Project acronym:	EVITA
Project title:	E-safety vehicle intrusion protected applications
Project reference:	224275
Programme:	Seventh Research Framework Programme (2007–2013) of the European Community
Objective:	ICT-2007.6.2: ICT for cooperative systems
Contract type:	Collaborative project
Start date of project:	1 July 2008
Duration:	42 months

Deliverable D1.2.5.2:
Presentation Slides from the
Final EVITA Workshop on
Security of Automotive On-Board Networks

Editor: Olaf Henniger (Fraunhofer Institute SIT)

Dissemination level:	Public
Deliverable type:	Other
Date:	23 November 2011
Workshop venue:	Honda Academy, Erlensee, Germany

Abstract

Car-to-car communication heralds a new era of traffic safety and intelligent traffic management, but at the same time also entails new threats. To provide a secure basis for car-to-car communication, the European research project EVITA designed, verified, and prototyped security building blocks for automotive on-board networks. The security building blocks are deployed inside lab cars demonstrating various applications that require security measures. As the project draws to a close, the EVITA consortium held a Workshop on Security of Automotive On-Board Networks in order to present major results of the project to the public. The workshop took place at the Honda Academy in Erlensee, Germany, on the day before the Car 2 Car Forum 2011 of the Car 2 Car Communication Consortium. All interested parties were invited to attend the Final EVITA Workshop.

Contents

Workshop
"Security of Automotive On-Board Networks“

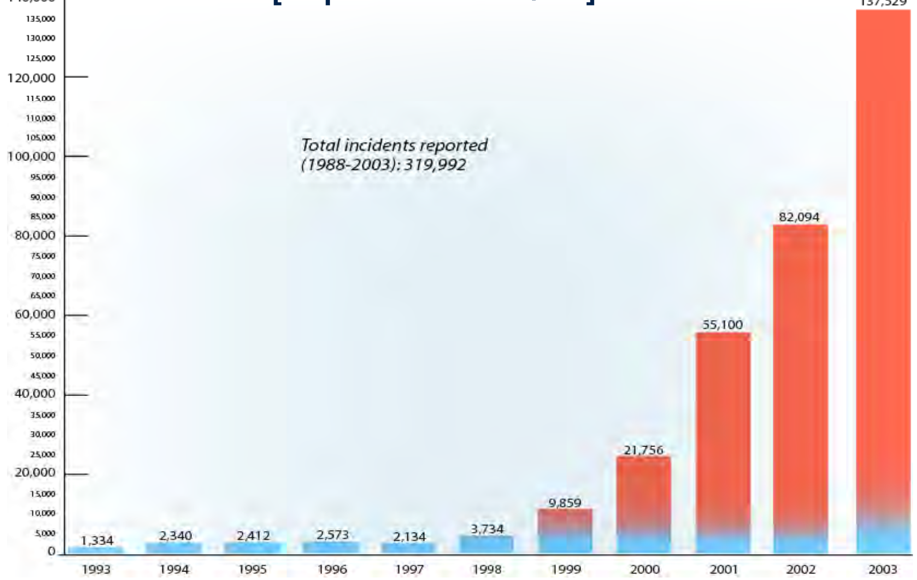
Trusted Computing in Mobile and Embedded Systems

23. November 2011

Hans.brandl@infineon.com

IT System Attacks are increasing despite all Security and Encryption Features

[Reports to CERT / CC]



Computing Platforms:
The Problem and the Solution

Inadequate Security on standard computing Platforms

- The problem of platform security exists since the early 70's
- General purpose Computers lack fundamental security mechanisms. There are encryption modules , but attacks circumventing.
- Most attacks occur through manipulations of the integrity, not on hacking algorithm!
- What is necessary, is an affordable hardware security module and the necessary OS functionality for the computing platform, which allows at least
  - Measurement of the integrity of the platform
  - Secure storage and digital signing of data, keys and certificates

Today's Perception of System Trust

Who is TCG?

- The Trusted Computing Group (TCG) is an international industry standards group
- The TCG develops specifications amongst its members
  - Upon completion, the TCG publishes the specifications
  - Anyone may use the specifications once they are published
- The TCG publicizes the specifications and uses membership implementations as examples of the use of TCG Technology
- The TCG is organized into a work group model whereby experts from each technology category can work together to develop the specifications
  - This fosters a neutral environment where competitors and collaborators can develop industry best capabilities that are vendor neutral and interoperable

TCG Standards and its Community

Global Standardization:
TPM 1.2 spec (2003) is ISO/IEC 11889 standard (2008)

91 TCG Specifications published to-date (since 2003)

Worldwide TPM shipment:
400 million -500 million

Adoption Examples:
Healthcare
Government
E-Commerce
Financial Applications

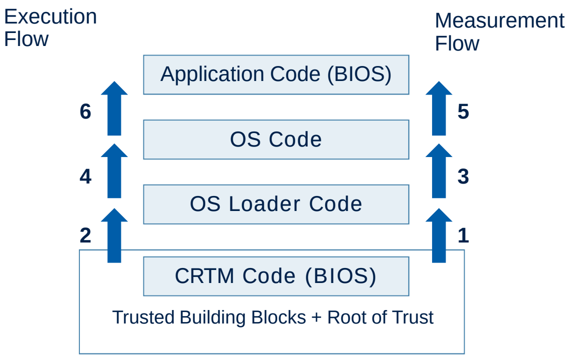
TCG Community	# of Organizations
Australia	1
Austria	2
Belgium	1
Canada	8
Greater China	5
Finland	1
France	6
Germany	12
India	1
Israel	4
Japan	12
Korea	3
Netherlands	2
Norway	1
Russia	1
Sweden	1
Switzerland	2
United Kingdom	11
United States	79

Where do we see TCG Technology today?

- Commercialized and available
  1. High Assurance Platforms (HAP)
  2. Self-encrypting drives (SEDs)
  3. Network security (TNC)
  4. Trusted Platform Modules (TPMs)

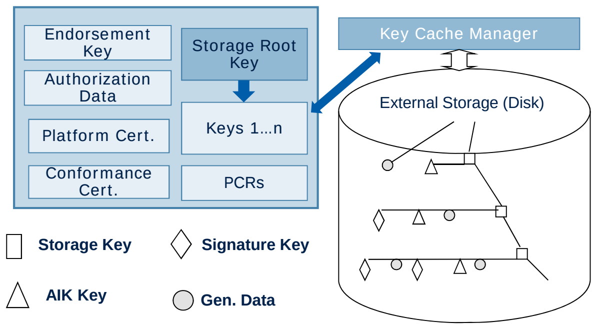
- Applications/solutions that use TCG Technology
  1. Machine Identity
  2. VPN/wireless access
  3. Data at rest
  4. SCADA
  5. Clientless endpoint meta data mana
  6. Hardware-based cloud subscriber management
  7. Trusted execution

Trusted Platform Module
Providing the Root for the Chain of Trust



- The Core Root of Trust for Measurement (CRTM) MUST be an immutable portion of the Platform's initialization code that executes upon a Platform Reset. The Platform's execution MUST begin at the CRTM upon any Platform Reset.
- The trust in the Platform is based on this component. The trust in all measurements is based on the integrity of this component.

Trusted Platform Module
A nearly unlimited, secure Storage Key Hierarchy



- Storage Root Key (SRK) forms the root of a key hierarchy in which other lower-order keys, but also data (blobs), are securely stored. Their trustworthiness therefore depending on the SRK. With the help of the TSS Core Services the storage area is extended to external memory and therefore nearly unlimited.
- The SRK is automatically generated by the owner in a "Take Ownership" operation. If the owner of a TPM gives up this ownership, this also deletes the SRK and also makes all the keys protected by it completely unusable, which is welcome for data protection purposes.

Do we really need Security and Trust for Embedded ?

- **In the past embedded systems were small computers in an isolated environment with stable and fixed programs:**
  - **No attacks via networks**
  - **No real economical motivation for hacking**
  - **Small and well defined functionality with fixed loaded code, nothing dynamic**
  - **No real economical advantage from interception and eavesdropping**
  - **Embedded systems were an island of tranquility and peace**
- **The situation has already changed:**
  - **Embedded networks are now connected to the internet. Attack methods from other networks are also applied to embedded networks**
  - **The entire value of equipment may be embodied as stored parameters in an embedded system, which becomes a target worth hacking**
  - **Security and safety is mandatory in a changing world**
  - **STUXNet woke up the industry**

Embedded systems have lost their security innocence

Embedded Systems Security and Trust: No Longer Just Data Encryption

- **Integrity of the whole system:** detecting modifications of the code, data or hardware structure which might be caused either by accident (system faults) or external attacks (viruses etc.)
- **Safety:** operational conditions, error tolerance, fault handling, failsafe conditions, automatic detection of error conditions, automatic and protected handover to replacement systems
- **Protection against cloning and copyright violation**
- **Digital Rights Management for handling data and content**
- **Communication security:** preventing misuse of communication links, authentication of participants, access rights, policy enforcement etc.
- **Privacy**

New Embedded Platform Requirements

- **Multi Tenant Structures for multifunctional applications:**
- **Example: Cars or mobile phones**
  - **Manufacturer**
  - **Service provider**
  - **Owner**
- **New protection models against the outside: e.g. protecting the device against its owner**
- **New security and conformance paradigma (new attacks are expected in the future, counter measurements are needed today)**
- **Working under attack means operate under an erroneous environment.**
- **Override the complexity barrier of everyday product (like cars) will need TC functionality and is also a matter for strategic product design.**

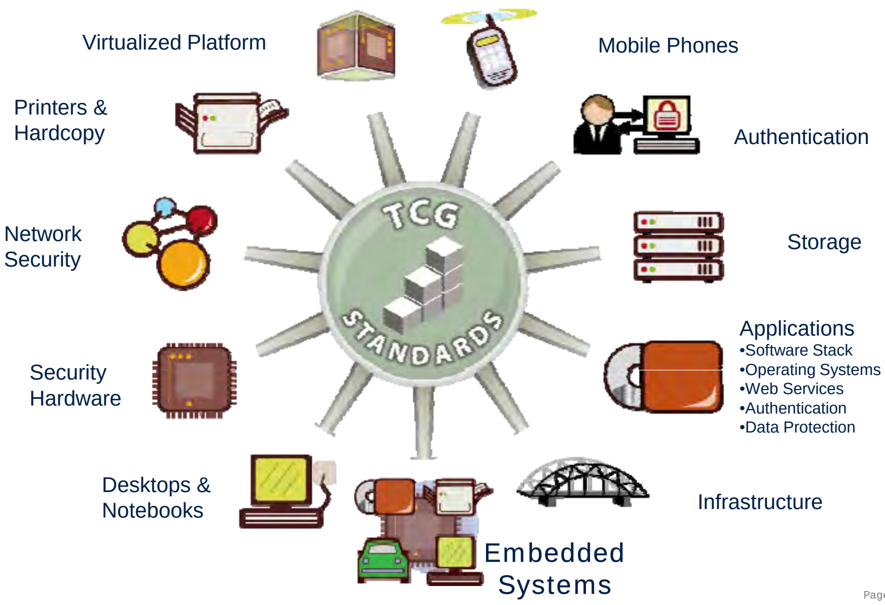
TCG Embedded Systems Work Group

To address the upcoming demands from society and market , TCG has established the Embedded Systems (EmSys) Work Group to adapt existing standards and create new standards for the needs of embedded platforms

- **EmSys works on technical specifications such as :**
- Additional TPM interfaces for embedded systems:
  - I2C, SPI etc.
- Additional TPM functionalities for embedded such as:
  - Secure boot, local attestation, remote activation and many more
- Integrated TPM and support for specific environments like integrated, trusted sensors or active TPM modules

Page 13

Complete Trusted Enterprise Solutions



Page 14

EmSys also works on Solution Specs

- Systems and use cases for
  - Automotive
  - SmartGrids
  - Industrial Control
  - Medical
  - Critical Infrastructures and much more

- Seamless Integration into existing infrastructures like PKI
- Deployment support for devices and data (esp. certificate management)

Collaboration and Liaisons:

- Intensive cooperation with research organizations and universities

15 Page 15

Trusted Computing

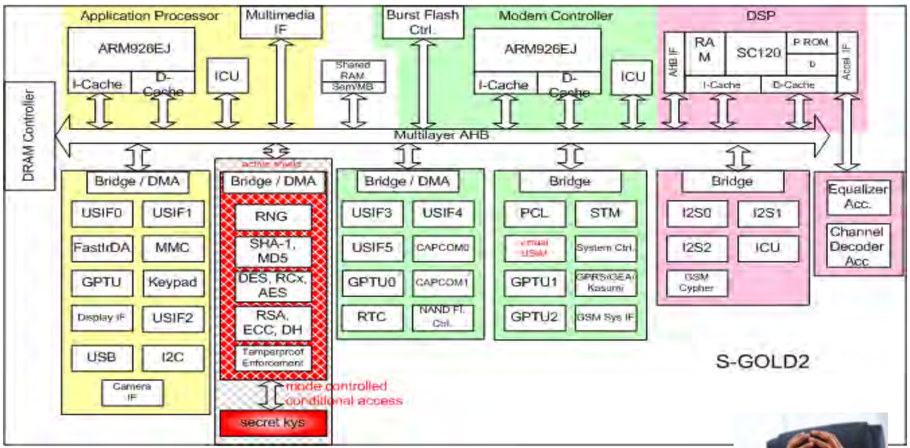
Market Errors and Bewilderments

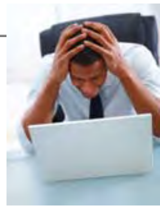
Or

Learning fromMistakes

Page 16

How can we integrate trust and security into a high complexity mobile phone baseband controller ?

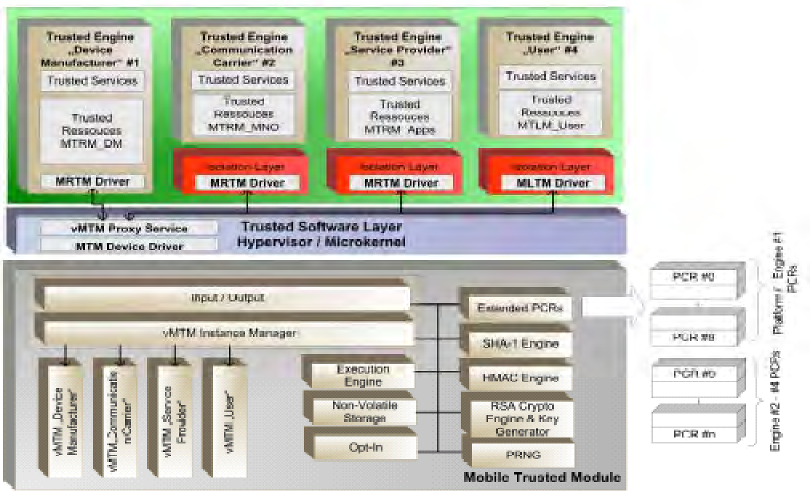




Customers really liked the chip,
However no one activated the TPM !

17

Mobile Trusted Module for Mobile Phones or Automotive



- An impressive specification, but no business ....

Page 18

A new approach for Automotive Security
Defining new embedded standards according to market

Applications		Security Solutions
■ Theft protection	→	■ Immobilizer/ RKE ■ Spare part IDs and authentication ■ Secure authentication infrastructure
■ Brand protection / IP protection	→	■ Spare Part IDs and authentication for e-parts ■ Secure RFID Tags for mechanical parts
■ Tuning protection	→	■ Power train with integrated hardware security module

Security Trends

- Physical attacks upcoming
- Highly professional criminal organizations with considerable budgets

----

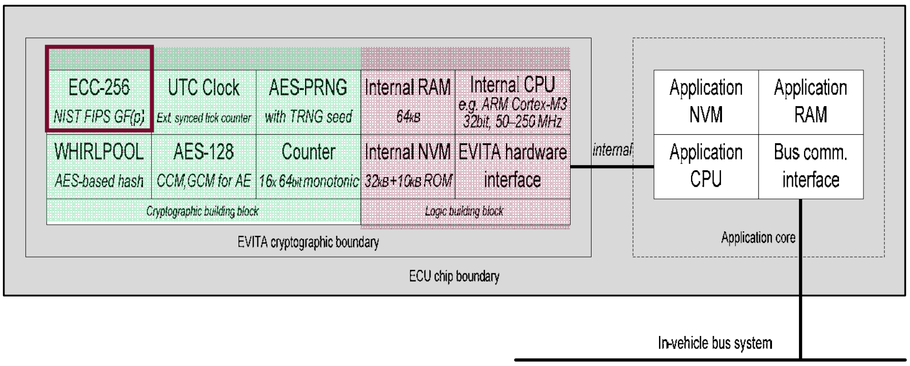
- Ad hoc Security Validation
- Security architectures against logical attack emerging
- No tamperproof security controller deployed yet

Security in Automotive Applications
Focus Areas for Microcontroller Implementations

- Immobilizer
  - standard today within all new cars (mostly realized in SW for Central Body- & PT-ECU)
  - enhancements targeted for future cars
    - up to ≤10 ECUs connected via CAN or Flexray might share a car specific secret symmetrical 128-bit AES key
    - mutual challenge response protocol is used to proof authentication at startup process
    - for reliability reasons, a majority decision process can be implemented
- Component Anti-Theft Protection
  - Immobilizer mechanisms as described above can be beneficial be re-used
  - in case of detected non-authorized module, operation might be restricted or permitted
- Secure Boot
  - proof integrity of Boot SW
    - e.g. protection of secure SW algorithms (like asymmetrical SW-RSA, ...)
    - AES HW extension mandatorily recommended in order to minimize startup delays
- Tuning Protection
  - Debugger Interface Lock in case of enabled TP
  - prevent unauthorized Read Out (IP-Protection)
  - prevent unauthorized Flash Programming & Reprogramming
- Car to Car Communication (considered as a stretched target in the future)
  - e.g. secure asymmetrical PGP based data exchange
    - requires HW extension for real time coding & decoding
      - e.g. secure separate µC with Multi Precision Arithmetic (MPA) extension

EVITA Hardware Security Module

- Functional description and programming via the new TPM2.0 EmSys spec (still in work) will be possible.



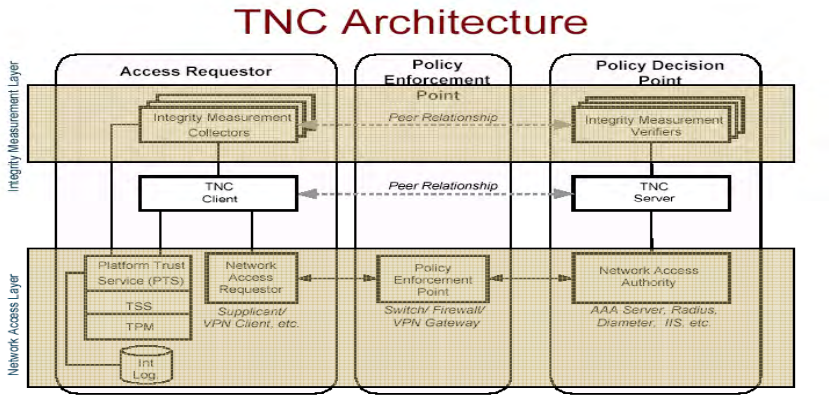
EmSys Standard: Trusted und Secure Boot

Security levels for boot loader

	Security Features					Ease of Management
	Software			Hardware		
	CRC ECC	Hash	Signature	Write Protected Bootloader	TPM	
Normal Boot	O	-	-	-	-	Easy, but no protection
Secure Boot (by digest)		O		Root of Trust (Reference Value)		Bad
Secure Boot (by signature)		O	O	Root of Trust (Signer's public key)		Good + Easy to update OS image without modifying Bootloader
Trusted Boot		O		Root of Trust	Root of Trust (Secure Storage)	Good (for connected device) + Device Authentication + Integrity Protection + Integrity Report

Increased Trust and Security for Car Networks: Trusted Network Connect (TNC) standard

TNC
- **Node integrity + policy control/enforcement (TC functions)**
- **Encryption, Node authentication, key management**



Page 23

What about the Future of Embedded Trusted Modules ?

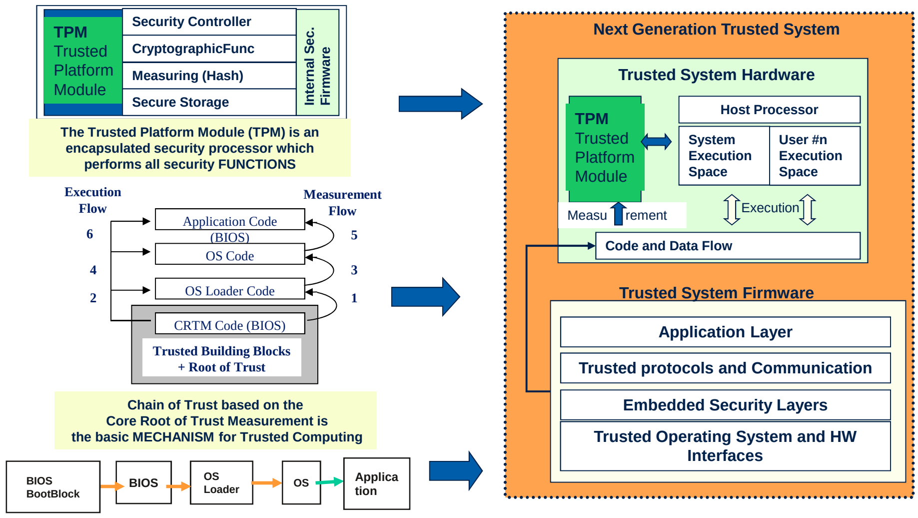
Use and extend widely the capabilities of Trusted Computing standards:

- Crypto agility: Add additional cryptographic algorithms
- Security agilty: Include the En-/de-cryption as required
- Function agility: e.g. Typical embedded like remote activation etc

Remember: TC is a functional standard,
Your Imagination is the limit

Page 24

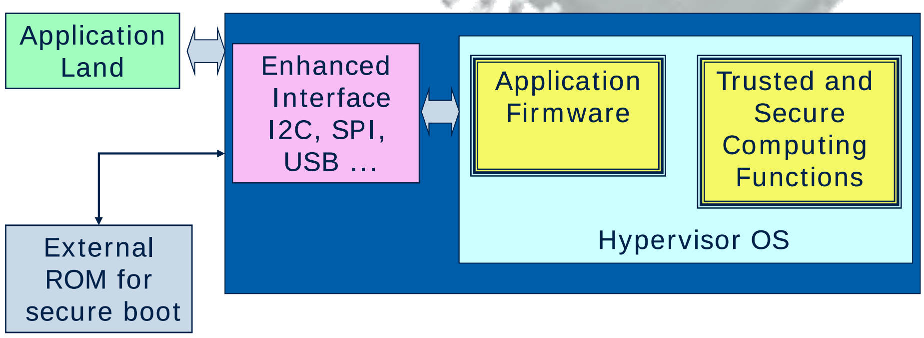
Future Embedded System Design: Integrated Trust Module due to Cost and Security Reasons



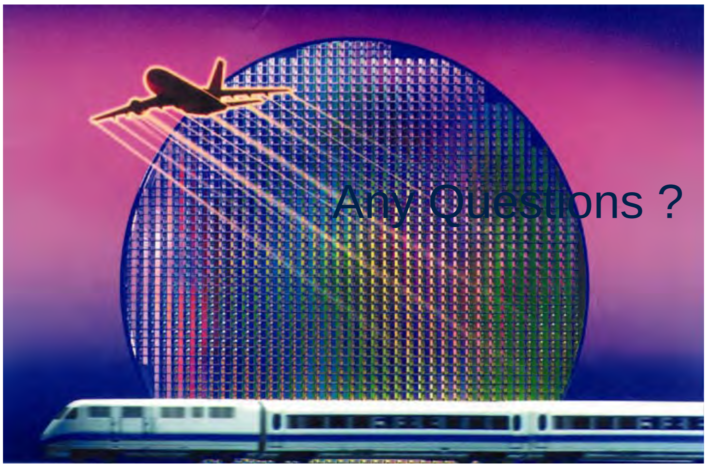
Active, standalone Trust and Security Controller

Todays TPM consist out of 16/32 bit machines, MMU, multiple interface controllers and are CC certifiable for EAL4+ and more

- Why not integrate the host processor into the TPM and get a secure and trusted general purpose controller ?



Trust and Security will become a Necessity for Future Embedded Applications



Page 27

EVITA: Motivation, Objectives, and Approach

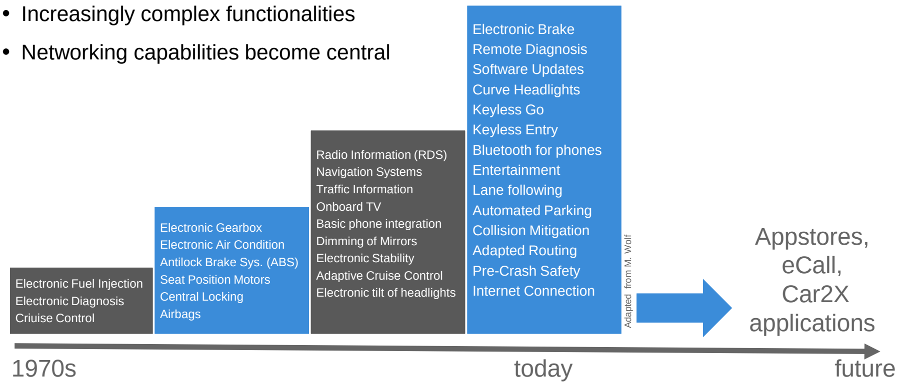
Yves ROUDIER
EURECOM
Email: yves.roudier@eurecom.fr

Final EVITA Workshop
Security of Automotive On-Board Networks
November 23, 2011, Erlensee

Motivation, objectives, and approach of the EVITA project

Vehicles, Electronics, and Security

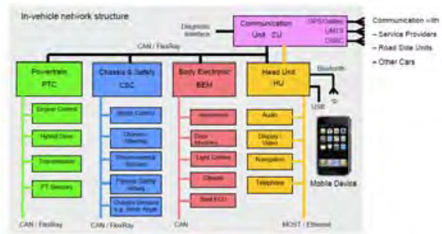
- Increasingly complex functionalities
- Networking capabilities become central



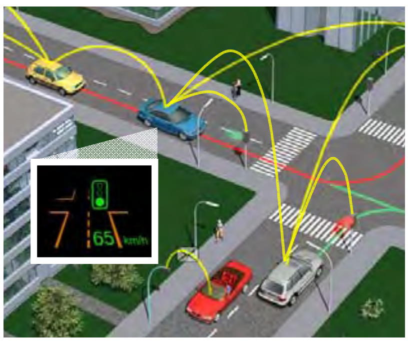
- Security: { ECU authentication, Vehicle immobilizers, Software authentication, Secure flashing, Payment systems, Secure and trusted communication }

Communication over On-Board Networks

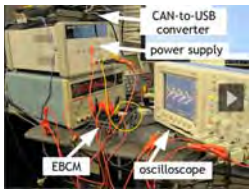
- Electronic Control Units (ECUs)
- Data sent periodically between ECUs, sensors, and actuators
  - Paradigm: signal based, communication buses (CAN, Flexray …)
  - Functional requirements: low latency, robustness



Tomorrow: Car2X-based Safety Applications



New Security Threats



- Potential attacks on
  - External interfaces, e.g., for Car2X communication
  - Physical attacks on on-board network

- Increasing awareness:
  - *"Physical cryptanalysis of keeloq code hopping applications"* – Eisenbarth et al. (2008)
  - *"Experimental Security Analysis of a Modern Automobile" – Koscher et al. (2010)*

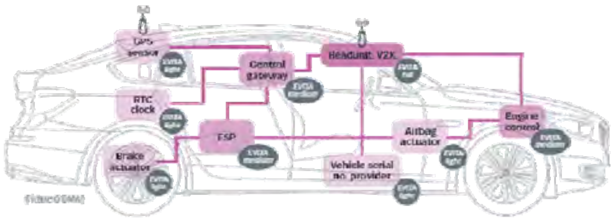
⇒ For Future Car2X applications, new security mechanisms have to be applied.

EVITA: Main Objectives

- "E-safety Vehicle Intrusion Protected Applications"
  - Project started in July 2008
- Holistic approach
  - Chain of trust from sensor to remote vehicle
  - Secure software engineering process
- Achievements
  - in-car communication protection
  - on-board system integrity protection
  - Support for scalable and secure vehicle-to-vehicle communication
  - Motivated risk analysis
  - Formal proofs
  - Security tests

EVITA: Approach

- Development of Hardware Security Modules deployed with ECUs
  - Accelerated cryptography
  - Key protection
  - Trusted computing base
  - Secure Storage
  - Cost-effective



- In-car cryptographic protocols
  - Key management, message integrity, policy management, distributed logging
- Software framework integrating authentication, encryption, access control, etc.
  - Encapsulates software/hardware partitioning between ECU and HSM

EVITA: Summary

- Security requirements are increasing due to enhanced connectivity
- Security is crucial for Car2X applications deployment
  - Preparation of standardization within Car2Car Communication Consortium
  - ITS standards development within ETSI ITS Working Group 5
- First ever prototype of a general-purpose secure on-board system
  - Overall security methodology
  - Prototypes demonstrated today
- EVITA results already adopted by major research projects

More details can be found at: *http://evita-project.org/*

Secure On-Board Architecture Specification

Marko Wolf
ESCRYPT GmbH – Embedded Security
Leopoldstraße 244
80804 München, Germany

Short Recap: Need for Automotive Hardware Security

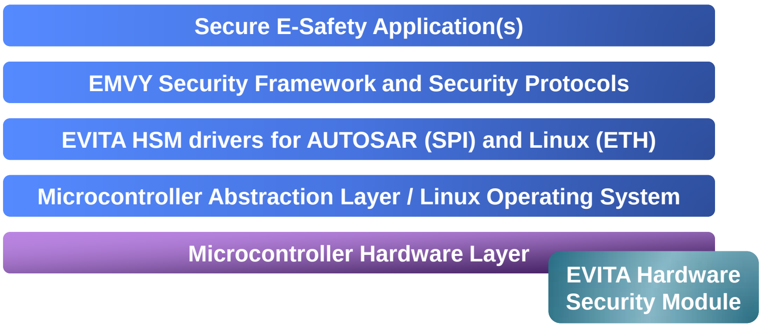
Local and remote software attacks
☑ Security-critical assets shielded in hardware

Insider, offline, physical tampering attacks
☑ Physical tamper protection

High performance security requirements
☑ Cryptographic hardware accelerators

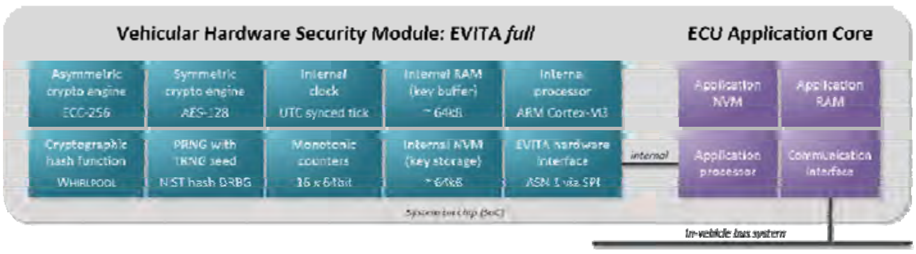
Costly to extend general-purpose hardware
☑ Cost-efficient special optimized circuits

EVITA Electronic Control Unit Security Architecture



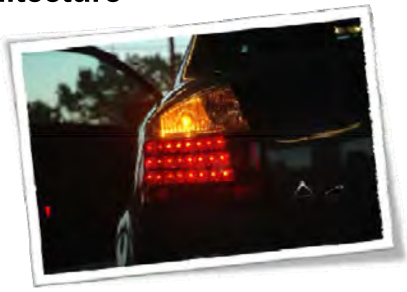
- EVITA HSM as **security anchor** for automotive microcontroller applications
- Linux and **AUTOSAR** integration via SPI and TCP/IP available
- Integrated into **EMVY** in-vehicle security software framework

EVITA Hardware Security Module (HSM) Architecture



- EVITA Hardware Security Module (HSM) as **microcontroller extension**
- Becomes “deeply” integrated via **System-on-Chip** (SoC) ASIC design
- **Generic interface** to use security building blocks with different concrete cryptographic algorithms (for capability, updates, ..)
- **Autonomous processor** for flexible hardware-protected security processing

EVITA Hardware Deployment Architecture



EVITA security extension in every ECU?

- **Yes, but ...**

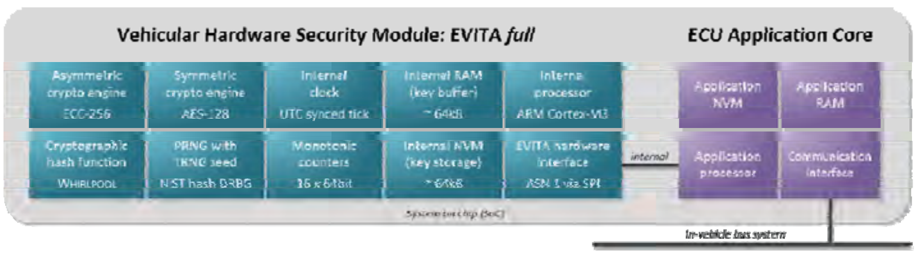
EVITA uses 3 different HSM classes to meet:

- Different **cost** constraints
- Different security **protection** requirements
- Different **functional** security requirements

By applying module classes EVITA 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

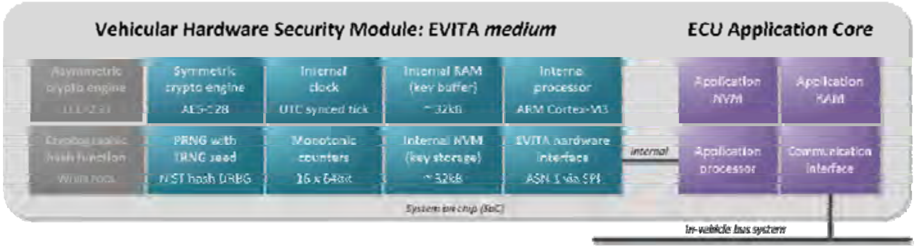
EVITA Hardware Deployment Architecture: EVITA *full*



- **High-performance asymmetric cryptography** for V2X digital signatures generation/verification (i.e., hardware accelerated ECC and hash function)
- **High-performance symmetric cryptography** for large-scale encryptions (e.g., protected multimedia, large external secure storage realizations)
- Powerful internal processor & memory for flexible cryptography (e.g., RSA)

➲ Foreseen for in 1 – 2 high-performance communication controllers such as V2X communication unit (head unit) and central gateway

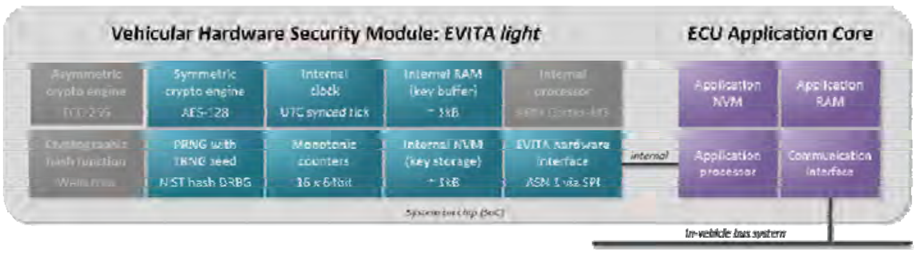
EVITA Hardware Deployment Architecture: EVITA *medium*



- Virtually identical to the EVITA *full* version except in that it has no dedicated asymmetric crypto hardware and no dedicated hash function hardware
- **Fast symmetric cryptography hardware**, but rather slow software based – but nonetheless practicable – **firmware asymmetric cryptography**
- Meets all in-vehicle security use cases, but not suitable for V2X

➲ Foreseen in 2 – 4 central multi-purpose ECUs such as engine control, front/rear module, immobilizer etc. with strong cost & security requirements

EVITA Hardware Deployment Architecture: EVITA *light*

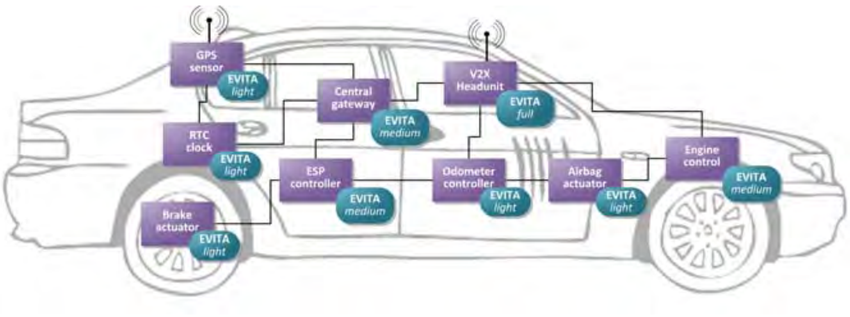


- **Cost-optimized symmetric crypto hardware** with small internal (key) memory that allows to process and generate protected information

➲ Foreseen in less, but security-critical ECUs that provide or process security critical information ECUs such as
  - Critical sensors: e.g., wheel, acceleration, pedal sensors
  - Critical actuator: e.g., breaks, door locks, turn signal indicator
  - Critical small controllers: e.g., GPS module, lighting, clock

EVITA Hardware Deployment Architecture: Holistic Security

Efficient, cost-effective, flexible, and holistic in-vehicle EVITA hardware security module(s) deployment respecting the different cost and performance constraints, and different functional (security) requirements.



EVITA Hardware Security Module Interface Specification

- About 50 pages at deliverable D3.2 pg. 36-86
- Security building blocks (SBB)
  - Encryption and decryption
  - Message authentication codes
  - Hashes and HMAC
  - Signature generation and verification
  - Random numbers
  - Secure Counters
- Security functionality
  - Key management (e.g., key creation, agreement, import, export, status)
  - Secure boot and authenticated boot (e.g., ECR extension, retrieve, preset, compare)
  - Secure "tick" clock with external UTC synchronization for data time stamping or key expiry
  - HSM administration and auditing

EVITA Hardware Security Module Interface Specification

- **Multi-sessions** (i.e., interruptible) for most hardware security blocks (e.g., AES, MAC, digital signatures, and hash functions) via and separate `init()`, `update()`, and `finish()` session management commands
- **Multi-threading** possible on availability of hardware blocks (e.g., one can call PRNG and two AES in parallel if blocks available)
- **Asynchronous** (i.e., non-blocking) hardware interface
- EVITA key uses can (but do not necessarily have to) have additional **individual authorizations** via:
  - ***password*** given on function invocation (including failure counter)
  - inherent ***bootstrap*** verification by verifying a bootstrap reference
  - ***combination*** of password and bootstrap reference
- EVITA **commands are not protected** at hardware level, ***but*** remember SoC integration (in case command protection is required, we propose a TPM-like approach to establish a session key and "rotating" nonces)

EVITA HSM Specification Highlights: Individual Key Control

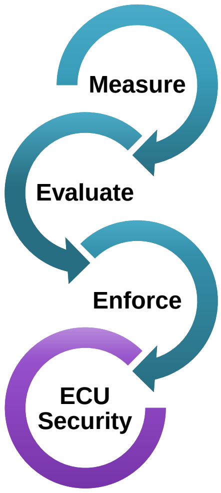
- Keys have 10 individual `use_flags` each with:
  - `encrypt`
  - `decrypt`
  - `sign`
  - `verify`
  - `utcsync`
  - `transport`
  - …
- 4 individual transport restrictions
  - `internal`
  - `migratable`
  - `oem`
  - `external`
- 3 individual usage authorization
  - `password`
  - `ecr`
  - `ecr+password`

➲ Enables very fine-grained purpose, transport and access control
➲ Enables *least-privilege* security design principle (*Saltzer, 1974*)

Local bound secure storage			Symmetric-key „digital signatures“		
use_flag	**trnsp_flag**	**auth_flag**	**use_flag**	**trnsp_flag**	**auth_flag**
encrypt	internal	pw + ecr(i..j)	sign	internal	pw + ecr(i..j)
decrypt	internal	ecr(i..j)	verify	migratable	none

EVITA HSM Specification Highlights: Bootstrap Protection

- *Secure boot* and *authenticated boot*
  - – HSM as hardware-protected Core Root of Trust (CRT) to initialize the chain of trust
  - – Multi-stage bootstrap possible starting with CRT
  - – Subsequent step by step measurements of upper layers (e.g., bootloader, OS, application)
  - – HSM internal ECU Configuration Registers (ECRs) store fingerprints of measured code
  - – Immediate response by HSM upon mismatch of measurement and reference ECRs → ***Secure Boot***
  - – Indirect response by HSM key control bound to certain ECR values (cf. slide before!) → ***Authenticated Boot***



EVITA Hardware Security Module Prototype Implementation

- Programmable FPGA hardware prototype with internal PowerPC processor
- High-performance crypto hardware
  - – AES-128 symmetric cipher: 80 Mbit/s
  - – ECC-256 asymmetric cipher: 450 sig/s
  - – WHIRLPOOL hash function: 128 Mbit/s

- TCP/IP and SPI interface software drivers for Linux and AUTOSAR

➲ Detailed HSM design, realization, and evaluation results in "**Design, Implementation, and Evaluation of a Vehicular Hardware Security Module**" to be published at *International Conference on Information Security and Cryptology* (ICISC 2011) in Seoul on November 30 – December 2, 2011.

EVITA Security Module In Comparison with Existing HSMs

	full	*medium*	*light*	HIS SHE	TPM	Smartcard
Cryptographic algorithms						
ECC/RSA	●/●	●/●	○/○	○/○	○/●	⊙/⊙
AES/DES	●/⊙	●/⊙	●/○	●/○	○/○	⊙/⊙
WHIRLPOOL/SHA	●/●	●/●	○/○	○/○	○/●	⊙/⊙
Hardware acceleration						
ECC/RSA	●/○	○/○	○/○	○/○	○/○	○/○
AES/DES	●/○	●/○	●/○	●/○	○/○	○/○
WHIRLPOOL/SHA	●/○	○/○	○/○	○/○	○/○	○/○
Security features						
Secure/authenticated boot	●/●	●/●	⊙/⊙	●/○	○/●	○/○
Key control per use/bootstrap	●/●	●/●	●/⊙	○/●	⊙/●	○/○
PRNG with TRNG seed	●	●	●	●	●	●
Monotonic counters 32/64 bit	●/●	●/●	●/●	○/○	●/○	○/○
Tick/UTC-synced internal clock	●/●	●/●	●/●	○/○	○/○	○/○
Internal processing						
Programmable/preset CPU	●/⊙	●/⊙	○/⊙	○/●	○/●	⊙/⊙
Internal V/NV (key) memory	●/●	●/●	⊙/⊙	●/●	●/○	●/○
Asynchronous/parallel IF	●/⊙	●/○	●/○	●/○	○/○	○/○

Annotation: ● = available, ○ = not available, ⊙ = partly or optionally available

Conclusions: EVITA Vehicular HSM

- Provides a **hardware-protected security anchor for software** layers through hardware-encapsulated generation, storage, and processing of security-critical material and provision of basic security functions
- Detailed specification of **efficient, flexible and generic** security interface
- Applies **Trusted Computing ideas** (e.g., authenticated boot) **with meaningful extensions** (e.g., symmetric cryptography, individual use flags, individual authorizations for invocation and transports)
- **Accelerates security mechanisms** by applying cryptographic accelerators (e.g., ECC, AES, WHIRLPOOL, RNG)
- **Compatible with HIS SHE security functionality** for easy deployment
- **Tamper-protection** via on-chip integration (+ further measures)

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

Secure On-Board Protocols

Hendrik C. Schweppe

EURECOM
2229 route des crêtes
06560 Sophia Antipolis, France

Overview

1. Motivation for Secure On-Board Protocols
2. Key Distribution and Key Management for On-Board Networks
3. Master/Client Communication in EVITA Security Framework
4. Coping with Limitations of the CAN Bus
5. Security Maintenance Scenarios
6. Model-Based Security Analysis, Evaluation, and Verification

Motivation

- Security in distributed systems *as found in the vehicle* depends on
  - Integrity of the local and remote ECUs
  - Mutual trust in received and computed data

- Limitations of current automotive bus systems
  - Latency requirements
  - Payload restrictions
  - Communication groups

⇒ Integration of communication with security framework to protect both:
platform and communication.

On-Board Protocols developed in EVITA

- Distribution of cryptographic key material
  - Securely deploying keys from external entities to the vehicle
  - A secure way in order to distribute keys between ECUs
  - Refreshing of keys at bus-attached sensor nodes
- Session-keying and protocols for confidential, fresh, and authentic communication
  - Establishment of session keys between ECUs
  - Session key establishment between key masters
- Authentic communication
  - Secure Transport protocols
  - Addressing of nodes and software components
  - Gateways between physical and logical network lborders
- Intrusion detection and response
  - Message formats, synchronized system states, interactions with policies.
  - Common programming interfaces for filter-plugins and action-plugins
- Over-the-air firmware update procedures and protocols:
  - Update process for ECUs and sensors for platform configuration and corresponding firmware, including pairing/registration of nodes with KM nodes.
  - Integrity checks of platform
- Policy management and access control
  - Configuration of policies and policy-updates: , backend policy definition, compressed vehicle native format, policy-synchronization
  - Format of policies and messages
  - Access control protocols and policy enforcement
  - Firewall rules as part of access control policy
- Furthermore:
  - Bootstrapping, On-board integrity check of platform
  - Maintenance: replacement of hardware components. (include key-distribution/key-swapping)
  - Time and counter synchronization between HSMs and ECUs
  - Secure Storage with HSM integration.

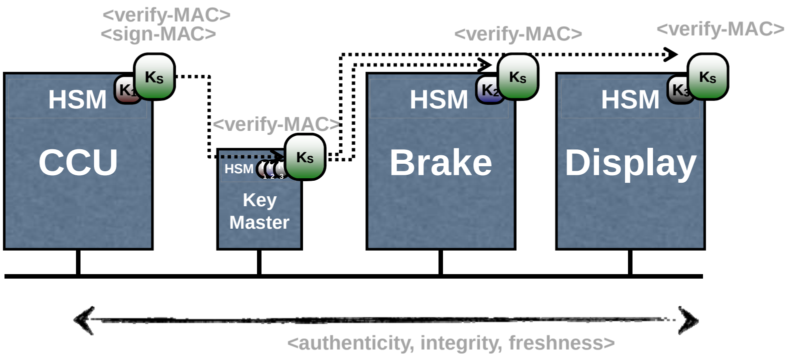
Hardware Security Modules

EVITA

- Store and Process Security Credentials
  - Keys have *use-flags*
    - Examples: encrypt, decrypt, sign, verify
  - 2nd step: use-flags can have *exportable* flag
    - e.g., only *decrypt* flag (=key) is exportable with specific transport key while *encrypt* stays internal
- This enables:
  - Asymmetric usage of symmetric key material!
  - Low Cost HSM for sensors

[D3.2]

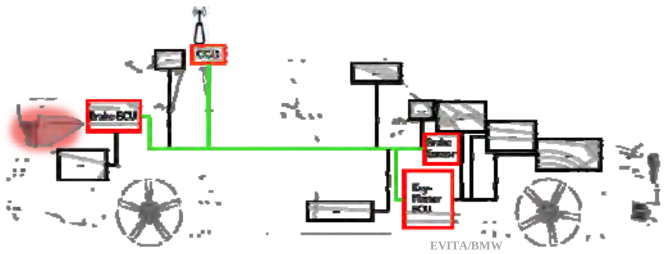
Key Distribution for Group Communication



- **Basic usage control at ECU/HSM**
- **Comprehensive access control at KeyMaster: Communication Groups and Access Control Policies**

[D3.3, WiVeC11]

Encapsulation of Protocols in Security Framework



- Software Security Framework provides high-level services by encapsulating complex protocols & services.
  - Application only needs "**secure_communication()** call"
    - Entity (i.e., communication group name)
    - Security requirements (e.g., authenticity, confidentiality)
    - Payload

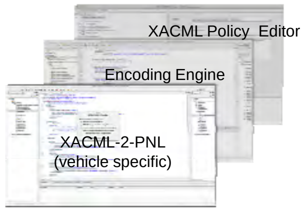
[D3.2,D3.3,D4.3]

Software Security Framework EMVY

- ECUs and sensors are differently equipped (CPU/RAM/..)
  - Thin client fashion:
    Core security services deployed on master(s) for all clients.
  - Developed on C vs. C++ on client vs. master
  - RPC-like interface

[D3.2,D3.3,D4.3]

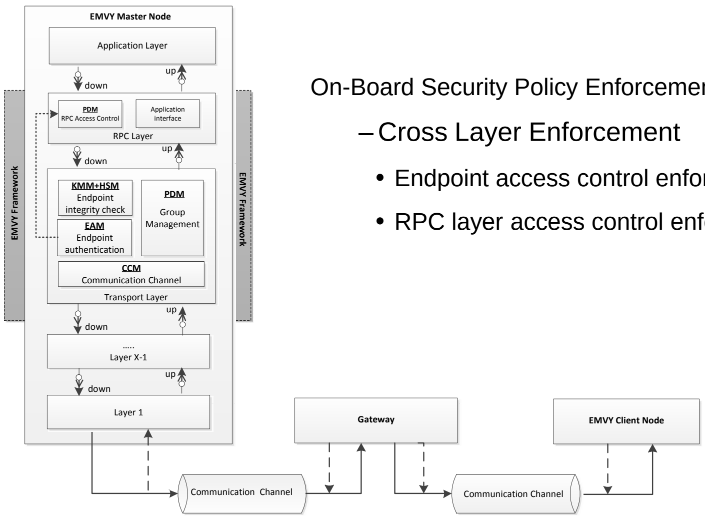
Software Security Framework EMVY



Security Policy Management System

- Example: Policy System
  - Policies defined in XACML format in backend
    - Rules include subject, object, action & vehicle state.
  - Compiled to vehicle specific format and transferred to Master ECU in the vehicle (Policy Decision Module)
  - Queried by client ECUs (Policy Enforcement Points) when necessary

[D3.3,D4.3,NFC11]



On-Board Security Policy Enforcement

- Cross Layer Enforcement
  - Endpoint access control enforcement
  - RPC layer access control enforcement

On-Board Decision and Enforcement

[D3.2,D4.3]

Transport Protocols: Secure Sessions

A transport protocol provides for:

- More flexible addressing in payload
- Larger payload
- Security payload

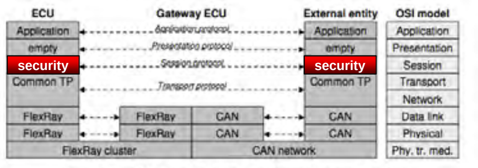
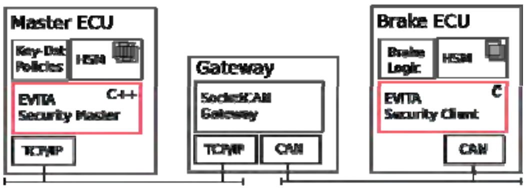


Figure 5-7. In-vehicle Data Exchange with Common Transport Protocol
EASIS [D1.2-10]



- EVITA CAN to Ethernet Gateway:
- CAN communication with ISO-TP
- Linux gateway with VW's open source SocketCAN

[D3.3, WiVeC11, D4.3]

Analysis of MAC Truncations

Depending on

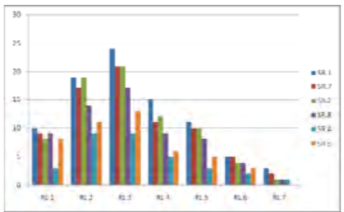
- the risk of an attack
- the severity of an attack

=> choose level of protection EVITA [D2.3,D3.2]

- Truncation of MAC increases risk of false positives
- Number of trials limited by *bus* and *HSM throughput*
  We limit failed verifications at *100 per second.*

- Table shows expected time for
  P(false-validation-of-MAC=1)=0.5

=> Length of MAC:
- up to 256 bits (for fast buses and critical data)
- allow truncation down to 32 bits (low speed buses and non-critical data)

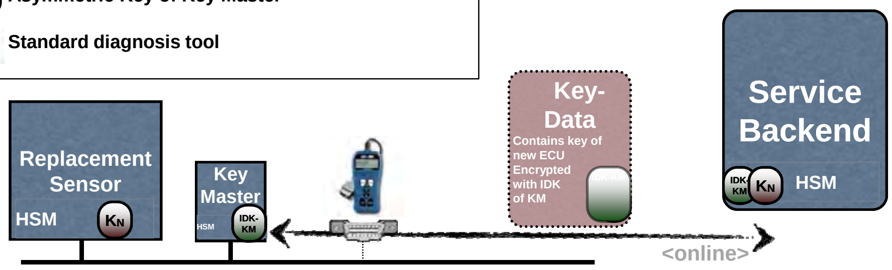


bits	time to collide
0	0
16	5.5 min
24	23.3 h
32	35.5 weeks
48	44750 years
64	2932747010 years
96	1.25961E+19 years
128	5.40996E+28 years
192	9.97962E+47 years
256	1.84092E+67 years

[D3.3, WiVeC11]

Maintenance: Online Use Case

- K_N Symmetric Key of Sensor: Must be delivered to Key Master
- IDK-KM Asymmetric Key of Key Master
- Standard diagnosis tool



Steps:

Establishment of connections between vehicle system and backend by the workshop

I Two-way-authenticated connection: Key Master <-> Backend

II Reception of key-data blob from backend

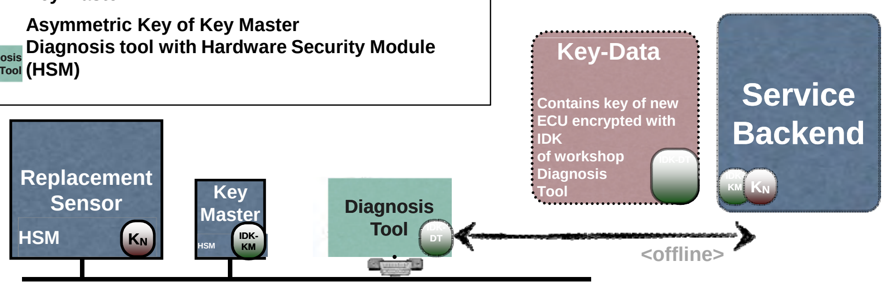
III Import of key K_N at Key Master

[D3.3]

Secure On-Board Communication Protocols – H. Schweppe, EURECOM, Sophia-Antipolis, France

Maintenance: Offline Use Case

- K_N Symmetric Key of Sensor: Must be delivered to Key Master
- IDK-KM Asymmetric Key of Key Master
- Diagnosis Tool: Diagnosis tool with Hardware Security Module (HSM)



Steps:

I Offline transfer of key-data for specific workshop (along with the part to be replaced)

II Import of K_N at Diagnosis Tool (only temporary and for re-encryption)

III Export of K_N at Diagnosis Tool (Transport Key: Key Master node)

IV Import of key K_N at Key Master

[D3.3]

Model-Based Analysis, Evaluation & Verification

- Built model of protocols in TTool and Matlab/Simulink
- Created "AVATAR" UML profile for TTool
  - Combines model of functional and security aspects!
  - Proofs functional aspects in <UPAAL> and security aspects in <ProVerif>
- Proofs of *Key Distribution* and *Remote Firmware Update* protocols done within EVITA
- Simulative evaluation of CAN bus load with MAC in Transport Protocol
- Practical evaluation of Key Distribution & communication: <20ms including network, HSM, and application processing.

[D3.4, VTC11]

Summary

EVITA HSM and simTD CCU Module

- Various on-board security protocols needed
  - Reduced complexity on application level by integration with security framework & architecture
  - ⇒ Achieved comprehensive solution.
- Applicable to different on-board networks
  - Solution is applicable to different types of ECUs
  - Applicable to different types of on-board networks
- Working prototype on Ethernet, proof of concept on CAN
- Security and functionality validated through model based verification

EVITA Publications on On-Board Protocols

[D3.2] B. Weyl et al., EVITA: Secure On-Board Architecture Specification, 2010

[D3.3] H. Schweppe et al., EVITA: *Secure On-Board Protocols Specification*, 2010

[D3.4.4] A. Fuchs et al., EVITA: *On-Board Architecture and Protocols Verification, 2010*

[D3.4.4] A. Fuchs et al., EVITA: *On-Board Architecture and Protocols Attack Analysis, 2010*

[D4.3.2] H. Seudié et al., EVITA: *Implementation of the Software Framework, 2010*

[NFC11] M.S. Idrees et al., Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates, 3rd Nets4Cars, LNCS 6596/2011 Oberpfaffenhofen, 2011

[WiVeC11] H. Schweppe et al., C2X Communication: Securing The Last Meter, 4th IEEE Wireless Vehicular Communication, San Francisco, 2011

[VTC11] G. Pedroza et al., A Formal Methodology Applied to Secure Over-the-Air Automotive Applications, 74th IEEE Vehicular Technology Conference, San Francisco, 2011

[VDI11] H. Schweppe et al., Securing Car2X Applications with effective Hardware-Software Co-Design for Vehicular On-Board Networks, 27th VDI Automotive Security, Berlin, 2011

Hendrik Schweppe
+33 4 93 00 82 02
schweppe@eurecom.fr

EURECOM
2229 route des crêtes
06560 Sophia-Antipolis
http://www.eurecom.fr/

EVITA Final Review

Integration in AUTOSAR

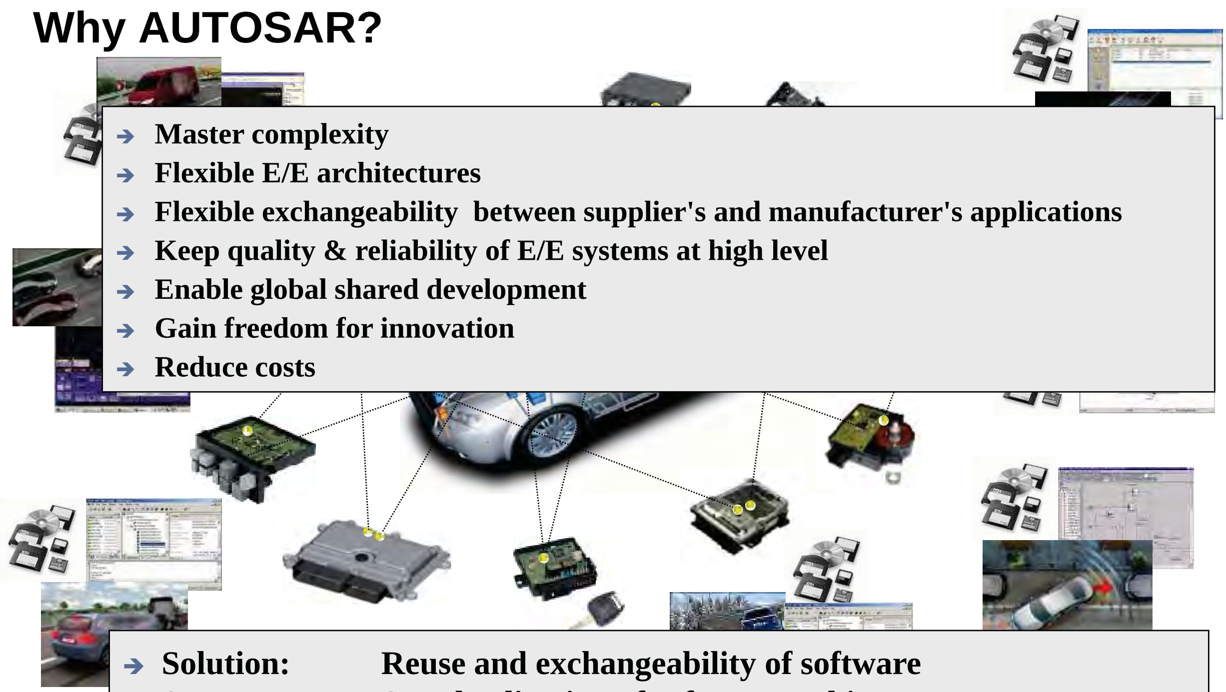
Hervé Seudié

Robert Bosch GmbH

Postfach 30 02 40

70442 Stuttgart, Germany

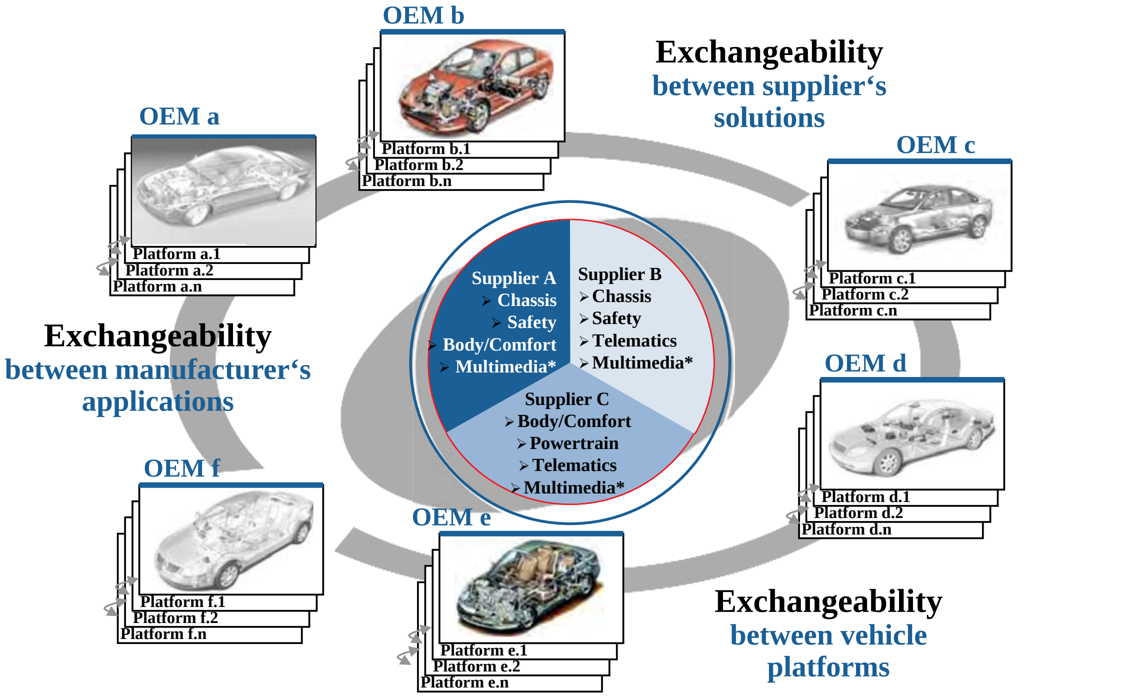
Why AUTOSAR?



- ➔ **Master complexity**
- ➔ **Flexible E/E architectures**
- ➔ **Flexible exchangeability between supplier's and manufacturer's applications**
- ➔ **Keep quality & reliability of E/E systems at high level**
- ➔ **Enable global shared development**
- ➔ **Gain freedom for innovation**
- ➔ **Reduce costs**

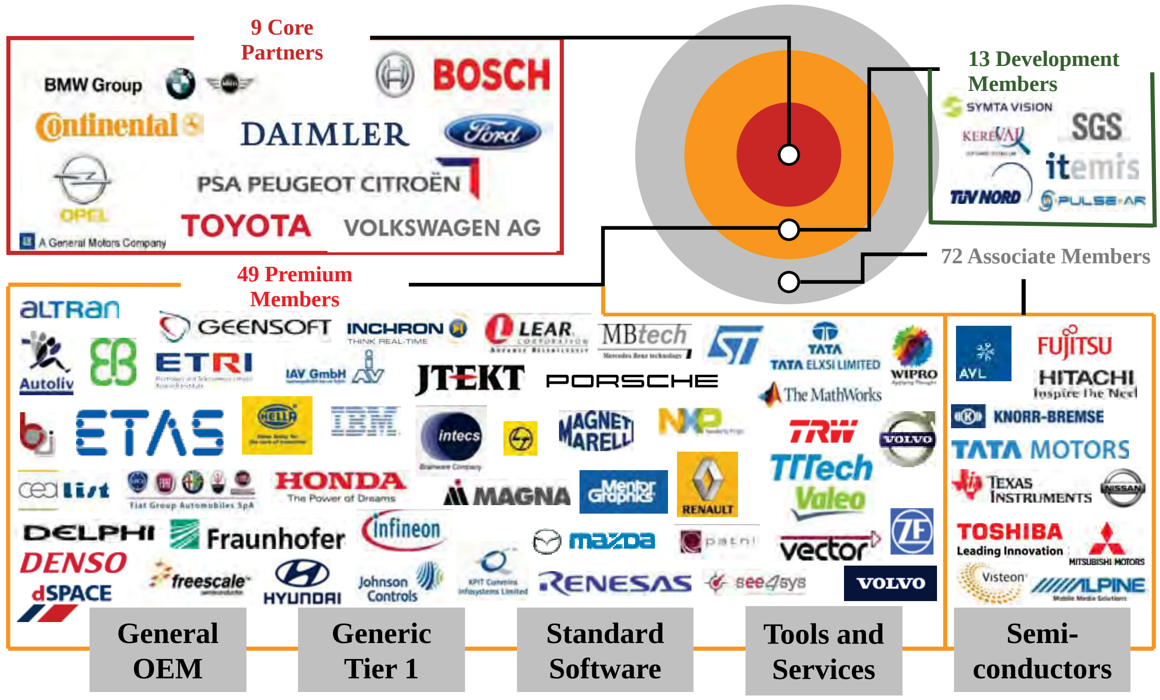
- ➔ **Solution:** **Reuse and exchangeability of software**
- ➔ **Strategy:** **Standardization of software architecture**

AUTOSAR Stakeholders

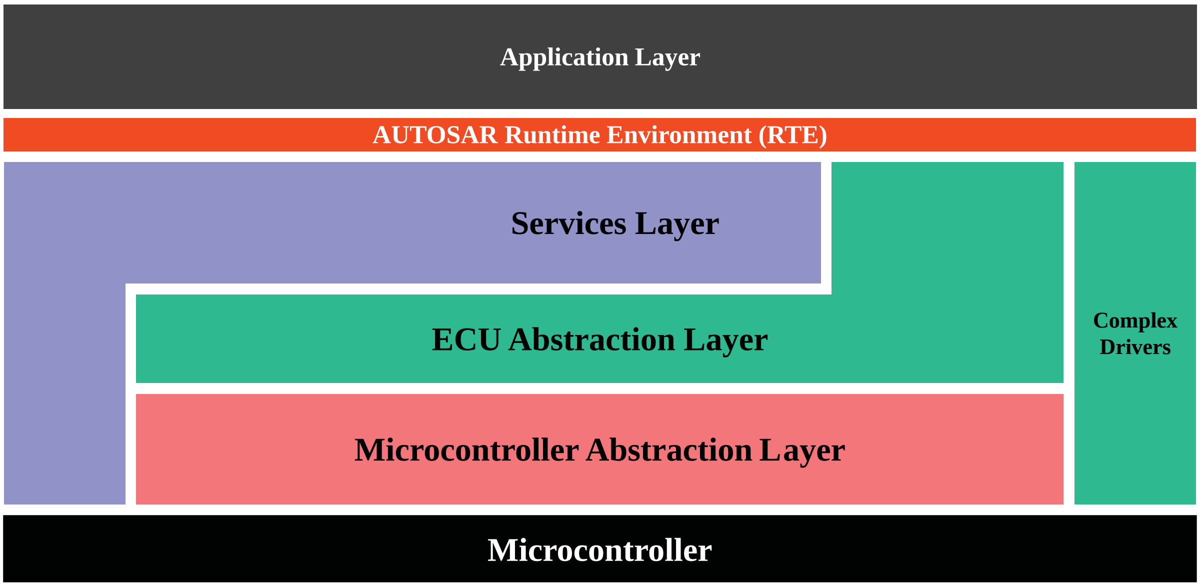


* Multimedia: Application interfaces only

AUTOSAR Partners

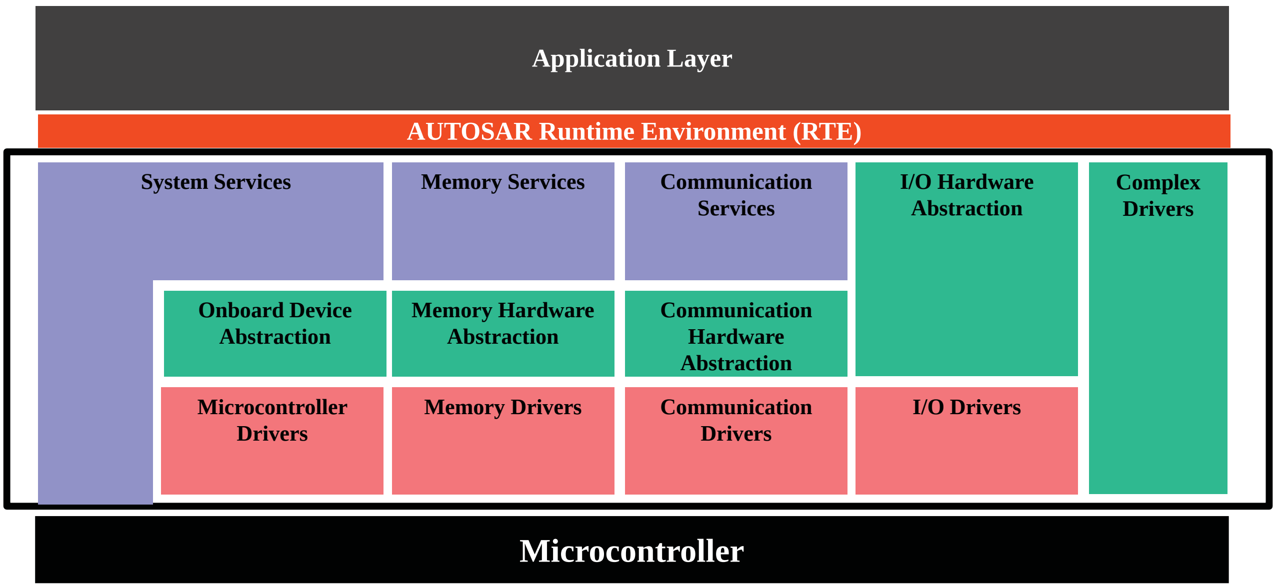


AUTOSAR Layers



Objective: - Decoupling of Hardware and Application Software
- Relocation / reuse of SW-C* between ECU

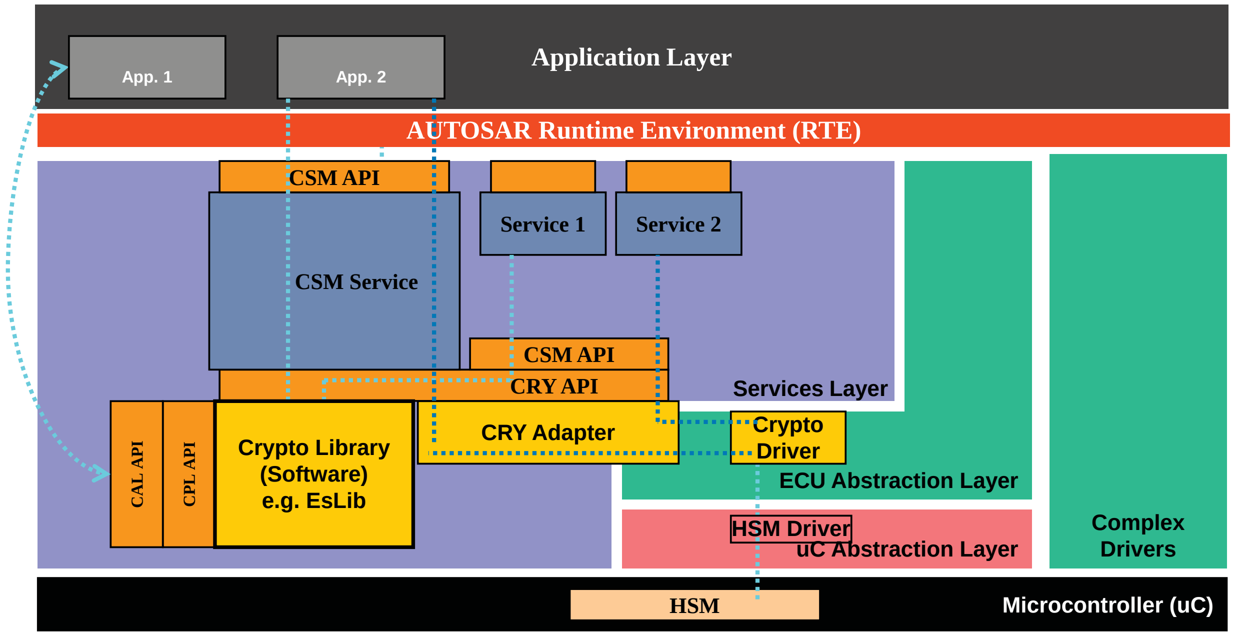
AUTOSAR: Basic Software Layer



BSW-Layers

The EVITA project has used Bosch CUBAS as BSW

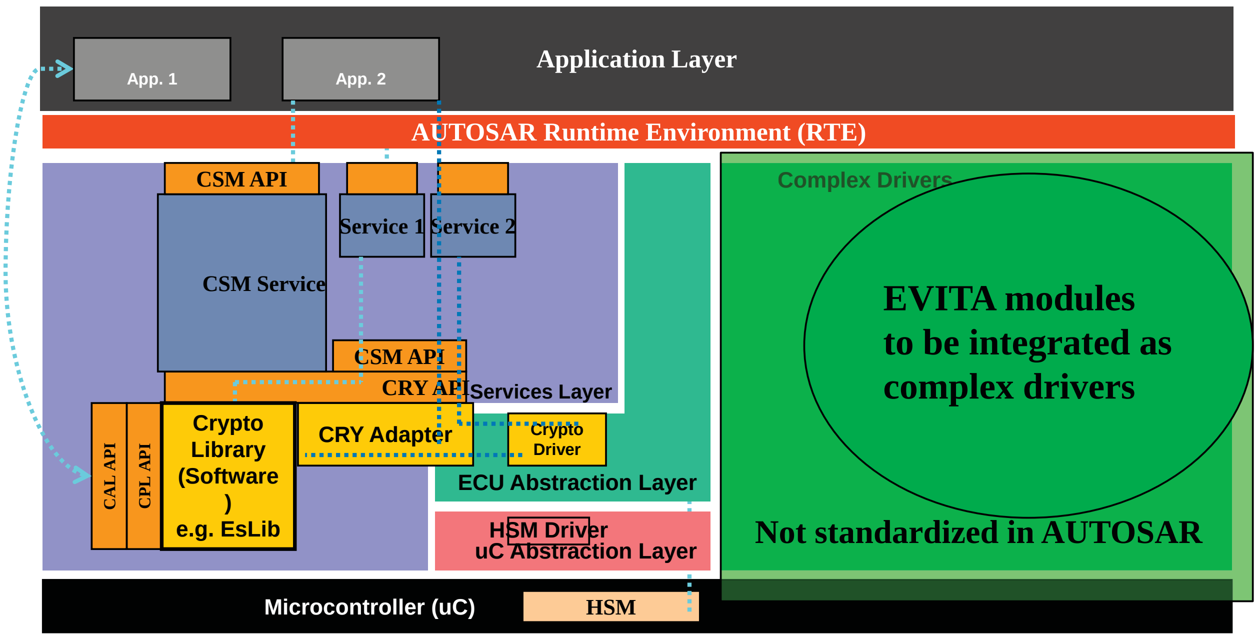
Standardized Cryptographic interfaces of AUTOSAR



HSM: Hardware Security Module CAL: Cryptographic Abstraction Layer (static, synchronous)

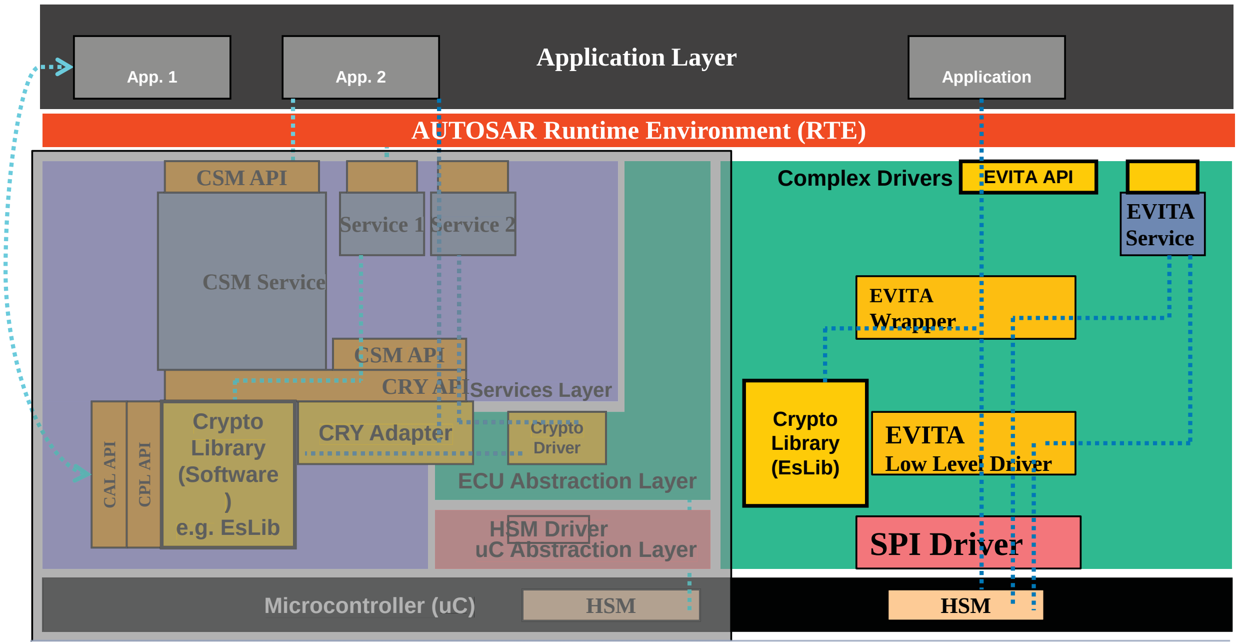
CSM: Crypto Service Manager (dynamic, asynchronous) CRY: (Low-level) Crypto Interface

Where to integrate the EVITA modules?



Constraint: EVITA has no AUTOSAR speficified components

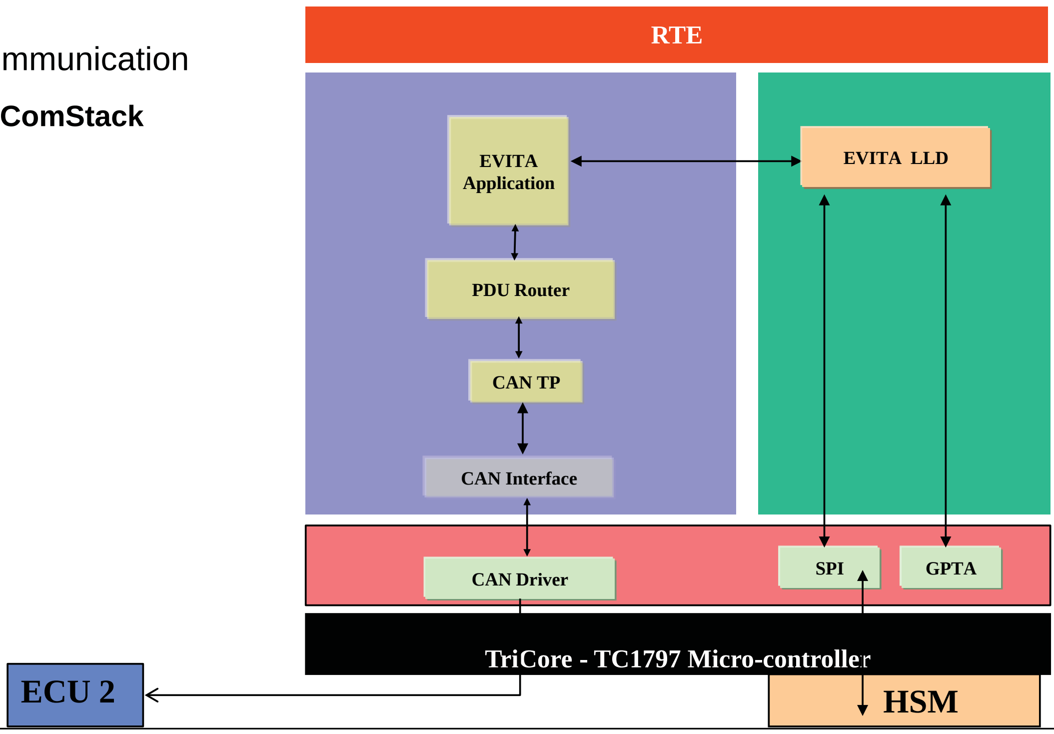
AUTOSAR Layers with integrated modules



Low Level Driver / EVITA Security application / Wrapper / EVITA API for application layer software

AUTOSAR Communication with EVITA modules: simplified view

- Secure Communication
  - **Use of ComStack**



Summary

- Prototypic integration of EVITA in real automotive software architecture AUTOSAR
  - Security with and without hardware support

- Hardware Security Modules access via Low level driver using SPI communication
  - SPI only for demonstration purpose
  - Production in the future as ASIC: see PRESERVE project, which develops an ASIC based on the EVITA result

- Secure communication using AUTOSAR / CAN bus / TC 1797 / FPGA
  - See demonstration !

Thank you for your attention!

Questions?

Hervé Seudié
Robert Bosch GmbH
Herve.seudie@de.bosch.com

EVITA Prototype & Demonstrator Overview

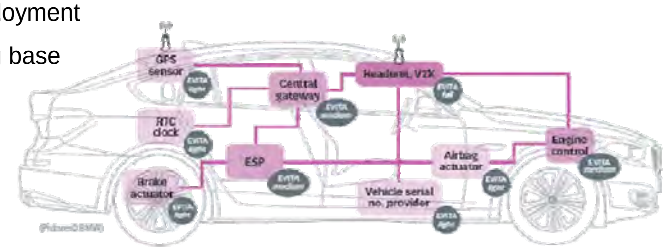
Dr. Benjamin Weyl
BMW Group Research and Technology
Hanauer Str. 46
80992 München, Germany

Overview

1. Goals of the EVITA Demonstrators
2. Desktop Demonstrator
3. Vehicle Demonstrator Active Brake
4. Vehicle Demonstrator Valet Parking Privacy
5. AUTOSAR Demonstrator
6. Summary & Outlook

Goals of the EVITA Demonstration Scenarios

- Demonstrate Hardware Security Modules deployed with ECUs
  - – Cost-effective deployment
  - – Trusted computing base
  - – Key protection
  - – Secure Storage



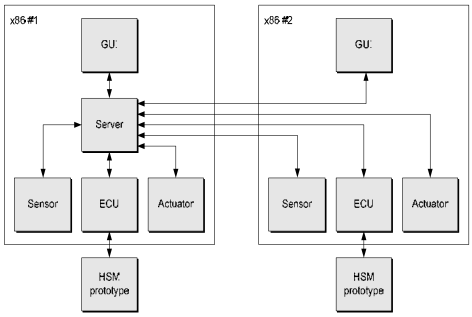
- Demonstrate in-car protocols to secure ECU-ECU & Sensor communication
- Demonstrate software security framework integrating authentication, encryption, access control, etc.
- Demonstrate EVITA HSM integration with Microcontroller (AUTOSAR ECUs)

EVITA Desktop Demonstrator – Overview

- Visualization of securing in-vehicle communication using HSMs
  - – DUC-10: Secure sensor data acquisition
  - – DUC-11: Secure actuator command transmission
- Visualization of securing V2X communication using HSMs
  - – DUC-20: Active brake authenticity
- Visualization of multiple attack scenarios (MUC-10, MUC-11, MUC-20)
  - – Detection of manipulated messages
  - – Detection of injected / replayed messages
- Visualization of different HSM types (light, medium, full)
- Detailed visualization of HSM activity, internal data and processes
- Interaction with HSM prototype, connected via TCP/IP using HSM-IP-LIB

EVITA Desktop Demonstrator – Internals

- **GUI** for user interaction, flow control and visualization
- **Server** for application interconnection and message forwarding
- **Sensor** for data acquisition using HSM software library
- **Actuator** for command execution using HSM software library



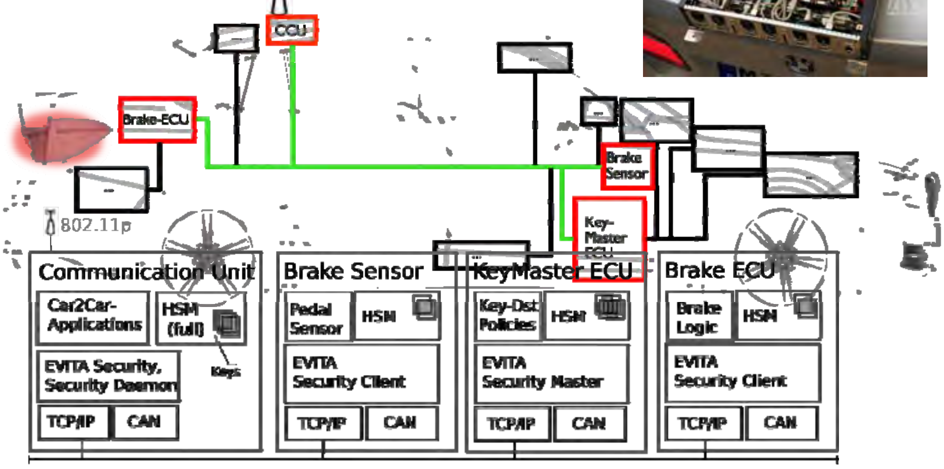
- **ECU** for data evaluation and command generation using HSM prototype platform

EVITA Desktop Demonstrator @ escar 2011 in Dresden

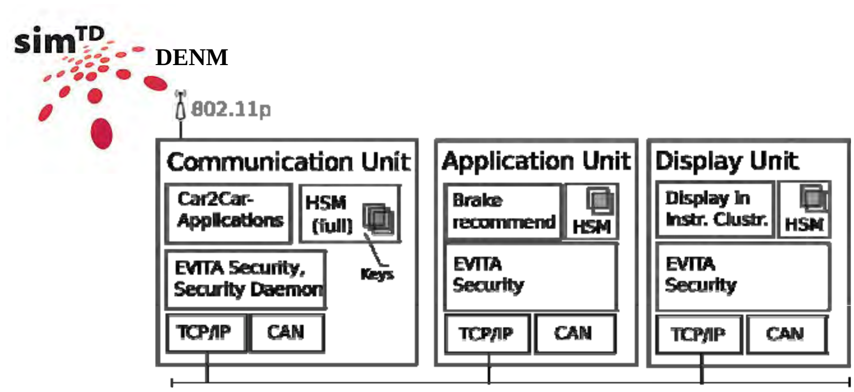
Vehicle Demonstrator Active Brake: Use Case

- Use Case: Car2Car Emergency Brake Notification
  - Vehicle notifies the following vehicle of a braking action
  - Driver reacts to situation
- Use Case: Car2Car Active Emergency Brake
  - Vehicle reacts autonomously
  - Driver may still influence reaction
- Core Requirements
  - Integrity & authenticity of Car2X messages
  - End-to-end security from sensor to actuator
  - Fast signature generation & verification

Vehicle Demonstrator Active Brake: Securing the On-board Network



Vehicle Demonstrator Active Brake: Securing the On-board Network



Vehicle Demonstrator Active Brake: Visualization of Security in Sending Vehicle

- Visualization of key management protocol & secure communication
- Mounted attack in Sending Vehicle between Sensor and ECU
- Detect data manipulation on the on-board network

Vehicle Demonstrator Active Brake: Securing the External Communication

- EVITA security components have been integrated with the sim^{TD} project
- Integrated with Car2X (sim^{TD}) communication radio unit based on 802.11p

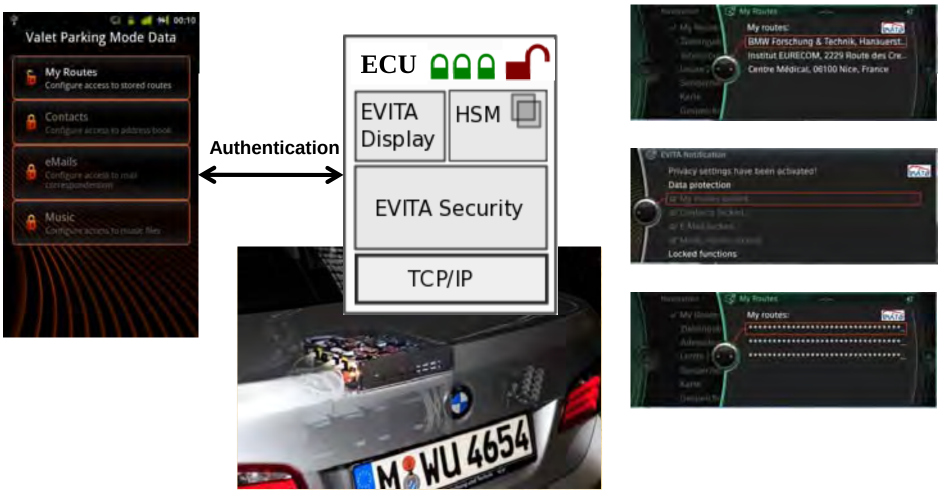
- Communication Security
  - Communication is authenticated & integrity-protected
  - Usage of EVITA Hardware Security Module
  - Performance: factor 15-20 for signature generation & verification!

Vehicle Demonstrator Valet Parking: Privacy Protection within the Vehicle

- Use Case: Valet Parking Privacy Application
  - Protection of personal data within the vehicle
  - Activation when leaving the car

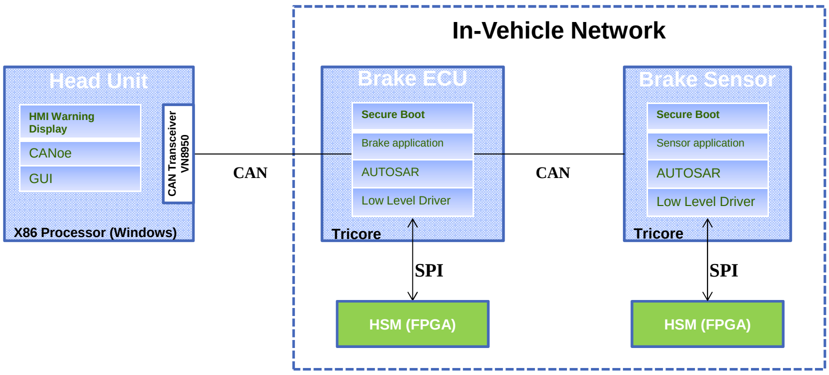
- Secure Storage & Access Control
  - Secure storage of data with EVITA HSM
  - Access control with user-defined policies:
  - Driver protects, e.g., personal usage data

Vehicle Demonstrator Valet Parking: Privacy Protection within the Vehicle



AUTOSAR Demo Overview

- **Scope**: Secure communication between AUTOSAR ECUs
- **Use Cases**: Sensor Manipulation & Secure Boot



Demonstrator Events

BMW-EURECOM
Pressevent
September 2011
Sophia Antipolis

9th escar conference
November 2011
Dresden

Summary

- With enhanced connectivity, security requirements are increasing
- Security is crucial for Car2X application deployment
  - Integration with sim[TD] for efficient Car2X communication
  - Preparation of standardization within Car2Car Communication Consortium
  - ITS standards development within ETSI ITS Working Group 5
- EVITA designed and implemented the first ever prototype of a general-purpose secure on-board system *combining Hardware and Software*
- *Successfully demonstrated EVITA results at various occasions*

Outlook

- EVITA results are already adopted by major research projects

  SEIS
  Sicherheit in Eingebetteten IP-basierten Systemen

  – SEIS project applies EVITA Security Framework for Secure IP-based Middleware

  PRESERVE
  preparing secure v2x communication systems

  – PRESERVE project develops an ASIC based on the EVITA result

  CAR 2 CAR COMMUNICATION CONSORTIUM
  ETSI World Class Standards

- Input for preparation of standardization activities within C2C-CC and ETSI

Thank you for your attention.

BMW Group
Research and Technology

Legal Framework of Automotive On-Board Networks

Jos Dumortier
K.U.Leuven – ICRI
www.icri.be

Overview

1. Introduction: what are the main legal issues?
2. The ITS legal framework
3. Privacy protection in automotive on-board networks
4. Liability issues in automotive on-board networks
5. Conclusions

1. Legal Issues

- V2X
  - automatic actions (e.g. braking) following V2V or V2I communications
- eToll
  - collection of personal information in wide-area toll systems
- eCall
  - tracking, data minimalization and value-added services
- Nomadic Devices
  - privacy and security of communications networks
- Aftermarket
  - liability for malware, infected software patches, etc.
- Diagnosis
  - application of data protection legal framework (who is the controller?)

2. The ITS Legal Framework

- Directive 2010/40/EU

  Framework for the deployment of Intelligent Transport Systems in the field of road transport and for the interface with other modes of transport

  Commission issues specifications between 2010 and 2017 to address the compatibility, interoperability and continuity of ITS solutions across the EU

  Delegated acts: opinion of the European Data Protection Supervisor of 22/07/2009

- Electronic Road Tolling

  Directive 2004/52/EC: interoperability of electronic road tolling systems in the Union

  Commission Decision 2009/750/EC: regulatory framework for EETS (e.g. OBE in vehicle)

3. Privacy protection in Automotive On-Board Networks

- European Convention of Human Rights
  - On-Board Automotive Networks should fulfill the conditions imposed by Art. 8 ("necessary in a democratic society")
- Directive 95/46/EC
  - Scope: processing of personal data
  - Who is the controller? Who is the processor?
  - Applicable law: issue for cross-border ITS
  - Data minimalization, storage duration, anonymisation
- Directive 2001/58/EC
  - Scope: public electronic communications networks
  - Issues; security provisions, breach notification, access to terminal equipment, traffic and location data

4. Liabilities with regard to Automotive On-Board Networks

- Liability: a complex set of (primarily national) rules
- Important factor in determining liabilities: legal framework for Vehicle Type Approval
  - UNECE and WVTA
  - Directive 2007/46/EC
- Vienna Convention on Road Traffic (1968): "*driver shall at all times be able to control his vehicle* "
- Directive 2001/95/EC: General Product Safety (consumer products)
- Directive 85/374/EEC on liability for defective products (consumer protection)

5. Conclusions

- EVITA contributes substantially to the implementation of the most essential legal principles in the area of privacy and personal data protection, for example, by developing technologies to protect personal data against unauthorized access
- EVITA ensures the legally required level of security appropriate to the risks represented by the processing and the nature of the data by proposing a risk analysis approach to identify what level of security protection may be required for particular on-board assets.
- EVITA solutions need to fit in the interoperability framework for ITS in the Union and does so by applying open standards
- Liability for accidents might be expected to partially shift away from the driver towards vehicle manufacturers and their on-board systems suppliers and more and more also to external information providers (role – and limits – of contracts)

Legal framework of automotive on-board networks

Jos Dumortier
K.U.Leuven – ICRI
Sint-Michielsstraat 6
B-3000 Leuven
(t) +32 (0)16 32 51 49
www.icri.be / jos.dumortier@law.kuleuven.be

Jos Dumortier
time.lex - Information & Technology Law
Congresstraat 35
B-1000 Brussel
(t) +32 (0)2 229 19 47
www.timelex.eu / jos.dumortier@timelex.eu

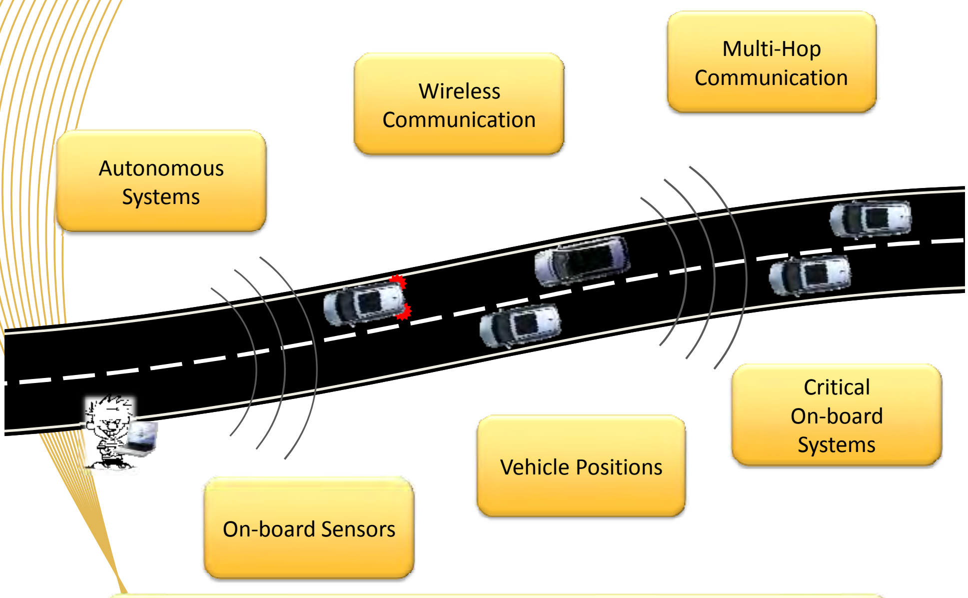
PRESERVE
preparing secure v2x communication systems

EVITA & PRESERVE

Uptake of EVITA in PRESERVE

SEVENTH FRAMEWORK PROGRAMME

Frank Kargl | f.kargl@utwente.nl | V9 | 23.11.2011



New Challenges for Security and Privacy

SEVECOM	PRECIOSA	EVITA	oversee
Secure IVC	ITS Privacy	In-Vehicle Security	Secure Autom. App. Platform
SeVeCom Baseline Architecture	Privacy Enforcing Runtime Architecture	On-Board Security Architecture	Open Platform for Vehicle Apps
Hooking Architecture	ITS Privacy Guidelines	FPGA HW Prototype	Secure Access to Comm. Channel
Prototype Implementation	Prototype Implementation	Demonstration Prototype	Platform Implementation

SeVeCom

- FP6 STREP Project
- 1.1.2006 – 31.3.2009

PRECIOSA

- FP7 STREP Project
- 1.3.2008 – 31.8.2010

PRESERVE 23.11.2011 EVITA & PRESERVE Cooperation 5

EVITA

- FP7 STREP Project
- 1.7.2008 – 31.12.2011

PRESERVE 23.11.2011 EVITA & PRESERVE Cooperation 6

Status before PRESERVE

SeVeCom, PRECIOSA, EVITA results not integrated

Evita FPGA HSM to costly for deployment in FOTs

No strong and scalable security solution in FOTs

PRESERVE Mission: Design, integrate, and test a secure and scalable V2X Security Subsystem for FOTs and Pilot Deployments

PRESERVE 23.11.2011 EVITA & PRESERVE Cooperation 8

PRESERVE
preparing secure v2x communication systems

FP7-ICT-2009-6.2, STREP, No. 269994
1.1.2011 – 31.12.2014

RENAULT

TRIALOG a new world of innovation

UNIVERSITY OF TWENTE.

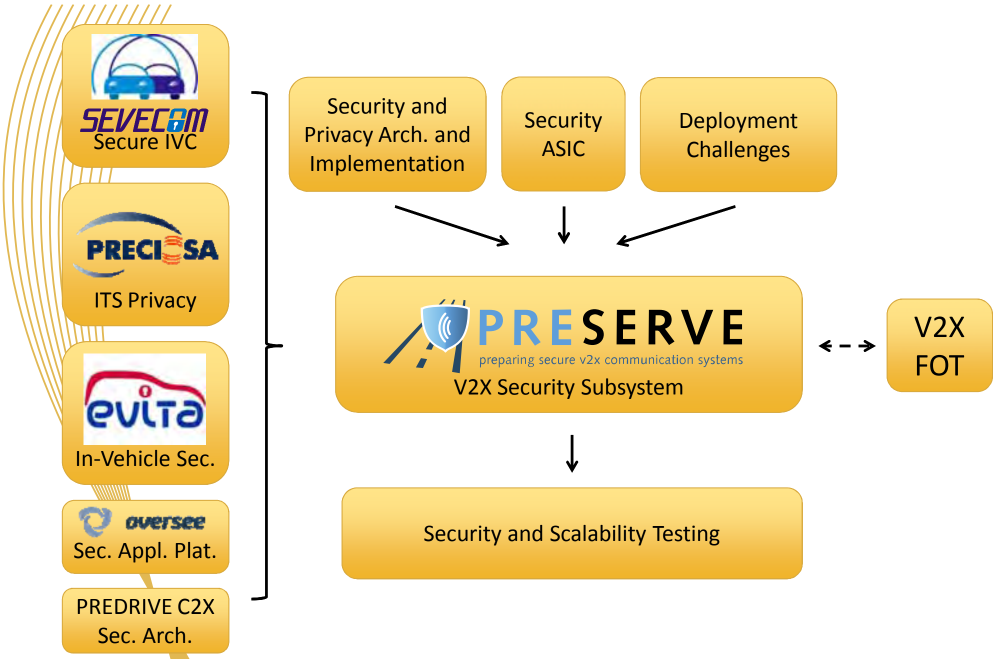
escrypt Embedded Security

KTH ROYAL INSTITUTE OF TECHNOLOGY

Fraunhofer SIT

Fraunhofer AISEC

PRESERVE 23.11.2011 EVITA & PRESERVE Cooperation 10



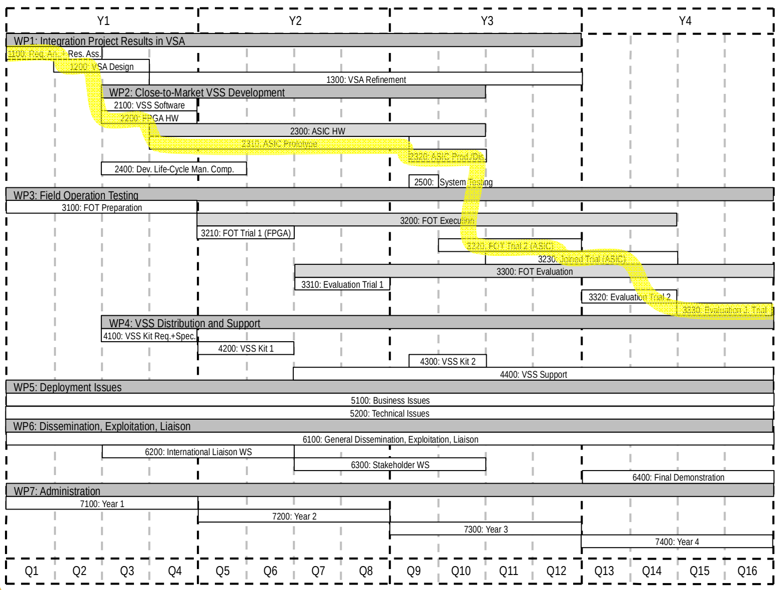
PRESERVE Objectives

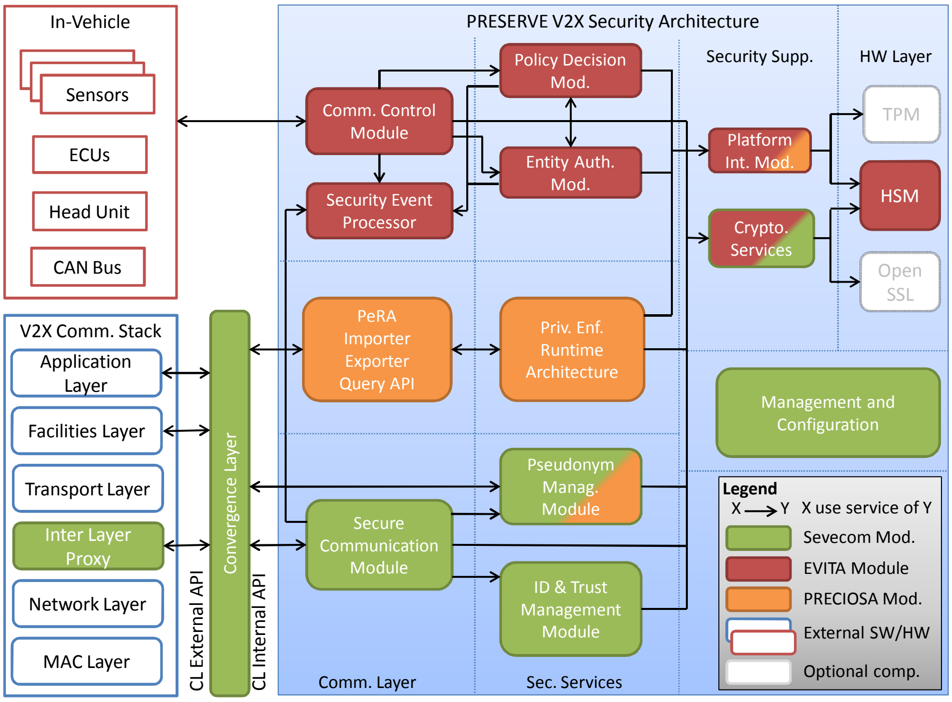
- Integrated V2X security architecture and implementation based on SeVeCom, EVITA, and PRECIOSA results
- Meet performance and cost requirements of current FOTs and future products, esp. build security ASIC
- Provide “ready-to-use” V2X security subsystem
- Solve open deployment and technical issues hindering standardization and product development

PRESERVE WPs

- WP1: Integration Project Results in VSA (V2X Security Architecture)
- WP2: Close-to-Market VSS (V2X Security Subsystem) Development
- WP3: Field Operation Test
- WP4: VSS Distribution and Support
- WP5: Deployment Issues
- WP6: Dissemination, Exploitation, Liaison
- WP7: Administration

PRESERVE Timing





PRESERVE HSM

- Based on “EVITA Full” FPGA design
- Early 2012: PRESERVE FPGAHSM for
  - early tests with Score@F
  - verification of PRESERVE design before ASIC production
- Mid 2013: PRESERVE ASIC HSM
  - Allows cost-effective large-scale testing and deployment
  - USB 2.0 interface for easy integration in various OBUs
  - Target price-point: <100 EUR
  - Performance Target: 1000 verifications/s

23.11.2011 EVITA & PRESERVE Cooperation 17

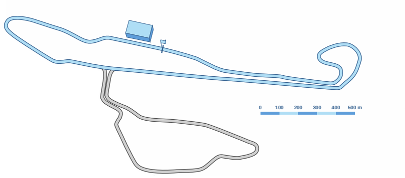
3 Phase Testing

Trial 1: Internal, smale-scale, lab-test

Trial 2: Internal, large-scale, hybrid testbed

Joint trial: with Score@F FOT, large-scale, real vehicles

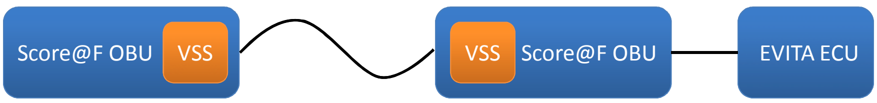
SCORE@F



Cooperation Proposal

evita PRESERVE preparing secure v2x communication systems

- EVITA HSM basis for the PRESERVE ASIC
- Aim that PRESERVE VSS will be compatible with other EVITA components
- Joint demo at ITS World Congress 2012 in Vienna



PRESERVE
preparing secure v2x communication systems

Expected Outcome

- Harmonized V2X Security Architecture ✔
- V2X Security Subsystem (incl. PKI backend)
- Cheap and scalable security ASIC for V2X
- Testing results VSS under realistic conditions
- Results for deployment challenges