PRESERVE

preparing secure v2x communication systems

PREparing SEcuRe VEhicle-to-X Communication Systems

Deliverable 6.1

Y1 Dissemination Report

Project:	PRESERVE
Project Number:	IST-269994
Deliverable:	D6.1
Title:	Y1 Dissemination Report
Version:	v1.1
Confidentiality:	Public
Editors:	Frank Kargl (UT)
Date:	04. May 2012

SEVENTH FRAMEWORK PROGRAMME

Part of the Seventh Framework Programme

Funded by the EC - DG INFSO

Document History

Version	Status	Author	Date
0.1	Initial version	F. Kargl	2012-01-23
0.2	Integrated input from J. Petit and K. Bayarou.	J. Petit, K. Bayarou	2012-02-06
0.3	Integrated reviews and input from partners	F. Kargl, C. Schleiffer, A. Kung, B. Lonc, K. Bayarou, P. Papadimitratos	2012-02-09
1.0	Prepared final version	F. Kargl	2012-02-10
1.1	Integration of reviewer comments	J. Petit	2012-05-04

Approval

	Name	Date
Prepared	F. Kargl	2012-02-06
Reviewed	All Partners	2012-02-09
Authorised	F. Kargl	2012-02-10

Circulation

Recipient	Date of submission
Project partners	2012-02-10
European Commission	2012-02-10

Table of Contents

1 Executive Summary

1.1 Contact Information

University of Twente (Coordinator)	
Name:	Frank Kargl
Address:	University of Twente Faculty of EEMCS P.O.-Box 217 7500 AE Enschede The Netherlands
Email:	f.kargl@utwente.nl
Phone (Office):	+31 53 489 4302
KTH Stockholm	
Name:	Panos (Panagiotis) Papadimitratos
Address:	KTH EES LCN Osquldas vag 10 SE-100 44 Stockholm Sweden
Email:	papadim@kth.se
Phone (Office):	+46 8 790 4263
Renault SAS	
Name:	Brigitte Lonc
Address:	Renault API: FR TCR RUC T 62 1 avenue du Golf 78288 Guyancourt France
Email:	brigitte.lonc@renault.com
Phone (Office):	+33 (0)1 76 85 14 87
Escrypt GmbH	
Name:	Christian Schleiffer
Address:	escrypt GmbH - Embedded Security Leopoldstr. 244 80807 München Germany
Email:	christian.schleiffer@escrypt.com
Phone (Office):	+49 89 208039-132
Fraunhofer	
Name:	Dr.-Ing. Kpatcha Bayarou
Address:	Fraunhofer Institute for Secure Information Technology SIT Secure Mobile Systems (SIMS) Rheinstrasse 75 D-64295 Darmstadt Germany
Email:	kpatcha.bayarou@sit.fraunhofer.de
Phone (Office):	+49(0)6151/869-274
Trialog	
Name:	Antonio Kung
Address:	25 rue du general Foy 75008 Paris France
Email:	antonio.kung@trialog.com
Phone (Office):	+33 (0) 1 44 70 61 03

1.2 Summary and Intended Audience

This deliverable is summarizing dissemination and exploitation activities in Y1 of the PRESERVE project (1.1.2011 - 31.12.2011). It is intended for use within the PRESERVE project and the European Commission. It consists of three parts:

1. An overview chapter describing the status of the project and the dissemination plan
2. A chapter on foreseen and actually conducted dissemination activities in Y1
3. A chapter on planned future dissemination and exploitation activities

2 Overview

2.1 Status of the Project

The description of work states the following objectives for the PRESERVE project:

1. Create an **integrated V2X Security Architecture (VSA)** and demonstrate a close-to-market implementation termed **V2X Security Subsystem (VSS)**.
2. Prove that the **performance and cost requirements** for the VSS arising in current FOTs and future product deployments **can be met** by the VSS.
3. **Provide** a **ready-to-use VSS** implementation to FOTs and interested parties and the support for it so that a close-to-market security solution can be installed as part of those larger FOTs.
4. Solve open **deployment** and **technical issues** hindering standardization and product-pre-development.

More fine-grained objectives are outlined in this table below:

Type of objective	Objective	Description	Milestone	Verification in project
Integrated V2X security architecture and implementation based on SeVeCom, EVITA, and PRECIOSA results	O1.1 + O1.2	Harmonizing the security architectures and providing the VSA as input to on-going architecture standardization	M1.1 + M1.2	D1.1, D1.2, D 1.3, D6.1, D6.2, D6.3
	O1.3	Integrating and refining prototype implementations of SeVeCom, PRECIOSA, and EVITA into a joined V2X Security Subsystem (VSS).	M2.1 + M2.2	D2.1, D2.2, D2.3, D4.1, D4.2, D4.3
Meet performance and cost requirements of current FOTs and future products	O2.1	Perform and evaluate field-operational-test (FOT) in a hybrid testbed	M3.1 + M3.2	D3.1, D3.2
	O2.2	Provide an ASIC implementation of the required security hardware	M2.2	D2.2, D2.3
	O2.3	Extend testbed to full FOT level	M3.3	D3.2
Provide “ready-to-use” V2X security subsystem	O3.1	Packaging of the VSS including documentation and testing	M2.1 + M2.2	D4.1, D4.2, D4.3
	O3.2	Providing integration support to third-parties	M2.2 + M3.3	D4.3 + D3.3
Solve open deployment and technical issues hindering standardization and development	O4.1	Organizational Issues	M4.1 + M4.2	D5.1, D5.2, D5.3, D5.4
	O4.2	Technical Issues	M4.1 + M4.2	D5.1, D5.2, D5.3, D5.4

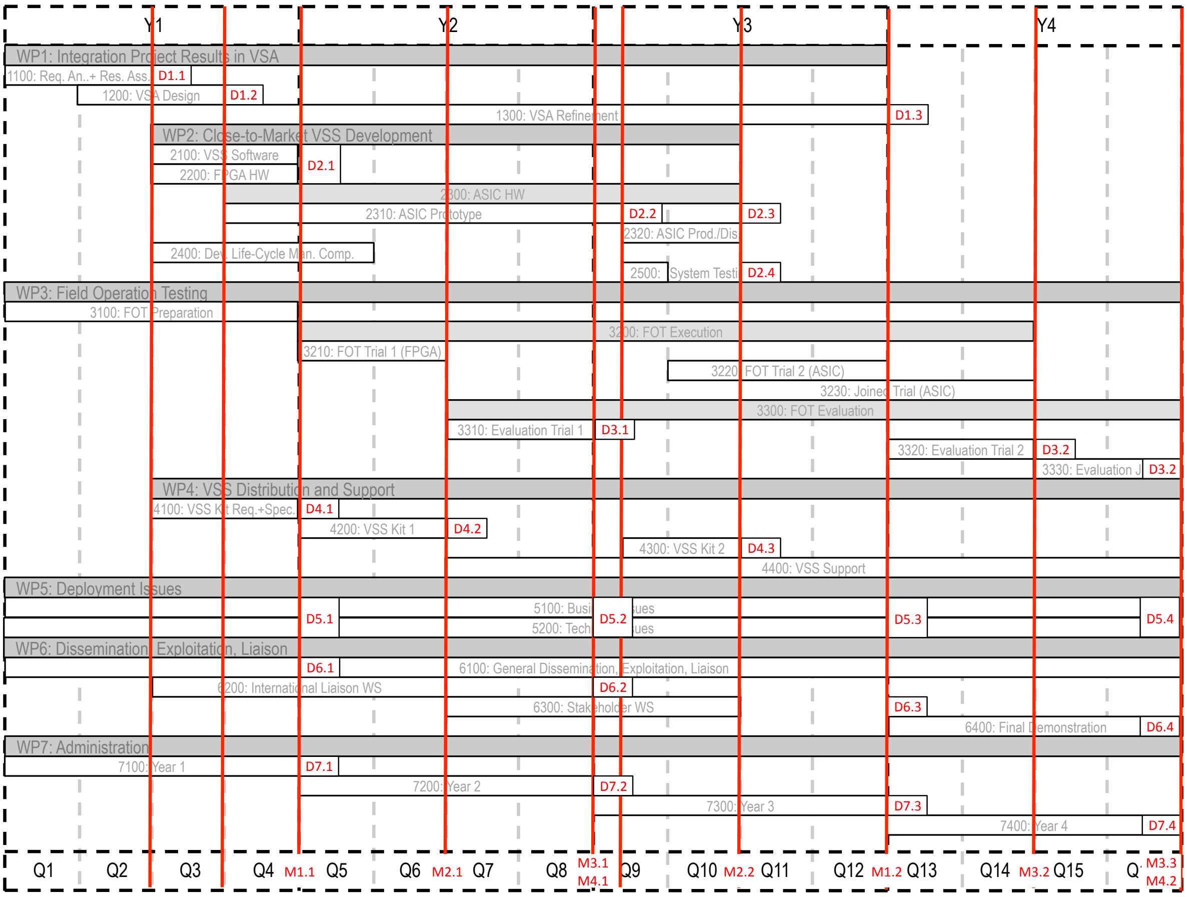
Corresponding Milestones are:

Milestone number	Milestone name	Sub-milestones	Work package(s) involved	Expected date [1]	Means of verification[2]
M1	VSA	M1.1: First version of V2X security architecture is ready for dissemination and distribution to standardization bodies and stakeholders has started.	WP1, WP6	M12	D1.1, D1.2, D6.1
		M1.2: Final Version of VSA is available and harmonized with standardization bodies and stakeholders.	WP1, WP6	M36	D1.3, D6.2, D6.3
M2	VSS	M2.1: FPGA-based VSS Kit is available for partner projects and interested stakeholders	WP2, WP4	M18	D2.1, D4.1, D4.2
		M2.2: ASIC-based VSS Kit is tested and available for partner projects and interested stakeholders	WP2, WP4	M30	D2.2, D2.3, D2.4, D4.3
M3	FOT	M3.1: FOT Trial 1 results available	WP3	M24	D3.1
		M3.2: FOT Trial 2 results available	WP3	M42	D3.2
		M3.3: Joined FOT Trial results available	WP3	M48	D3.3
M4	DIS	M4.1: Deployment issues results are taken into consideration by industry, standardization, and other stakeholders	WP5, WP6	M24	D5.1, D5.2, D6.1, D6.2
		M4.2: Deployment issues results have been successfully been integrated into on-going standardization and deployment preparation	WP5, WP6	M48	D5.3, D5.4, D6.3, D6.4

[1] Measured in months from the project start date (month 1).

[2] Show how both the participants and the Commission can check that the milestone has been attained. Refer to indicators if appropriate.

This translates to the following timeplan:



As can be seen, PRESERVE was expected to reach its first milestone M1.1 at the end of Y1. Deliverables D1.1 “Security Requirements of VSA” and D1.2 “V2X Security Architecture V1” were delivered on time, containing a harmonized and integrated view on security requirements (D1.1) on which a harmonized and integrated V2X Security Architecture (VSA) was designed (D1.2).

Furthermore, deliverables D2.1 “FPGA-based VSS Prototype”, D4.1 “VSS Distribution Environment”, D5.1 “Deployment Issues Report V1” and D7.1 “Year 1 management report” are submitted together with this deliverable. D2.1 and D5.1 will be provided in preliminary versions that will be extended within a short timeframe as described and explained therein.

At the end of Y1, there are some foreseeable deviations from the workplan, especially in WP3 where we will have an additional joint test with the French FOT Score@F already in early 2012. At the same time, plans for a joint trial (task 3230) in 2013/2014 are questioned by the incompatible lifetime of other FOT projects that all end their testing activities earlier than this. This will be addressed by an amendment to the DoW in February 2012.

Other work (on VSS development, VSS kit 1 specification, deployment issues) is progressing as expected or with only minor delays.

2.2 Dissemination Plan

2.2.1 Dissemination Plan

Dissemination activities with the following stakeholders are foreseen in the DoW at the institution, industry and academic level:

- Institution level. The stakeholders are
  - Policy makers who will have to deal with security and trust (e.g. public authorities and related organisations). They are concerned about evaluation criteria, e.g. which level of security to mandate, and the harmonisation of these criteria. This is also consistent with the third recommendation of the eSecurity WG report presented to the eSafety forum steering group on March 18th 2010
  - Data protection agencies as well at the article 29 working group party, in order to ensure that a privacy by design approach is made possible with the PRESERVE contribution
- Industry level. Dissemination and liaison will take place with the eSafety stakeholders, the C2C-CC consortium. Active participation to standardisation (e.g. ETSI) is also expected. Two partners (Renault and Fraunhofer) are members in the respective ETSI and C2C-CC security working groups, UTWENTE, KTH, and escrypt are members in C2C-CC, and the other partners (KTH, Trialog, Escrypt) will be involved by those working group on an individual basis depending on topics. There will be dedicated contact persons for the ETSI and C2C-CC Security working groups to ensure that PRESERVE results will be presented there and taken into consideration.
- Research level. It is expected that a number of significant research results will be produced in the course of the project in particular as part of work conducted in WP5. For dissemination of results, academic partners (U.Twente, KTH, Fraunhofer) of the PRESERVE project will target highly-ranked journals and magazines, and well visible and attended, high-quality venues (conferences, workshops, and symposia). The researchers gathered in this project have a history in publishing there and often have been involved as TPC members/chairs or guest editors. These activities will be continued and extended throughout the project duration. A minimum of five refereed publications should be accepted per project year. We further plan to organize a special issue on V2X security & privacy of one of the listed magazines or journals during the project duration. We also will propose a V2X security & privacy workshop to be held adjunct with a larger conference of the Pervasive/Ubiquitous Computing community to ensure dissemination of our topics and results to this closely related discipline.

2.2.2 Dissemination Activities foreseen in WP6

The objectives of WP6 (Dissemination, Exploitation, Liaison) are as follows:

- To organize general dissemination, exploitation, and liaison as well as organize and maintain specific contacts to important stakeholders like OEMs, suppliers, standardization bodies, related research projects in Europe and beyond.
- To publish the PRESERVE research results in high-ranked journals and to present our work at top-class conferences in the security and ITS domain.
- To advance the research field of security and privacy in ITS and ubiquitous computing by proposing journal special issues or research community workshops.
- To organize specific workshops (potentially co-located to other events) to showcase PRESERVE results and discuss challenges, requirements, and progress.

This is reflected in the following tasks:

Task 6100: General Dissemination, Exploitation, Liaison (M1 to M48, 28 MM)

Publish PRESERVE results through a broad variety of channels, liaise with partner projects and other stakeholders to exchange requirements and results, organize interaction with the advisory board, and organize workshops inviting participants from the ITS, security&privacy, and ubiquitous computing community for information and exchange.

Task 6100 includes the following subtasks:

- Subtask 6110: Webpage (M1 to M48): Setup and maintain a web representation of PRESERVE.
- Subtask 6120: Dissemination Y1 (M1 to 12): Dissemination and liaison activities (create initial awareness and setup links to potential VSS users)
- Subtask 6130: Dissemination Y2 (M13 to 24): Dissemination and liaison activities (negotiate details of VSS usage in other projects or organizations)
- Subtask 6140: Dissemination Y3 (M25 to 36): Dissemination and liaison activities (promote initial results among stakeholders and scientific community)
- Subtask 6150: Dissemination Y4 (M37 to 48): Dissemination and liaison activities (promote final results among stakeholders and scientific community)
- Subtask 6160: Advisory Board (M1 to M48): Keep close contact to members of advisory board, timely dissemination of results to advisory board, requesting regular feedback, organization of advisory board meetings.

In this task, close liaison is especially foreseen with the Car-2-Car Communication Consortium, ETSI TC ITS, the national French FOT Score@F, other European and national FOTs, especially DRIVE C2X, FOTsis, and simTD, and other research projects and industry stakeholders.

Task 6200: International Liaison Workshop (M1 to M18, 6.5 MM)

Note that there is a deviation in the WP between the timeframe listed in the text (until M12) and shown in the timeline (until M18). We will address this deviation later in this report.

Organize first dissemination workshop with international participation to ensure worldwide awareness. Workshop planned for M11 or M12.

Purpose: Generate international awareness and retrieve world-wide feedback and input.

Target audience: European FOTs and related projects from other continents, industry members active in V2X.

Task 6300: Stakeholder Workshop (M19 to M30, 5.5 MM)

Organize second dissemination workshop aiming specifically at stakeholders from industry to discuss progress and receive input. Workshop planned when first ASIC prototypes are available. Workshop planned for M29 or M30.

Purpose: Present FPGA Kit and ASIC Prototype and create industry interest to adopt VSS.

Target Audience: OEMs and suppliers, European FOTs and related projects from other continents.

Task 6400: Final Demonstration (M37 to M48, 8.5 MM)

Organize final demonstration of project results, preferably together with other FOT project(s). Demonstration planned for M47 or M48.

Purpose: present VSS Kit and FOT results and ensure long-term exploitation of VSS.

Target Audience: OEMs and suppliers, European FOTs and related projects from other continents.

Progress on these tasks is to be reported in this Y1 Dissemination Report, which is to include:

- Press releases
- Scientific publications
- Flyers
- Web site
- Handbook
- Plan for use and dissemination.

D6.1 also includes an initial dissemination and exploitation plan.

3 Y1 Dissemination Activities

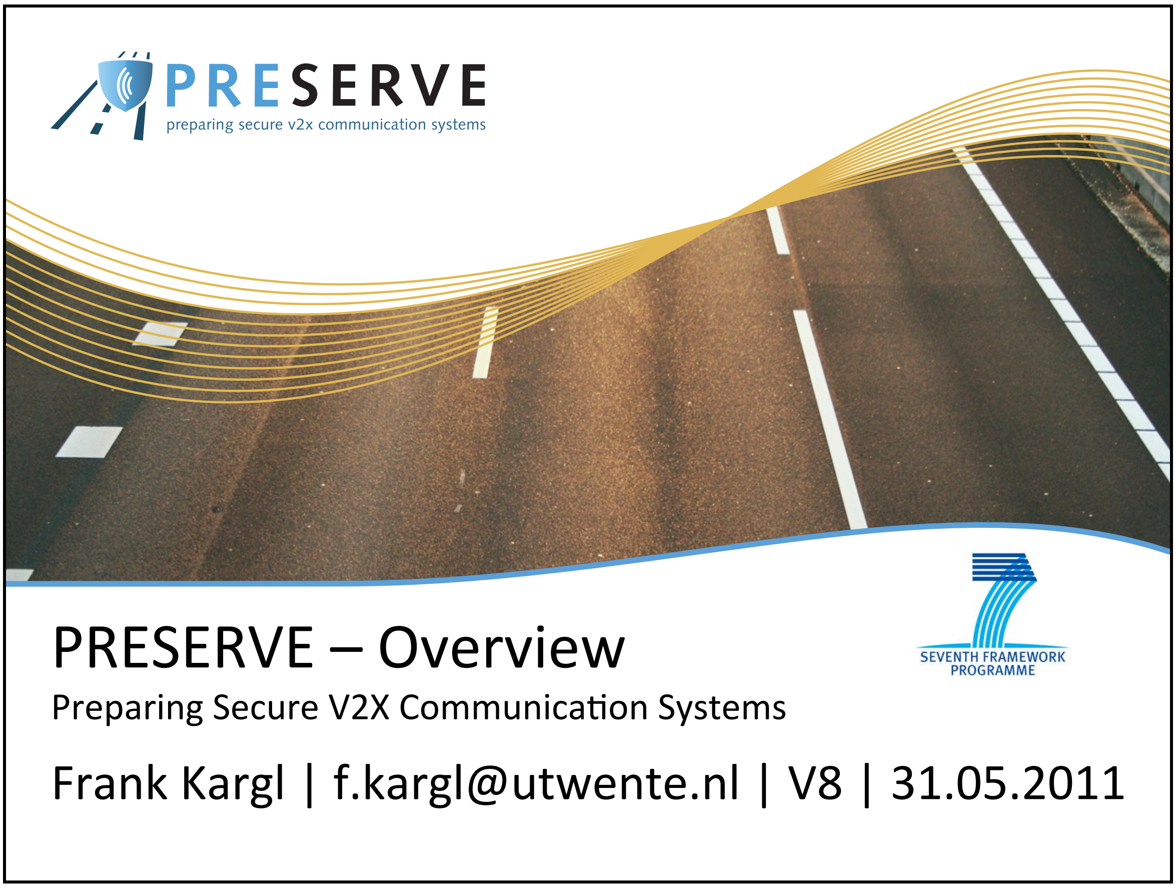
This chapter lists dissemination and liaison activities in Y1 of the project

3.1 Dissemination Material

In 2011, PRESERVE has created a range of dissemination material to present its results and on-going work to interested parties. We created the following **logo** for the PRESERVE project:

PRESERVE
preparing secure v2x communication systems

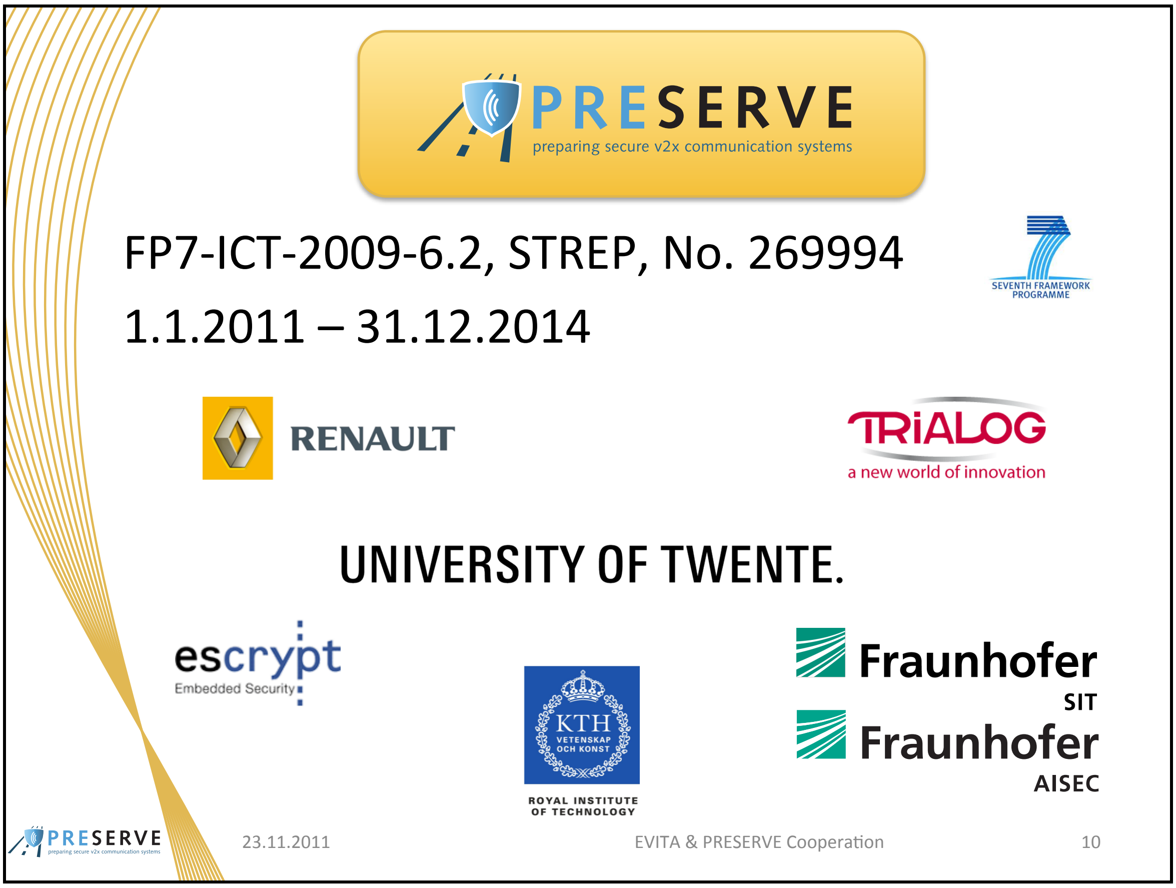
A consistent cooperate identity was created including standard document and presentation templates:


PRESERVE
preparing secure v2x communication systems
SEVENTH FRAMEWORK PROGRAMME

PRESERVE – Overview

Preparing Secure V2X Communication Systems

Frank Kargl | f.kargl@utwente.nl | V8 | 31.05.2011

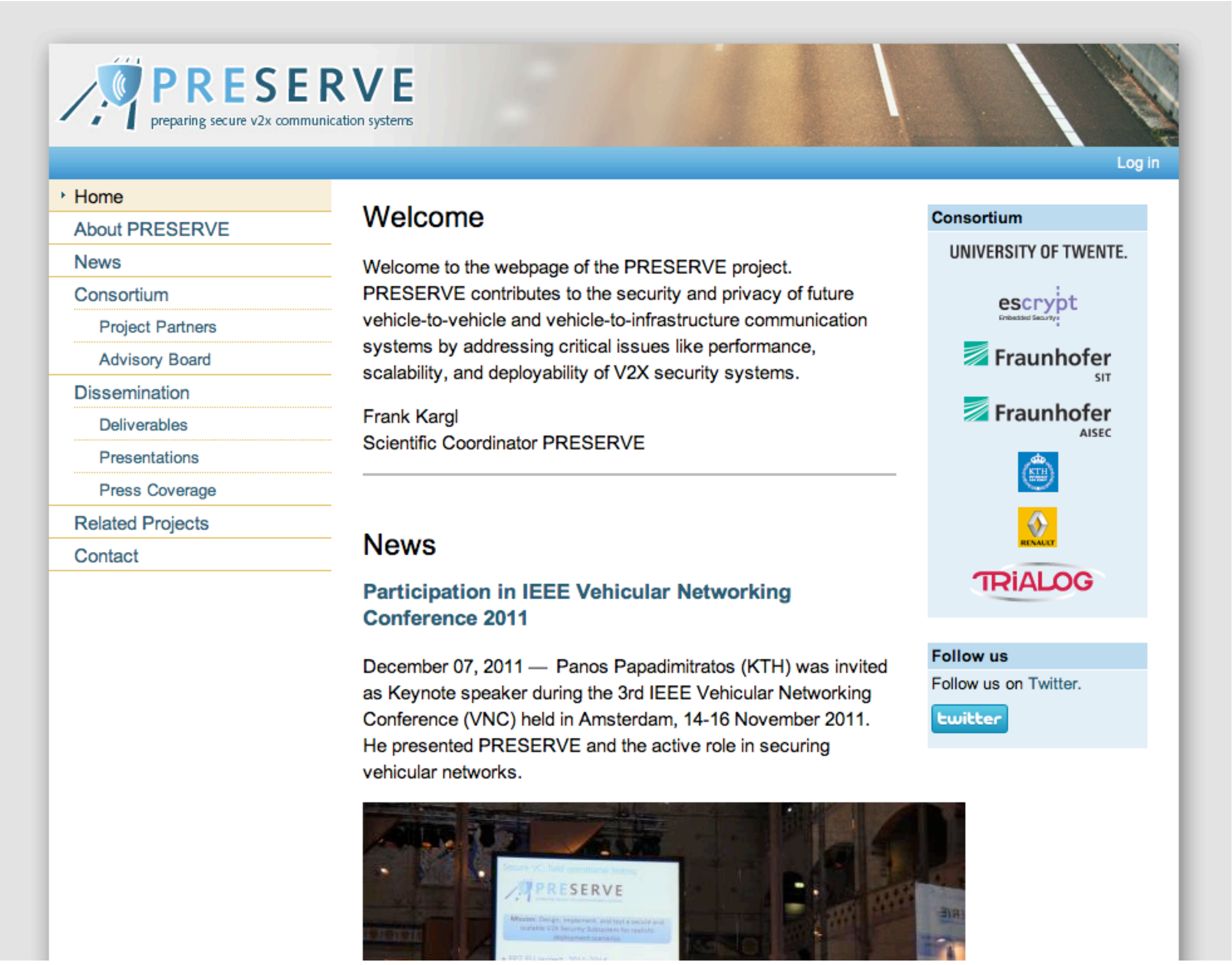

PRESERVE
preparing secure v2x communication systems
SEVENTH FRAMEWORK PROGRAMME
RENAULT
TRIALOG
a new world of innovation
UNIVERSITY OF TWENTE.
escrypt
Embedded Security
KTH
VETENSKAP OCH KONST
ROYAL INSTITUTE OF TECHNOLOGY
Fraunhofer
SIT
Fraunhofer
AISEC
PRESERVE

FP7-ICT-2009-6.2, STREP, No. 269994

1.1.2011 – 31.12.2014

23.11.2011 EVITA & PRESERVE Cooperation 10

We also established a **website** at the URL http://www.preserve-project.eu/ where up-to-date information on the project is available. We also maintain a **twitter** account named @preserveproject that provides recent news in a fast and convenient way.



Welcome

Welcome to the webpage of the PRESERVE project. PRESERVE 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.

Frank Kargl
Scientific Coordinator PRESERVE

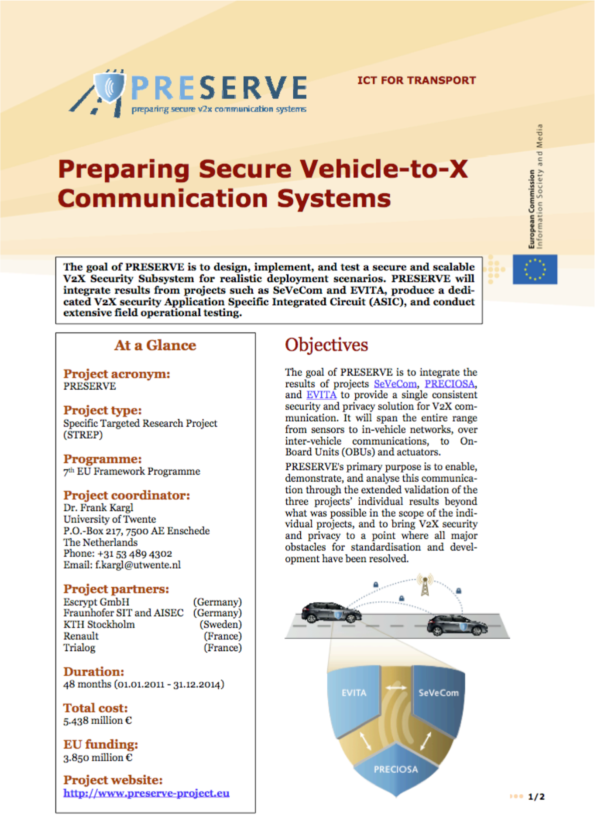
News

Participation in IEEE Vehicular Networking Conference 2011

December 07, 2011 — Panos Papadimitratos (KTH) was invited as Keynote speaker during the 3rd IEEE Vehicular Networking Conference (VNC) held in Amsterdam, 14-16 November 2011. He presented PRESERVE and the active role in securing vehicular networks.

Follow us on Twitter.

PRESERVE also created a **factsheet** that is available through the webpage or via the EC:


PRESERVE
preparing secure v2x communication systems
ICT FOR TRANSPORT
European Commission
Information Society and Media
EVITA
SeVeCom
PRECIOSA
1/2

Preparing Secure Vehicle-to-X Communication Systems

The goal of PRESERVE is to design, implement, and test a secure and scalable V2X Security Subsystem for realistic deployment scenarios. PRESERVE will integrate results from projects such as SeVeCom and EVITA, produce a dedicated V2X security Application Specific Integrated Circuit (ASIC), and conduct extensive field operational testing.

At a Glance

Project acronym:
PRESERVE

Project type:
Specific Targeted Research Project (STREP)

Programme:
7th EU Framework Programme

Project coordinator:
Dr. Frank Kargl
University of Twente
P.O.-Box 217, 7500 AE Enschede
The Netherlands
Phone: +31 53 489 4302
Email: f.kargl@utwente.nl

Project partners:

Escrypt GmbH	(Germany)
Fraunhofer SIT and AISEC	(Germany)
KTH Stockholm	(Sweden)
Renault	(France)
Trialog	(France)

Duration:
48 months (01.01.2011 - 31.12.2014)

Total cost:
5.438 million €

EU funding:
3.850 million €

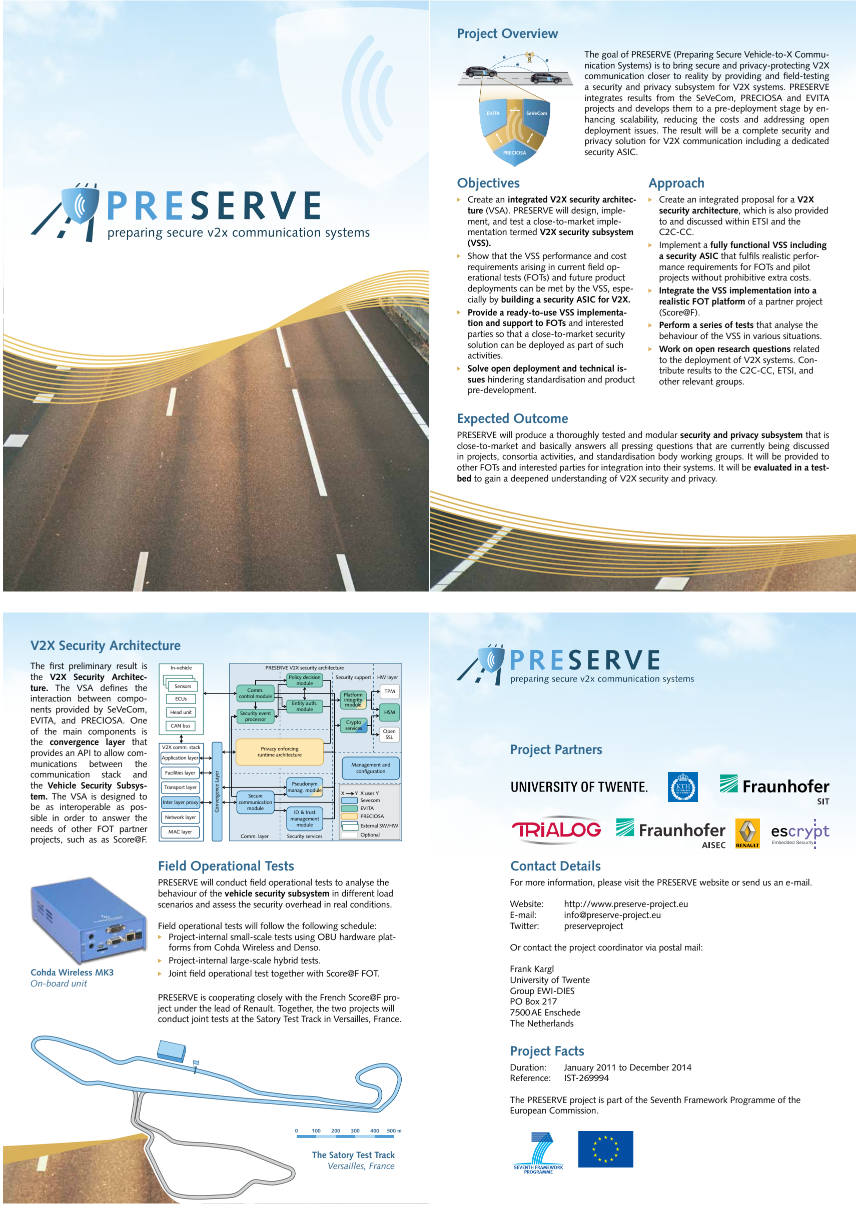
Project website:
http://www.preserve-project.eu

Objectives

The goal of PRESERVE is to integrate the results of projects SeVeCom, PRECIOSA, and EVITA to provide a single consistent security and privacy solution for V2X communication. It will span the entire range from sensors to in-vehicle networks, over inter-vehicle communications, to On-Board Units (OBUs) and actuators.

PRESERVE's primary purpose is to enable, demonstrate, and analyse this communication through the extended validation of the three projects' individual results beyond what was possible in the scope of the individual projects, and to bring V2X security and privacy to a point where all major obstacles for standardisation and development have been resolved.

Furthermore, a **flyer** was created that is used for dissemination at meetings or events



PRESERVE

preparing secure v2x communication systems

Project Overview

EVITA
SeVeCom
PRECIOSA

The goal of PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) is to bring secure and privacy-protecting V2X communication closer to reality by providing and field-testing a security and privacy subsystem for V2X systems. PRESERVE integrates results from the SeVeCom, PRECIOSA and EVITA projects and develops them to a pre-deployment stage by enhancing scalability, reducing the costs and addressing open deployment issues. The result will be a complete security and privacy solution for V2X communication including a dedicated security ASIC.

Objectives

- Create an **integrated V2X security architecture** (VSA). PRESERVE will design, implement, and test a close-to-market implementation termed **V2X security subsystem (VSS).**
- Show that the VSS performance and cost requirements arising in current field operational tests (FOTs) and future product deployments can be met by the VSS, especially by **building a security ASIC for V2X.**
- **Provide a ready-to-use VSS implementation and support to FOTs** and interested parties so that a close-to-market security solution can be deployed as part of such activities.
- **Solve open deployment and technical issues** hindering standardisation and product pre-development.

Approach

- Create an integrated proposal for a **V2X security architecture**, which is also provided to and discussed within ETSI and the C2C-CC.
- Implement a **fully functional VSS including a security ASIC** that fulfils realistic performance requirements for FOTs and pilot projects without prohibitive extra costs.
- **Integrate the VSS implementation into a realistic FOT platform** of a partner project (Score@F).
- **Perform a series of tests** that analyse the behaviour of the VSS in various situations.
- **Work on open research questions** related to the deployment of V2X systems. Contribute results to the C2C-CC, ETSI, and other relevant groups.

Expected Outcome

PRESERVE will produce a thoroughly tested and modular **security and privacy subsystem** that is close-to-market and basically answers all pressing questions that are currently being discussed in projects, consortia activities, and standardisation body working groups. It will be provided to other FOTs and interested parties for integration into their systems. It will be **evaluated in a testbed** to gain a deepened understanding of V2X security and privacy.

V2X Security Architecture

The first preliminary result is the **V2X Security Architecture.** The VSA defines the interaction between components provided by SeVeCom, EVITA, and PRECIOSA. One of the main components is the **convergence layer** that provides an API to allow communications between the communication stack and the **Vehicle Security Subsystem.** The VSA is designed to be as interoperable as possible in order to answer the needs of other FOT partner projects, such as as Score@F.

Field Operational Tests

PRESERVE will conduct field operational tests to analyse the behaviour of the **vehicle security subsystem** in different load scenarios and assess the security overhead in real conditions.

Field operational tests will follow the following schedule:

- Project-internal small-scale tests using OBU hardware platforms from Cohda Wireless and Denso.
- Project-internal large-scale hybrid tests.
- Joint field operational test together with Score@F FOT.

PRESERVE is cooperating closely with the French Score@F project under the lead of Renault. Together, the two projects will conduct joint tests at the Satory Test Track in Versailles, France.

Cohda Wireless MK3
On-board unit

The Satory Test Track
Versailles, France

PRESERVE

preparing secure v2x communication systems

Project Partners

UNIVERSITY OF TWENTE. KTH Fraunhofer SIT TRIALOG Fraunhofer AISEC RENAULT escrypt Embedded Security

Contact Details

For more information, please visit the PRESERVE website or send us an e-mail.

Website:	http://www.preserve-project.eu
E-mail:	info@preserve-project.eu
Twitter:	preserveproject

Or contact the project coordinator via postal mail:

Frank Kargl
University of Twente
Group EWI-DIES
PO Box 217
7500 AE Enschede
The Netherlands

Project Facts

Duration:	January 2011 to December 2014
Reference:	IST-269994

The PRESERVE project is part of the Seventh Framework Programme of the European Commission.

SEVENTH FRAMEWORK PROGRAMME

The operational information for PRESERVE partners is not maintained in a project handbook (as originally foreseen) but instead, we use a Wiki and an SVN repository maintained by UT to collect all project-related information and documents. The Wiki is also used for reporting purposes.

3.2 Reviewed Publications

The following scientific papers on V2X Security and Privacy were published by PRESERVE partners in 2011. If not noted otherwise, the publications were peer-reviewed.

1. S. Dietzel, “Privacy Implications of In-Network Aggregation Mechanisms for VANETs”, IEEE, WONS 2011 (Invited paper)
2. N. Ristanovic, P.Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, J.-Y. Le Boudec , “Adaptive Message Authentication for Multi-Hop Networks”, IEEE, WONS 2011 (Invited paper)

3. C. Neuberg, P. Papadimitratos, C. Fragouli, R. Urbanke, “A Mobile World of Security - the Model”, IEEE Information Theory Society CISS 2011
4. M. Fiore, C. Casetti, C.-F. Chiasserini, P. Papadimitratos , “Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks”, IEEE/IFIP Med-Hoc-Net 2011
5. F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischof, "Research Challenges in Intervehicular Communication: Lessons of the 2010 Dagstuhl Seminar", IEEE Communications Magazine, vol. 49, no. 5, pp. 158 - 164, May 2011 (Invited paper)
6. A. Kung, J-C. Freytag, and F. Kargl, "Privacy-by-Design in ITS Applications - The Way Forward", Second International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN 2011), Lucca, Italy, June 2011
7. V. Manolopoulos, P. Papadimitratos, S. Tao, A. Rusu, Securing Smartphone Based ITS," IEEE International Conference on ITS Telecommunications (IEEE ITST), St. Petersburg, Russia, August 2011
8. G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, “On the Performance of Secure Vehicular Communication Systems,” IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), September 2011
9. R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, “Collaborative Location Privacy,” IEEE 8th International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS), Valencia, Spain, October 2011.
10. Marco Fiore, Claudio Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, vol. 99, no. PrePrints, 2011
11. Petit, J.Y. and Mammeri, Z., “Dynamic Consensus for Secured Vehicular Ad Hoc Networks”, In: Proceedings of the 7th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE WiMob 2011, October 2011
12. Norbert Bißmeyer, Hagen Stübing, Elmar Schoch, Stefan Götz, Jan Peter Stotz, Brigitte Lonc, A Generic Public Key Infrastructure FOR Securing Car-to-X Communication, ITS World Congress 2011, Orlando, USA
13. J. Petit, M. Feiri, and F. Kargl, "Spoofed Data Detection in VANETs using Dynamic Thresholds", Proceedings of the 3rd IEEE Vehicular Networking Conference (VNC 2011), Amsterdam, The Netherlands, IEEE, pp. 25-32, 11/2011

3.3 Press Coverage and Presentations

PRESERVE participated in broad variety of events either presenting the project or giving broader presentations on ITS security where PRESERVE was also introduced. PRESERVE was also covered by various media channels.

The following press and outreach activities were conducted:

28-01-2011 Presentation of PRESERVE project at **Drive C2X Kickoff** inTorino, Italy.

23-03-2011: UT issues **press release** on start of PRESERVE (see http://www.utwente.nl/archief/2011/03/autos_die_veilig_communiceren.docx/, in Dutch). Following the press-release, coverage in national magazine and website

04/05-04-2011**:** Presentation of PRESERVE at **ITS Concertation Meeting**, Brussels, Belgium.

06-04-2011: PRESERVE press article on Dutch website “**Wetenschap24**”: http://www.wetenschap24.nl/nieuws/artikelen/2011/april/Auto-s-in-gesprek.html

06/07-04-2011: Presentation of the project to members of **C2C-CC Security WG** at C2C-CC Security Meeting in FFM, Germany.

14/15-04-2011: **Keynote speech** on security of vehicular communication systems at **ISC Workshop on Ad hoc and sensor network security** at KN Toosi University.

14-04-2011: Presentation of PRESERVE during **FOTsis Kickoff** meeting in Madrid, Spain.

20-04-2011: Mentioning of PRESERVE in **Scientific American** (Blog) Article: http://www.scientificamerican.com/article.cfm?id=wireless-car-hacking

03/04-05-2011: Presenting PRESERVE at the **ETSI TC ITS WG 5 Meeting**, Vienna, Austria.

01-06-2011: PRESERVE is featured in an article in Issue 8 / 2011 of the Dutch magazine **'De Ingenieur'** in a special issue on communicating vehicles: http://www.utwente.nl/ewi/dacs/news/archive/2011/files/08_Dossier_autos.pdf

06/07-09-2011: Presentation of PRESERVE at the **OVERSEE General Assembly**, Berlin, Germany

20-09-2011: Presentation of PRESERVE **poster** and participation in **podium discussion** at stakeholder forum at **ITS Europe 2011**, Lille, France.

21-10-2011: Participation in **panel discussion on Security and Privacy** at **7th International Workshop on Vehicle Communications** organized by COMeSafety 2, co-located with ITS WC, Orlando, Florida.

24/25-10-2011: Presentation of PRESERVE objectives and first result (VSA) at **iMobility Plenary Meeting**, Brussels, Belgium. Discussion with other European projects (especially FOTsis).

14-11-2011: **Keynote Presentation** on "Security on Wheels” at **IEEE VNC 2011**, Amsterdam, Netherlands

23-11-2011: Presentation of PRESERVE Progress and Cooperation Plans at **EVITA Final Workshop** at the Honda Academy, Erlensee, Germany.

3.4 Liaisons with other Projects and Stakeholders

As explained in detail in Sec. 2.2.4, PRESERVE aimed at building strong working relationships with a number of key projects and organizations, especially Score@F, C2C-CC Security WG, ETSI TC ITS WG5, CAMP (VSC-3), EVITA, OVERSEE, DRIVE C2X, FOTsis, and ITSSv6.

At a very early stage, we established links by presentations of PRESERVE at kick-off meetings or project meetings and via meetings and discussions at community venues like conferences or workshops. With some of these projects, we also had series of confcalls or working meetings.

Score@F is a key partner of PRESERVE, as we aim to integrate the VSS Kit 1 into the Score@F platform already early in 2012. Therefore, we held regular phonecalls and meetings to discuss the technical platforms and prepare the integration. Renault is a key partner in this, as they are coordinator of Score@F and member of PRESERVE. Unfortunately, due to on-going legal discussions about IPR matters, the cooperation agreement is still not signed. This is on-going and we are pushing to have remaining issues being resolved.

C2C-CC Security WG and **ETSI TC ITS WG5** are key partners for PRESERVE for harmonization and standardization. PRESERVE provided various reports and documents to both organizations. Furthermore, Brigitte Lonc from Renault is co-chair of ETSI TC ITS WG5, ensuring a very close interaction. Members from PRESERVE are active in almost all C2C-CC Security WG Task-Forces, actively contributing to the work there and bringing the status from C2C-CC into PRESERVE.

We had a series of phone-calls and meetings with key persons from **CAMP VSC-3** (Tom Schaffnit, Mike Shulman, André Weimerskirch) to harmonize the mutual approaches to security. As a result, CAMP is interested in testing the PRESERVE ASIC once it becomes available. As a first step, we agreed on a joint demo proposal for the ITS WC 2012 in Vienna to demonstrate the interoperability or the PRESERVE FPGA with the CAMP On-board Equipment.

Regarding **FOTsis**, there was already a series of contacts to exchange information about the two projects. PRESERVE has provided a text proposal for a formal liaison agreement to FOTsis that is evaluated now by the FOTsis steering committee. A technical workshop between the two projects is planned for spring 2012.

The same applies to **DRIVE C2X**. PRESERVE has also provided a text proposal for a formal liaison agreement to DRIVE C2X that is evaluated now by the DRIVE C2X steering committee. A meeting with the DRIVE C2X coordinator is planned and F. Kargl and J. Petit will attend the next DRIVE C2X steering board meeting.

With **EVITA**, we held a regular series of meetings to discuss a liaison agreement, which is crucial for our project to achieve full integration of previous project's results. There remain open issues about required background IPR which are currently resolved. Nevertheless, we plan a demonstration of an integrated EVITA-PRESERVE system at the ITS WC 2012 in Vienna. Due to a significant overlap of partners, we maintained a close contact with EVITA.

We have signed a cooperation agreement with the **OVERSEE** project on 4.4.2011. Furthermore, PRESERVE presented its plans and preliminary results at the OVERSEE general assembly on 6.9.2011. Further contacts are planned.

PRESERVE kept regular contact with **Advisory Board**. During our Kickoff-Workshop, AB members from Audi, Volkswagen, Daimler, and Denso participated and provided valuable input and requirements. During the Q4 meeting, we met with members from the AB (VW, Audi, BMW, Denso) to present our D1.1 and D1.2 results and discuss next steps. The AB was also deeply involved in designing the deployment use cases in D5.1.

Technical reports and draft deliverables disseminated to partners included:

1. PRESERVE TR 1: Performance Metrics and Requirements
2. PRESERVE TR 2: Privacy Position Statement
3. PRESERVE TR 3: Position of Security Processing in the Communication Stack
4. Drafts of D1.1 and D1.2

3.5 *Table of all Y1 Dissemination Activities*

The following table lists all dissemination activities in Y1 in detail in chronological order.

Date	Type or Venue	Activity	Impact & Audience
January-February 2011	Dissemination Material	Setting up of domain, webpage, twitter account and preparation of information material, e.g. factsheet and project presentation (UT)	General dissemination
Continuously	Dissemination Material	Update of webpage, project presentation, twitter feeds	General dissemination
27-01-2011	Publication and Presentation at Wireless On-Demand Network Services Conference (IEEE WONS 2012),	F. Kargl (UT) organized special Session on "Security and Privacy in Mobile Networks" with contributions from two PRESERVE partners (UT, KTH) Publications in Proceedings: S. Dietzel, "Privacy Implications of In-Network Aggregation Mechanisms for VANETs", IEEE,	Dissemination of current research results and awareness of project to academic community. Publications in Proceedings

	Bardonecchia, Italy	WONS 2011 N. Ristanovic, P.Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, J.-Y. Le Boudec , “Adaptive Message Authentication for Multi-Hop Networks”, IEEE, WONS 2011	
28-01-2011	Drive C2X Kickoff, Torino, Italy	F. Kargl, UT, presented the PRESERVE project at Drive C2X Kickoff	Raising awareness among Drive C2X members, talks about cooperation potential with various Drive C2X members
01-02-2011	PRESERVE Kickoff, Enschede, Netherlands	PRESERVE Kickoff Workshop with strong participation from industry (Audi, Volkswagen, Daimler, Denso, NEC, Iridium ACS) and relevant projects / organisations (C2C-CC, ETSI, DRIVE C2X, FOTsis)	Valuable input from stakeholders is taken into account in WP1 (requirements). Agreed on cooperation with Drive C2X
01-03-2011	Technical meeting with NXP, Enschede, Netherlands	First technical meeting with NXP to discuss about MK3 OBU platform	Discussion of requirements and technical specifications
23-03-2011	PRESERVE Press Release	UT issues press release about PRESERVE project. Coverage in Dutch National newspapers and magazines.	Raised Awareness in general public.
23-03-2011	Publication and Presentation	C. Neuberg, P. Papadimitratos, C. Fragouli, R. Urbanke, “A Mobile World of Security - the Model”, IEEE Information Theory Society CISS 2011	Academic Dissemination of research results
04-04-2011	Liaison Workshop with Score@F, Paris, France	Preparation of Cooperation with Score@F. Plans to integrate VSS into Score@F platform.	Agreement and plan for joint tests.
04/05-04-2011	ITS Concertation Meeting, Brussels, Belgium	Presentation of PRESERVE to other ITS projects by Antonio Kung, Trialog, discussions with FOTsis and SUNSET	Alerting the ITS community on the need to reach a technical understanding on privacy-by-design (follow-up of the eSecurity WG) Raised awareness, cooperation plans esp. with FOTsis
06/07-04-2011	C2C-CC Security Meeting in FFM, Germany	Presentation of the project to members of C2C-CC Security WG.	Agreement on close cooperation between PRESERVE and C2C-CC
14-04-2011, 06-05-2011, 13-05-2011, 24-06-2011	CAMP-VSC3 Confcalls	Series of Confcalls to discuss and align security solutions	Mutual exchange of requirements, discussion of harmonization of solutions, CAMP-VSC3 interested in testing PRESERVE ASIC
14/15-04-2011	ISC Workshop, Sweden	Keynote speech by P. Papadimitratos, KTH, on security of vehicular communication systems at KN Toosi University/ISC Workshop on Ad hoc and sensor network security	Raised awareness on security issues in VCS
14-04-2011	FOTsis Kickoff, Madrid, Spain	Presentation of PRESERVE during FOTsis Kickoff meeting	Raised awareness among FOTsis partners and

			agreement on cooperation
20-04-2011	Scientific American Blog	Mentioning of PRESERVE in Scientific American Article: http://www.scientificamerican.com/article.cfm?id=wireless-car-hacking	Raised Awareness
31-04-2011	NXP, Eindhoven, The Netherlands	Meeting with NXP to discuss MK3 platform (selected radio hardware in Score@F).	Adjusted implementation and testing plans, NXP interested in cooperation.
02-05-2011	C2C-CC Sec. WG Meeting, Vienna, Austria	Attending the C2C-CC Sec. WG meeting, Vienna	Prepared joint position for following ETSI meeting
03/04-05-2011	ETSI Meeting, Vienna, Austria	Presenting PRESERVE at the ETSI TC ITS WG 5 Meeting, Vienna	Agreement on collaboration, PRESERVE provided input to ETSI TC ITS WG5
04-05-2011	eSafety Forum Membership	KTH joint eSafety Forum	Closer link to eSafety Forum
10-05-2011	Publication and Presentation at IEEE/IFIP Med-Hoc-Net 2011	M. Fiore, C. Casetti, C.-F. Chiasserini, P. Papadimitratos , "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks", accepted paper at the IEEE/IFIP Med-Hoc-Net 2011	Academic Dissemination of research results
16-05-2011	Meeting PRESERVE-SUNSET at Novay, Enschede, Netherlands	F. Kargl presented PRESERVE to SUNSET project	Agreement on Collaboration
05-2011	Publication in IEEE Communications Magazine	F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischof, "Research Challenges in Intervehicular Communication: Lessons of the 2010 Dagstuhl Seminar", IEEE Communications Magazine, vol. 49, no. 5, pp. 158 - 164, 05/2011.	Academic dissemination of challenges and future research issues resulting from research seminar co-organized by F. Kargl
07-06-2012	ITS European Congress, Lyon, France	Contribution by Brigitte Lonc, Renault, to the CeS2 Special Session at ITS European Congress Lyon, Summary published on ComeSafety2 website. Moderator: Juhani Jääskeläinen (Head of Unit - ICT for Transport)	Liaison with COMeSafety2 projects. Integration of security and privacy sub-system in the COMeSafety2 Cooperative ITS architecture
20-06-2011	Publication and Presentation at Second International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN 2011)	A. Kung, J-C. Freytag, and F. Kargl, "Privacy-by-Design in ITS Applications - The Way Forward", Second International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN 2011), Lucca, Italy, June 2011.	Academic dissemination of research results
30-06-2011	Technical Meeting, Darmstadt	Coordination of Public key Infrastructure (PKI) specification and activities between Car-2-car Communication Consortium and PRESERVE project	Harmonization of approaches
13-07-2011	Stuttgart/Böblingen	Frank Kargl (UT) meeting representatives from CAMP and C2C-CC that were at Daimler/Böblingen	Alignment of architecture and

		for the ITS Concertation Meeting	demonstration plans
08-2011	Publication and Presentation at IEEE International Conference on ITS Telecommunications (IEEE ITST), St. Petersburg, Russia	V. Manolopoulos, P. Papadimitratos, S. Tao, A. Rusu, Securing Smartphone Based ITS," IEEE International Conference on ITS Telecommunications (IEEE ITST), St. Petersburg, Russia, August 2011	Academic dissemination of research results
28-08-2011	Publication and Presentation at first International Workshop on Privacy by Design (PBD 2011), Vienna, Austria	M. Kost, J.-C. Freytag, F. Kargl, A. Kung, “Privacy Verification Using Ontologies”. First International Workshop on Privacy by Design (PBD 2011), August 28, 2011, Vienna, Austria.	Academic dissemination of research results
01-09-2011	Publication	G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, “On the Performance of Secure Vehicular Communication Systems,” IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)	Academic dissemination of research results
06/07-09-2011	OVERSEE General Assembly, Berlin, Germany	Presentation by J. Petit (UT) of PRESERVE and discussion about joint demo and integration of OVERSEE results into the VSS	Aligned work plan
12-09-2011	Coordination meeting with NXP in Enschede, Netherlands	Meeting with NXP to discuss MK3 platform (selected radio hardware in Score@F).	NXP provides information that supports hardware integration of HSM
13-09-2011	Collaboration meeting with EVITA at Fraunhofer SIT, Darmstadt, Germany	Meeting to discuss collaboration with EVITA (including cooperation agreement).	Plan for next steps for finalizing cooperation agreement and agreement on joint demo and dissemination activities
20-09-2011	ITS Europe, Lille, France	Presentation by B. Lonc (Renault) of PRESERVE poster and participation in podium discussion at stakeholder forum organized by SCORE@F participants from OEM, suppliers, academics, french regional and national authorities, and Ertico	Awareness and security testing objectives in the French FOT
26-09-2011	Publication in IEEE Transactions on Mobile Computing	Marco Fiore, Claudio Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, vol. 99, no. PrePrints, 2011	Academic dissemination of research results
10-2011	ETSI TC ITS Meeting	Discussion with INRIA on IPv6 security and cross-layer architecture (pseudonym change).	Harmonization on security with IP and non-IP communication
10-10-2011	Publication and Presentation at IEEE WiMob 2011, Shanghai, China	Petit, J.Y. and Mammeri, Z., Dynamic Consensus for Secured Vehicular Ad Hoc Networks, In: Proceedings of the 7th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE WiMob 2011,10 October 2011	Academic dissemination of research results
17-10-2011	Publication and Presentation at IEEE MASS 2011, Valencia, Spain	R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, “Collaborative Location Privacy,” IEEE 8th International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS), Valencia, Spain, October 2011	Academic dissemination of research results
20-10-2011	Presentation at Publication at ITS	Norbert Bißmeyer, Hagen Stübing, Elmar Schoch, Stefan Götz, Jan Peter Stotz, Brigitte Lonc, A	Academic dissemination of

	World-Congress, Orlando, Florida	Generic Public Key Infrastructure FOR Securing Car-to-X Communication, ITS World Congress 2011, Orlando, USA	research results
21-10-2011	7th International Workshop on Vehicle Communications organized by COMeSafety 2, co-located with ITS WC, Orlando, Florida	F. Kargl (UT) participated in panel discussion on Security and Privacy	Discussions with stakeholders, coordination and harmonization with various related projects
24/25-10-2011	iMobility Plenary Meeting, Brussels, Belgium	Presentation of PRESERVE objectives and first result (VSA). Discussion with other European projects (especially FOTsis).	Raised awareness of project and project results. Coordination with FOTsis
14/16-11-2011	IEEE VNC 2011, Amsterdam, Netherlands	Frank Kargl co-chaired and co-organized IEEE VNC2011, organization and moderation of panel discussion on "LTE vs. IEEE 802.11p – which technology to go for?", Amsterdam, Netherlands	Academic forum for dissemination and discussion
14-11-2011	Keynote Presentation at IEEE VNC 2011, Amsterdam, Netherlands	P. Papadimitratos gave keynote talk on "Security on Wheels"	Raised awareness of project and project results
14-11-2011	Publication and Presentation at IEEE VNC 2011, Amsterdam, Netherlands	J. Petit, M. Feiri, and F. Kargl, "Spoofed Data Detection in VANETs using Dynamic Thresholds", Proceedings of the 3rd IEEE Vehicular Networking Conference (VNC 2011), Amsterdam, The Netherlands, IEEE, pp. 25-32, 11/2011.	Academic dissemination of research results
17-11-2011	Meeting with representatives from Toyota ITC in Enschede, Netherlands	Meeting between representatives from Toyota ITC and PRESERVE. Presentation of PRESERVE status and discussion of cooperation opportunities.	Raises awareness in the Japan.
23-11-2011	Presentation, Collaboration discussion	Presentation by F. Kargl (UT) of PRESERVE Progress and Cooperation Plans at EVITA Final Workshop, Honda Academy, Erlensee	Agreed on approach regarding cooperation agreement, aligned uptake of cooperation, planning joint demonstration at ITS WC in Vienna
24/25-11-2011	C2C-CC Forum 2012, Honda Academy, Erlensee	PRESERVE Partners attending C2C-CC Forum 2012, Honda Academy, Erlensee, Poster of PRESERVE shown.	Collaboration discussions with many stakeholders, raised awareness. Confirmation of use of PRESERVE in ScoreF french FOT and liaison with DriveC2X security leader.
01-12-2011	Meeting with Advisory Board and EVITA	As part of our Q5 meeting, we met with members from VW, Audi, and BMW and the coordinator of EVITA to present our recent results (esp. the VSA), explain our plans for 2012, and receive feedback to align our work with the interests of stakeholders. Furthermore, we had discussions with EVITA to resolve open issues regarding the cooperation agreement and plan the joint demo.	Harmonization with stakeholders and EVITA. Some progress towards cooperation agreement.

2011-12	Contributions to ETSI TC ITS	Contributions for next ITS WG5 meeting: specification of ITS cross-layer architecture, SN-SAP specification, performance requirements report. Convergence with Drive C2X SAP specification	Discussion of PRESERVE results in ETSI TC ITS WG5
2011-12	Contributions to C2C-CC	Contribution of PRESERVE technical reports on performance requirements, APIs, and architecture to C2C-CC Security WG	Discussion of PRESERVE results in ETSI TC ITS WG5
Continuously	ETSI	PRESERVE partners Renault and Fraunhofer regularly attend ETSI TC ITS WG5 meetings and confcalls	Contribution of results, contribution to documents, alignment with standardization process
Continuously	Car2Car Communication Consortium	PRESERVE partners Renault, Fraunhofer, escrypt, and UT regularly attend C2C-CC Sec. WG meetings and confcalls, contributions to taskforces PKI, secure hardware and assurance levels, HW/SW integration and initiation of a privacy taskforce	Contribution of results, contribution to documents, alignment with work in C2C-CC

4 Plan for Dissemination and Exploitation Activities in Y2 and Beyond

In this chapter, we will discuss our dissemination plans for Y2 and beyond, including plans for exploitation of PRESERVE results by the PRESERVE partners (especially industrial partners).

4.1 International Liaison Workshop

We aimed at organizing a joint workshop together with partners from CAMP already at ITS WC 2011 in Orlando, Florida. However, due to tight deadlines in CAMP, we decided to postpone and shift focus. We have now proposed to organize a special session on "ITS Security Roadmap for Harmonization and Deployment" at the next ITS World Congress 2012 in Vienna with confirmed attendance of stakeholders from the US and Europe. If this special session is not accepted, we plan to organize a separate workshop attached to ITS WC or standalone. We also proposed two demo activities at ITS WC 2012, one involving a joint demo with the EVITA project, the other one a joint demo with CAMP/VSC-3 as part of the joint EU-US showcase.

We argue that these activities will fulfil the intended purpose of Task 6200 and even extend it by a joint demo, which was not foreseen in the original DoW. In combination with the venue that typically attracts all major international stakeholders, a broad aware of PRESERVE, dissemination of PRESERVE results, and discussion of security and privacy harmonization needs can be achieved.

4.2 PRESERVE Summer School

We achieved to acquire extra funding from the EIT ICT Labs Activity Line on ITS to organize a summer school on security and privacy in ITS during the summer or autumn 2012. This will attract a large number of (especially junior) researchers from all over Europe and beyond to hear about the latest findings in ITS security and privacy protection as well as discuss about the challenges ahead. We plan to make this a highly interactive event and publish a report about the outcomes in a well-established magazine.

4.3 Liaison Activities

Liaison activities with partner projects have top priority in 2012. First of all, this relates to our collaboration with Score@F, where integration of the VSS is to be achieved, followed by joint tests and evaluations. When this is achieved, this can be the basis for more joint dissemination activities later on.

Next, we continue to work on an agreement with EVITA and its partners, especially BMW which is required to conduct the joint demo at ITS WC Vienna.

Close links will be maintained with ETSI TC ITS and C2C-CC Sec. WG where PRESERVE partners will continue to actively inject PRESERVE results and other contributions.

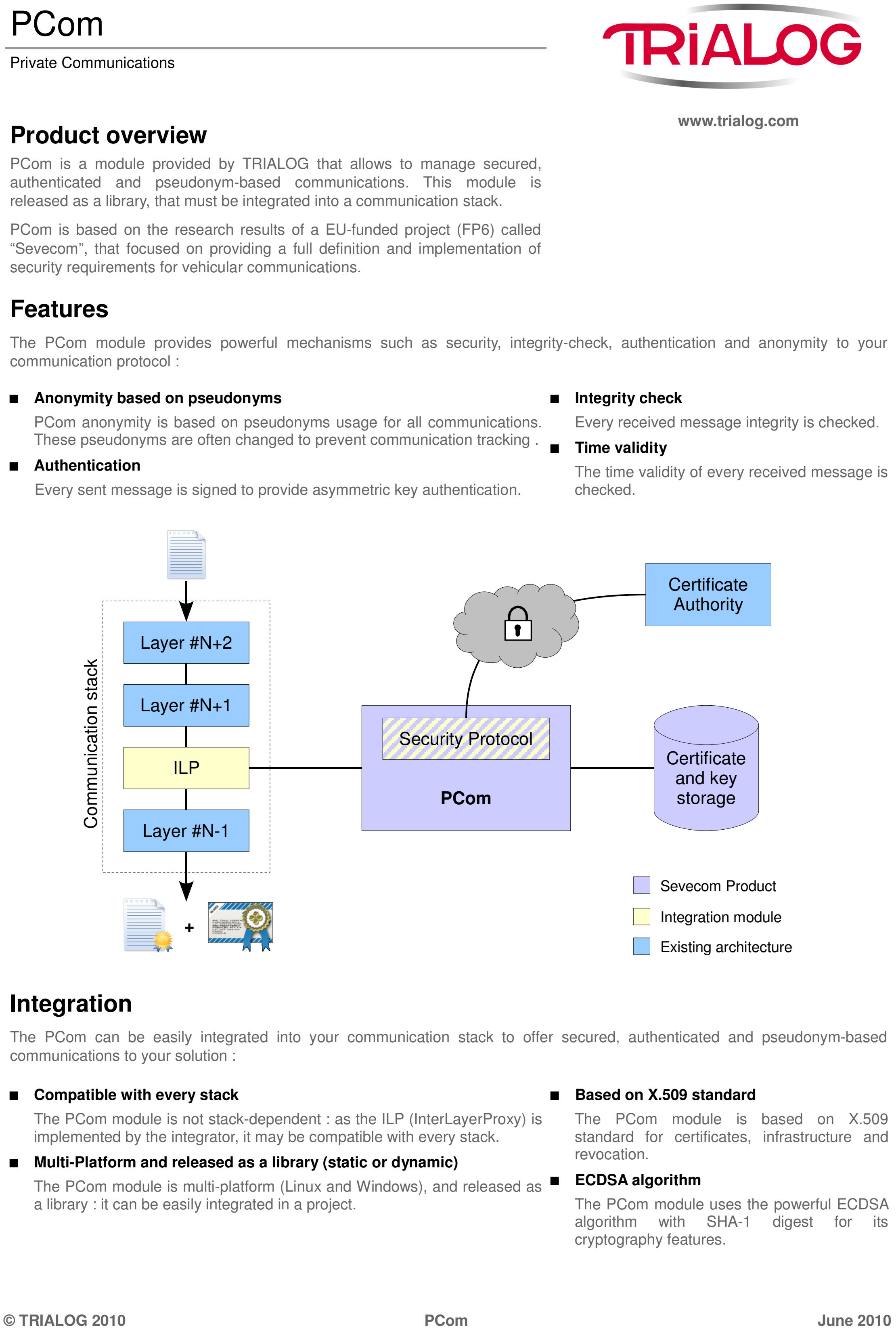
With CAMP / VSC-3 we will work on a joint demo for the ITS WC Vienna but also aim at preparing a later test of the PRESERVE VSS / HSM in their systems.

With DRIVE C2X, FOTsis, and OVERSEE we will have joint technical meetings. In the case of DRIVE C2X and FOTsis we aim at supporting them in matters of security and privacy protection. With DRIVE C2X, we can envision also a security plug-testing to investigate compatibility issues.

4.4 Plans of Different Partners for Dissemination and Exploitation

This section is part of the confidential Annex 1 of D6.1

5 Appendix A – PCOM Factsheet



PCom

Private Communications

TRIALOG

www.trialog.com

Product overview

PCom is a module provided by TRIALOG that allows to manage secured, authenticated and pseudonym-based communications. This module is released as a library, that must be integrated into a communication stack.

PCom is based on the research results of a EU-funded project (FP6) called "Sevecom", that focused on providing a full definition and implementation of security requirements for vehicular communications.

Features

The PCom module provides powerful mechanisms such as security, integrity-check, authentication and anonymity to your communication protocol :

- **Anonymity based on pseudonyms**
  PCom anonymity is based on pseudonyms usage for all communications. These pseudonyms are often changed to prevent communication tracking .
- **Authentication**
  Every sent message is signed to provide asymmetric key authentication.
- **Integrity check**
  Every received message integrity is checked.
- **Time validity**
  The time validity of every received message is checked.

▨	Sevecom Product
□	Integration module
▨	Existing architecture

Integration

The PCom can be easily integrated into your communication stack to offer secured, authenticated and pseudonym-based communications to your solution :

- **Compatible with every stack**
  The PCom module is not stack-dependent : as the ILP (InterLayerProxy) is implemented by the integrator, it may be compatible with every stack.
- **Multi-Platform and released as a library (static or dynamic)**
  The PCom module is multi-platform (Linux and Windows), and released as a library : it can be easily integrated in a project.
- **Based on X.509 standard**
  The PCom module is based on X.509 standard for certificates, infrastructure and revocation.
- **ECDSA algorithm**
  The PCom module uses the powerful ECDSA algorithm with SHA-1 digest for its cryptography features.

© TRIALOG 2010 PCom June 2010