Fraunhofer SIT

Secure automotive on-board networks

Basis for secure vehicle-to-X communication

Dr.-Ing. Olaf Henniger
Fraunhofer SIT / Darmstadt
2 December 2010

Presentation overview

Fraunhofer SIT

- EVITA project overview
- Security challenges
- Security toolbox
- Prototype and demonstration
- Summary

Presentation overview

Fraunhofer SIT

- **EVITA project overview**
- Security challenges
- Security toolbox
- Prototype and demonstration
- Summary

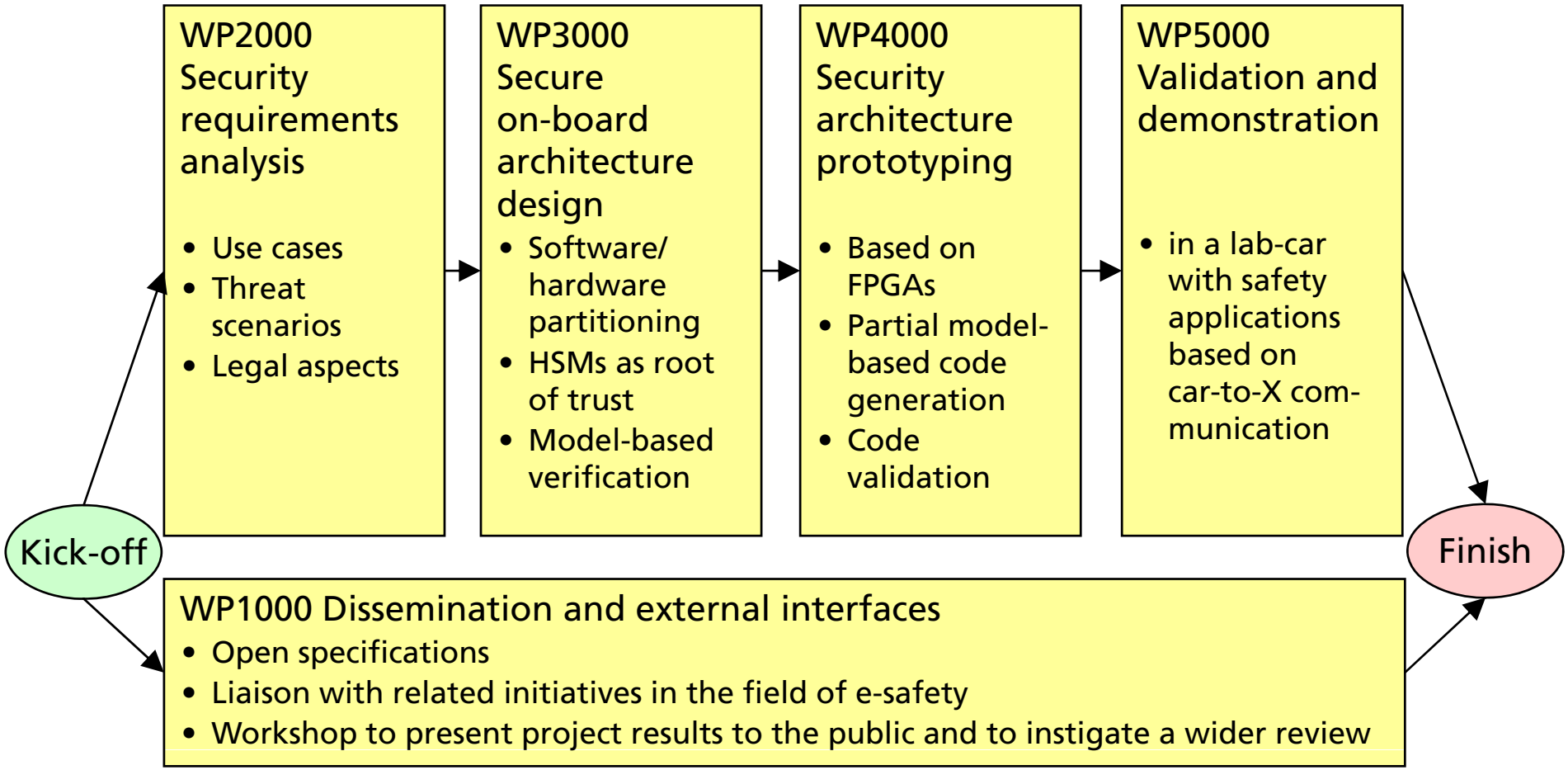
Related European projects

- SeVeCom (2006–2009) dealt with the protection of *external* vehicular communication
- PRECIOSA (2008–2010) dealt with the protection of *privacy* in vehicular communication
- EVITA (2008–2011) deals with the protection of *on-board* networks
  - *Internal* on-board security is basis for secure *external* vehicular communication
  - Objectives: To design, verify, and prototype building blocks for secure automotive *on-board networks*
  - Website: http://evita-project.org

EVITA project partners

EVITA project outline

Fraunhofer SIT



Presentation overview

Fraunhofer SIT

- EVITA project overview
- **Security challenges**
- Security toolbox
- Prototype and demonstration
- Summary

Possible attack goals

Fraunhofer SIT

- To gain personal advantages
- To gain reputation as a hacker
- To harm others

Summary of security requirements on automotive on-board networks

Fraunhofer SIT

- **Integrity of hardware security module**
  - Tamper prevention/detection
- **Integrity and authenticity of on-board software and data**
  - Unauthorized alteration must be infeasible / detectable.
- **Integrity and authenticity of on-board communication**
  - Unauthorized modification must be detectable by the receiver.
- **Confidentiality of in-vehicular communication and data**
  - Unauthorized disclosure of confidential data must be infeasible.
- **Proof of platform integrity and authenticity to other entities**
  - Remote attestation of integrity and authenticity of the platform configuration
- **Access Control to in-vehicle data and resources**
  - Enable availability and well-defined access to all data and resources

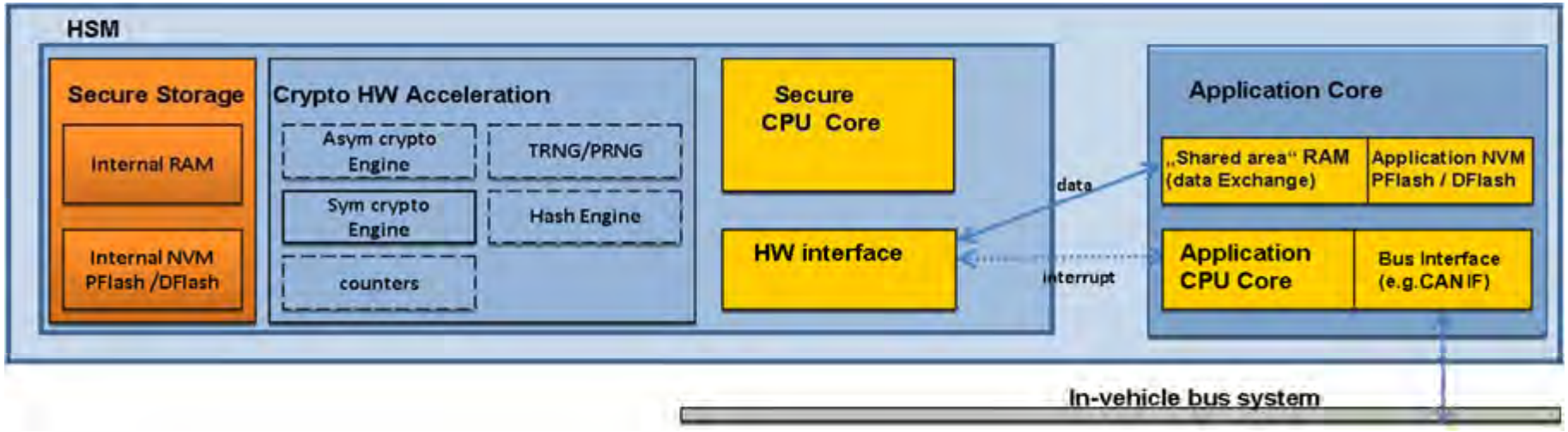
Presentation overview

Fraunhofer SIT

- EVITA project overview
- Security challenges
- **Security toolbox**
- Prototype and demonstration
- Summary

General structure of EVITA hardware security modules

Fraunhofer SIT



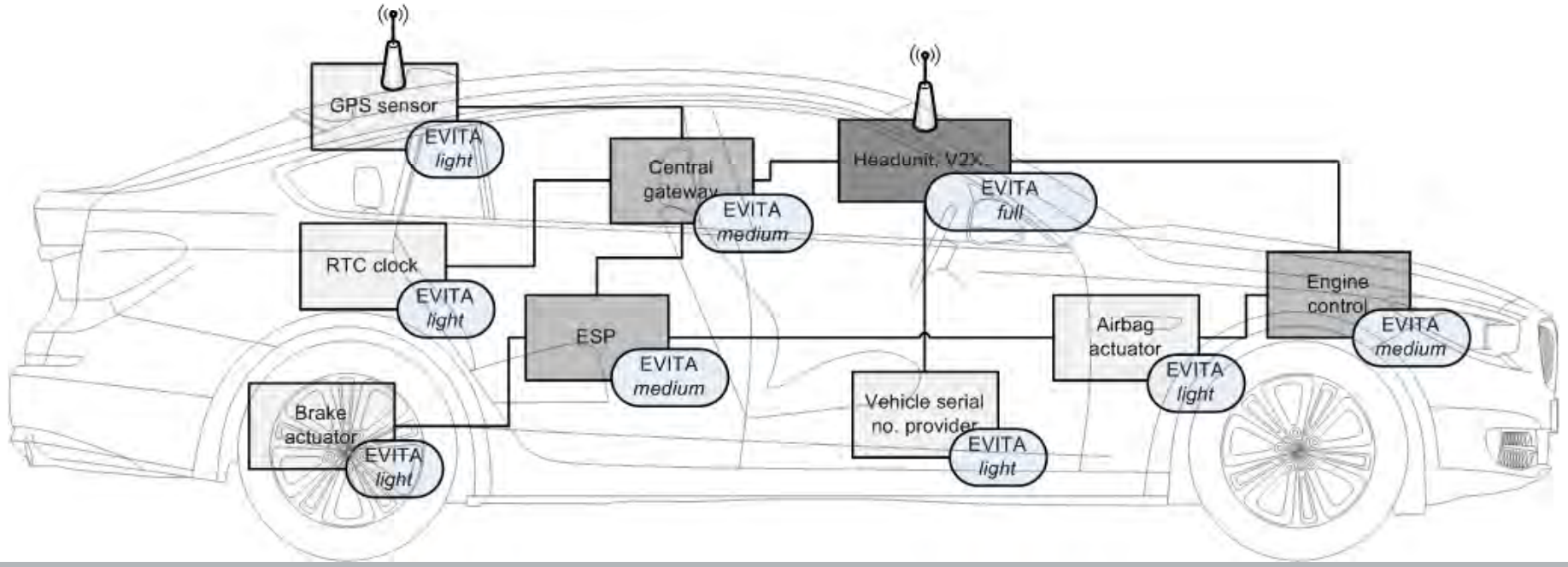
- Hardware security module (HSM) with a programmable secure core for flexibility
- Integrated into the same chip as the application CPU
- Tamper-resistant security anchor
  - Secure storage of cryptographic keys and certificates
- Acceleration of cryptographic functions

EVITA hardware deployment architecture

Fraunhofer SIT

EVITA HSM in every ECU, but
3 different HSM classes to meet

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



EVITA HSM classes

Fraunhofer SIT

- **Full HSM**: With asymmetric cryptographic engine, for protecting external communication
- **Medium HSM**: Without asymmetric cryptographic engine, for protecting internal ECUs
- **Light HSM**: Only symmetric cryptographic engine, for sensors and actuators

EVITA software architecture

Fraunhofer SIT

- Layered architecture:
  - **Low-level drivers** for interaction between **microcontroller** and **HSM**
  - **Security library**
    - Using the low-level driver to provide the required security functionality
    - **API** to upper layers
    - Cryptographic **protocols**, tailored to constraints of on-board networks
- Using AUTOSAR v3.0

Presentation overview

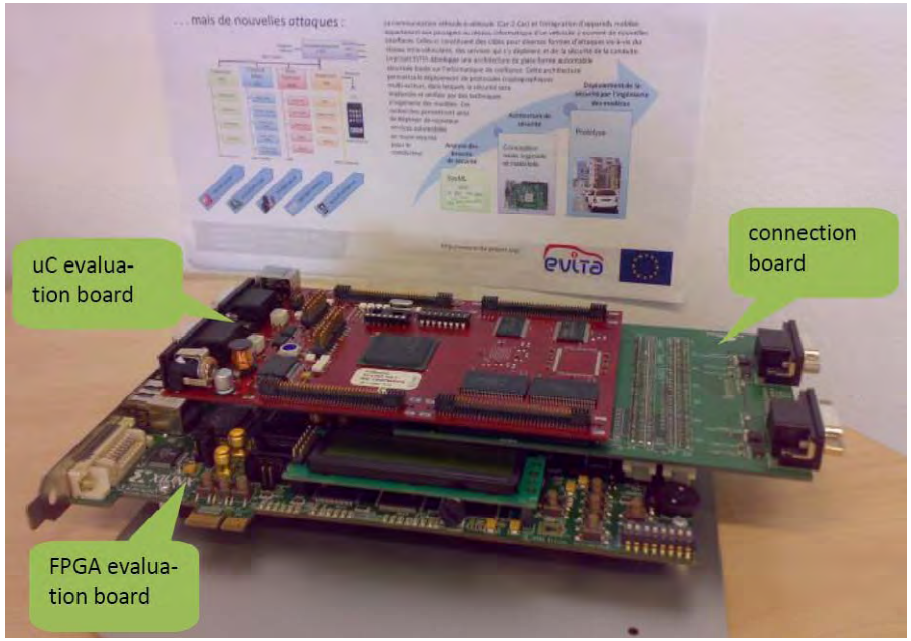
Fraunhofer SIT

- EVITA project overview
- Security challenges
- Security toolbox
- **Prototype and demonstration**
- Summary

Security hardware prototype

Fraunhofer SIT

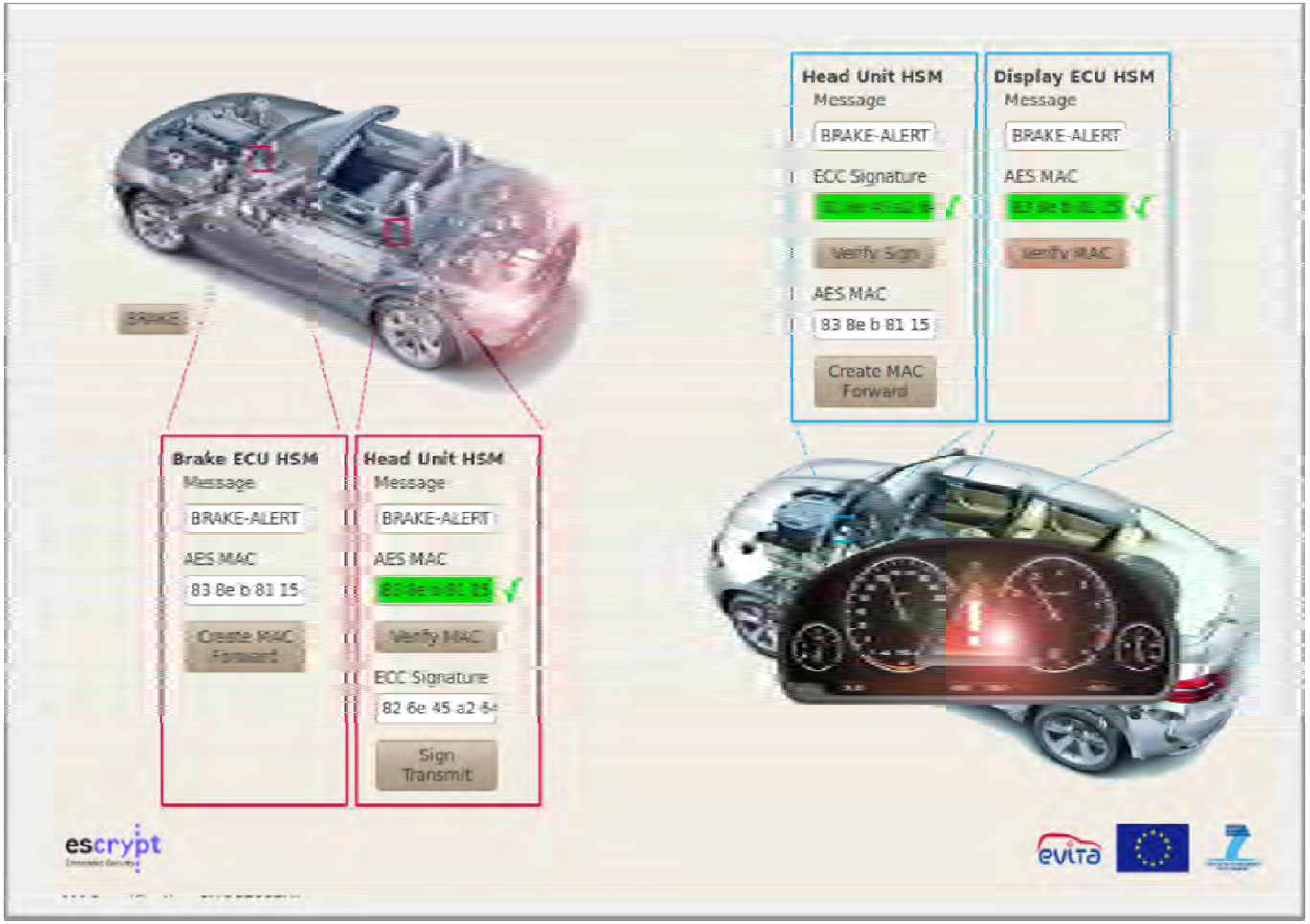
- Consists of
  - Off-the-shelve microcontroller
  - Extended with an HSM, prototyped on an FPGA
  - connected via a standardized interface for inter-chip communication (SPI)
- Next HSM prototype may be on an ASIC
- Future solution should have the HSM integrated onto the microcontroller chip.



Prototype-based demonstration

Fraunhofer SIT

- **Desktop** demonstration showcase
- **Real-world vehicle** demonstration showcase



Presentation overview

Fraunhofer SIT

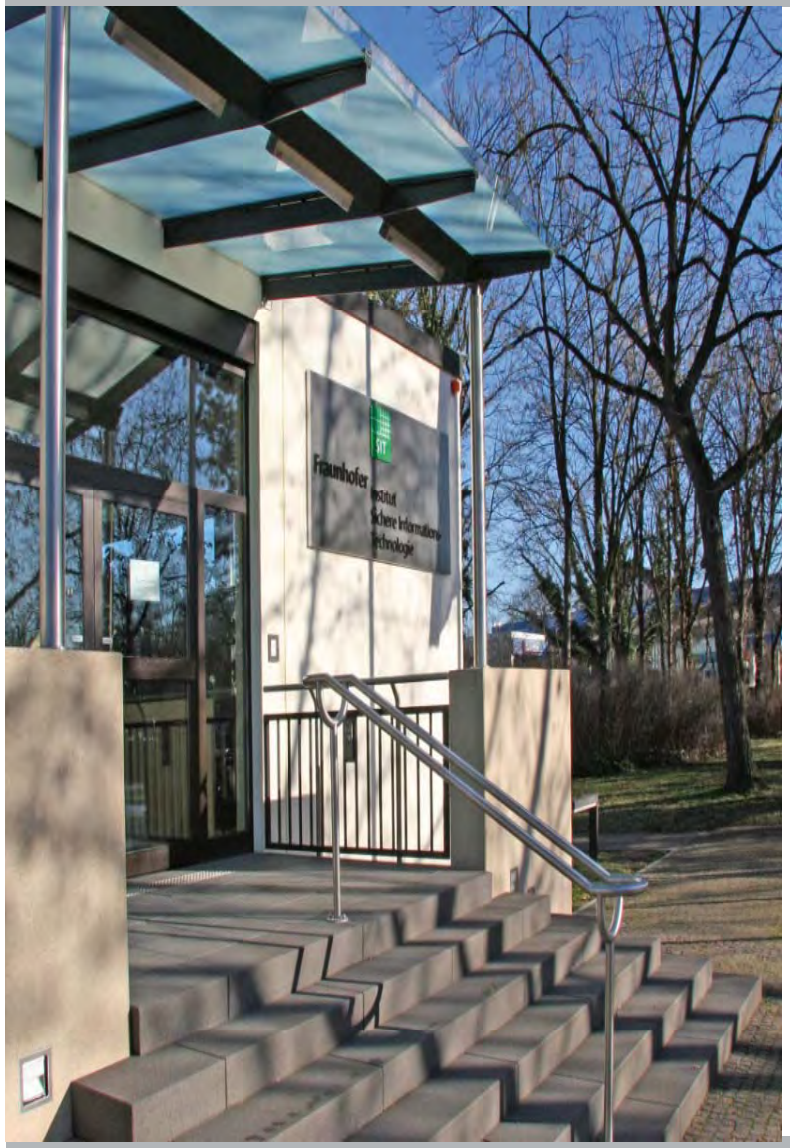
- EVITA project overview
- Security challenges
- Security toolbox
- Prototype and demonstration
- **Summary**

Summary

Fraunhofer SIT

- EVITA provides security toolbox for on-board networks
- EVITA **HSMs**
  - provide a **reliable security anchor**
  - apply ideas from **Trusted Computing** (e.g., authenticated boot)
  - **accelerate** cryptographic functions (e.g., ECC, AES, WHIRLPOOL, RNG)
  - **tamper-protection** via on-chip integration (+ further measures)

Thank you! Questions?



Fraunhofer Institute for
Secure Information Technology
Department Secure Mobile Systems
Rheinstraße 75
D-64295 Darmstadt

Dr.-Ing. Olaf Henniger
Telefon: +49 6151 869 264
Fax: +49 6151 869 224
E-Mail: olaf.henniger@sit.fraunhofer.de
Internet: http://www.sit.fraunhofer.de