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 D1.2.6:
Final Liaison Documentation

Authors:	Antonio Kung, Michel Sall (Trialog); Olaf Henniger (Fraunhofer Institute SIT); Benjamin Weyl (BMW Group Research and Technology GmbH); Marko Wolf (escrypt GmbH); Hervé Seudié (Robert Bosch GmbH)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Date:	19 March 2012

Abstract

The objective of the EVITA project is 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 aids based on vehicle-to-vehicle and vehicle-to-infrastructure communication. Because EVITA deals with issues germane also to other e-safety projects and activities, liaison with other projects and activities is important in order to exchange information, use synergy effects and jointly work on harmonized and integrated approaches over various projects. This document summarises the liaison activities carried out during the EVITA project.

Contents

List of abbreviations

CALM	Communication Architecture for Land Mobile Environment
GST	Global System for Telematics
HSM	Hardware Security Module
ITS	Intelligent Transport System
RSU	Road Side Unit
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
WG	Working Group

Document history

Version	Date	Description
D1.2.3v1.0	2010-02-28	Mid-term liaison documentation
D1.2.3v1.1	2010-03-10	Description of liaison activities extended
D1.2.6v1.0	2012-03-19	Final liaison documentation

1 Introduction

1.1 Background

Intelligent Transport Systems (ITS) including networked vehicles will enhance the safety of drivers and other road users, minimize pollution and maximize the efficiency of travel. The EVITA project addresses the issues related to vehicle intrusion vulnerabilities arising from networking vehicles. Consequently, liaison activities are needed and desirable in order to share information, exchange know-how, rely on previous work and achievements and jointly develop solutions for Car2X environments.

1.2 Purpose and scope

The purpose of this deliverable is to provide an overview of the liaison activities carried out within the EVITA project. The activities involve liaisons with the following stakeholders:

- stakeholders from the ITS application area,
- stakeholders from the automotive sector,
- stakeholders in the security and trust domain.

1.3 Organisation of the document

The document includes sections on the liaison to

- existing e-safety projects,
- existing security projects, and
- related working groups.

A template is used for these items of liaison, giving brief descriptions of the liaison projects and working groups in tabular form and describing liaison activities within the EVITA project below each table. Furthermore, the document includes a list of dissemination activities.

2 External interfaces

2.1 Projects in the area of e-safety

2.1.1 EASIS

Brief description	EASIS (Electronic Architecture and System Engineering for Integrated Safety Systems) is a European FP6 project that has addressed the issue of integrating different vehicle safety systems into a complete network. The result is a powerful and highly dependable in-vehicle electronic architecture enabling following technologies: A software platform for in-vehicle electronic systems, a vehicle on-board electronic hardware infrastructure that supports the requirements of integrated safety systems in a cost effective manner, methods and techniques for handling critical dependability-related parts of the development lifecycle, an engineering process and a suitable tool chain.
Website	www.easis-online.org
Timeline	2004–2007
EVITA partners involved	Bosch, Continental, MIRA

The EVITA project uses a generalized topology of on-board networks of contemporary and next-generation high-end cars as reference architecture for the use case descriptions [1]. This topology is based on the EASIS project.

2.1.2 SeVeCom

Brief description	SeVeCom (Secure Vehicle Communication) is a European FP6 project that has addressed the issue of Secure Vehicle Communication. The result is an architecture that has been adopted by the car-to-car communication consortium as well as a protocol independent implementation. Features provided are secure beaconing, secure geocast, secure georouting as well as pseudonym management for privacy protection.
Website	www.sevecom.org
Timeline	2006–2009
EVITA partners involved	Trialog, Bosch, K.U. Leuven

EVITA work is complementary to SeVeCom in that EVITA focuses on intrusion threats stemming from communication. Liaison discussion has taken place with SeVeCom (University of Ulm, Trialog) to ensure this. The EVITA liaison workshop on 27 August 2009 featured a presentation about SeVeCom (from École Polytechnique Fédérale de Lausanne).

[2] has suggested that EVITA implementation specification should follow SeVeCom baseline architecture [3], so that both specifications could form a solid overall contribution.

2.1.3 CVIS

Brief description	CVIS (Cooperative Vehicle-Infrastructure Systems) is a European FP6 integrated project focusing on co-operative systems for road transport. It intends to develop and integrate the essential basic and enabling technologies readily available for both vehicle and roadside. Major input towards CALM standardisation is anticipated. CVIS involves work on security, and an enhancement of GST (in terms of telematics architecture) and a companion to SeVeCom (end-to-end security for CVIS versus communication security for SeVeCom).
Website	www.cvisproject.org
Timeline	2006–2010
EVITA partners involved	Trialog, Bosch

The CVIS project has included from the start significant activities related to security in particular related to application security (e.g. authentication and authorisation requirements). An article of the "Guardian" was published in March 2009 criticizing CVIS for creating privacy issues[1]. Consequently discussion was held between the CVIS, SeVeCom and PRECIOSA projects to ensure that features for privacy protection as planned in the latter two IST projects were effective for suitable data protection in CVIS applications. As a matter of fact, the contributions from SeVeCom, PRECIOSA and EVITA form a set of technologies that could be readily used in those applications.

2.1.4 Safespot

Brief description	Safespot is a European FP6 integrated project. The objective is to understand how intelligent vehicles and intelligent roads can cooperate to produce a breakthrough for road safety. The aim is to prevent road accidents by developing a Safety Margin Assistant that detects in advance potentially dangerous situations and that extends in space and time drivers' awareness of the surrounding environment. The Safety Margin Assistant will be an Intelligent Cooperative System based on Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication
Website	www.safespot-eu.org
Timeline	2006–2010
EVITA partners involved	Bosch, MIRA, and Continental

Safespot applications exhibit communication requirements which have influenced EVITA in terms of encryption performance, in particular the EVITA full HSM.

2.1.5 PRECIOSA

Brief description	The goal of the European FP7 collaborative project PRECIOSA (Privacy Enabled Capability In co-Operative systems and Safety Applications) is to demonstrate that co-operative systems can comply with future privacy regulations by demonstrating that an example application can be endowed with technologies for suitable privacy protection of location related data. The approach is to create a policy enforcement perimeter based on the secure binding of policy metadata and data item.
Website	www.preciosa-project.org
Timeline	2008–2010
EVITA partners involved	Trialog

[1] *Big Brother is watching: surveillance box to track drivers is backed*. See http://www.guardian.co.uk/uk/2009/mar/31/surveillance-transport-communication-box

PRECIOSA addresses the overall issue of data protection in ITS applications and therefore focuses on both vehicle units, road side units (RSU) and control centres. Various discussions have taken place notably from a legal point of view. The EVITA liaison workshop on 27 August 2009 featured a presentation about PRECIOSA (from University of Ulm).

It was also decided in PRECIOSA that the implementation specification would follow the SeVeCom baseline architecture [3] so that the three specifications from SeVeCom, PRECIOSA and EVITA could be merged into one contribution.

2.1.6 COMeSafety

Brief description	The European FP6 specific support action COMeSafety provides a platform for both the exchange of information and the presentation of results. Regular electronic newsletters and publications at major conferences and press events complement the dissemination efforts. For European and worldwide harmonization, liaisons are established and workshops are organized to bring together the eSafety Forum and all stakeholders. COMeSafety provides an open integrating platform, aiming for the interests of all public and private stakeholders to be represented. The COMeSafety project provides an overall European ITS framework architecture including a basic security architecture.
Website	www.comesafety.org
Timeline	2008–2010
EVITA partners involved	BMW F+T

A presentation about COMeSafety has been given by BMW Group Research and Technology at the EVITA General Assembly in February 2009. The COMeSafety project has been presented to the project and the basic COMeSafety security architecture has been introduced and described. This architecture has been considered within [4] (Section 4.4).

2.1.7 sim^{TD}

Brief description	sim^{TD} ("Sichere Intelligente Mobilität – Testfeld Deutschland) is a project funded by the German government carrying out the so far world's largest field test of vehicle-to-X communication.
Website	www.simtd.de
Timeline	2008–2012
EVITA partners involved	Fraunhofer SIT, Continental, Bosch, BMW F+T

The EVITA liaison workshop on 27 August 2009 featured a presentation about sim^{TD} (from Continental). In addition, results have been shared at the C2C-CC Liaison Security Workshop in Wolfsburg on 5 November 2009.

The EVITA demonstrator vehicles include sim^{TD} CCUs (communication control units) for V2X communication and use EVITA HSMs instead of the sim^{TD} security daemon software library for securing the V2X messages.

2.1.8 SEIS

Brief description	SEIS ("Sicherheit in eingebetteten IP-basierten Systemen") is a project funded by the German government dealing with securing IP-based automotive electronics networks and providing solutions for enabling IP-based communication within on-board networks.
Website	www.eenova.de/projekte/seis
Timeline	2009–2012
EVITA partners involved	BMW F+T, Bosch, Continental, Fraunhofer SIT, Infineon

The SEIS project has used the security requirements and risk analysis of EVITA [5] as well as the security and trust model of EVITA [6] as input.

2.1.9 OVERSEE

Brief description	The objective of the European FP7 collaborative project OVERSEE (Open VEhiculaR SEcurE platform) is to develop an open vehicular IT platform that provides a protected standardised in-vehicle runtime environment as well as on-board access and communication point. The approach is to enforce a strong level of isolation between independent applications ensuring that vehicle functionality and safety cannot be harmed by one of the applications.
Website	www.oversee-project.eu
Timeline	2010–2012
EVITA partners involved	escrypt, Trialog

A presentation about OVERSEE was made by escrypt during the EVITA General Assembly in January 2010. The OVERSEE platform will integrate technology for vehicle intrusion protection from EVITA.

2.1.10 PRESERVE

Brief description	PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) contributes to the security and privacy of future vehicle-to-vehicle and vehicle-to-infrastructure communication systems by addressing critical issues like performance, scalability, and deployability of V2X security systems. This project addresses the challenges of secure and privacy-friendly communication between vehicles.
Website	www.preserve-project.eu/
Timeline	2011–2014
EVITA partners involved	Fraunhofer SIT, Trialog, escrypt

PRESERVE combines the results of the three projects SeVeCom, PRECIOSA and EVITA in the context of a Field Operational Test (FOT) project. It focuses on security and privacy issues. The EVITA, OVERSEE, and PRESERVE projects were presented during the Concertation Meeting "ICT for Transport" on 4–5 April 2011 in Brussels. EVITA will be an input to PRESERVE, which will provide a security subsystem to other FOT projects.

The Final EVITA Workshop on Security of Automotive On-Board Networks on 23 November 2011 included a presentation on the "Uptake of EVITA results in the PRESERVE project". A cooperation agreement between EVITA and PRESERVE has been drafted. EVITA partners plan a joint demonstration with the PRESERVE project at the ITS World congress in Vienna in October 2012, based on the EVITA desktop and vehicle demonstrators.

2.2 Projects in the area of trust and security

2.2.1 SERENITY

Brief description	SERENITY was a European FP6 integrated project. It dealt with system engineering for security and dependability. The primary goal of the SERENITY project was to enhance security and dependability for ambient intelligence ecosystems by capturing security expertise and making it available for automated processing. SERENITY provided a framework supporting the automated integration, configuration, monitoring and adaptation of security and dependability mechanisms for such ecosystems. These mechanisms were specified using so-called SERENITY security and dependability (S&D) patterns that provide, among other important information, an interface to applications that shall use the patterns, rules that guide the monitoring of the patterns at runtime, and a specification of the S&D properties provided by the patterns. To this end, an S&D property specification language was defined.
Website	www.serenity-project.org
Timeline	2006–2009
EVITA partners involved	Fraunhofer SIT, K.U. Leuven

Basic elements of the security-requirements language and of the Security Modelling Framework of Fraunhofer SIT, which are applied in the EVITA project, are results of the SERENITY project. Specific instantiations of security properties, the Security Building Blocks, and the corresponding security-engineering process are extensions developed within the EVITA project.

The security and dependability property specification language of SERENITY has been used and extended to specify security properties relevant for the EVITA use cases [5]. Furthermore, the property language and the underlying Security Modelling Framework (SeMF) was the basis for the trust model and security engineering process developed within the EVITA project [6]. Finally, the property language will be used for the security evaluation of the EVITA architecture and protocols.

2.2.2 FORWARD

Brief description	FORWARD is a European FP7 coordination action. It aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of cyber-threats defences, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures.
Website	www.ict-forward.eu
Timeline	2008–2009
EVITA partners involved	EURECOM

The EVITA project proposal has been introduced (by Fraunhofer SIT) in an invited presentation at the 1st FORWARD Workshop in April 2008.

2.2.3 AVANTSSAR

Brief description	AVANTSSAR is a European FP7 project. It deals with the automated validation of trust and security of service-oriented architectures.
Website	www.avantssar.eu
Timeline	2008–2010
EVITA partners involved	–

Views on abstract secure channels have been exchanged with AVANTSSAR. It turned out that the AVANTSSAR approach is very different from what is needed in the EVITA project. AVANTSSAR focuses on services and abstract secure channels, while the EVITA project needs to take a closer look and to take into account also concrete hardware (in particular as far as trust and attack scenarios are concerned).

2.2.4 TERESA

Brief description	TERESA (Trusted Computing Engineering for Resource Constrained Embedded Systems (RCES) Applications) plans to define, demonstrate and validate an engineering discipline for trust that is adapted to resource constrained embedded systems. We define trust as the degree with which security and dependability requirements are met. TERESA has the following objectives: • Provide guidelines for the specification of sector-specific RCES trusted computing engineering. Software process engineers in a given sector can then use the guidelines to define a trusted computing engineering process that is integrated with the software engineering process used in their RCES sector. • Define a trusted computing engineering approach that is suited to the following sectors: Automotive; home control; industry control; metering
Website	www.teresa-project.org/
Timeline	2010–2012
EVITA partners involved	Trialog, Fraunhofer SIT, escrypt MIRA and BMW are involved in the advisory board.

TERESA can influence EVITA in the way security components are integrated in AUTOSAR. It will collect information from EVITA partners on typical automotive engineering process and investigate how patterns based processes can be used.

2.3 Liaison working groups

2.3.1 eSafety Forum and eSecurity WG

Brief description	The eSecurity Working Group was set up within the eSafety Forum as a discussion platform involving all stakeholders with two objectives: to discuss vulnerability aspects of electronics and communications in road transport while taking into account existing practice and emerging Research and Technology Development (RTD) initiatives, and to agree on recommendations to eliminate the vulnerabilities.
Website	www.esafetysupport.org/en/esafety_activities/esafety_working_groups/esecurity.htm
Timeline	2007–2010
EVITA partners involved	Trialog, K.U. Leuven, BMW F+T

The eSecurity WG has worked since 2007 on vulnerabilities of ITS systems. The eSecurity WG has operated on a voluntary basis, with several EVITA partners being active participants. The EVITA liaison workshop on 27 August 2009 featured a presentation (from Trialog) about the eSecurity Working Group of the eSafety Forum.

The eSecurity WG was closed in 2010 by the eSafety Forum after the publication of the approved WG report. However, the report concluded that another item of work had to be carried out in order to address privacy (more specifically, discuss recommendations for privacy-by-design). One of the chairs of the WG (Antonio Kung) sent an explanation to the European

Commission asking for advice. It is expected that, when a decision about continuation of this WG is made, activities related to it will be carried out in the PRESERVE project.

2.3.2 Article 29 Working Party

Brief description	The Working Party on the Protection of Individuals with regard to the Processing of Personal Data (also known as Article 29 Working Party) is based on Article 29 of "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". The Article 29 Working Party is operating with the help of the European Commission (DG Justice and Freedom). Its members are representatives of the member state data protection agencies. The Working Party provides opinion about directives from the commission in order to assess compliance with data protection principle.
Website	ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm
EVITA partners involved	Trialog, K.U. Leuven

Liaison with the Article 29 Working Party was mainly through the eSecurity WG of the eSafety Forum (see Section 2.3.1) with the objective to agree on measures to cope with privacy of location-oriented applications.

2.3.3 Car2Car Communication Consortium (C2C-CC)

Brief description	The Car 2 Car Communication Consortium is a non-profit organisation dedicated to increasing road traffic safety and efficiency by means of inter-vehicle communications.
Website	www.car-to-car.org
Timeline	since 2004
EVITA partners involved	BMW F+T, Fraunhofer SIT, Bosch, EURECOM, Continental

The C2C-CC Liaison Security Workshop in Wolfsburg on 5 November 2009 included a presentation about the EVITA project (from Bosch) to share EVITA results between the C2C-CC Security WG, COMeSafety, ETSI Security WG5, eSafety eSecurity WG, PRECIOSA and sim^{TD}.

The EVITA project successfully participated in the Car 2 Car Forum, the annual assembly of the members of the C2C-CC, on 23–24 November 2010 at Renault Square Com in Paris, France, and attracted broad interest. EVITA project results were presented in an exhibition booth (with poster, desk-top secure active-brake demonstration, and brochures) and were also presented at a workshop session. The presentation led to the creation of a taskforce on hardware security and assurance levels in the C2C-CC Security WG. EVITA project partners actively participated in this Taskforce "Secure hardware" of the C2C-CC Security WG. EVITA results had a bearing on the work of this taskforce.

The EVITA desktop and vehicle demonstrators were a major part of the exhibition at the Car 2 Car Forum on 24–25 November 2011 at the Honda Academy in Erlensee, Germany. The Car 2 Car Forum 2011 included an invited talk about EVITA in a plenary session. The chairman of C2C-CC Security WG gave a plenary presentation about "EVITA results in C2C-CC". This highlights the impact of the EVITA project on the work of the C2C-CC.

2.3.4 ETSI TC ITS WG 5

Brief description	ETSI TC ITS is responsible for standardisation to support the development and implementation of Intelligent Transport Systems (ITS) service provision, but not including ITS application standards, radio matters and electromagnetic compatibility. WG 5 is on security.
Website	portal.etsi.org/Portal_common/bottom.asp?TbId=711&SubTB=711&TABID=&Param=&qOSTB=702,%20707,%20708,%20709,%20710,%20711&qOTB=702
EVITA partners involved	EURECOM, Bosch

C2C-CC and ETSI TC ITS are working closely on different standardization activities. C2C-CC harmonized in general the input coming from their members based on the results of the projects within which they have been active. The harmonized input is shared with corresponding working groups at ETSI TC ITS and considered for standardisation. In this scope standardisation proposals and contributions based on the EVITA project are discussed within the C2C-CC during the harmonisation process. The result rightly serves as input to the ETSI TC ITS WG 5 via a close link between the ETSI TC ITS WG5 Security and the C2C-CC Security WG. The link between the two organisations is managed by a liaison officer, who is member of both organisations.

2.3.5 ISO/TC 22/SC 3/WG 16

Brief description	ISO TC 22 “Road vehicles”/SC 3 “Electrical and electronic equipment”/WG 16 “Functional safety” develops a new multipart standard ISO 26262 “Road vehicles – Functional safety”.
Website	www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=46752
EVITA partners involved	MIRA

The draft of ISO 26262 has been taken into account in the elicitation of security requirements in the EVITA project.

2.3.6 Motor Industry Software Reliability Association (MISRA)

Brief description	MISRA’s mission statement is to provide assistance to the automotive industry in the application and creation of within-vehicle systems of safe and reliable software.
Website	www.misra.org.uk
EVITA partners involved	MIRA

The MISRA guidelines for safety analysis of vehicle-based programmable systems have been taken into account in the elicitation of security requirements in the EVITA project.

2.3.7 HIS

Brief description	HIS (“Herstellerinitiative Software”) is an industry consortium. Its goal is to achieve and use joint standards for software modules, process maturity levels, software tests, software tools, and programming of control units.
Website	www.automotive-his.de
EVITA partners involved	BMW F+T, Bosch, escrypt

The EVITA consortium has checked whether the SHE (Secure Hardware Extension) specification of the HIS (Hersteller-Initiative Software) consortium would be applicable for EVITA and decided that it would be desirable to support the SHE interface as an additional interface to the more comprehensive EVITA hardware interface. The SHE compliance has been discussed within the [4] (Section 4.5.5)

2.3.8 CAMP VSC consortium

Brief description	The Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications (VSC) Consortium is an industry consortium sponsored by the US National Highway Traffic Safety Administration (NHTSA). The goal of CAMP is to accelerate the deployment of active safety features in the US by developing the pre-competitive enabling elements. CAMP is a mechanism for OEMs to work together, along with the US Department of Transport and suppliers, on specific research projects. The VSC project was established using the CAMP mechanism to evaluate vehicle safety applications enabled or enhanced by communications.
Timeline	since 2002

Several conference calls took place with participation of the EVITA partners escrypt, Trialog, and BMW in collaboration with the C2C-CC with the goal to establish a close link between the activities in order to harmonise the CAMP VSC approach with European approaches.

2.3.9 SAE Vehicle Electrical System Security Committee

Brief description	The SAE (Society of Automobile Engineers) Vehicle Electrical System Security Committee is responsible for developing and maintaining Recommended Practices and Information Reports in the area of vehicle electrical systems' security. The committee's scope is on-board vehicle electrical systems that affect vehicle control or otherwise act contrary to the occupants' interests if the systems are manipulated by an attacker. The goals of the committee are to identify and recommend strategies and techniques related to preventing and detecting adversarial breaches, and mitigating undesirable effects if a breach is achieved.
Website	www.sae.org/servlets/works/committeeHome.do?comtID=TEVEES18

MIRA made a presentation about the EVITA project to the SAE Vehicle Electrical System Security Committee on 4 August 2011 in Troy, MI, USA.

2.3.10 Embedded Systems WG of the TCG

Brief description	Although the TPM already is used in a number of non-PC applications, including digital copiers, kiosks, gaming systems, and industrial systems, the Embedded Systems WG of the TCG (Trusted Computing Group) will facilitate the continued evolution of Trusted Computing as a source for security in these markets and to help facilitate the ecosystem to support the concepts of a hardware root of trust.
Website	www.trustedcomputinggroup.org/developers/embedded_systems
Timeline	since 2011

EVITA has been presented at a meeting of the Embedded Systems WG of the TCG in Munich. At the EVITA Workshop on Security of Automotive On-Board Networks on 23 November 2011 in Erlensee, the chairman of the Embedded Systems WG of the TCG, gave the keynote address on "Trusted computing for mobile and embedded systems".

3 Dissemination

3.1 Publications and Presentations

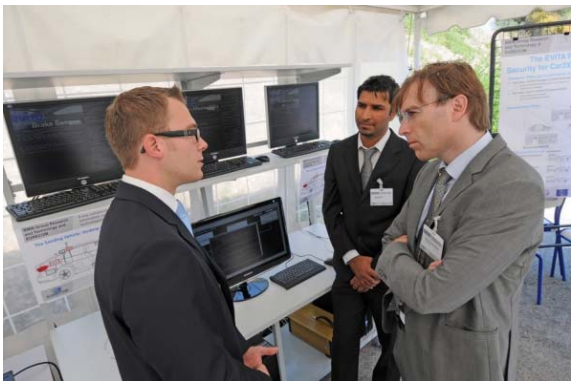
The following publications and presentations about aspects of the EVITA project have been accepted and given at conferences and workshops:

- M. Wolf: Vehicular security hardware. In: 6th escar (Embedded Security in Cars) Conference. Hamburg, Germany (November 2008)
- A. Fuchs and R. Rieke: Identification of authenticity requirements in systems of systems by functional security analysis. In: Workshop on Architecting Dependable Systems at the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-2009). Estoril, Lisbon, Portugal (June 2009)
- M. Wolf: Designing secure automotive hardware for enhancing traffic safety. In: *CAST Workshop "Mobile Security for Intelligent Cars"*. Darmstadt, Germany (27 August 2009)
- T. Kosch: Privacy and Data Protection for Drivers: A Contribution from the EVITA project. In: *ITS World Congress*. Stockholm, Sweden (September 2009)
- A. Weimerskirch, K. Schramm, L. Wolleschensky, T. Wollinger: The dilemma of data security, privacy, control and liability in V2X. In: *ITS World Congress*. Stockholm, Sweden (September 2009)
- B. Weyl, O. Henniger, A. Ruddle, H. Seudié, M. Wolf, and T. Wollinger: Securing vehicular on-board IT systems: The EVITA Project. In: *25th VDI/VW Automotive Security Conference*. Ingolstadt, Germany (October 2009)
- F. Stumpf, B. Weyl, C. Meves, M. Wolf: A security architecture for multipurpose ECUs in vehicles. In: *25th VDI/VW Automotive Security Conference*. Ingolstadt, Germany (October 2009)
- O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl: Security requirements for automotive on-board networks. In: *9th International Conference on ITS Telecommunication*. Lille, France (October 2009)
- H. Seudié: Vehicular on-board security: EVITA project. In: *C2C-CC Forum* Wolfsburg, Germany (4 November 2009)
- H. Seudié: Vehicular on-board security: EVITA project. In: *C2C-CC Liaison Security Workshop*. Wolfsburg, Germany (5 November 2009)
- O. Henniger and H. Seudié: EVITA-project.org: E-safety vehicle intrusion protected applications. In: *7th escar (Embedded Security in Cars) Conference*. Düsseldorf, Germany (November 2009)
- L. Apvrille, O. Henniger, Y. Roudier, H. Seudié, B. Weyl, M. Wolf: Secure Automotive On-Board Electronics Network Architecture, (Poster summary), In: *33rd FISITA 2010 World Automotive Congress*, Budapest, Hungary, May 30 – June 4, 2010.
- A. Groll, J. Holle, M. Wolf, T. Wollinger: Next Generation of Automotive Security: Secure Hardware and Secure Open Platforms. In: *17th ITS World Congress*. Busan, South Korea (October 2010)
- D. Knorreck, L. Apvrille, and R. Pacalet: Partitioning of in-vehicle systems-on-chip: a methodology based on DIPLODOCUS. In: *13th Sophia-Antipolis MicroElectronics Forum, SAME 2010*. Sophia-Antipolis, France (October 2010)

- G. Pedroza, L. Apvrille, R. Pacalet: Formal security model for verification of automotive embedded applications. In: *3rd Annual SAFA Workshop, SAFA 2010*. Sophia-Antipolis, France (October 2010)
- H. Seudié: Use Case: Hazardous Location Warning: Security. In: *C2C Forum* Paris, France (November 2010)
- M.S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger: Secure automotive on-board protocols: A case of over-the-air firmware updates. In: *3rd International Workshop on Communication Technologies for Vehicles*, Oberpfaffenhofen, Germany (March 2011)
- H. Schweppe, B. Weyl, Y. Roudier, M.S. Idrees, T. Gendrullis, M. Wolf: Securing car2X applications with effective hardware-software co-design for vehicular on-board networks. In: *27th VDI/VW Automotive Security Conference*, Berlin, Germany (October 2011), VDI-Bericht 2131, pp. 45-57
- G. Pedroza, L. Apvrille, D. Knorreck: AVATAR: A SysML environment for the formal verification of safety and security properties. In: *11th International Conference on New Technologies of Distributed Systems (NOTERE)*, Paris, France (May 2011)
- H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, D. Scheuermann: Car2X communication – Securing the last meter. In *4th International Symposium on Wireless Vehicular Communications (WIVEC 2011)*, San Francisco, CA, USA (September 2011)
- G. Pedroza, M.S. Idrees, L. Apvrille, Y. Roudier: A formal methodology applied to secure over-the-air automotive applications. In *74th IEEE Vehicular Technology Conference (VTC2011-Fall)*, San Francisco, CA, USA (September 2011)
- T. Gendrullis, M. Wolf: Design, Implementation, and Evaluation of a Vehicular Hardware Security Module. In: *14th International Conference on Information Security and Cryptology* (ICISC 2011), Seoul, South Korea (November–December 2011)

3.2 Public Demonstrations

EURECOM and BMW F+T presented the EVITA vehicle demonstrator at the EURECOM press event in October 2011 in Sophia-Antipolis.



BMW F+T, escrypt, and EURECOM showed the EVITA vehicle demonstrator and desktop demonstrator at the 9th International Embedded Security in Cars (escar) conference in Dresden on 9–10 November 2011.

Finally, the consortium showed the desktop and vehicle demonstrators that were developed in EVITA at the Final EVITA Workshop on Security of Automotive On-Board Networks on 23 November 2011 and at the Car 2 Car Forum on 24–25 November 2011 at the Honda Academy in Erlensee.

4 Conclusions

EVITA has carried out liaison work in the relevant domains and has established links towards various projects and initiatives. In addition, dissemination of EVITA results at conferences supported the distribution of results toward other projects. The liaison and dissemination work further assured to incorporate valuable feedback, such as compliance with other initiatives, e.g. the SHE specification.

The results of EVITA are direct input to the PRESERVE project, which will in turn liaise with FOT projects in order to provide a security enabler.

References

[1] E. Kelling, M. Friedewald, T. Leimbach, M. Menzel, P. Saeger, H. Seudié, and B. Weyl, Specification and evaluation of e-security relevant use cases. Deliverable D2.1 of EVITA, 2009.

[2] S. Idrees, Y. Roudier, H. Schweppe, B. Weyl, R. El Khayari, O. Henniger, D. Scheuermann, H. Seudié, H. Platzdasch, Secure on-board protocols specification. Deliverable D3.3 of EVITA, 2010.

[3] SeVeCom Consortium. Baseline Security Specification. Deliverable 2.1-App.A, 2009.

[4] B. Weyl, M. Wolf, F. Zweers, T. Gendrullis, M.S. Idrees, Y. Roudier, H. Schweppe, H. Platzdasch, R. El Khayari, O. Henniger, D. Scheuermann, A. Fuchs, L. Apvrille, G. Pedroza, H. Seudié, J. Shokrollahi, A. Keil. Secure On-Board Architecture Specification, EVITA Deliverable D3.2, 2010.

[5] A. Ruddle, D. Ward, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henniger, R. Rieke, M. Ritscher, H. Broberg, L. Apvrille, R. Pacalet, and G. Pedroza, Security requirements for automotive on-board networks based on dark-side scenarios. Deliverable D2.3 of EVITA, 2009.

[6] C. Jouvray, A. Kung, M. Sall, A. Fuchs, S. Gürgens, and R. Rieke, Security and trust model. Deliverable D3.1 of EVITA, 2009.