QUARTERLY PROGRESS REPORT

Grant Agreement number: 224275

Project acronym: EVITA

Project title: E-safety vehicle intrusion protected applications

Funding Scheme: Collaborative project

Date of preparation of the latest version of Annex I: 4 February 2011

Quarter covered: from 1 July 2011 to 30 September 2011

Project co-ordinator name, title and organisation: Dr.-Ing. Olaf Henniger, Fraunhofer Institute for Secure Information Technology

Tel.: +49 6151 869 264

Fax: +49 6151 869 224

E-mail: olaf.henniger@sit.fraunhofer.de

Project website address: http://evita-project.org

1 Work progress and achievements during the quarter

1.1 WP1000 (RTD/scientific coordination and dissemination/ external interfaces)

1.1.1 T1100 (RTD/scientific coordination)

What has been achieved?

– Organisation of meetings and conference calls.

Status: On schedule, no problems.

1.1.2 T1200 (Public dissemination and external interfaces)

What has been achieved?

– EVITA demonstrators and a project summary were presented at the BMW/EURECOM press event on 30 September in Sophia Antipolis, France. See the press release: http://www.eurecom.fr/resources/documents/0_Institut/Media_Kit/communiques/2011_BMWEURECOM_EN.pdf.

– Preparation of the EVITA demonstration at the escar Conference 9–10 November 2011 in Dresden, Germany

– Preparation of the EVITA final workshop and final review on 23 November 2011 at the Honda Academy in Erlensee, Germany

– The following papers related to EVITA have been presented:

  • H. Schweppe[1], Y. Roudier[1], B. Weyl[2], L. Apvrille[3], D. Scheuermann[4]: Car2X communication – Securing the last meter. In *4th International Symposium on Wireless Vehicular Communications (WIVEC 2011)*, 5–6 September 2011, San Francisco, CA, USA

  • G. Pedroza[3], M.S. Idrees[1], L. Apvrille[3], Y. Roudier[1]: A formal methodology applied to secure over-the-air automotive applications. In *74th IEEE Vehicular Technology Conference (VTC2011-Fall)*, 5–8 September 2011, San Francisco, CA, USA

  • H. Schweppe[1], T. Gendrullis[5], M.S. Idrees[1], Y. Roudier[1], B. Weyl[2], M. Wolf[5]: Securing car2X applications with effective hardware-software co-design for vehicular on-board networks. In *27. VDI/VW-Gemeinschaftstagung Automotive Security*, 11–12 October, 2011, Berlin, Germany

[1] EURECOM

[2] BMW F+T

[3] Institut Télécom

[4] Fraunhofer Institute SIT

[5] escrypt

– Liaison activities with
  - C2C-CC WG SEC (Security Working Group of the Car 2 Car Communication Consortium):
    - Presentation and discussion of EVITA progress and results at the meeting of C2C-CC WG SEC in Paris on 11–12 July 2011;
    - active membership in hardware security task force of C2C-CC
  - SAE (Society of Automobile Engineers) Vehicle Electrical System Security Committee: David Ward[6] was invited to make, and made, a presentation about the EVITA project to this committee on 4 August 2011 in Troy, MI, USA.
  - European project PRESERVE:
    - Further discussion of cooperation agreement: Who beyond the PRESERVE project needs what kind of Access Rights to which EVITA Foreground and Background? The PRESERVE demonstrators should be useable also after the end of the PRESERVE project. The PRESERVE prototypes should be useable by third parties in field-operational tests outside the PRESERVE project.
    - FEAT agreed to grant Access Rights to the source code of the HSM low-level drivers developed in EVITA to PRESERVE partners for the purposes of the PRESERVE project even before the general cooperation agreement has been signed.
    - Personal meetings, telephone interviews, and telephone conferences
  - European project OVERSEE: Personal meetings, telephone interviews, and telephone conferences;
– The results of EVITA and their possible use have been discussed with
  - costumers and potential customers in the automotive industry (OEMs and suppliers)
  - several research institutes in Europe.

Status: On schedule, no problem

1.2 WP2000 (Security requirements engineering)

1.2.1 T2100 (E-security relevant use cases)

Status: Finished

1.2.2 T2200 (Dark-side scenarios)

Status: Finished

1.2.3 T2300 (Security requirements analysis)

Status: Finished

[6] MIRA

1.2.4 T2400 (Legal framework and requirements)

What has been achieved?

– Deliverable D2.4 “Legal framework and requirements on automotive on-board networks” has been completed and submitted in electronic form.

– The envisaged schematic overview of requirements, potential risks, and obligations relating to different possible use cases and dark side scenarios remained unfinished and has been skipped.

Status: Finished

1.3 WP3000 (Secure on-board architecture design)

1.3.1 T3100 (Adapted security and trust model)

Status: Finished

1.3.2 T3200 (Secure on-board architecture)

What has been achieved?

– Update of HSM specification in D3.2 “Secure On-Board Architecture Specification” based on experiences from WP4000.

Status: Finished

1.3.3 T3300 (Secure on-board protocols)

What has been achieved?

– Update of D3.3 “Secure On-Board Protocols Specification” based on feedback from T3400.

Status: Finished

1.3.4 T3400 (Model-based verification)

Status: Finished

1.4 WP4000 (Security architecture implementation)

1.4.0 General

What has been achieved?

– Bi-weekly joint conference calls on WP4000 and WP5000

– Deliverable D4.0.3 “Security Architecture Implementation – Progress Report” has been completed, internally reviewed, finalised and submitted in electronic form.

1.4.1 T4100 (Security hardware)

What has been achieved?

– Bug-fixing and updating of the implementation of HSM firmware and library on PowerPC of FPGA

Status: Finished

1.4.2 T4200 (Basic software)

What has been achieved?

– Secure boot realization

– Trialog has continued to test the functionality of the HSM low-level drivers (LLD).

– FEAT fixed bugs and updated the HSM LLD.

– Institut Télécom has continued modelling the HSM LLD. The UML/SysML models now better reflect the control part of the drivers. A document describing how to generate C code from driver models has been drafted.

Status: Finished, except for LLD modelling and model-based code generation

– The delay of LLD modelling and model-based code generation does not affect the rest of the tasks because a hand-made LLD is available.

1.4.3 T4300 (Security library)

What has been achieved?

– Successful implementation, test, debugging, and incremental integration into Software Security Framework EMVY of

  • KMM (Key Master Module)

  • PDM (Policy Decision Module)

  • CAN/TP gateway

  • CCM (Communication Control Module) group communication

  • SSM (Secure Storage Module)

  • EMVY extensions for testing purposes

– Replacing HSM simulator with HSM hardware

– Successful implementation, test, and debugging of Ethernet interface of HSM firmware

– Specification, design, implementation, test, debugging, and integration of the Linux HSM driver

– Integration activities in AUTOSAR Stack

Status: Behind schedule

– Technical problems during the integration of the different components caused delays. Nevertheless, several intermediate versions of the Security Library have been available since June 2011.
– The original implementation plan was based on a microcontroller (as ECU), a FPGA (as HSM) and HSM LLD to enable the communication between both hardware devices. The software components running on the microcontroller had to be integrated into the AUTOSAR environment. Due to requirements from the vehicle demonstrators, the implementation was extended to Linux and TCP/IP components running on the microcontroller, which caused additional efforts and delay with respect to the original time schedule. The interfaces had to be adapted since the Linux HSM driver and the HSM LLD are using the same ASN.1 interface.
– What will be done: A desktop demonstration of a secure communication using the HSM FPGA communicating via the HSM LLD in an AUTOSAR environment will be set up till the final review.

1.4.4 T4400 (Code validation)

What has been achieved?

– Successful implementation, test, debugging, and incremental integration of the SWD (Security Watchdog) and associated protocol implementations into EMVY
– Manual inspection and testing of the source code, in particular of drivers, which has already resulted in the finding of some vulnerabilities
– Development of testing tools, notably fuzzers
– Automated testing has started

Status: On schedule

– Incremental tests of subsystems as they become available.

1.5 WP5000 (Demonstration)

What has been achieved?

– Bi-weekly joint conference calls on WP4000 and WP5000
– The deliverable D5.1.1 “Demonstrator specification” has been completed, internally reviewed, finalized, and submitted in electronic form.
– Implementation of Sensor/ECU applications for the demonstration
– Successful emulation of the simTD security daemon software library with the EVITA HSM
– Desktop demonstrator is working with key establishment and secure communication between Active-Brake Sensor and Active-Brake ECU using a Key Master ECU for key distribution and policy decision.

– All ECUs are running with FPGA HSMs and TCP/IP interface.

– simTD CCU is integrated into demonstration vehicle and uses an FPGA HSM as well. It secures car2X messages with EVITA hardware. The messages are received in the vehicle and signatures verified accordingly.

– A GUI has been implemented in order to show the actual/real process flow of key distribution and secured communication for the Active-Brake scenario.

– Valet-parking scenario has been integrated in the car; privacy policies can be configured on a CE application and transmitted to the vehicle, where the policy is enforced.

Status: On schedule, except for CAN communication and AUTOSAR integration

2 Deliverables and milestones tables

2.1 Deliverables

Table 1 lists all deliverables based on the revised Description of Work and indicates whether they have already been delivered.

Table 1 List of deliverables

Del. no.	Deliverable name	WP no.	Lead participant	Nature[7]	Dissemination level[8]	Due delivery date from Annex I	Delivered Yes/ No	Actual/ forecast delivery date	Comments
D0	Final public report	000	FRAUNHOFER (SIT)	R	PU	2011-12-31	No	2011-12-31	
D1.2.1	Draft dissemination strategy	1000	FRAUNHOFER (SIT)	R	PU	2008-10-31	Yes	2008-12-11	Version 1.1: 2009-12-04
D1.2.2	Public area of project website	1000	FRAUNHOFER (SIT)	O	PU	2008-10-31	Yes	2008-11-7	
D1.2.3	Mid-term liaisons documentation	1000	TRIALOG	R	PU	2010-02-28	Yes	2010-03-01	Version 1.1: 2010-03-11
D1.2.4	Mid-term dissemination strategy	1000	FRAUNHOFER (SIT)	R	PU	2010-04-30	Yes	2010-05-14	Version 1.1: 2011-01-05
D1.2.5	Project workshop	1000	FRAUNHOFER (SIT)	O	PU	2010-06-30	Yes	2010-07-01	
D1.2.6	Final liaisons documentation	1000	TRIALOG	R	PU	2011-12-31	No	2011-12-31	
D1.2.7	Final dissemination strategy	1000	FRAUNHOFER (SIT)	R	PU	2011-12-31	No	2011-12-31	
D2.1	Specification and evaluation of e-security relevant use cases	2000	CONTINENTAL TEVES	R	PU	2009-02-28	Yes	2009-03-04	Version 1.2: 2009-12-30

[7] **R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

[8] **PU** = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)

Del. no.	Deliverable name	WP no.	Lead participant	Nature[7]	Dissemination level[8]	Due delivery date from Annex I	Delivered Yes/ No	Actual/ forecast delivery date	Comments
D2.3	Security requirements based on dark-side scenarios	2000	MIRA	R	PU	2009-03-31	Yes	2009-03-31	Version 1.1: 2009-12-30
D2.3	Legal framework and requirements report	2000	K.U. Leuven	R	PU	2011-06-30	Yes	2011-09-13	Version 1.1: 2011-09-19
D3.1.1	Security and trust model – Draft	3000	TRIALOG	R	PU	2009-06-30	Yes	2009-07-15	
D3.1.2	Security and trust model	3000	TRIALOG	R	PU	2009-11-30	Yes	2009-11-24	
D3.2	Secure on-board architecture specification	3000	BMW F+T	R	PU	2010-02-28	Yes	2010-03-11	Version 1.3: 2011-08-15
D3.3	Secure on-board protocols specification	3000	EURECOM	R	PU	2010-06-30	Yes	2010-07-20	Version 1.4: 2011-06-15
D3.4.1	Architecture and protocols verification and attack analysis – Draft	3000	FRAUNHOFER (SIT)	R	PU	2009-12-31	Yes	2010-03-31	
D3.4.3	Architecture and protocols verification	3000	FRAUNHOFER (SIT)	R	PU	2010-09-30	Yes	2010-12-30	
D3.4.4	Attack analysis	3000	FRAUNHOFER (SIT)	R	PU	2010-09-30	Yes	2010-12-30	
D4.0.1	Security architecture implementation – Progress report V0.1	4000	INFINEON	R	PU	2010-02-28	Yes	2010-04-08	
D4.0.2	Security architecture implementation – Progress report V0.2	4000	INFINEON	R	PU	2010-09-30	Yes	2010-10-31	
D4.0.3	Security architecture implementation – Progress report V1.0	4000	INFINEON	R	PU	2011-06-30	Yes	2011-07-15	
D4.1.1	Hardware implementation specification	4000	ESCRYPT	R	RE	2010-06-30	Yes	2010-08-30	
D4.1.2	Security hardware FPGA prototype – Version 1	4000	ESCRYPT	P	CO	2010-09-30	Yes	2010-09-23	
D4.1.3	Security hardware FPGA prototype	4000	ESCRYPT	P	CO	2010-12-31	Yes	2011-01-31	
D4.2.1	Basic software – Version 1	4000	FUJITSU	P	CO	2010-09-30	Yes	2010-09-23	
D4.2.2	Basic software	4000	FUJITSU	P	CO	2011-03-31	Yes	2011-05-12	
D4.3.1	Implementation of software framework – Version 1	4000	BOSCH	P	CO	2011-03-31	Yes	2011-06-01	
D4.3.2	Implementation of software framework	4000	BOSCH	P	CO	2011-06-30	No	2011-11-23	
D4.4.1	Test specification	4000	EURECOM	R	CO	2010-12-31	Yes	2011-05-12	
D4.4.2	Test results	4000	EURECOM	R	PU	2011-06-30	No	2011-12-31	
D5.1.1	On-board communication demonstrator specification	5000	ESCRYPT	R	RE	2010-12-31	Yes	2010-12-30	Version 1.0: 2011-08-18
D5.1.2	On-board communication demonstrator	5000	ESCRYPT	D	PU	2011-12-31	No	2011-11-23	

2.2 Milestones

Table 2 lists all milestones based on the revised Description of Work and indicates whether they have been actually achieved.

Table 2 List of milestones

Mile-stone no.	Milestone name	Due achievement date from Annex I	Achieved Yes/No	Actual/forecast achievement date	Comments
M1	Requirements available	2009-03-31	Yes	2009-03-31	
M2	Security and trust model and secure on-board architecture available	2010-02-28	Yes	2010-03-11	
M3	Protocol specification and model-based verification available	2010-09-30	Yes	2010-12-30	
M4	FPGA prototype, basic software, and security software framework available	2011-06-30	No	2011-11-23	Parts of D4.3.2 are delayed.
M5	Final validation and demonstrator available	2011-12-31	No	2011-11-23	

3 Project management

3.1 Management achievements

What has been achieved?

– A quarterly progress report including a person-month overview per beneficiary and work package for January–March 2011 has been compiled and sent to the European Commission.

– A quarterly cost overview for January–March 2011 has been compiled for internal use by the EVITA Steering Committee.

3.2 Project meetings

Table 3 lists the physical meetings of the project partners within the reporting period.

Table 3 Physical project meetings within the reporting period

Meeting	Date	Venue
Integration Workshop	2011-07-21/22	Munich, Germany
Integration Workshop	2011-08-17	Munich, Germany
Integration Workshop	2011-09-08/09	Langen, Germany
Integration Workshop	2011-09-27/28	Sophia Antipolis, France

3.3 Person-month overview

Table 4 through Table 7 give a tabular overview of target person-months over the entire project duration and actual person-months spent so far per beneficiary and per work package. The target person-months are taken from the revised Annex I of the Grant Agreement.

The project budget is based on the targeted person-months and conservative estimates of the costs per person-months. The actual costs per person-month may be slightly lower than the estimates. In that case, more person-months than targeted are within the budget. The actual costs per person-months will be determined for the periodic report.

Fraunhofer, Infineon, MIRA, Trialog, K.U. Leuven, Institut Télécon, and EURECOM have in total already spent more person-months than targeted. For Fraunhofer, K.U. Leuven, Institut Télécom, and EURECOM, however, the projected costs are still within the budget.

Table 4 Person-month overview for management activities

Management			TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
WP0000	Project coordination and management	Actual	16,06	16,06	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		Target	16,00	16,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Total		**Actual**	**16,06**	**16,06**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
		Target	**16,00**	**16,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**

Table 5 Person-month overview for RTD activities

RTD			TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
WP1000	RTD coordination/ dissemination/ external interfaces	Actual	39,52	21,11	1,29	2,57	3,33	1,03	0,00	2,20	4,00	0,00	3,99	0,00	0,00	0,00	0,00
		Target	47,00	19,00	5,00	3,00	4,00	1,00	0,00	3,00	5,00	0,00	7,00	0,00	0,00	0,00	0,00
WP2000	Security requirements engineering	Actual	105,62	27,73	3,00	3,20	0,00	0,00	4,96	13,30	0,00	39,60	3,47	4,00	6,36	0,00	0,00
		Target	97,00	27,00	3,00	3,00	0,00	0,00	5,00	9,00	0,00	36,00	3,50	4,00	6,50	0,00	0,00
WP3000	Secure on-board architecture design	Actual	146,54	30,50	10,32	4,74	12,00	8,07	0,00	0,00	11,75	0,00	12,25	16,76	40,15	0,00	0,00
		Target	111,50	27,00	8,00	5,00	12,00	6,00	0,00	0,00	9,00	0,00	10,50	13,00	21,00	0,00	0,00
WP4000	Security architecture implementation	Actual	152,77	0,00	13,85	0,00	41,96	22,25	9,07	0,00	11,00	0,00	0,00	20,45	25,69	1,00	7,50
		Target	138,00	0,00	12,00	0,00	40,00	19,00	9,00	0,00	5,00	0,00	0,00	22,00	22,50	1,00	7,50
Total		**Actual**	**444,45**	**79,34**	**28,46**	**10,51**	**57,29**	**31,35**	**14,03**	**15,50**	**26,75**	**39,60**	**19,71**	**41,21**	**72,20**	**1,00**	**7,50**
		Target	**393,50**	**73,00**	**28,00**	**11,00**	**56,00**	**26,00**	**14,00**	**12,00**	**19,00**	**36,00**	**21,00**	**39,00**	**50,00**	**1,00**	**7,50**

Table 6 Person-month overview for demonstration activities

Demonstration			TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
WP5000	Demonstration	Actual	42,96	0,00	7,68	4,94	15,03	2,27	0,00	0,00	0,00	0,00	6,54	0,00	0,00	1,50	5,00
		Target	55,50	0,00	10,00	5,00	20,00	4,00	0,00	0,00	0,00	0,00	10,00	0,00	0,00	1,50	5,00
Total		**Actual**	**42,96**	**0,00**	**7,68**	**4,94**	**15,03**	**2,27**	**0,00**	**0,00**	**0,00**	**0,00**	**6,54**	**0,00**	**0,00**	**1,50**	**5,00**
		Target	**55,50**	**0,00**	**10,00**	**5,00**	**20,00**	**4,00**	**0,00**	**0,00**	**0,00**	**0,00**	**10,00**	**0,00**	**0,00**	**1,50**	**5,00**

Table 7 Overall person-month overview

		TOTAL	Fraunhofer	Bosch	Continental Teves	ESCRYPT	Infineon	Fujitsu	MIRA	TRIALOG	K.U. Leuven	BMW F+T	Institut Telecom	Eurecom	FSEU	FEAT
TOTAL ACTIVITIES	Actual	503,47	95,40	36,14	15,45	72,32	33,62	14,03	15,50	26,75	39,60	26,25	41,21	72,20	2,50	12,50
	Target	465,00	89,00	38,00	16,00	76,00	30,00	14,00	12,00	19,00	36,00	31,00	39,00	50,00	2,50	12,50

3.4 Project status

Compared to the revised Description of Work, some tasks are behind schedule. This has been compensated by parallelisation of the remaining subtasks in WP4000 and WP5000.