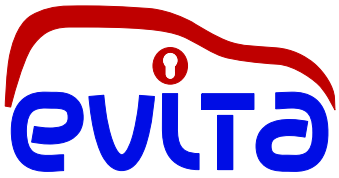

Project acronym:	EVITA
Project title:	E-safety vehicle intrusion protected applications
Project reference:	224275
Programme:	Seventh Research Framework Programme (2007-2013) of the European Community
Objective:	ICT-2007.6.2: ICT for cooperative systems
Contract type:	Collaborative project
Start date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

Project summary

Period covered:	from 1 July 2008 to 31 December 2011
Dissemination level:	Public

Project coordinator:	Fraunhofer Institute for Secure Information Technology	(Germany)
Project partners:	BMW Research and Technology	(Germany)
	Continental Teves AG & Co. oHG	(Germany)
	escrypt GmbH	(Germany)
	EURECOM	(France)
	Fraunhofer Institute for Systems and Innovation Research	(Germany)
	Infineon Technologies AG	(Germany)
	Institut Télécom	(France)
	Katholieke Universiteit Leuven	(Belgium)
	MIRA Ltd.	(UK)
	Robert Bosch GmbH	(Germany)
	TRIALOG	(France)
	Fujitsu Semiconductor Europe GmbH	(Germany)
	Fujitsu Semiconductor Embedded Solutions Austria GmbH	(Austria)

Contact:	Dr.-Ing. Olaf Henniger
	Fraunhofer Institute SIT
	Rheinstraße 75, 64295 Darmstadt, Germany
Email:	olaf.henniger@sit.fraunhofer.de
Tel.:	+49 6151 869 264
Fax:	+49 6151 869 224
Project website:	http://evita-project.org

Executive summary

A modern car may be equipped with up to 70 embedded ECUs (electronic control units) connected via various vehicular buses, forming a complex distributed system. The automotive on-board networks will get additional interfaces for vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communication in order to facilitate new automotive safety applications. While V2X communication heralds a new era of traffic safety, new security requirements need to be considered in order to prevent malicious attacks on the automotive electronics. The objective of EVITA, a project co-funded by the European Union within the Seventh Framework Programme for research and technological development, was to design, verify, and prototype security building blocks for automotive on-board networks. Thus, EVITA provides a basis for the secure deployment of electronic safety applications based on V2X communication.

EVITA has developed a unified approach to security and safety risk analysis for automotive on-board networks. Starting from relevant use cases and security threat scenarios, EVITA has identified security requirements for automotive on-board networks. Also legal requirements on privacy and data protection and liability issues have been considered.

Based on security requirements and automotive constraints, EVITA has designed a secure on-board architecture and secure on-board communications protocols. The security functions are partitioned between hardware and software. The root of trust is placed into HSMs (hardware security modules) to ensure a sufficient data throughput and attack resistance. Keys and certificates are to be stored securely in the non-volatile memory of the HSM. The HSMs are to be integrated on the same chip as the ECUs. To enable cost-efficiency and flexibility, EVITA has specified different classes of HSMs: full, medium, and light. This allows satisfying different cost constraints and different security requirements. Based on the secure on-board architecture, secure on-board communications protocols have been designed. In order to ensure that the identified security requirements are satisfied, selected parts of secure on-board architecture and communications protocols have been modelled using UML and verified using a set of complementary model-based verification tools.

The HSMs have been prototyped on FPGAs, connected with ECUs via standardised inter-chip communication interfaces. Low-level drivers for interacting with the HSMs have been developed based on AUTOSAR, today's standard automotive software architecture. The software security framework uses the HSMs to provide security functionality to applications running on the ECUs. For rapid prototyping, the security functionality has also been coded purely in software. The code has been validated to ensure its correctness.

Secure communication has been deployed on board of lab cars demonstrating e-safety applications based on V2X communication. Cryptographic methods ensure the integrity and authenticity of information exchanged. It has been demonstrated that cryptographic hardware is able to meet the performance requirements of V2X communication. Releasing HSMs for deployment in cars on public roads requires further efforts and is out of scope of the EVITA project.

In order that the entire automotive industry may benefit from the EVITA results and to facilitate standardised interfaces, the secure on-board architecture and communications protocol specifications have been published as open specifications. The EVITA project partners have liaised with related initiatives in the fields of e-safety and embedded security to achieve multilateral synergies.

I. Project objectives and context

A. Project objectives

A significant further reduction of road traffic fatalities is expected from introducing vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communication. Examples for electronic safety aids deployed in vehicles (e-safety applications) are local danger warnings, traffic light pre-emption, and electronic emergency brakes. While these functionalities inspire a new era of safety and efficiency in transportation, new security requirements need to be considered in order to prevent attacks on these systems. Attacks may originate outside or inside the vehicle, resulting for instance in the injection of illegitimate messages influencing the traffic flow.

While related projects such as NoW[1] (Network on Wheels) and SeVeCom[2] (Secure Vehicular Communication) focussed on the security challenges of the external communication and proposed solutions for privacy-preserving trustworthy V2X communication, the EVITA project focused on securing the internal on-board system in order to prevent, or at least detect, illegal tampering. Attacks on V2X communication can only be averted if trustworthy V2X communication is combined with on-board security avoiding the transmission of manipulated messages to the external communication partners.

The objective of the EVITA project was to design, to verify, and to prototype building blocks for secure automotive on-board networks protecting security-relevant components against tampering and sensitive data against compromise. This is an essential prerequisite to the safe operation of V2X communication. Thus, EVITA addressed "advanced, reliable, fast and secure vehicle-to-vehicle and vehicle-to-infrastructure communication for new functionalities" as stated in the objective ICT-2007.6.2 "ICT for Cooperative Systems" of the European Union's Seventh Framework Programme for research and technological development.

The following requirements had to be met in order to achieve secure on-board networks:

– Distributed security: All electronic components of a vehicle and the connections between them need to be protected because a network is only as secure as its weakest part.
– Real-time capability: A vehicle performing V2X communication needs to sign and verify up to several thousand messages per second.
– Cost–effectiveness: In the automotive industry cost effective solutions tailored to the specific needs are necessary. It is not acceptable to pay for unused hardware capabilities.

These requirements are not met by today's off-the-shelve security solutions such as smart cards and Trusted Platform Modules (TPMs) because they are not designed to fit to the automotive system environment. The existing security solutions had to be adapted to the automotive domain.

B. Project context

A modern automobile within the premium product segments is equipped with up to 70 embedded electronic control units (ECUs) providing a diversity of system functions such as engine control, steering and braking systems, navigation systems, traffic control. These appli-

[1] http://network-on-wheels.de
[2] http://www.sevecom.org

cations are realised as embedded systems and range from simple ECUs to infotainment systems equipped with high-end processors whose computing power approaches that of current PCs. These ECUs are connected via various vehicular buses (e.g. CAN, MOST, LIN, etc.) forming a complex highly networked and distributed system.

So far, only niche applications in the automotive domain, e.g. electronic immobilizers, access control, secure flashing, secure activation of functions or protection of mileage counter, have relied on security technologies. Today's security solutions are based on a software approach. In this approach secret keys are coded in the ECU software. Everyone who can code and run applications on the ECU has the possibility to manipulate or work around these security functions. The vast majority of software and hardware in today's cars are not equipped with security functionality at all. The reason is that car IT systems did not need security functions, because there was little incentive for malicious manipulation. Furthermore, security tends to be an afterthought in any IT system because the achievement of the core function is the main focus when designing a system.

II. Main scientific and technological results

A. Security requirements analysis

At the beginning of the project, use cases for automotive on-board networks that are expected to require security measures have been selected and described [1] in order to infer security requirements from them. Based on these use cases, dark-side scenarios of potential abuse of e-safety applications have been elaborated in order to identify threats to cars, infrastructure and human lives. The dark-side scenarios have been structured as attack trees that identify threats against an instance of an automotive on-board network [2]. The methodologies for risk and security requirements analysis have been adapted to the given context. Starting from the use cases and dark-side scenarios, clear and precise security requirements for automotive on-board networks have been identified [2]. At the highest level, the security objectives that are covered are:

- to prevent unauthorized manipulations of vehicular on-board electronics,
- to prevent unauthorized modifications of vehicle applications especially regarding safety and m-commerce applications,
- to protect privacy of vehicle drivers,
- to protect intellectual property of vehicle manufacturers and suppliers,
- to maintain the operational performance of applications and security services.

Also legal requirements on privacy and data protection and liability issues in V2X communication have been considered [3].

B. Secure on-board architecture design

A security and trust meta-model has been established applicable to the security requirements identified before. Different security architectural approaches have been compared and deliberated about. A formal security modelling framework has been devised [4]. A security engineering process that refines design-independent security requirements into more specific ones

that can be satisfied by cryptographic means has been introduced. The refinement process is supported by so-called security building blocks with pre-verified properties.

Based on the security requirements, the security and trust model, and the automotive constraints, a secure on-board architecture has been designed with the required roles, modules, and hardware and software interfaces [5]. The security functions have been partitioned between hardware and software. The root of trust is placed into hardware security modules (HSMs) to ensure a sufficient data throughput and attack resistance. The HSMs are tamper-resistant cryptographic coprocessors with a programmable secure core, integrated on the same chips as the ECUs. Keys and certificates are stored securely in the non-volatile memory of the HSMs to prevent attackers from altering them.

To enable cost-efficiency and flexibility, different classes of HSMs have been specified. This allows satisfying different cost constraints and different security requirements:

– Full HSM for protecting the in-vehicle domain against vulnerabilities due to V2X communication: This includes an asymmetric cryptographic engine for creating and verifying electronic signatures. The full HSM provides the maximum level of functionality, security, and performance of all the different HSM variants.
– Medium HSM for securing the on-board communication: The medium HSM resembles the full HSM, but contains a little less performing microprocessor and no asymmetric cryptographic engine in hardware. However, it is able to perform some non-time-critical asymmetric cryptographic operations in software, e.g. for the establishment of shared secrets.
– Light HSM for securing the interaction between ECUs and sensors and actuators: It only contains a symmetric cryptographic engine and an I/O component in order to fulfill the strict cost and efficiency requirements that are typical for sensors and actuators.

Table 1 presents the components of the different HSM classes. Figure 1 illustrates an instance of an automotive on-board network in which security-critical components are protected using HSMs of the three classes. A single HSM attached to the unit that provides the wireless communication to the outside world is not enough because the behaviour of the system depends on messages received from other components inside the vehicle. If these components were not protected as well, attackers could exploit these vulnerabilities.

Table 1 Components of automotive HSM classes

	Full HSM	**Medium HSM**	**Light HSM**
RAM (random-access memory)	✓	✓	optional
NVM (non-volatile memory)	✓	✓	optional
Symmetric cryptographic engine	✓	✓	✓
Asymmetric cryptographic engine	✓		
Hash engine	✓		
Counters	✓	✓	optional
Random-number generator	✓	✓	optional
Secure CPU	✓	✓	
I/O component	✓	✓	✓

EVITA has specified hardware and software interfaces. The hardware interface provides the application software with access to the HSM functionality. It is asynchronous (i.e. non-blocking), almost completely multi-session capable (i.e. interruptible), and partly also multi-threading capable. It is compliant to the Secure Hardware Extension (SHE) specification of

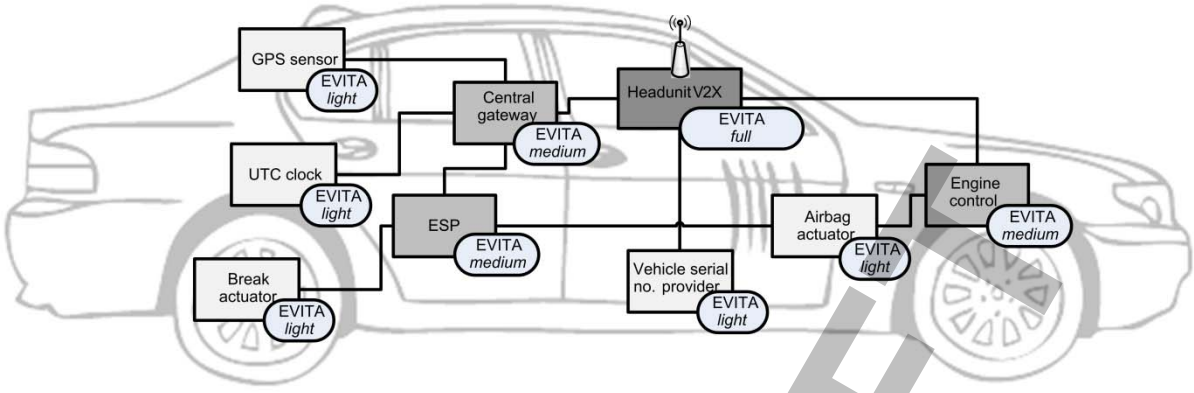

Figure 1 Instance of a secure on-board network with full, medium, and light HSMs attached to ECUs, sensors, and actuators

the automotive HIS consortium[3]. It covers access to all HSM components, higher-level security functionality such as secure boot and secure time stamping and all necessary security management functionality, e.g. device administration, key creation, and key import/export.

Based on the secure on-board architecture, secure on-board communications protocols have been designed, supporting the security requirements and enabling the specified use cases [6]. In order to ensure that the identified security requirements are satisfied, selected parts of the secure on-board architecture and the communication protocols have been modelled and verified using a set of complementary model-based verification tools [7][8].

C. Security architecture prototype

The HSMs have been prototyped on FPGAs (field-programmable gate arrays) and connected with ECUs via standardised inter-chip communication interfaces. An FPGA, a connection board, and an ECU are stacked on top of each other in a compact form [9].

Low-level drivers (LLDs) have been integrated into the ECUs for interacting with the HSMs. The LLDs are based on AUTOSAR, today's standard automotive software architecture [9]. The LLDs can in part be generated from UML models [10]. The security software running on the ECUs uses the HSMs to provide the required security functionality to applications running on the ECUs. For rapid prototyping, the security functionality has also been implemented purely in software. The security software deployed in the prototype is a comprehensive, modular security library providing application-programming interfaces (APIs) to the security functionality. The code has been validated to ensure its correctness [11].

D. Prototype-based demonstration

At the end of the project, secure communication has been deployed in desktop-based demonstrators and on board of lab cars demonstrating e-safety applications based on V2X communication (valet parking privacy application, car 2 car emergency brake notifications and car 2 car active emergency brake) [12]. Cryptographic methods ensure the integrity and authenticity of exchanged information and protect electronic components against theft, tampering, and un-

[3] http://www.automotive-his.de

authorised cloning. Cryptographic hardware has demonstrated to meet the real-time performance requirements of V2X communication.

III. Potential impact

A. Contributions to standardisation of automotive on-board security

A standardised solution for secure automotive on-board networks is desirable because

- It will reduce technical barriers that would arise if each company developed different solutions independently;
- Around the world, the automotive industry faces the same security problems;
- Standards enable third-party semiconductor manufacturers to independently start chip development and production.

Therefore, EVITA strived to establish a basis for a standard for secure automotive sensor/actuator networks and to assure a broad utilisation of EVITA results in the automotive industry. The impact of EVITA's results will be multiplied by other vehicle manufacturers and electronics suppliers taking up the developed secure architecture specification and protocols.

B. Liaison and dissemination activities

A strategy for a systematic distribution of the project results through a variety of communication channels has been devised to ensure a broad utilisation [13]. In order that the entire automotive industry may benefit from the project results, the EVITA deliverables are published as open specifications on the project website[4] unless confidential implementation know-how is involved.

The motivation, objectives, and approach of the project as well as project results have been presented at the relevant academic and industry events, see for instance [14][15][16].

To ensure that related work is taken into account, the EVITA project partners liaised with related initiatives in the fields of e-safety and embedded security to achieve multilateral synergies. EVITA results have been introduced into industry consortia such as the Car 2 Car Communication Consortium (C2C-CC), which harmonises the contributions received and forwards them to standardisation bodies such as ETSI TC ITS for formal standardisation.

A liaison workshop has been held in August 2009[5] and a dissemination workshop in July 2010[6]. A Final EVITA Workshop[7], including live vehicle demonstrations, took place in November 2011 immediately before the Car 2 Car Forum, the annual assembly of members of the C2C-CC. A summary of liaison activities can be found in [17].

[4] see http://evita-project.org/deliverables.html
[5] see http://www.cast-forum.de/en/workshops/infos/118
[6] see http://www.cast-forum.de/en/workshops/infos/129
[7] see http://evita-project.org/workshop.html

C. Potential beneficiaries

The intended primary beneficiaries of the EVITA results are car, truck, and motorcycle manufacturers, automotive electronics suppliers, and semi-conductor manufacturers who are all invited to take up the open specifications of EVITA. Also industry consortia such as the C2C-CC and other organisations dedicated to electronic car safety aids are intended to benefit from the EVITA results.

In a broader sense, by helping to reduce road transport problems, the EVITA results are intended to benefit the society as a whole.

Secondary beneficiaries of EVITA results are all industries that have to cope with communication security problems similar to that in the automotive sector. Similarly complex communication networks are embedded, for instance, in airplanes, power stations, robots, house control systems, and remote maintenance systems. The development of a cost-efficient HSM in the EVITA project will help many embedded applications to efficiently improve their security.

References

[1] EVITA Deliverable D2.1: Specification and evaluation of e-security relevant use cases.

[2] EVITA Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios.

[3] EVITA Deliverable D2.4: Legal framework and requirements of automotive on-board networks.

[4] EVITA Deliverable D3.1: Security and trust model.

[5] EVITA Deliverable D3.2: Secure on-board architecture specification.

[6] EVITA Deliverable D3.3: Secure on-board protocols specification.

[7] EVITA Deliverable D3.4.3: On-board architecture and protocols verification.

[8] EVITA Deliverable D3.4.4: On-board architecture and protocols attack analysis.

[9] EVITA Deliverable D4.0.3: Security architecture implementation – Progress Report.

[10] EVITA Deliverable D4.2.3: LLD modelling, verification and automatic C-code generation.

[11] EVITA Deliverable D4.4.2: Test results.

[12] EVITA Deliverable D5.1.2: On-board communication demonstrator description.

[13] EVITA Deliverable D1.2.7: Final dissemination strategy.

[14] Henniger, O.; Apvrille, L.; Fuchs, A.; Roudier, Y.; Ruddle, A.; Weyl, B.: Security requirements for automotive on-board networks. In: *9th International Conference on ITS Telecommunication*. Lille, France (October 2009)

[15] Apvrille, L.; El Khayari, R.; Henniger, O.; Roudier, Y.; Seudié, H.; Weyl, B.; Wolf, M.: Secure automotive on-board electronics network architecture. In: *FISITA 2010 World Automotive Congress*. Budapest, Hungary (May – June 2010)

[16] Wolf, M.; Gendrullis, T.: Design, implementation, and evaluation of a vehicular hardware security module. In *14th International Conference on Information Security and Cryptology*, Seoul, South Korea, November/December 2011

[17] EVITA Deliverable D1.2.6: Final liaison documentation.