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 D1.2.7:
Final dissemination strategy

Authors:	Olaf Henniger, Roland Rieke (Fraunhofer Institute SIT); Benjamin Weyl (BMW Group Research and Technology GmbH); Marko Wolf (escrypt GmbH); Michael Friedewald (Fraunhofer Institute ISI); Alastair Ruddle (MIRA); Hervé Seudié (Robert Bosch GmbH); Antonio Kung (Trialog); Enno Kelling (Continental Teves AG & Co. oHG); Yves Roudier (EURECOM); Ludovic Apvrille (Institut Télécom); Wolfgang Wiewesiek (Fujitsu Semiconductor Europe GmbH)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Date:	1 April 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. In order to enable the broadest possible uptake of the project results, key documents of the EVITA project are released as open specifications. This dissemination strategy addresses how to systematically distribute the project results through a variety of communication channels to potential users in order to ensure their broad utilisation.

Contents

List of tables

Document history

Version	Date	Changes
D1.2.1v1.0	2008-12-11	Draft dissemination strategy released
D1.2.1v1.1	2009-12-4	Disposition of the comments received at the first EVITA project review; Update of the table of events where EVITA results may be submitted
D1.2.4v1.0	2010-05-14	Mid-term dissemination strategy released
D1.2.4v1.1	2011-01-05	Correction of EVITA contacts to potential liaison working groups and initiatives.
D1.2.7v1.0	2012-04-01	Final dissemination strategy released

1 Introduction

The EVITA project aims at designing, verifying, and prototyping security building blocks for automotive on-board networks. Thus, it provides a basis for secure deployment of electronic safety aids based on vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communication.

This report describes the final EVITA dissemination strategy. It is based on the EVITA description of work and draft and mid-term dissemination strategies reviewed by independent reviewers. This report is structured as follows: Section 2 determines the purpose and objectives of the dissemination efforts for the EVITA project. Section 3 describes the potential users targeted by the dissemination activities. Section 4 identifies the basic elements of the projected content to be disseminated. Section 5 describes the channels through which the content can best be delivered to potential users. Section 6 describes activities that the EVITA partners are committed to carry out. Section 7 describes how to evaluate the success of the dissemination activities.

2 Purpose and objectives of dissemination efforts

The purpose of the dissemination activities is to assure a broad utilisation of EVITA results in the automotive industry and to establish a basis for a standard for secure automotive sensor/ actuator networks. A standardised solution 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;
- On the basis of a standard, third-party semiconductor manufacturers will be able to independently start a chip development and consecutive production.

To achieve a broad utilisation of the EVITA results, the objectives are:

- Distribution of public EVITA deliverables outside the consortium;
- Dissemination of EVITA results via publications and exhibitions;
- Establishment of liaisons to achieve multilateral synergies and contributions to the activities of liaison organisations on topics related to in-vehicle security.

3 Potential beneficiaries of EVITA results

3.1 Primary 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 Car 2 Car Communication Consortium (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.

3.2 Secondary beneficiaries

Secondary beneficiaries of the 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 hardware security module (HSM) in the EVITA project will help many embedded applications to efficiently improve their security.

4 Content to be disseminated

All key documents of the EVITA project are released as public reports in order to enable maximum benefits and the broadest possible uptake. As exceptions to this rule, the following restrictions apply:

1. Premature results are not released to the public.
2. Proprietary implementations of the public architecture and protocols are not publicly released.

Table 1 lists all deliverables available to third parties. Some deliverables are marked "restricted" and will be made available to third parties only after the agreement of the EVITA consortium. Especially other automobile manufacturers and suppliers are third parties to whom the consortium intends to give additional input regarding implementation details.

Table 1 List of deliverables available to third parties

Del. no.	Deliverable name	Dissemination level	Nature
D0	Final public report	Public	Report
D1.2.2	Public area of project website	Public	Other
D1.2.5.1	Presentation slides of EVITA dissemination workshop	Public	Other
D1.2.5.2	Presentation slides of final EVITA workshop	Public	Other
D1.2.6	Final liaisons documentation	Public	Report
D1.2.7	Final dissemination strategy – final	Public	Report
D2.1	Specification and evaluation of e-safety use cases	Public	Report
D2.3	Security requirements based on dark-side scenarios	Public	Report
D2.4	Legal framework and requirements report	Public	Report
D3.1.2	Security and trust model	Public	Report
D3.2	Secure on-board architecture specification	Public	Report
D3.3	Secure on-board protocols specification	Public	Report
D3.4.3	Architecture and protocols verification	Public	Report
D3.4.4	Attack analysis	Public	Report
D4.0.3	Security architecture implementation – Progress report V1.0	Public	Report
D4.1.1	Hardware implementation specification	Restricted	Report
D4.2.3	LLD modelling, verification, and automatic C-code generation	Public	Report
D4.4.2	Test results	Public	Report
D5.1.1	On-board communication demonstrator specification	Restricted	Report
D5.1.2	On-board communication demonstrator	Public	Demonstrator

In order to assure the quality of deliverables, deliverables are checked by at least two reviewers from the EVITA consortium during their development.

5 Dissemination channels

5.1 Overview

To ensure a comprehensive and appropriately targeted dissemination, the EVITA consortium uses a variety of communications channels:

– website,

– liaisons with other working groups and project consortia,

– publications,

– workshops and exhibitions,

– brochures,

– promotional video,

– direct communication.

5.2 Website

To make the EVITA deliverables and public presentations readily accessible, the website evita-project.org has been established. It is used as the primary dissemination channel to the public and as an archive for public information about EVITA. It allows potential users to access EVITA deliverables and publications whenever they need them. In order to keep track of the dissemination of the EVITA deliverables, downloading public EVITA deliverables from the website requires registration with a valid e-mail address. The website will be maintained for at least 5 years after the project start.

5.3 Liaisons with other working groups and project consortia

To achieve multilateral synergies, the EVITA consortium liaised with other initiatives dealing with aspects of V2X communication and into which potential users of the EVITA results are already tied in. Table 2 alphabetically lists working groups with which liaisons have been established and the points of contact responsible for dissemination activities of the EVITA consortium. In particular, EVITA results are introduced into industry consortia such as the Car 2 Car Communication Consortium, which harmonises the contributions received and forwards them to standardisation bodies such as ETSI TC ITS for formal standardisation.

Table 3 alphabetically lists project consortia potentially taking up EVITA results. In particular, a cooperation agreement between the EVITA and PRESERVE consortia is intended to be signed, expressing their interest to cooperate with the goal to enable integration of EVITA results into the V2X security subsystem that is currently being developed in the PRESERVE project.

Table 2 Liaison working groups

Liaison organisation	Link	Description	Contact from EVITA
Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data)	ec.europa.eu/justice/data-protection/article-29/index_en.htm	The 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". It gives advice about the level of data protection in the European Union and third countries.	Trialog, K.U. Leuven
Car 2 Car Communication Consortium / Security Working Group	www.car-to-car.org	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.	BMW F+T, Bosch, Continental, EURECOM, Fraunhofer SIT
Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications Consortium (VSCC)	www.nhtsa.dot.gov	CAMP VSCC 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 precompetitive 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.	escrypt
ETSI TC ITS WG 5 Security	portal.etsi.org/Portal_common/bottom.asp?TbId=711&SubTB=711&TABID=&Param=&qOSTB=702,%20707,%20708,%20709,%20710,%20711&qOTB=702	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.	Bosch, Continental, EURECOM, Fraunhofer SIT
HIS consortium	www.automotive-his.de/	HIS 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.	BMW F+T
ISO/TC 22/SC 3/WG 16	www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=46752	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".	MIRA, BMW F+T
MISRA group	www.misra.org.uk	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.	MIRA

Liaison organisation	Link	Description	Contact from EVITA
SAE (Society of Automobile Engineers) Vehicle Electrical System Security Committee	www.sae.org/servlets/works/committeeHome.do?comtID=TEVEES18	This 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.	MIRA
TCG (Trusted Computing Group) Embedded Systems WG	www.trustedcomputinggroup.org/developers/embedded_systems	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 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.	BMW F+T, Fraunhofer SIT

Table 3 Liaison projects

Liaison organisation	Link	Description	Contact from EVITA
OVERSEE consortium	www.oversee-project.com/	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.	escrypt, Trialog
PREDIT groups	www.predit.prd.fr	PREDIT is a French programme of research, experimentation and innovation in land transport.	Institut Télécom
PRESERVE consortium	www.preserve-project.eu	The European FP7 collaborative project PRESERVE (Preparing secure V2X communication systems) contributes to the security and privacy of future V2X communication systems by addressing critical issues like performance, scalability, and deployability of V2X security systems.	Fraunhofer SIT, Trialog, escrypt
SEIS consortium	www.eenova.de/projekte/seis	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.	BMW F+T, Bosch, Continental, Fraunhofer SIT, Infineon

5.4 Publications

After project completion, project results will be published in journals and as PhD theses. Table 4 lists journals where EVITA results are planned to be submitted.

Table 4 Targeted journals

Journal	Link
IEEE Intelligent Transportation Systems Magazine	sites.ieee.org/itss/introduction/magazine/
IEEE Transactions on Intelligent Transportation Systems	sites.ieee.org/itss/introduction/transactions/
IEEE Transactions on Vehicular Technology	ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=25
IET Intelligent Transport Systems	digital-library.theiet.org/IET-ITS

During the project, results have been presented at conferences. A list of academic and industry events where EVITA results have been presented can be found in the final liaison documentation (EVITA deliverable D1.2.6).

Jointly developed results are also published jointly. Before the submission of papers, the other project partners involved must be notified and be given opportunity to comment and contribute.

5.5 Exhibitions

During the project, demonstrators have been presented at workshops and exhibitions. A list of events where the EVITA demonstrators have been presented can be found in the final liaison documentation (EVITA deliverable D1.2.6).

After the end of the project, EVITA partners involved in WP5000 (Demonstration) plan a joint demonstration with the PRESERVE project and possibly also the OVERSEE project at the ITS World congress in Vienna in October 2012. The demonstration is planned to be based on EVITA demonstrators using HSM prototypes developed in PRESERVE.

5.6 Brochures

A brochure (frequently asked questions about secure automotive on-board networks and answers) and flyers have been produced and are distributed along workshops, conferences, and exhibitions.

5.7 Promotional video

After editing, footage of the live-demonstrations at the Car 2 Car Forum on 24–25 November 2011 at the Honda Academy in Erlensee will be made available via the EVITA website.

If approved by the European Commission, the promotional animation video shown at the Final EVITA Workshop and the Car 2 Car Forum 2011 will also be put on the website.

5.8 Direct communication

The partners directly inform automobile manufacturers, truck manufacturers, and automotive electronics suppliers of the project results, making sure that awareness is high.

6 Planned activities per partner

6.1 BMW Group Research and Technology GmbH

The EVITA results are exploited and used in further in-house development projects. Given the typical duration of automotive development cycles (research, pre-development, series development), a couple of years are still to pass before the research results will be ‘on the road’.

6.2 Continental Teves AG & Co. oHG

Continental Teves has already started and will continue to exploit the results of EVITA in all electronics development departments within the Continental Automotive Group. This is done via the Continental Automotive Security Working Group led by Stefan Goetz. Every Business Unit will be able to take the results into account when developing new generations of their products or systems according to customer needs. The EVITA results are a good basis for discussions with customers and silicon and service suppliers.

Stefan Goetz will also bring the results into the C2C-CC Security Working Group where he is actively participating.

6.3 escrypt GmbH

Escrypt applies EVITA knowledge and results with their customers and potential customers in the automotive industry (OEMs and suppliers) in Europe, Asia and the United States. Thus, EVITA has notably helped escrypt to improve and enhance their visibility and reputation in the area of automotive security all over the world. Furthermore, escrypt also tries to transfer EVITA knowledge and experiences to related industries, such as earthmoving machines/ heavy utility vehicles and harvesting machines. Escrypt helps major semiconductor manufacturers to implement the EVITA specification into real industrial product realizations of HSMs. Escrypt further advises their numerous customers from industry automation and from the health/medical area to apply EVITA results to their products to increase their IT security, for instance, for securing machine-to-machine (M2M) communications or enhancing privacy of medical data.

Escrypt will also transfer and advance their EVITA knowledge and experience into ongoing related research projects, in particular, the OVERSEE project and the PRESERVE project, but also into all related future research projects.

Within the EVITA project escrypt has also gained new knowledge and valuable experience in the areas of automotive security design, (hardware and software) security architectures, and automotive security engineering, which escrypt will reuse in upcoming projects in various different industry sectors.

6.4 EURECOM

Two PhD theses are expected to be defended in 2012 out of the topics investigated in the EVITA project and further publications are expected. EURECOM also plans to exploit their know-how from the EVITA project in other ITS research projects to which they contribute. This will in particular be the case for the French field-operational test SCORE@F (Système

Coopératif Routier Expérimental Français) and in relationship with the C2C-CC. EURECOM also plans to further contribute to the standardisation work in ETSI TC ITS WG 5. Furthermore, EURECOM plans to develop tools for security testing in particular in collaboration with Institut Télécom. Research in this area will be based on the experimental results obtained during code validation in EVITA. Finally EURECOM plans to exploit EVITA results in teaching, in security or distributed software courses, as well as in a curriculum on ITS envisioned in the coming years.

6.5 Fraunhofer Institute for Secure Information Technology

Within the Embedded Systems Work Group of the Trusted Computing Group, Fraunhofer SIT will actively contribute to the development of standards for trusted computing in embedded systems. A journal paper summarising EVITA results is in preparation. The EVITA results are planned to be exploited through consultancy assignments with industry. Fraunhofer SIT also transfers EVITA results into the PRESERVE project.

6.6 Fujitsu Semiconductor Embedded Solutions Austria GmbH

FEAT developed low level software drivers for the EVITA demonstrators. The knowledge obtained throughout the membership (started mid of 2010) will be utilized in creating standardised software modules for the automotive market. In first place this will be a host driver for a newly developed hardware IP from FSEU that supports the EVITA light category. By providing standard drivers to automotive tier-1 and OEM, the dissemination of cryptographic know-how is fostered and the utilization of cryptographic methods is made as simple as possible. FEAT will also develop the software for cryptographic successor IPs.

6.7 Fujitsu Semiconductor Europe GmbH

FSEU started already before their membership in EVITA (joined mid of 2010) the development of a low-cost embedded cryptographic hardware IP. With the partners at EVITA this development prospered essentially. Assessment of requirements and review of the specification of that new IP gained in quality. Shortly after the EVITA project ended, FSEU has an FPGA-based implementation in place which meets a little more than EVITA light category requires. The IP satisfies SHE requirements. At the Embedded World fair in Nuremberg on 28 February and 1 March 2012, FSEU presented their development to the public. In the second quarter of 2012, first 32-bit microcontrollers with embedded cryptographic engine will be shipped to lead customers.

6.8 Infineon Technologies AG

Infineon announced that the next generation of their microcontrollers (which will become available 2014/15) will include a first HSM implementation based on EVITA specifications.

6.9 Institut Télécom

Institut Télécom has already made new official releases of TTool (ttool.telecom-paristech.fr) that include new features developed in the scope of EVITA. In particular, TTool now implements the AVATAR profile, based on SysML. From an AVATAR model, formal security proofs can be conducted. Also, executable code can be automatically generated. Those new features are therefore available to other users of TTool, and are expected to be reused in the future for other embedded system domains, in particular aeronautics. Several publications and PhD theses are expected in 2012 on those new features.

The overall methodological work achieved with EURECOM will also be continued. This includes particularly security extensions for requirements management: Efficient security requirement capture, security requirement tracing and refinement at design and testing level. Publications and PhD theses are expected in that field, as well as research and industrial collaborations.

6.10 MIRA Ltd.

MIRA will, where appropriate, include consideration of possible security issues in future functional safety assessment services for customers in the automotive sector and for other industries with similar safety and security issues. It is expected that this will lead to further development and refinement of the unified approach to safety and security risk analysis that was piloted by MIRA in the EVITA requirements engineering activities.

In addition, MIRA will continue to liaise with relevant standardization bodies, such as the SAE Vehicle Electrical System Security Committee, US National Highway Traffic Safety Administration, and MISRA (Motor Industry Software Reliability Association), in order to promote risk-based approaches for assessing security threats to on-board automotive systems.

6.11 Robert Bosch GmbH

Bosch announced that the next generation of their Engine Control Units (which is expected for end of 2014) will include an HSM implementation based on EVITA specifications. Bosch also brings EVITA results into the C2C-CC Security Working Group.

6.12 TRIALOG

TRIALOG will transfer EVITA results into the PRESERVE and OVERSEE projects and liaise with other related initiatives in the field of V2X communication.

7 Success criteria and conclusions

By following this strategy, it will be ensured that the dissemination and exploitation efforts achieve the goal of a broad utilisation of the EVITA results. The dissemination activities will be successful if relevant stakeholders consider EVITA results as a basis for a standard for secure automotive sensor/actuator networks or for product development.