PRESERVE

preparing secure v2x communication systems

PREparing SEcuRe VEhicle-to-X Communication Systems

Deliverable 6.3

Y3 Dissemination Report

Project:	PRESERVE
Project Number:	IST-269994
Deliverable:	D6.3
Title:	Y3 Dissemination Report
Version:	v1.0
Confidentiality:	Public
Editors:	Frank Kargl, Jonathan Petit (UT)
Date:	28. February 2014

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	2014-01-13
0.2	Integrated reviews and input from partners	F. Kargl	2014-02-08
1.0	Prepared final version	F. Kargl, J. Petit	2014-02-14

Approval

	Name	Date
Prepared	F. Kargl	2014-02-14
Reviewed	All Partners	2014-02-15
Authorised	F. Kargl	2014-02-16

Circulation

Recipient	Date of submission
Project partners	2014-02-28
European Commission	2014-02-28

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 1 22, 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:	Trialog, 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 Y3 of the PRESERVE project (1.1.2013 - 31.12.2013). 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 Y3
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

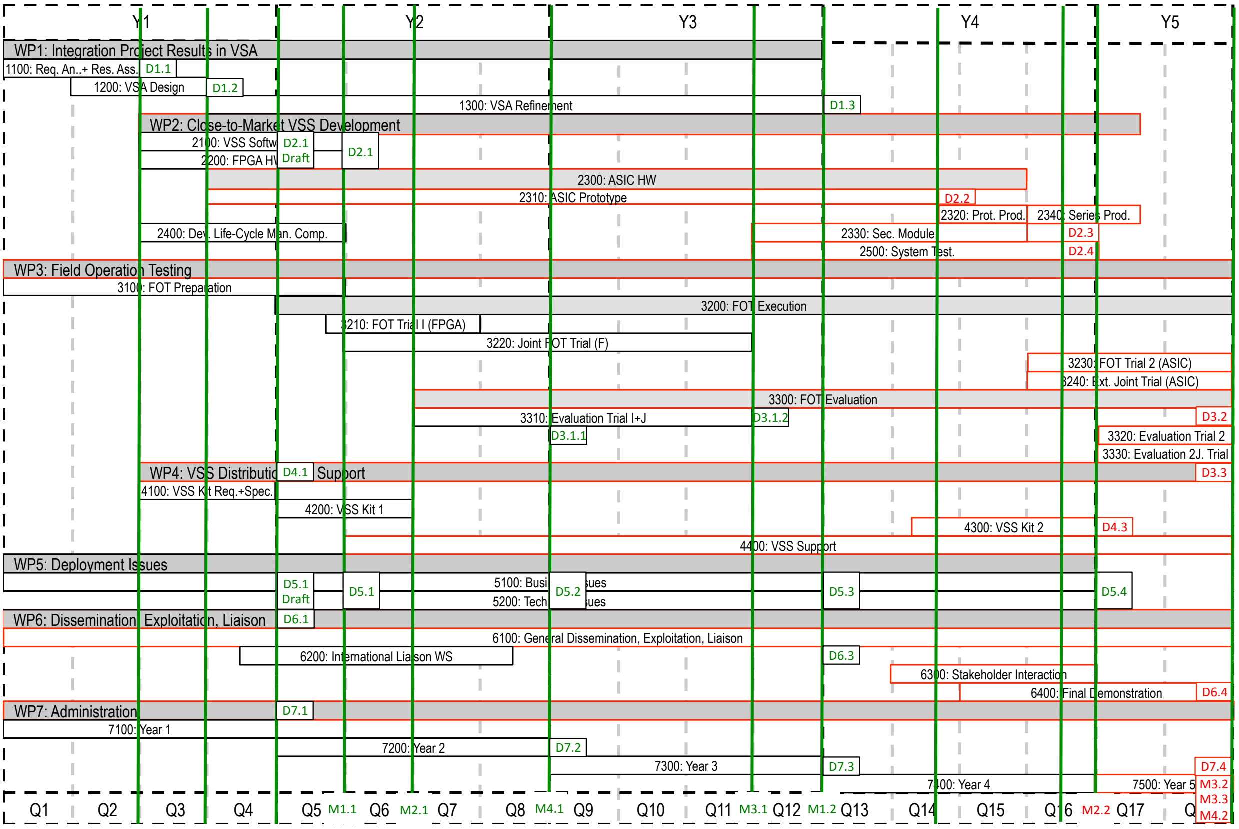
Corresponding Milestones are:

Milestone number	Milestone name	Sub-milestones	Work package(s) involved	Expected date [3]	Means of verification[4]
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 and joint trial 1 results available	WP3	M26	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

[3] Measured in months from the project start date (month 1). The months are consistent with the requested third amendment text.

[4] 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[5]:



As can be seen, PRESERVE was expected to reach milestones M1.2 and M3.1 during Y3. Deliverables D6.2 “Y2 Dissemination Report” and D3.1 “FOT Trial 1 Results” were delivered on time. Deliverables D1.3 “V2X Security Architecture V2” is delivered together with this report (D6.3 “Y3 Dissemination Report”).

D7.3 provides a detailed status discussing including potential deviations from the upcoming work plan.

We constitute that Milestones 1.2 and M3,1 have been reached according to plan.

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

[5] The timing shown corresponds to the requested third amendment.

  - 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 regularly 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)[6]

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.

[6] Note that timing corresponds to the requested amendment 3.

- 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 54): Dissemination and liaison activities (promote final results among stakeholders and scientific community)
- Subtask 6160: Advisory Board (M1 to M54): 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)[6]

Organize first dissemination workshop with international participation to ensure worldwide awareness. Workshop planned during Y2.

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 Interaction (M40 to M48, 5.5 MM) [6]

Interact with stakeholders from industry to discuss progress and receive input. A meeting with selected stakeholders (OEMs and suppliers, European FOTs and related projects from other continents) is planned as part of the Advisory Board meeting for M48.

This task also includes the participation to the Harmonization Task Group 6 (HTG #6), which fosters the harmonization between US and EU w.r.t development and deployment of future ITS. Fraunhofer SIT will actively participate in HTG #6.

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 (M43 to M54, 8.5 MM) [6]

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 Y2 Dissemination Report, which is to include:

- Press releases
- Scientific publications
- Flyers
- Web site
- Handbook

- Plan for use and dissemination.

D6.2 also includes an initial dissemination and exploitation plan.

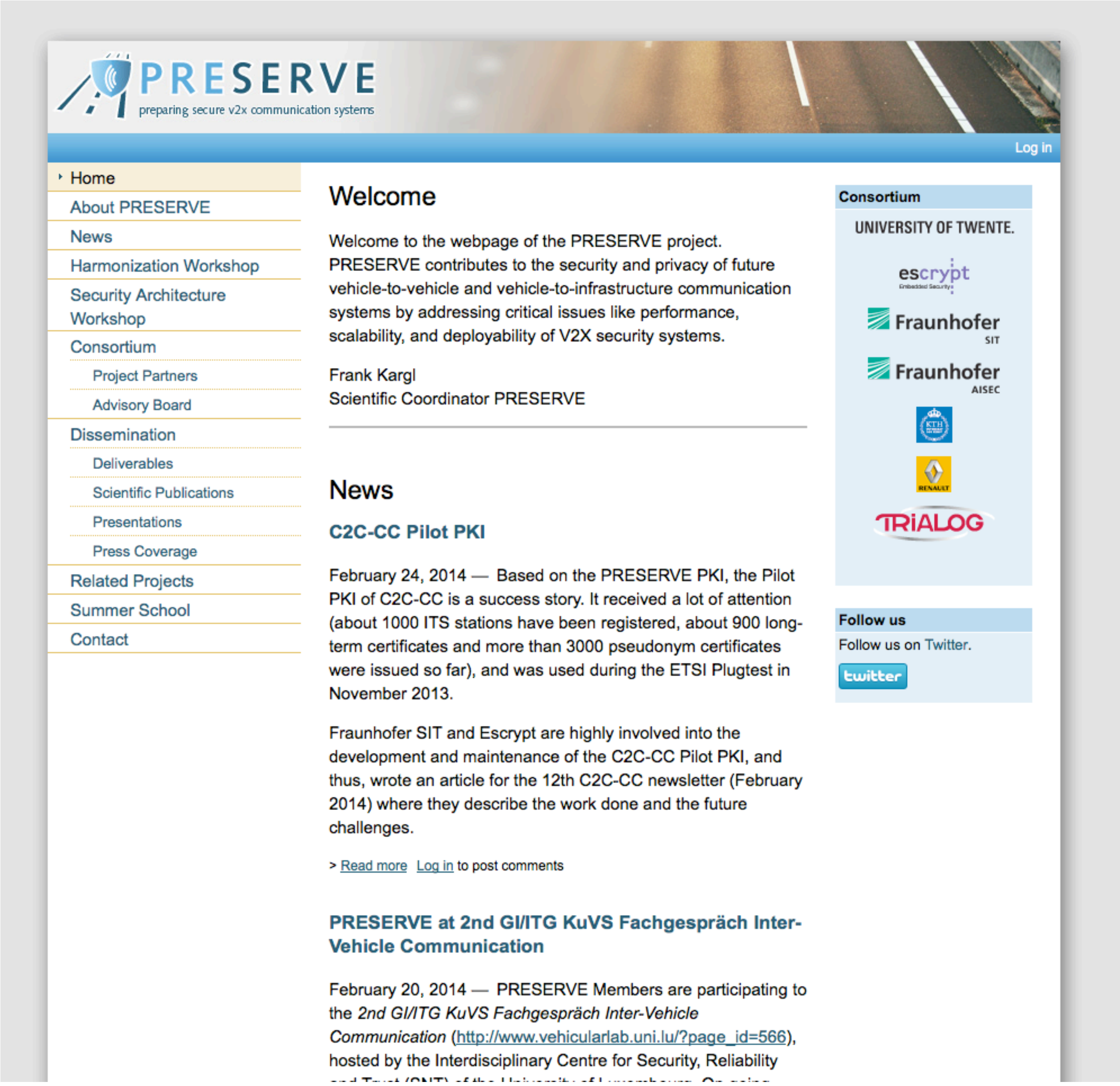
3 Y3 Dissemination Activities

This chapter lists dissemination and liaison activities in Y3 of the project

3.1 Dissemination Material

Already in 2011, PRESERVE had created a range of dissemination material to present its results and on-going work to interested parties.

In 2013, we continued to maintain 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

C2C-CC Pilot PKI

February 24, 2014 — Based on the PRESERVE PKI, the Pilot PKI of C2C-CC is a success story. It received a lot of attention (about 1000 ITS stations have been registered, about 900 long-term certificates and more than 3000 pseudonym certificates were issued so far), and was used during the ETSI Plugtest in November 2013.

Fraunhofer SIT and Escrypt are highly involved into the development and maintenance of the C2C-CC Pilot PKI, and thus, wrote an article for the 12th C2C-CC newsletter (February 2014) where they describe the work done and the future challenges.

> Read more Log in to post comments

PRESERVE at 2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication

February 20, 2014 — PRESERVE Members are participating to the *2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication* (http://www.vehicularlab.uni.lu/?page_id=566), hosted by the Interdisciplinary Centre for Security, Reliability

Follow us on Twitter.

Other dissemination material was created for dedicated events and will be discussed later.

Operational information for PRESERVE partners is maintained in 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 and maintaining minutes.

3.2 Reviewed Publications

The following scientific papers on ITS / V2X Security and Privacy were published by PRESERVE partners in 2013. If not noted otherwise, the publications were peer-reviewed.

With 13 peer-reviewed publications, 2013 has again been a highly successful year for PRESERVE where the project was able to be highly visible at a number of premiere publication venues in the field. This started with ACM SIGMOBILE's and SIGSAC's joint conference on wireless security issues, where PRESERVE partners was able to publish two papers and one paper at a co-located workshop. In November, PRESERVE members had two presentations at the new specialized workshop on Security, Privacy & Dependability for Cyber Vehicles (CyCar) co-located with the high-profile ACM CCS conference. Then, PRESERVE partners achieved four accepted papers at IEEE's Vehicular Networking Conference, three on security-related topics resulting from our PRESERVE research activities.

D5.3 provides more detailed discussions of these research results.

Scientific Publications in 2013

1. N. Bißmeyer, J. Petit, and K. Bayarou, "Copra: Conditional pseudonym resolution algorithm in VANETs", Wireless On-demand Network Systems and Services (WONS), 2013 10th Annual Conference on, pp. 9-16, 2013.

2. F. Kargl, A. Friedman, and R. Boreli, "Differential Privacy in Intelligent Transportation Systems", Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA, ACM, pp. 107–112, 2013.

3. R. Wouter van der Heijden, S. Dietzel, and F. Kargl, "SeDyA: Secure Dynamic Aggregation in VANETs", Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA, ACM, pp. 131–142, 2013.

4. N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, "VeSPA: Vehicular Security and Privacy-preserving Architecture", Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy, 2013.

5. M. Fiore, C. Ettore Casetti, C-F. Chiasserini, and P. Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks", Mobile Computing, IEEE Transactions on, vol. 12, no. 2, pp. 289-303, Feb., 2013.

6. M. Laganà, M. Feiri, M. Sall, M. Lange, A. Tomatis, and P. Papadimitratos, "Secure Communication in Vehicular Networks – PRESERVE Demo", Proceedings of the 5th IEEE International Symposium on Wireless Vehicular Communications, 2013.

7. N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos, "Towards a secure and privacy-preserving multi-service vehicular architecture", World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a, pp. 1-6, 2013.

8. R. Moalla, B. Lonc, H. Labiod, and N. Simoni, "Security architecture for cooperative ITS-S vehicles", 11th International Embedded Security in Cars Conference, 2013.

9. M. Feiri, J. Petit, and F. Kargl, "Efficient and Secure Storage of Private Keys for Pseudonymous Vehicular Communication", Proceedings of the 2013 ACM CCS Workshop on Security, Privacy & Dependability for Cyber Vehicles, New York, NY, USA, ACM, pp. 9–18, 2013.

10. C. Höfer, J. Petit, R. Schmidt, and F. Kargl, "POPCORN: Privacy-preserving Charging for Emobility", Proceedings of the 2013 ACM CCS Workshop on Security, Privacy & Dependability for Cyber Vehicles, New York, NY, USA, ACM, pp. 37–48, 2013.
11. M. Feiri, J. Petit, and F. Kargl, "The Impact of Security on Cooperative Awareness in VANET", Vehicular Networking Conference (VNC), 2013 IEEE, 2013.
12. S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems", Vehicular Networking Conference (VNC), 2013 IEEE, 2013.
13. N. Bißmeyer, K. Henrik Schröder, J. Petit, S. Mauthofer, and K. Bayarou, "Short Paper: Experimental Analysis of Misbehavior Detection and Prevention in VANETs", Vehicular Networking Conference (VNC), 2013 IEEE, 2013.

3.3 Press Coverage, Presentations, General Liaison

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

The following outreach activities were conducted. Note that we do not list presentations of accepted papers at conferences and workshops where listed already in Section 3.2.

Selected activities will thereafter be discussed in separate sections.

2013-01-08 Meeting with state police Bavaria to discuss implications of C2X introduction for their work and potential security implications.

2013-01-15/16 Technical meeting with DRIVE C2X, NEC, Heidelberg, to collaborate on V2X integration into DRIVE C2X.

2013-01-15/17 Participation to ETSI TC ITS WG5 and ETSI Security Workshop to update ETSI on PRESERVE results.

2013-02 Technical Program Co-Chairing of the IEEE VTS Vehicular Technology Conference to provide the community a venue for publication and discussion of (also C2X security-related) results.

2013-02-28 Presentation of PRESERVE project and results to University of McGill and Universite Polytechnique de Montreal (DIVA Network of Excellence), Montreal, Canada

2013-02/04 Jonathan Petit spends a research stay at the University of California, Berkeley in the PATH group to collaborate on future security and privacy challenges in automated driving.

2013-04-11 Presentation of PRESERVE to Palo Alto Research Center (PARC) , California, U.S.A.

2013-04-18/19 Presentation of PRESERVE to Stanford University, California, U.S.A.

2013-04-22 Presentation of PRESERVE to Toyota ITC, California, U.S.A.

2013-04-26 Presentation of PRESERVE to UCLA, California, U.S.A.

2013-04-29 Presentation of PRESERVE to Mercedes-Benz Research and Development Center, California, U.S.A.

2013-05-15 escrypt hosts C2C-CC Security Working Group Meeting in Munich.

2013-06-02/03 Enhanced PRESERVE VSS Kit 1 Demo shown at IEEE WiVec 2013 in Dresden, Germany.

2013-06-04 Participation of PRESERVE members to C2C-CC Security Working Group Meeting in Ulm

2013-06-05 Joint PRESERVE-C2C-CC Security Architecture Workshop organized in Ulm, Germany.

2013-06-13/14 Enhanced PRESERVE VSS Kit 1 Demo shown at DRIVE C2X event (Gothenburg, Sweden)

2013-06 Renault submits patent application on the process for remote loading of pseudonym certs delivered by a CA to vehicles.

2013-07-23 Presentation of PRESERVE results on Misbehavior Detection at GI KuVS Summer School on "Application-Tailored Networks" in Berlin.

2013-09-22/25PRESERVE members participate to a Dagstuhl Seminar on Inter-vehicular communications and give a short presentation on research results and future research challenges in ITS security.

2013-09-24 PRESERVE organizes a dedicated security session at the Score@F 3rd stakeholders forum.

2013-09-26/27 Participation of PRESERVE members to C2C-CC Security Working Group Meeting in Gaimersheim, Germany.

2013-11-05 Presentation of PRESERVE at Compass4D general assembly, Verona, Italy to discuss potential future collaboration.

2013-11-11 Cooperation meeting with AB member Audi to discuss industry security roadmap.

2013-11-18 Participation of PRESERVE members to C2C-CC Security Working Group Meeting

2013-11-18 Presentation of PRESERVE research results at the University of Linkoping, Sweden

2013-11-19/20 Participation of PRESERVE partners at the annual C2C-CC Forum 2013 in Munich with presentation on our results on “Misbehavior Detection and Attacker Revocation".

2013-11-25/29 Successful participation to ETSI Plugtest shows interoperability of PRESERVE solution with other implementations of V2X standards.

2013-11-29 Presentation on security and privacy for intelligent electric vehicles including PRESERVE results to students visiting University of Ulm (SIA - Schüler-Ingenieur-Akademie, http://www.sia-bw.de/)

2013-12-02 Presentation at French workshop: Systèmes coopératifs ‘Car to Car’ et ‘Car to infrastructure’. Atelier recherche Gendarmerie Nationale, Les objects connectés : sécurité et liberté.

2013-12-06 Meeting with ITRI, Taiwan, to prepare cooperation agreement and plan use of ITRI 802.11p modems in PRESERVE tests.

*3.4 Joint **PRESERVE**-C2C-CC **Security Architecture Workshop***

On June 5th 2013, PRESERVE and the security and architecture working groups of the C2C-CC jointly organized a security architecture workshop in Ulm, Germany. The goal of this workshop was to bring together a large number of stakeholders in the field to discuss a number of architecture- and implementation-related questions that would directly contribute to the refinement and finalization of the PRESERVE V2X Security Architecture (VSA) in Deliverable 1.3.

Interest by participants was so large that we had to close the registration as room capacity was limited and we also wanted to ensure an effective atmosphere for discussions which ruled out accepting too many participants. The final list of participation included 28 participants from industry and academia:

1.	Nikolaos	Alexiou	KTH
2.	Boris	Atanassow	Denso
3.	Norbert	Bissmeyer	SIT
4.	Lutz-Peter	Breyer	Denso
5.	Thierry	Ernst	INRIA
6.	Daniel	Estor	escrypt
7.	Mark	Etzel	Security Innovation
8.	Michael	Feiri	UT
9.	Sibylle	Froeschle	OFFIS
10.	Stylianos	Gisdakis	KTH
11.	Holger	Heinemann	VECTOR
12.	Anke	Jentzsch	VW
13.	Christophe	Jouvray	Trialog
14.	Frank	Kargl	UT
15.	Alexander	Kiening	AISEC
16.	Jürgen	Kopsch	MARBEN product
17.	Tim	Leinmüller	Denso
18.	Hans	Löhr	BOSCH
19.	Brigitte	Lonc	Renault
20.	Rim	Moalla	Renault
21.	Jonathan	Petit	UT
22.	Corinne	Rosier	Mitsubishi Electric
23.	Michel	Sall	Trialog
24.	Elmar	Schoch	Audi
25.	Alexander	Stuehring	OFFIS
26.	Rens	van der Heijden	Ulm University
27.	Timo	van Roermund	NXP
28.	Andras	Varadi	Lesswire

Throughout the day, the agenda focused on a number of selected challenges where we still see open and pressing issues. Each topic was introduced by an expert with a short presentation, followed by extensive time for discussion.

WEDNESDAY, 05.06.2013		
10:00	*Welcome*	*PRESERVE, C2C-CC*
10:15	*Presentation of the PRESERVE V2X Security Architecture*	*Norbert Bissmeyer, Fraunhofer SIT*
10:30	*Discussion: are we ready for day one? What is missing from the picture?*	*Elmar Schoch, Audi*
11:00	*Combining IP and non-IP communication security*	*Thierry Ernst, ITSSv6*
11:35	*Stack Parallelism to exploit full potential of HSM*	*Daniel Estor, Escrypt*
12:10	*Lunch*	
13:10	*Verification on Demand & Cert. Omission and Distributed Congestion Control*	*Michael Feiri, University of Twente*
13:45	*Meta-data and signaling*	*Norbert Bissmeyer, Fraunhofer SIT*
14:20	*PKI Development*	*Alexander Kiening, Fraunhofer AISEC*
14:55	*Coffee break*	
15:30	*Podium discussion:* *Security Architecture Roadmap*	*Moderator: Frank Kargl, University of Twente*
17:00	*Closing of PRESERVE architecture workshop*	
19:00	*Dinner (at your own expense)*	*Zunfhaus Ulm*

After a short presentation of the PRESERVE VSA from D1.1 by Norbert Bißmeyer, the head of the C2C-CC security WG, Elmar Schoch, presented his views on the question whether we are ready for day one deployment or whether important aspects where missing from the picture. Thierry Ernst from the ITSSv6 projects presented his view on challenges for combining IP and non-IP communication security and participants discussed ways how to, e.g., use similar certificate formats or HSM APIs for both worlds. Daniel Estor from escrypt triggered a more implementation-focused discussion on stack parallelism caused by multi-core HSMs. Next, Michael Feiri from University of Twente highlighted the close relationships of security-related VoD and certificate omission mechanisms with distributed congestion control and suggested that both should be integrated. Meta-data and cross-layer signalling is a topic that PRESERVE is bringing up already for years in ETSI and C2C-CC as an important mechanism, not only for security. Alexander Kiening from Fraunhofer AISEC, representing the German CONVERGE project, set an interesting focus on PKI development in heterogenous networks, involving C2X as well as cellular networks. In the end, Elmar Schoch (representing the C2C-CC Sec. WG), Tim Leinmüller (representing the C2C-CC Arch. WG), and Frank Kargl (representing PRESERVE) summarized some lessons learned and outlined important elements of a future roadmap to come to an enhanced security architecture.

Results of the workshop were presented to the ITS community at the ETSI ITS Workshop in February 2014 in Berlin, Germany and are also discussed in detail in Deliverable 1.3.

3.5 Demonstration Activities

Following our successful demonstration activities in 2012, we showed an enhanced version of our demonstrator at two venues in 2013: at the IEEE WiVec Conference (part of VTC spring) in Dresden Germany and at the DRIVE C2X @TSS event in Gothenburg, Sweden. Both activities helped to raise the awareness about the PRESERVE VSS Kit 1 in the ITS community.

3.6 EU-US Cooperation and Outlook on Automated Driving

As a direct continuation of our 2012 contributions to HTG #1., Dr. Jonathan Petit from PRESERVE visited the UCB PATH laboratory from February to April 2013. The goal of this research stay was twofold: interaction with the ITS community in the bay area and working on identifying the security-related challenges of communicating automated vehicles with the automated driving experts in PATH.

Dr. Petit was highly active, giving presentations on ITS security and privacy and PRESERVE at six different occasions to groups at Berkeley, Stanford, Toyota, Mercedes, PARC, and UCLA. For visibility of PRESERVE and security and privacy issues related to ITS in the US, this has to be considered a huge success.

In 2014, PRESERVE intends to continue our contribution to EU-US exchange by participation to HTG#6.

3.7 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.

Building upon links to those projects that were established in years 1 and 2, we continued our close collaboration especially with **Score@F** where we conducted and concluded extensive joint tests. We held regular phonecalls and integration meetings to integrate the technical platforms and especially cooperation with Hitachi was very fruitful. Renault is a key partner in this, as they are coordinator of Score@F and member of PRESERVE. The two projects signed a formal Memorandum of understanding to describe the terms of our collaboration. A legally binding cooperation agreement could not be signed because of legal concerns and missing signatures of single Score@F partners. We signed an MoU with Hitachi aiming to continue our collaboration beyond the end of Score@F.

We also had regular contacts with **DRIVE C2X** where we succeeded to integrate our VSS Kit 1 with the DRIVE C2X communication solution of NEC and participated to their final demonstration event in Gothenburg.

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. The joint architecture workshop that was organized by the chairs of the C2C-CC Sec. and Arch. WGs and the PRESERVE coordinator was a highlight of this cooperation in 2013 and provided important input to C2C-CC and PRESERVE.

Contacts with **CAMP** were only sporadic in 2012 and 2013, however, interaction with U.S. researchers in academia in industry was still very active as reported above. HTG#6 contributions in 2014 will ensure that this link will remain tight. CAMP is still interested in testing the PRESERVE ASIC once it becomes available.

Regarding **FOTsis**, there was less active exchange between the two projects.

We started a liaison activity with **COMPASS4D**, which we identified as a potentially suitable collaboration partner for a second joint FOT.

PRESERVE kept regular contact with **Advisory Board**. Beyond individual contacts during meetings of ETSI, C2C-CC, conferences, or workshops, we invited the AB to an official meeting during our Q12 meeting on 04.12.2012 which participation from Daimler and Denso. Unfortunately, the representative from Audi had to cancel participation on short notice. PRESERVE presented a detailed status overview to the AB and received their feedback. The topics discussed with the AB included the security architectures in V2X, in-vehicle security, HSM plans and activities in industrial companies, privacy and pseudonym strategies, and business models for C2X security.

3.8 Table of all Y3 Dissemination Activities

The following table lists all dissemination activities in Y3 in detail in chronological order.

Date	Event / Title / Activity	Type	Partners involved	Result
2013-01-08	Meeting with state police Bavaria to discuss implications of C2X introduction for their work	Other	University of Twente	Increased awareness about project results at important stakeholder
2013-01-15/16	Technical meeting with DRIVE C2X, NEC, Heidelberg	Liaison	University of Twente	Integration of PRESERVE into DRIVE C2X
2013-01-15/17	Participation to ETSI TC ITS WG5 and ETSI Security Workshop	Liaison	Renault, Fraunhofer SIT	Increased awareness about project and research results
2013-02	Technical Program Co-Chairing, IEEE VTS Vehicular Technology Conference	Other	KTH	Increased awareness about project and research results
2013-02	Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, M. Fiore, C. Casetti, C. Chiasserini, and P. Papadimitratos	Publication	KTH	Increased awareness about project and research results
2013-02	VeSPA: vehicular security and privacy-preserving architecture, N Alexiou, M Laganà, S Gisdakis, M Khodaei, P Papadimitratos, Paper accepted, ACM HotWiSec 2013	Publication	KTH	Increased awareness about project and research results
2013-02	Secure Communication in Vehicular Networks PRESERVE VSS Kit 1 Demo, M. Lagana, M. Feiri, M. Sall, M. Lange, A. Tomatis, P. Papadimitratos, Demo accepted, IEEE WiVec 2013	Publication, Demo	KTH, University of Twente, Trialog	Increased awareness about project and research results
2013-02-28	Presentation of PRESERVE to University of McGill and Universite Polytechnique de Montreal (DIVA Network of Excellence), Montreal, Canada	Presentation, Liaison	University of Twente	Increased awareness about project and research results, Liaison with DIVA Network of Excellence
2013-03	Submission of abstract to TRA 2014; towards demonstrating testing results from the collaboration with Score@F	Publication	KTH, Renault, University of Twente	Increased awareness about project and FOT results
2013-03-11	Co-chairing Workshop on Mobile Ad-hoc Networks in Stuttgart, Germany	Other	University of Twente	Increased awareness about project and research results
2013-03-18/20	IEEE WONS2013: CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs, Calga-	Publication, Presentation	Fraunhofer SIT, Univer-	Presentation of research results

	ry, Canada		sity of Twente	
2013-04-11	Presentation of PRESERVE to Palo Alto Research Center	Presentation	University of Twente	Presentation of research results, increase awareness of PRESERVE in US
2013-04-18/19	Presentation of PRESERVE to Stanford University	Presentation	University of Twente	Presentation of research results, increase awareness of PRESERVE in US
2013-04-17/19	Presentation of two papers at 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13): "Differential Privacy in Intelligent Transportation Systems" and "SeDyA: Secure Dynamic Aggregation in VANETs"	Presentation	University of Twente	Presentation of research results, increase awareness of PRESERVE
2013-04-19	Presentation of paper at ACM HotWiSec 2013 Workshop (co-located with WiSec '13): "VeSPA: Vehicular Security and Privacy-preserving Architecture"	Presentation	KTH	Presentation of research results, increase awareness of PRESERVE
2013-04-22	Presentation of PRESERVE to Toyota ITC	Presentation	University of Twente	Presentation of research results, increase awareness of PRESERVE in US
2013-04-26	Presentation of PRESERVE to UCLA	Presentation	University of Twente	Presentation of research results, increase awareness of PRESERVE in US
2013-04-29	Presentation of PRESERVE to Mercedes-Benz Research and Development Center	Presentation	University of Twente	Presentation of research results, increase awareness of PRESERVE in US
2013-05-01/04	Secure Communication in Vehicular Networks PRESERVE VSS Kit 1 Demo, M. Lagana, M. Feiri, M. Sall, M. Lange, A. Tomatis, P. Papadimitratos, IEEE WiVec 2013 (Dresden)	Demonstration	KTH	Presentation of research results, increase awareness of PRESERVE
2013-05-15	Organization of C2C-CC Security Working Group Meeting in Munich	Liaison	escrypt	Updating C2C-CC on current PRESERVE status. Agreement on joint work.
2013-05-29	Rim Moalla, Brigitte Lonc, Houda labiod; C-ITS Security: Standards and experimentations; Nevers, France	Presentation	Renault	presentation of ITS security standardization activities and PRESERVE project
2013-06-04	Participation to C2C-CC Security Working Group Meeting in Ulm	Liaison	University of Twente, escrypt	Increased awareness about project and research results
2013-06-05	PRESERVE-C2C-CC Security Architecture workshop in Ulm	Presentation, Liaison	All partners	Input for D1.3
2013-06-03/07	Towards a Secure and Privacy-preserving Multi-service Vehicular Architecture, N. Alexiou, M. Laganà, S Gisdakis, P Papadimitratos, IEEE D-SPAN/WoWMoM 2013	Presentation	KTH	Presentation of research results
2013-06-13/14	Secure Communication in Vehicular Networks PRESERVE VSS Kit 1 Demo, M. Lagana, M. Feiri, M. Sall, M. Lange, A. Tomatis, P. Papadimitratos, DRIVE C2X event (Gothenburg)	Demonstration	KTH	Presentation of research results, increase awareness of PRESERVE
2013-06	Patent submitted on the process for remote loading of pseudonym certs delivered by a CA	Patent	Renault	Benefit of free G5 communication to update security

	to vehicles			credentials
2013-07-23	Presentation of PRESERVE results on Misbehavior Detection at GI KuVS Summer School on "Application-Tailored Networks" in Berlin	Presentation	University of Twente	Presentation of research results, increase awareness of PRESERVE
2013-09-22/25	Dagstuhl Seminar on Inter-vehicular communications	Presentation, Dissemination	University of Twente	Presentation of research results, increase awareness of PRESERVE, working on future research roadmap
2013-09-24	Score@F 3rd stakeholders forum: organization of a PRESERVE session	Presentation	Renault, Trialog	Presentation of PRESERVE results to large audience (> 200 attendees), industrial and public & regional organizations
2013-09-26/27	Participation to C2C-CC Security Working Group Meeting in Gaimersheim	Liaison	escrypt	Updating C2C-CC on current PRESERVE status.
2013-11-04	Michael Feiri, Jonathan Petit, Frank Kargl, "Efficient and Secure Storage of Private Keys for Pseudonymous Vehicular Communication", CCS Workshop (Cycar), Berlin	Presentation, Publication	University of Twente	Presentation of research results of PRESERVE
2013-11-04	Christina Hofer, Jonathan Petit, Robert Schmidt, Frank Kargl, “POPCORN: Privacy-Preserving Charging for eMobility”, CCS Workshop (Cycar), Berlin	Presentation, Publication	University of Twente	Presentation of research results of PRESERVE
2013-11-05	Presentation of PRESERVE at Compass4D general assembly, Verona, Italy	Presentation, Liaison	University of Twente	discussion about joint FOT options
2013-11-11	Cooperation meeting with Audi (AB member)	Liaison	University of Twente	Discussing status of ETSI / C2C-CC activities and collaboration
2013-11-14/15	R.Moalla, B. Lonc, H. Labiod, N. Simoni: Security architecture for cooperative ITS-S vehicles, ESCAR conference	Presentation, Publication	Renault	Presentation of research results of PRESERVE
2013-11-18	Participation to C2C-CC Security Working Group Meeting	Liaison	escrypt	Updating C2C-CC on current PRESERVE status
2013-11-18	Presentation of PRESERVE Research results at the University of Linkoping, Sweden	Presentation	University of Twente	Increased awareness of PRESERVE, research challenges
2013-11-14/20	Norbert Bißmeyer,"Misbehavior Detection and Attacker Revocation", C2C-CC Forum 2013, Munich	Presentation	Fraunhofer SIT	Presentation of research results of PRESERVE
2013-11-19/20	Participation to C2C-CC Forum at MAN Munich	Liaison	escrypt	Dissemination PRESERVE status in discussions with other participants
2013-11-25/29	Participation to ETSI Plugtest	Dissemination	Trialog, University of Twente	Current status of the PRESERVE VSS was presented to the community, interoperability with other standard implementations was proven.
2013-11-29	Presentation on security and privacy for intelligent electric vehicles including PRESERVE results to students visiting University of Ulm (SIA - Schüler-Ingenieur-Akademie, http://www.sia-bw.de/)	Presentation	University of Twente / University of Ulm	Presentation of PRESERVE results and general advertisement for ICT and engineer-

				ing studies
2013-11-29	Crypto Working Group meeting, Utrecht, Netherlands	Dissemination	University of Twente	discussion about security evolution and deployment issues, research challenges
2013-12-02	B. Lonc, A. Perraud (Renault) Systèmes coopératifs 'Car to Car' et 'Car to infrastructure'. Atelier recherche Gendarmerie Nationale, Les objects connectés : sécurité et liberté.	Presentation	Renault	presentation of security/privacy issues in V2X communications and discussion with French authorities
2013-12-06	Meeting with ITRI, Taiwan, to prepare cooperation agreement and plan use of ITRI 802.11p modems in PRESERVE test	Liaison	University of Twente	Preparation of FOT tests
2013-12-16/18	Michael Feiri, Jonathan Petit, Robert Schmidt, Frank Kargl,"The Impact of Security on Cooperative Awareness in VANET", Vehicular Networking Conference 2013, Boston	Presentation, Publication	University of Twente	Presentation of research results of PRESERVE
2013-12-16/18	Stylianos Gisdakis, Marcello Laganà, Thanassis Giannetsos, and Panos Papadimitratos, "SEROSA: SERvice Oriented Security Architecture for Vehicular Communications", IEEE VNC, Boston	Presentation, Publication	KTH	Presentation of research results of PRESERVE
2013-12-16/18	Norbert Bißmeyer, Klaus Henrik Schröder, Jonathan Petit, Sebastian Mauthofer, Kpatcha M. Bayarou,"Short Paper: Experimental Analysis of Misbehavior Detection and Prevention in VANETs", Vehicular Networking Conference 2013, Boston	Presentation, Publication	Fraunhofer SIT, University of Twente	Presentation of research results of PRESERVE

4 Plan for Dissemination and Exploitation Activities in Y4 and Beyond

In this chapter, we will discuss our dissemination plans for Y4 and beyond, including plans for exploitation of PRESERVE results by the PRESERVE partners (especially industrial partners). For confidentiality reasons, the later ones will be presented in Annex I.

4.1 Stakeholder Workshop

We aim at organizing a stakeholder workshop together with our yearly AB meeting in December 2014. This aims specifically at stakeholders from industry to discuss progress and receive input. The workshop is planned when first ASIC prototypes are available. This was originally foreseen for M29 or M30. Due to delays in ASIC production, the workshop will only be held in December 2014.

The purpose of the workshop will be to present the FPGA kit (which is already available and was showcased at the ITS WC 2012) and the ASIC prototype as well as our testbed and create industry interest to adopt the VSS. Our target audience are OEMs and suppliers, European FOTs and related projects from other continents.

4.2 Liaison Activities

Liaison activities with partner projects have high priority also in 2014. We will be in close contact with COMPASS4D to clarify the possibility of a joint test once the VSS Kit 2 is available.

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.

We will contribute our expertise and results to HTG#6 in order to support EU-US harmonization.

4.3 Plans of Different Partners for Dissemination and Exploitation

This section is part of the confidential Annex 1 of D6.3.