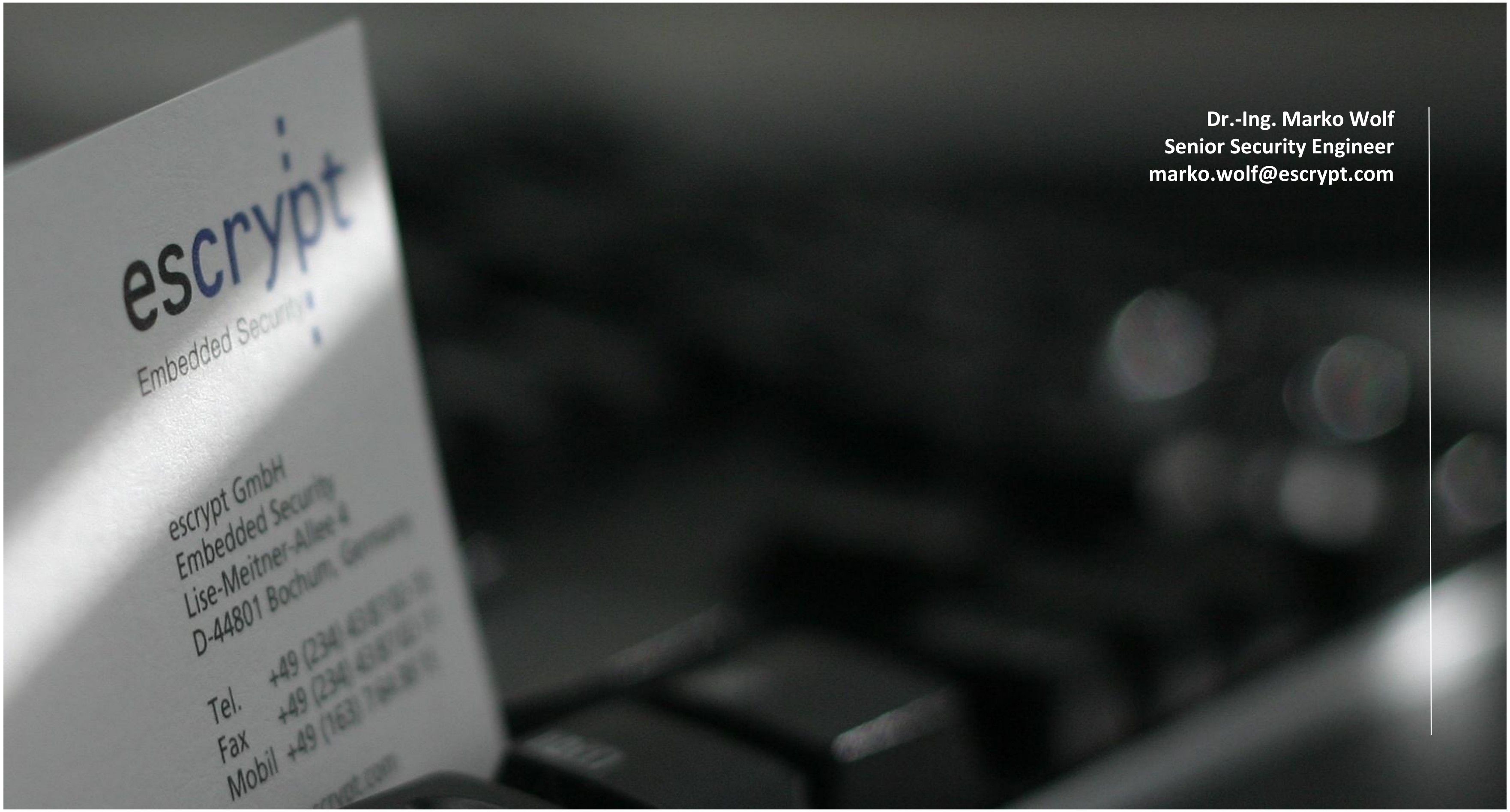


info@escrypt.com

escrypt Embedded Security

Conclusion and Outlook

- Standardized security hardware is **essential** for the security of **vehicular security mechanisms**
- Vehicular security hardware helps **preventing** almost **all software attacks** and **many physical attacks**
- Automotive proof security hardware (or even standards) **currently not available** (neither low-level nor high-level)
- However, open **EVITA** prototypes could be **promising opportunities** to act as effective, trustworthy and cost-effective hardware security anchors in vehicular environments



Dr.-Ing. Marko Wolf
Senior Security Engineer
marko.wolf@escrypt.com

escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

info@escrypt.com
phone: +49(0)234 43 870 209
fax: +49(0)234 43 870 211