PREparing SEcuRe VEhicle-to-X Communication Systems

Deliverable 6.4

Y4&5 Dissemination Report

Project:	PRESERVE
Project Number:	IST-269994
Deliverable:	D6.4
Title:	Y4&5 Dissemination Report
Version:	v1.0
Confidentiality:	Public
Editors:	Frank Kargl (UT), Norbert Bissmeyer (SIT)
Date:	28. June 2015

Part of the Seventh Framework Programme

Funded by the EC - DG INFSO

Document History

Version	Status	Author	Date
0.1	Initial version	F. Kargl	2015-05-25
0.2	Integrated reviews and input from partners	F. Kargl	2015-05-30
0.9	Prepared final draft	F. Kargl, N. Bissmeyer	2015-06-10
1.0	Prepared final version	F. Kargl	2015-06-28

Approval		
	Name	**Date**
Prepared	F. Kargl	2015-06-25
Reviewed	All Partners	2015-06-28
Authorised	F. Kargl	2015-06-28

Circulation	
Recipient	**Date of submission**
Project partners	2014-06-28
European Commission	2014-06-30

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:	Martin Moser
Address:	escrypt GmbH - Embedded Security, Leopoldstr. 244, 80807 München, Germany
Email:	martin.moser@escrypt.com
Phone (Office):	+49 89 208039-191
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 Y4 and Y5 of the PRESERVE project (1.1.2014 - 30.06.2015). It is intended for use within the PRESERVE project and the European Commission. It consists of four parts:

1. An overview chapter describing the status of the project and the dissemination plan according to the DoW (Chapter 2).
2. A chapter on dissemination activities in Y4&5 (Chapter 3).

3. A chapter on planned future dissemination and exploitation activities (Chapter 4).
4. An overall summary of results achieved in WP6 over the whole project duration (Chapter 5).

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

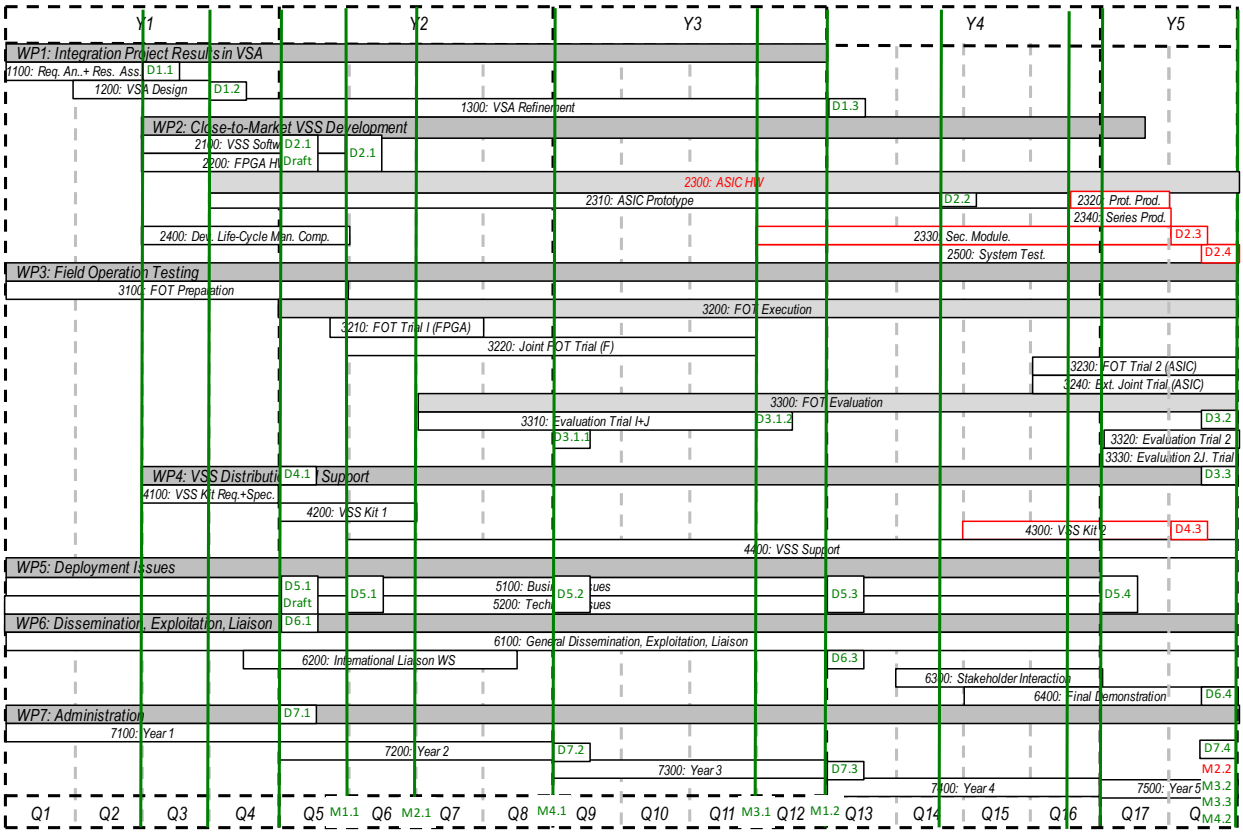
Corresponding Milestones are:

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	M54	D2.2, D2.3, D2.4, D4.3
M3	FOT	M3.1: FOT Trial 1 and joint trial 1 results available	WP3	M33	D3.1
		M3.2: FOT Trial 2 results available	WP3	M54	D3.2
		M3.3: Joined FOT Trial results available	WP3	M54	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	M54	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[3]:



As can be seen, PRESERVE is expected to conclude by end of June 2015. D7.4 provides a detailed status discussing including potential deviations from the upcoming work plan. Within WP7, PRESERVE is expected to achieve MS4.2 documented by this deliverable.

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

[3] The timing shown corresponds to the requested forth amendment.

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 M54, 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 M54): 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 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 Y4&5 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.

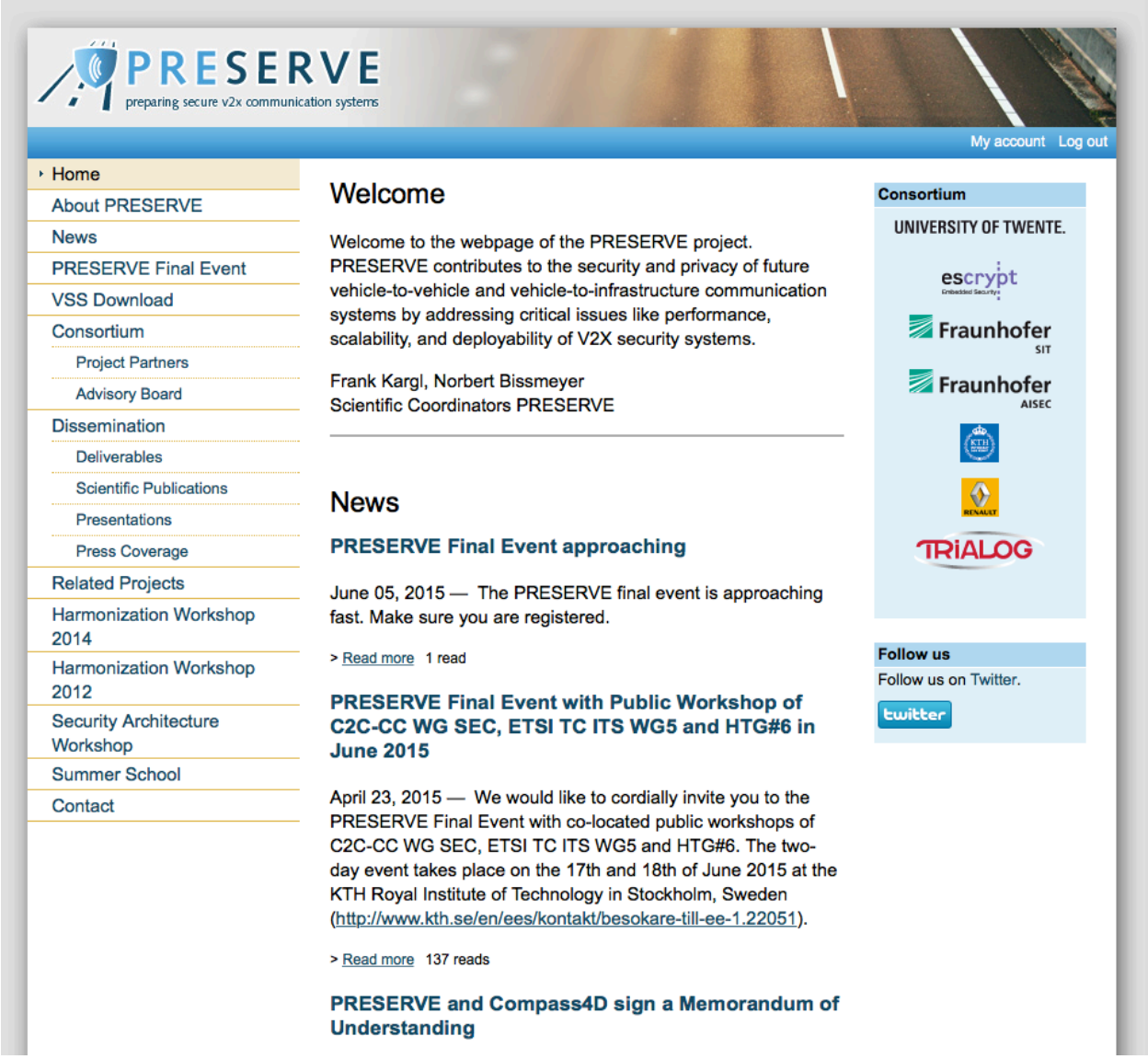
3 Year 4&5 Dissemination Activities

This chapter lists dissemination and liaison activities in Y4&5 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 2014/2015, 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.



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 2014/2015. If not noted otherwise, the publications were peer-reviewed.

With 22 scientific publications, the final one and a half years of PRESERVE have again been a highly successful in terms of scientific productivity and visibility where the project was also represented at a number of premiere publication venues in the field. Two survey articles on ITS-related topic were published in IEEE Communication Surveys and Tutorials which has an impact factor of 6.49. Furthermore, we had two additional journal publications in the field, ten publications at IEEE conferences or workshops, and five papers at workshops with technical reports. The list also includes three PhD theses of young researchers involved in PRESERVE.

D5.4 provides more detailed discussions of these research results.

Scientific Publications in 2014/2015:

1. P. Knapik, J. Petit, F. Kargl, E. Schoch, “Cooperative Home Light: Assessment of a Security Function for the Automotive Field,” IARIA Journal on Advances in Security, ISSN: 1942-2636, Vol. 7, Nr. 1&2, pp 1-14, 2014.
2. M. Feiri, J. Petit, and F. Kargl, “An evaluation framework for pre-distribution strategies of certificates in VANETs,” in Proceedings of 2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2014), Luxemburg, February 2014. http://www.vehicularlab.uni.lu/wp-content/uploads/2014/03/Proceedings_FG_IVC_2014.pdf (*)
3. M. Feiri, J. Petit, and F. Kargl, “Real world privacy expectations in vanets real world privacy expectations in vanets,” in Proceedings of 2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2014), Luxemburg, February 2014. http://www.vehicularlab.uni.lu/wp-content/uploads/2014/03/Proceedings_FG_IVC_2014.pdf (*)
4. R. W. van der Heijden and F. Kargl, “Open issues in differentiating misbehavior and anomalies for vanets,” in Proceedings of 2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2014), Luxemburg, February 2014. http://www.vehicularlab.uni.lu/wp-content/uploads/2014/03/Proceedings_FG_IVC_2014.pdf (*)
5. R. Moalla, B. Lonc, H. Labiod, N. Simoni, “Towards a Cooperative ITS Vehicle Application Oriented Security Framework,” in Proceedings of IEEE Intelligent Vehicles Symposium (IEEE IV 2014) pp.1043-1048, June 2014. doi: 10.1109/IVS.2014.6856548
6. S. Dietzel, R. van der Heijden, H. Decke, and F. Kargl, “A flexible, subjective logic-based framework for misbehavior detection in V2V networks,” in A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on, Sydney, Australia, IEEE, June 2014, pp. 1–6.
7. J. Petit, M. Feiri, and F. Kargl, “Revisiting attacker model for smart vehicles,” in Wireless Vehicular Communications (WiVeC), 2014 IEEE 6th International Symposium on, IEEE, Vancouver, Canada, IEEE, September 2014, pp. 1–5.
8. Rim Moalla, “Securing Future Cooperative ITS Applications,” Ph.D. Dissertation, Télécom ParisTech, September 2014.
9. N. Bißmeyer, “Misbehavior detection and attacker identification in vehicular ad hoc networks,” Ph.D. Dissertation, Technical University Darmstadt, November 2014.
10. M. Khodaei, H. Jin, and P. P. Papadimitratos, “Towards deploying a scalable & robust vehicular identity and credential management infrastructure,” in Proceedings of the IEEE

Vehicular Networking Conference 2014 (VNC 2014), Paderborn, Germany: IEEE, December 2014.

11. D. Förster, H. Löhr, and F. Kargl, “PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET),” in Proceedings of the IEEE Vehicular Networking Conference 2014 (VNC 2014), Paderborn, Germany: IEEE, December 2014.
12. S. Dietzel, J. Gürtler, R. van der Heijden, and F. Kargl, “Redundancy-based statistical analysis for insider attack detection in VANET aggregation schemes,” in Proceedings of the IEEE Vehicular Networking Conference 2014 (VNC2014), Paderborn, Germany, IEEE, December 2014.
13. M. Feiri, J. Petit, Jonathan and F. Kargl, “Formal model of certificate omission schemes in VANET,” in Proceedings of the IEEE Vehicular Networking Conference 2014 (VNC 2014). Paderborn, Germany: IEEE, December 2014. doi: 10.1109/VNC.2014.7013307
14. S. Dietzel, J. Petit, F. Kargl, and B. Scheuermann, “In-network aggregation for vehicular ad hoc networks,” IEEE Communications Surveys and Tutorials, vol. 16, no. 4, pp. 1909–1932, December 2014. doi: 10.1109/COMST.2014.2320091
15. J. Petit, F. Schaub, M. Feiri, F. Kargl, “Pseudonym Schemes in Vehicular Networks: A Survey,” IEEE Communications Surveys & Tutorials, vol.17, no.1, pp. 228-255, First quarter 2015. doi: 10.1109/COMST.2014.2345420
16. M. Fazouane, H. Kopp, R.W. van der Heijden, D. Le Métayer, F. Kargl, “Formal Verification of Privacy Properties in Electric Vehicle Charging,” Engineering Secure Software and Systems 2015 (ESSOS 2015), Springer LNCS-8978, pp. 17-33, March 2015. doi: 10.1007/978-3-319-15618-7_2
17. M. Feiri, J. Petit, F. Kargl, “The case for announcing pseudonym changes,” in Proceedings of 3rd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2015), Ulm, March 2015. (*)
18. D. Förster, H. Löhr, F. Kargl, “Discussing Different Levels of Privacy Protection in Vehicular Ad-Hoc Networks,” in Proceedings of 3rd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2015), Ulm, March 2015. (*)
19. S. Dietzel, A. Peter, F. Kargl, “Secure Cluster-based In-network Information Aggregation for Vehicular Networks,” In Proceedings of the IEEE 81st Vehicular Technology Conference (VTC2015-Spring), April 2015.
20. M. Feiri, R. Pielage, J. Petit, N. Zannone, F. Kargl, “Pre-distribution of certificates for pseudonymous broadcast authentication in VANET,” In Proceedings of the IEEE 81st Vehicular Technology Conference (VTC2015-Spring), April 2015.
21. S. Dietzel, “Resilient in Network Aggregation for Vehicular Networks,” Ph.D. Dissertation, University of Twente, April 2015.
22. S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, P. Papadimitratos, “Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems,” Intelligent Transportation Systems, IEEE Transactions on , vol.16, no.3, pp.1428-1438, June 2015, doi: 10.1109/TITS.2014.2369574.

(*) Technical report or non-reviewed workshop contribution.

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. We neither list smaller meetings with external partners. These can be found later in Section 3.9.

Selected activities will thereafter be discussed in separate sections.

Continously Participation to regular C2C-CC security working group confcalls and meetings to update C2C-CC on PRESERVE status and results (various partners).

Continously Participation to regular ETSI TC ITS security working group confcalls and meetings to update ETSI on PRESERVE status and results (mostly Renault).

Continously Participation to HTG#6 activities (mostly SIT).

2014-02-11 Demonstration of PRESERVE by Renault, Trialog, during Mobilité 2.0 organized by the French Transportation Ministry

2014-02-12/13 Presentation by Frank Kargl (UT) on "Is ITS Security ready for deployment?" at ETSI ITS Workshop in Berlin, Germany

2014-02-20/21 UT co-organizing 2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication, Luxembourg

2014-03-26 Presentation by Fethulah Smailbegovic (escrypt) on "Securing System on Chips" at DATE 2014 in Dresden, Germany

2014-03-31 Presentation on Privacy Protection in ITS by Frank Kargl (UT) at course on "HUMAN RIGHTS AND DIGITAL TECHNOLOGY" at American University Paris

2014-05-08 Presentation “Privacy in Automotive Networks – How to balance security and privacy?” by Frank Kargl (UT) at 16 SafeTRANS Industrial Day in Stuttgart, Germany

2014-05-12 Presentation “ID Management in Automotive Networks” by Frank Kargl (UT) at Bosch BOCSE Konferenz, Ludwigsburg, Germany

2014-06-03/04 Presentations by Martin Moser on V2X HSM and PKI at FISITA World Congress in Maastricht

2014-07-16/17 Participation of UT in DriveC2X final event in Berlin, Germany (with poster presentation)

2014-07-27 Poster at BMW Summer school on “Autonomous Driving in the Internet of Cars“ by M. Feiri "Jail breaking vehicles" (until 2015-08-01)

2014-09-18 Participation of F. Kargl (UT) at Daimler Road Privacy Workshop in Stuttgart, Germany

2014-09-22/26 Hosting and participation to ITS HTG#6 working group meeting at Fraunhofer SIT in Darmstadt

2014-09-24/25 Organization, hosting and participation to C2C-CC Security Working Group Meeting at Fraunhofer SIT in Darmstadt

2014-09-25 Organization, hosting and participation to ITS HTG#6 public stakeholder day at Fraunhofer SIT in Darmstadt

2014-12-08 Advisory Board in Munich, Germany

2014-10-23 Presentation by F. Kargl (UT) on data protection and privacy in automobiles at 16th VDI-Forum in Böblingen, Germany

2014-10-06/09 Keynote speech at IEEE Nets4Cars, P. Papadimitratos (KTH) on “vehicular communications safety and security”

2014-10-27/31 Organization of CySEP Winter School by KTH. Posters Presented "Deploying a Vehicular Credential Management System: Challenges Ahead" (M. Khodaei) and "Secure and Privacy Enhancing Location Based Services" (H. Jin)

2015-03-19/20 Participation to the ETSI Plugtest (Trialog, SIT)

2015-03-26 Presentation on C2X security at Bosch Workshop in Renningen, Germany

2015-05-21 Presentation of PRESERVE by N. Bissmeyer (Fraunhofer SIT) at the CAST-Workshop on Mobile und Embedded Security in Darmstadt, Germany

2015-06-17/18 PRESERVE Final Event at KTH Stockholm including workshops of C2C-CC, ETSI, and HTG#6

The following sections will provide details on some of these activities.

3.4 EU-US Cooperation in HTG#6 on Harmonized Cooperative ITS Security Policy

In 2014, PRESERVE continued its contribution to EU-US exchange by participation to HTG#6.

3.4.1 Summary of HTG#6 Activities between January 2014 and March 2015

The European Commission (EC) hosted the HTG6 team for its first week-long working session in Brussels, Belgium during January 2014. At this meeting, the gathered experts introduced themselves and briefed the team on their areas of expertise. The group discussed the scope of the project and began to define goals. As part of this discussion, attendees reviewed existing materials and ongoing initiatives expected to inform this task, including what was publicly available regarding: cooperative ITS security architectures; C-ITS applications and devices; and existing policies and standards. The team also identified key stakeholders and audiences for our work, created our deliverables list, and developed some tools for working together, including a standing outreach presentation that was updated after each meeting.

The second working session was held in Melbourne, Australia and hosted by Transport Certification Australia (TCA). This enabled the team to deeply delve into TCA’s established public key infrastructure (PKI) system from both technical and policy development standpoints. In addition, experts from the EC’s Joint Research Centre (JRC) presented on their Tachograph system. This system was of great interest as it is beginning a migration to the next generation of hardware, software and processes, therefore uncovering issues associated with system evolution. Both of these systems support commercial vehicle regulatory applications and administrators of both systems were considering whether to expand support C-ITS. This gave the team the insight that the identification of the gaps between existing systems’ capabilities and emerging C-ITS requirements was necessary. In this second meeting, the group examined the differences in the policy lifecycles and privacy regimes in the European Union, Australia, and the United States. In doing so, the team identified established processes that organizations such as ISO, ETSI, and NIST have for implementing policy, and added those references to the HTG6 document list.

During the third meeting, hosted by the U.S. Department of Transportation’s Volpe National Transportation Systems Center in Cambridge, Massachusetts, the team structured one of the first major pieces of analysis, an examination of why security is needed, and concluded that the role of security was not only to protect assets but also to protect access to those assets. Attendees established an initial list of C-ITS assets and recognized that the C-ITS applications

drove the need for security. Two existing tools became important during this session—the ITS Station concept and the Connected Vehicle Reference Implementation Architecture (CVRIA). One of our team's experts developed a list of C-ITS applications with unique qualities drawn from applications defined by the Europeans, the Australians and the CVRIA. Eventually, the members of HTG6 expect all these applications to be represented in the CVRIA.

In HTG6's fourth meeting, hosted by the EC at the JRC in Ispra, Italy at the end of June, the team continued the analysis—using the applications identified earlier and a sub-group began assigning security risks based on application requirements for Confidentiality, Integrity, and Availability (C,I, A). Another subset of the team also did a comparison of the JRC Tachograph and TCA PKI against the Credential Management Entity Protection Profile from the Common Criteria developed in the EU. This helped the team to both evaluate security policy requirements and the basis of the existing Protection Profile for providing policy. The team concluded the fourth meeting with a rough analysis and a plan to expand it to include the PRESERVE PKI and SCMS. With these two sub-teams up and running, the members of HTG6 formed two additional sub-teams—one to examine organizational roles and analysis; and one to develop a policy and legislative baseline, to provide HTG6 recommendations within the context of policy that exists today and identify gaps that could impede C-ITS success. The team launched one additional activity at this point: having recognized that the ITS station definition and the CVRIA definition were being used interchangeably a small group formed a sub-team formed to map these two concepts.

At the fifth meeting of HTG6 that was held in the US at a conference center in Sonoma, California in early August, members spent most of the time in sub-groups to continue the analyses underway and presenting out daily to the entire group for feedback. During breaks, the team began development of report outlines and checklists. This effort continued between meetings as well.

HTG6's initial stakeholder outreach took place in the U.S. after the August meeting. During this time, the team presented the basis for the activities undertaken by HTG6 to date and shared the progress of the analyses to date, including the emerging results. The team solicited feedback and comments from the stakeholders present that was used to refine the work of HTG6.

The sixth meeting took place at the Fraunhofer Institute for Secure Information Technology in Darmstadt, Germany, where the management was kind enough to invite us to use the facilities, both for our team meeting and for a day of outreach to European stakeholders. As part of the outreach to the European stakeholders, HTG6 members shared the presentations from the U.S. stakeholder meeting with those in attendance and again solicited feedback and comments on the work completed to date. The team then drafted a roadmap for the next steps necessary for the work. In addition to gathering important stakeholder feedback, the team continued working in sub-groups to move the analyses forward.

As part of our commitment to geographic equity, the seventh meeting was due to occur in the Pacific region and took place in Honolulu, Hawaii. In addition to meeting in sub-groups to expand and refine our work as necessary, the team began to identify the emerging results and possible areas for policy recommendations. The group also reviewed the work to date for gaps and areas where more analysis was needed.

For the eighth meeting in early December, HTG6 convened in Alexandria, Virginia. At this point, the team focused on finalizing the analyses, including refining recommendations, structuring the deliverables, and assigning responsibilities for subsequent document development and completion.

Since the eighth meeting, HTG6 member have worked, largely in their sub-groups, to finalize their parts of the work and draft documents. Draft documents are expected to be completed, reviewed, and edited during February and March of 2015. The team plans to conduct outreach and socialize the results between March and June 2015.

3.4.2 Summary of Anticipated HTG#6 Deliverables

- **Internationally Harmonized C-ITS Security Policy Executive Summary**
  This document gives an overview of HTG#6 from the objective of developing an end-to-end security policy framework for facilitating the successful implementation of C-ITS Credential Management Systems (CCMS) using harmonized security policies to key findings, including high-priority areas recommended for harmonization. This gives senior policy makers guidance for establishing security policies that meet their system's needs.

- **Public Key Infrastructure (PKI) Architecture Analysis and Recommendations for Harmonization**
  This document identifies the elements of a PKI system that are relevant to C-ITS Credential Management Systems and provides recommended options for harmonization, including guidelines and approaches for specific functions of the PKI. This document also serves to inform policymakers and implementers of the important aspects of PKI systems and the benefits and challenges associated with harmonization. Elements of PKI systems that would provide the greatest potential benefits from harmonization are highlighted.

- **A Harmonized Approach to Assessing Risk and Developing Security Controls for C-ITS**
  This report incorporates an analysis of the risk environment specific to C-ITS and the corresponding critical attributes of confidentiality, integrity, and availability. The results enable policymakers to identify the security risks in their own systems, evaluate the severity of those risks, and develop strategies for addressing them with technical, policy and physical controls. Harmonization is facilitated when current accepted practices and policies are incorporated into the analysis for each CCMS.

- **Co-operative ITS Credential Management System (CCMS) Functional Analysis**
  This document provides an overview of the functionality involved in making it possible for devices from different CCMS to trust each other. It also recommends actions for CCMS implementers.

- **Considerations for Cross-Jurisdictional CCMS Interactions**
  This report identifies issues CCMS managers will need to consider during the process of establishing trusted relationships between independent CCMS. In addition, it articulates the implications of the various choices available to resolve those issues.

Supporting Documents:

- **Glossary and Definition of Terms**
- **PKI Primer**

3.5 ETSI Plugtest

In the continuous effort to support rapid ITS deployment and to validate the ETSI ITS Release 1 standards, a fourth Plugtest[4] has been organized in March 2015 focusing on Co-operative

[4] http://www.etsi.org/news-events/events/846-plugtests-2015-itscms4

Mobile Systems standards from ETSI, CEN and ISO and to test the interoperability of ITS equipment from all key vendors.

The PRESERVE project participated to this event in order to validate the functional security implementation. Two main activities were relevant for security testing.

- In an inter interoperability test event two devices of different companies were connected in order to verify that security functions are working properly under normal conditions. The PRESERVE inter interoperability test results are detailed in PRESERVE Deliverable D3.3.
- In a conformance test event a single implementation of one company is connected with a test system that tests the correct behavior with respect to security in a semi-automated way. The conformance test considers also invalid behavior of a malicious sender which has to be detected by the implementation under test. The PRESERVE security conformance test results are detailed in in PRESERVE Deliverable D3.3.

3.6 Stakeholder Workshop with Advisory Board

In December 2014, we organized a stakeholder workshop with our advisory board. Originally, we envisioned a broader participation in order to present the 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. Due to delays in ASIC availability, we decided to limit the stakeholder workshop to only the advisory board and ensure strong participation and feedback from that group.

Reach-out to the full community was delayed to the final workshop where we put strong effort into assembling the full relevant community by co-locating with a number of interesting additional events as described in Section 3.8.

The AB meeting was attended by six members of our AB from Daimler, Denso, BMW, and Audi.

After a presentation of PRESERVE results and look back at the Y4, a first round of discussions centered on PKI and certificate management. We identified the still apparent and hard to resolve issue of a contradiction between short pseudonym certificate lifetime and potentially few connectivity options in vehicles. This is something that needs to be addressed on a ‘per OEM’ basis to find a trade-off between on-board storage for pre-loading of certs, required local security mechanisms and availability of connectivity (WLAN, cellular, …) in different models.

A following presentation showed results from the ETSI plugtest 2014 and our involvement in the preparation of plugtest 2015. OEMs and suppliers were highly interested in the ETSI conformance test tool which will be publicly available.

Another part of the meeting focused on the status of the HSM. After detailed explanations about the functioning of the ASIC, the AB recommended to use the PRESERVE ASIC as a functional benchmark to it with other solutions already available or becoming available on the market. How can we rank our solution? What is the justification of our PRESERVE HW design (e.g., one chip solution vs. two chip solution as promoted by NXP)?

The next topic was related to HTG#6 results. Norbert Bissmeyer provided an overview followed by a detailed discussion. Additional topics included liability, importance of misbehaviour detection.

At the end, AB members expressed their interest to receive and learn about benchmark results and cost- and business-model results. AB members will be invited to the final event to conclude their activities with PRESERVE.

3.7 Liaisons with other Projects and Stakeholders

As explained in detail in Sec. 2.2.4, PRESERVE aims at building strong working relationships with a number of key projects and organizations.

As the project progressed, we shifted focus on collaboration with different projects. Initially, we had very close collaboration especially **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. Beyond end of Score@F, we signed an MoU with Hitachi and close collaboration continued, e.g., with joint participation to ETSI plugtests.

Our collaboration with **DRIVE C2X** that led to an integration of our VSS Kit 1 with the DRIVE C2X communication solution of NEC was concluded with participation at their final event in July 2014.

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. Close collaboration is documented by joint activities in the final event of PRESERVE (see below).

Contacts with **CAMP** continued to be only sporadic in 2014/2015, however, interaction with U.S. researchers in academia and in industry was still very active due to our involvement in **HTG#6**.

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

We signed a MoU with **COMPASS4D** and started collaboration with them planning an integration of PRESERVE VSS Kit 2 into their platform. We identified some technical issues that are needed to be overcome.

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 Q16 meeting on 08.12.2014 which participation from Daimler, Denso, Audi, and BMW. PRESERVE presented a detailed status overview to the AB and received their feedback. Results of this meeting are discussed in the previous section.

3.8 PRESERVE Final Event

3.8.1 Event Organization

In June 2015, PRESERVE organizes its final event. Beyond presenting the PRESERVE results, our aim is to provide a complete picture of security and privacy protection in ITS. We therefore teamed up with the C2C-CC security WG, ETSI TC ITS WG 5, and HTG#6 to organize a two day special workshop where one day is devoted to PRESERVE and the other day will present the current status and results of the other parties. Thereby, we present the current status and roadmap of cooperative Intelligent Transport Systems (C-ITS) security in Europe, Australia and the United States.

On day one, the security working group of the Car-to-Car Communication Consortium presents ongoing and upcoming activities in the field of C-ITS security from an industry perspective followed by a presentation on status and activities of the ETSI TC ITS WG5. In the afternoon, the Harmonization Task Group #6 (HTG#6) presents final results of the harmonization effort regarding C-ITS security and privacy policies between Europe, Australia, and the United States.

On day two, the PRESERVE consortium presents the project results focusing on critical issues in C-ITS security and privacy like performance, scalability, and deployability of respective sys-

tems. In addition to talks there will be accompanying demos to experience C-ITS security first-hand. The final PRESERVE event is rounded up by discussions about the deployment status and the roadmap of C-ITS security for road safety applications and automated vehicles.

Participation to this two-day event was free of charge but required a registration. We had very good attendance with 45 participants.

Public Workshop of C2C-CC WG Sec and ETSI TC ITS WG5

The CAR 2 CAR Communication Consortium (C2C-CC) is dedicated to the objective of further increasing road traffic safety and efficiency by means of C-ITS. It supports the creation of European standards for communicating vehicles spanning all brands. As a key contributor the C2C-CC works in close cooperation with the European and international standardization organizations like the European Telecommunications Standards Institute (ETSI). The agenda is shown below.

Date:	17 June 2015	
Time:	9:00 - 12:30	
Location:	KTH University, Stockholm, Sweden (http://www.kth.se/en)	
Rooms:	to be announced	
Agenda:	9:00 – 9:15	Welcome
	9:15 – 10:45	Ongoing activities in C2C WG SEC • Certification policy development • PKI policy development and Pilot PKI operation • Protection profile development • Standards profile development
	10:45 – 11:00	Break

	11:00 – 11:45	Ongoing and upcoming activities in C2C WG SEC
		• Validation and Testing activities
		• Harmonization with infrastructure
		  ◦ under the DG move C-ITS platform and other form
		  ◦ with projects in EU (including Crypto agility)
		• International harmonization

	11:45 – 12:30	Activities in ETSI TC ITS WG5 with relation to international harmonization
	12:30 – 13:30	Lunch

Public Harmonized Cooperative ITS Security Policy Workshop

Harmonization Task Group #6 (HTG#6) is a cooperative effort between European Commission, Australian, and United States policy and technical experts. Harmonized cooperative ITS security is essential to ensuring cross-border interoperability. The results of HTG#6 provide guidance to developers worldwide on implementation and operation of security services. The results aiming for helping policy developers to create a harmonized set of policies to support end-to-end Co-operative ITS security. The agenda is shown below.

PRESERVE Final Event

The agenda of the PRESERVE Final Event is shown below.

Date:	17 June 2015	
Time:	13:30 - 17:00	
Location:	KTH University, Stockholm, Sweden (http://www.kth.se/en)	
Rooms:	to be announced	
Agenda:	13:30 – 15:00	Presentation of HTG#6 results • HTG6-1: Executive Summary • HTG6-2: C-ITS CMS Functional Analysis and Recommendations for Harmonization • HTG6-3: C-ITS CMS Architecture Analysis and Recommendations for Harmonization • HTG6-4: C-ITS CMS Inter-organizational Analysis and Recommendations for Harmonization
	15:00 – 15:30	Coffee break

	15:30 – 16:45	Presentation of HTG#6 results
		• HTG6-5: Categorizing and Controlling Risk through Harmonized C-ITS Security Policies
		• Discussion of methodologies
		  ◦ Risk categorization
		  ◦ Use of common criteria
		  ◦ Privacy analysis

	16:45- 17:00	Conclusion and summary

3.8.2 Report from PRESERVE Final Event

In the following, we summarize the two days of our final events.

On 17th and 18th of June, 2015, the Royal Institute of Technology (KTH) in Stockholm, Sweden, was hosting a unique event on security and privacy of cooperative Intelligent Transportation Systems (cITS). Not only was the European FP7 project PRESERVE holding its final event, but PRESERVE was joined by partners from the Car-2-Car Communication Consortium's security working group, represented by its chairman Henrik Broberg from Volvo Cars, by ETSI TC ITS Working Group 5, represented by its chair Brigitte Lonc, and by the Harmonization Task Group 6 of the International ITS Cooperation task force, represented by Suzanne Sloan from the US Department of Transportation and Wolfgang Höfs from the European Commission.

About 45 participants mostly from Europe and the U.S. joined the two day event to experience the results of the PRESERVE project and discuss one overarching question: is cooperative ITS security ripe for deployment? Participants came in equal shares from academia, OEMs, suppliers, and public organizations. As a result, discussions reflected the full spectrum of viewpoints on cITS security.

C2C-CC Security WG Status

Day one was devoted to on-going activities in standardization and harmonization. After a warm welcome from Frank Kargl (University of Twente), coordinator of the PRESERVE project, Henrik Broberg kicked off the day by giving a detailed insight into the work and achievements of the C2C-CC's security working group that he is chairing.

One focus of his talk and the discussion was the status of the C2C-CC pilot PKI and production root CA, the later one is expected to become available later this year. Another topic of interest was the work of the in-vehicle task force. A major issue here, which was repeatedly discussed

throughout the two days, is the matter of security evolution and flexibility. Too static demands and standards would prevent the security system from reacting to new threats. Therefore, we need to establish standards that are adaptable and allow the security system including the cryptographic mechanisms to evolve as the threats evolve.

Broberg also discussed the complementing relationship of the work in C2C-CC and in ETSI and warned that a reasonable minimum level of security is required to avoid a 'race to the bottom' in which cost advantages help those that implement weak security. This requires a certification process to be established to ensure this minimum level to be kept by all players. He also highlighted the fact that besides all the technical challenges, the cITS security community now also has to solve many organizational and economical issues to become ready for deployment and that the role of harmonization and standardization is crucial.

ETSI TC ITS WG 5 Status

This idea was taken up by Brigitte Lonc who is chairing the ETSI TC ITS working group 5 on security. In her talk, she reported about recent advancements in ETSI's ITS security standardization. She also stressed that the evolution of the security system to ensure scalability, extensibility, maintainability, and crypto-agility is currently being seen as one of the major challenges. ETSI's view on security services, PKI structure, and message formats and headers aligns nicely with the view of C2C-CC, showing the good level of harmonization achieved here. An interesting activity is the on-going work to extend IETF's TLS standard to allow vehicular certificates to be used in TLS authentication. Many participants welcomed this convergence of the ITS and Internet world.

Harmonization Task Group 6 Results

After lunch, the second half of the first day was devoted to the results of the Harmonization Task Group 6, which is active since 2014 and now presented their preliminary results on cITS security policy harmonization. The HTG raised the issue how one could ensure interoperability of systems if cars cross international borders and what level of international harmonization would be required especially with respect to PKI policies in order to allow, e.g., a European car to recognize a certificate from a US car. But also considerations regarding full car lifecycle including, e.g., private resale, are on HTG 6's agenda.

The challenge is to ensure that nearing operational deployments in various areas of the world will not be based on fundamentally incompatible assumptions regarding their security systems that would prevent this interoperability in the mid-term future. Here, the HTG presented a harmonized model of a trust management architecture termed CCMS or Cooperative-ITS Credential Management System and their recommendations of policy and trust harmonization. Like the previous speakers, flexibility and crypto-agility were also listed among the important requirements.

Overall, the HTG sees a strong need to act quickly on harmonization regarding operational processes for CCMS-CCMS and Inter-CCMS trust, auditing of PKIs, and identification of compliance standards, PKI bootstrap (installation, enrollment, certification), CA data center management, and vetting of organizations/personnel. As a multi-CCMS world is likely to occur, they recommend the development of a CCMS federation that regulates accreditation of new CCMS entities, sets policies with CCMS boards for the priority areas for harmonization, and takes ownership of standards to ensure that they are updated and evolved as needed.

With this, the first day of the workshop ended. Day two was then focusing on the achievements of the PRESERVE project. The second day was staged nicely in a former hospital chapel at KTH, the perfect place to 'preach' about the importance of security and privacy protection in cITS.

PRESERVE Final Event

The presentations started with an overview over the origins and results of PRESERVE, given by the project coordinator Frank Kargl from University of Twente. He illustrated how the idea for PRESERVE was built on top of results of a series of previous projects, namely SeVeCom, PRECIOSA, EVITA, and to some extent Oversee, from which PRESERVE also recruited most of its partners. The idea was to integrate their results in a way that they would become accessible to FOTs and pilot projects to be used in their work. Another goal of PRESERVE was to investigate scalability of security mechanisms and provide extensive testing results on the performance aspects of cITS security. Finally, at the time PRESERVE started there were still many open questions related to deployment of cITS security but also related to various research challenges that PRESERVE aimed to address.

This all culminates in the mission statement of PRESERVE: to design, implement, and test a secure and scalable V2X Security Subsystem for realistic deployment scenarios. Towards this goal, PRESERVE contributed many results that were presented throughout the day.

The first area of PRESERVE work focused on a harmonized V2X Security Architecture (VSA) which was presented by Norbert Bissmeyer from Fraunhofer SIT. The PRESERVE VSA, available in project deliverable D1.3, refines ETSI's ITS station reference architecture by detailing the various elements necessary for cITS security in the areas of ID management, message integrity, privacy protection, and misbehavior detection. The VSA also outlines their interactions and gives guidelines regarding implementation. Following discussions centered around communication with the backend, need for revocation mechanisms, and mechanisms for re-filling of pseudonyms via Road-Side Units (RSUs).

The VSA constitutes the basis for the implementation of PRESERVE's V2X Security Subsystem (VSS), which was presented in the following talk by Martin Moser from ESCRYPT. The VSS implements all major components of the VSA needed for a day 1 deployment both inside the vehicle and external PKI components. For the components on the vehicle side PRESERVE provides a software-only, open-source version of the VSS available for free download from the PRESERVE website. It already implements the full functionality of the VSS and runs on a variety of hardware including major CPU architectures (x86, ARM, MIPS, PPC).

The VSS comes in the form of a library which is integrated into the communication stack by means of a flexible API interface called harmonization layer. This harmonization layer allows fast and easy integration, as PRESERVE was able to show by integrating the VSS with communication stacks from Hitachi, NEC, Denso, and others. While the VSS can rely on software-backends like OpenSSL or ESCYPT Cycurlib for all cryptographic operations, it only unfolds its full power when adding the PRESERVE Hardware Security Module (HSM), an ASIC that was designed and built during the project. The HSM offers additional functionality like secure key storage, cryptographic acceleration, and a true random number generator (TRNG). As the HSM became available only shortly before this event, Martin Moser reported only preliminary benchmarks at reduced clock speed. For the most important performance figure, the ECDSA signature verifications, the measurements resulted in 805 verifications per second. For the final clock speed, we can interpolate a rate of 1,238 ver./s, well above the target rate of 1,000 ver./s that PRESERVE aimed for.

An external part of the VSS is the PKI backend. In close cooperation with C2C-CC and ETSI, PRESERVE partners SIT and ESCRYPT designed and realized two independent and interoperable implementations of the vehicular public key infrastructure which they then extended into C2C-CC's pilot PKI.

The following talk by Norbert Bissmeyer was then dedicated to PRESERVE's testing results. Over its lifetime, PRESERVE had a series of internal and external testing campaigns. After a first internal functional test of the VSS Kit in 2012, we conducted joint tests with the French Score@F project at the Versailles-Satory test track near Paris. Furthermore, PRESERVE participated in the two ETSI plugtests in 2013 and 2015 where it could demonstrate its good compatibility with ETSI standards and interoperability with other platforms. Finally, PRESERVE also conducted extensive tests in its internal testbed consisting of up to 25 NEXCOM OBUs

setup at KTH. Here, we investigated how large security payload leads to significantly increased packet loss in loaded channels and how the HSM can help to handle high verification loads which regular OBUs cannot handle anymore in software.

The next talk, given by Christophe Jouvray from Trialog, now focused on availability and exploitation of PRESERVE results. He reported that the VSS Kit was already downloaded more than 50 times since the availability of the VSS Kit 2 software-only version via the PRESERVE website in December 2014. Interested parties are requested to voluntarily fill-in a small form when downloading. From this we learned that the downloading organizations include 6 car makers, 21 solution providers, 10 research laboratories, and 5 standardization groups from countries in Europe (Germany, France, UK, Austria, Lithuania) and the rest of the world (China, India, Japan, Mexico, US, Israel, Taiwan). Our partners Trialog (VSS Software), ESCYPT (HSM, PKI), and Fraunhofer (SIT) are dedicated to continue exploitation of the main PRESERVE results beyond the end of the project.

The lunch break featured an integrated demo session, where participants could see a total of four demos from PRESERVE: One demo illustrated how the VSS can protect from external attackers, a second demo showed the PKI operations including refilling of pseudonyms from the pseudonym CA, a performance demo visualized HSM benchmarks, and the fourth demo consisted of a guided tour through the testbed.

After lunch, Panos Papadimitratos from KTH then continued with a presentation giving an overview over the work of PRESERVE on deployment and research challenges. With over 50 peer-reviewed scientific publications and over 100 presentations about project results given at conferences and other venues, PRESERVE made a substantial contribution to the state of the art in the field of cITS security and privacy. Through our close cooperation with C2C-CC Security WG and ETSI TC ITS WG 5 and active participation in Harmonization Task Groups 1 and 6, we also ensured that those results were disseminated and taken into consideration in harmonization and standardization. Other events like organization of the PRESERVE / EIT-ICTlabs summer school, the PRESERVE / C2C-CC security architecture workshop, research seminars, workshops, and conferences also contributed to keeping the research community connected and to ensure best use and uptake of research results in the process towards deployment.

The event continued with a panel discussion where William Whyte (Security Innovations, HTG), Henrik Broberg (Volvo Cars, C2C-CC), Panos Papadimitratos (KTH, PRESERVE), and Frank Kargl (University of Twente, PRESERVE) discussed the question whether we can finally implement and deploy security in cITS given the results from PRESERVE and other efforts. The experts agreed that the overall framework is well defined, but some work may be required within the subsystems, e.g., on misbehavior detection. It remains to be discussed whether all these problems need and even can be solved for a day 1 deployment or could better be solved stepwise in later revisions.

The panelists also realized that cITS is still a rapidly moving target and progress at times outpaces what is laid down in standards. Frank Kargl cautioned that a step-wise approach may be difficult once that first systems are deployed. As can be seen in the Internet, successful deployment in volume creates the need for backwards compatibility and makes introduction of novel features to core technologies a lot more complicated.

The following discussion centered a lot around the cost argument where industry warned about the dangers of too high costs, e.g., of HSMs. The question is which security level should be mandated from developers to not allow a race to the bottom where the one with least security enjoys the cost benefits but endangers security of all communicating parties. The group also discussed the effect a legal requirement for cITS deployment like currently discussed in the US would have. The discussion then moved on towards a more long-term perspective, where cITS may converge with the vision of automated driving. This will inevitably require a higher level of security and privacy protection compared to some day 1 applications.

This discussion was a good lead-over to the following invited talk by Jonathan Petit from University College Cork who spoke on 'Security and Privacy Challenges for Automated Vehicles'. He stressed that for automated vehicles we require a broader view on security including the sensors providing data but also the control algorithms that then make a vehicle react on such data. He highlighted the problem of secure sensor data by showing results from successful experiments on attacking an industrial LIDAR scanner. Another aspect of the talk focused on required privacy protection.

Conclusions

In the final wrap-up, Frank Kargl from PRESERVE and Wolfgang Höfs from the European Commission agreed that the two day event was a unique and very successful meeting of cITS experts from various domains that was very helpful in exchanging results and positions. Since the early days of initial research, cITS in general and the cITS security community involving researchers, developers, industry, and political stakeholders in specific managed to stay very well connected. This led to a fast and well harmonized development of standards based on initial results from academic research.

There was a general agreement that – also thanks to the contributions of PRESERVE – cITS security and privacy protection is well understood up to a level that, from our perspective, a day 1 deployment can move forward. At the same time, everyone is aware that this deployment but also future applications like automated driving will create new challenges and attacks and this requires the security system to be flexible and adaptable. The research activities should therefore not stop and the good dialogue and interchange between academia, industry, and political stakeholders should continue in the future. As this is a world-wide challenge, it should also be addressed in a world-wide, harmonized way.

As a project, PRESERVE hopes to have contributed to the vision of secure and privacy-preserving cITS that will make our mobility safer, more comfortable, more efficient, and also more friendly to our environment.

All slides from the event are available at: https://www.preserve-project.eu/final-event

3.9 Table of all Year 4&5 Dissemination Activities

The following table lists all dissemination activities in Y4&5 in detail in chronological order.

Date	Event / Title / Activity	Type	Partners involved	Result
2014-01-29	Petit Jonathan, Schaub Florian, Feiri Michael, Kargl Frank, "Pseudonym Schemes in Vehicular Networks: A Survey", IEEE Communications Surveys and Tutorials	Publication	University of Twente	Submission of research results of PRESERVE
2014-01-29	Reza Shokri, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, Jean-Pierre Hubaux, "Hiding in the Mobile Crowd: Location Privacy through Collaboration", IEEE Transactions on Dependable and Secure Computing	Publication	KTH	research results of PRESERVE (accepted for publication)
2014-02-04	Cooperation Meeting between Frank Kargl and Daimler representatives to discuss cooperation in ITS security and privacy, Sindelfingen, Germany	Liaison	University of Twente	agreement to cooperate towards more secure and privacy-preserving ITS systems
2014-02-11	Demonstration of PRESERVE during Mobilité 2.0 organized by the French Transportation Ministry	Demonstration	Trialog, Renault	increase awareness of PRESERVE
2014-02-12/13	Presentation by Frank Kargl on "Is ITS Security ready for deployment?" at ETSI ITS Workshop in Berlin	Presentation	University of Twente	raised awareness about project results and open issues within ETSI and the community at large.
2014-02-20/21	2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication, Luxembourg	Presentation	University of Twente	increase awareness of PRESERVE,

				presentation on going research work
2014-03-26	Presentation by Fethulah Smailbegovic on "Securing System on Chips" at DATE 2014 in Dresden	Presentation	ESCRYPT	Presentation of system-on-chip architectures used in PRESERVE
2014-03-31	Presentation by Frank Kargl at course on "HUMAN RIGHTS AND DIGITAL TECHNOLOGY" at American University Paris on Privacy Protection in ITS	Presentation	University of Twente	discussion with students and researchers of "International Affairs" at AUP
2014-03-31	Rim MOALLA, Houda LABIOD, Brigitte LONC, Noémie SIMONI "Towards a Cooperative ITS Vehicle Application oriented Security Framework"	Publication	Renault	Submission of research results of PRESERVE
2014-04-21	Participation to Workshop "Security in times of surveillance", Eindhoven	Liaison	University of Twente	Dissemination of research results of PRESERVE (re)
2014-04-28	Petit Jonathan, Feiri Michael, Kargl Frank, "Revisiting Attacker Model for Smart Vehicles", IEEE WiVec	Publication	University of Twente	Dissemination of research results of PRESERVE (accepted)
2014-05-08	Presentation “Privacy in Automotive Networks – How to balance security and privacy?” by Frank Kargl at 16 SafeTRANS Industrial Day in Stuttgart, Germany	Presentation	University of Twente	Dissemination of research results of PRESERVE
2014-05-12	Presentation “ID Management in Automotive Networks” by Frank Kargl at Bosch BOCSE Konferenz, Ludwigsburg, Germany	Presentation	University of Twente	Dissemination of research results of PRESERVE
2014-05-14	Feiri Michael, Djurre Broekhuis, Jonathan Petit, Frank Kargl, submission of a poster to IEEE WiSec 2014	Publication	University of Twente	Dissemination of research results of PRESERVE (rejected)
2014-06-03/04	Presentations by Martin Moser on V2X HSM and PKI at FISITA World Congress in Maastricht	Presentation	escrypt	Presentation of latest developments and PRESERVE results
2014-06-04	Participation to C2C-CC Security Working Group Meeting in Ingolstadt	Liaison	escrypt	Updating C2C-CC on current PRESERVE status
2014-06-08/11	Rim MOALLA, Houda LABIOD, Brigitte LONC, Noémie SIMONI "Towards a Cooperative ITS Vehicle Application oriented Security Framework", IEEE IV'14	Presentation	Renault	Dissemination of research results of PRESERVE
2014-07-16/17	Participation in DriveC2X final event	Liaison	UT	Dissemination and liaison
2014-07-27 - 2014-08-01	Poster at BMW Summer school: "M.Feiri, J.Petit, F.Kargl: Jail breaking vehicles"	Publication	University of Twente	Dissemination of research results of PRESERVE
2014-09-05	Submission to IEEE VNC 2014: "M.Feiri, J.Petit, F.Kargl: Formal Model of Certificate Omission Schemes in VANET"	Publication	University of Twente	Dissemination of research results of PRESERVE (submitted)
2014-09-05	Submission to IEEE VNC 2014: "S. Dietzel, J. Guertler, R.W. van der Heijden, F. Kargl: Redundancy-based Statistical Analysis for Insider Attack Detection in VANET Aggregation Schemes"	Publication	University of Twente	Dissemination of research results of PRESERVE (submitted)
2014-09-05	Submission to IEEE VNC 2014: "D. Foerster, H. Loehr, F. Kargl: PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET)"	Publication	University of Twente	Dissemination of research results of PRESERVE (submitted)
2014-09-05	IEEE WiVec 2014: "J.Petit, M.Feiri, F.Kargl: Revisiting Attacker Model for Smart Vehicles"	Presentation	University of Twente	Dissemination of research results of PRESERVE
2014-09-05	Submission to ESSOS 2015: "M. Fazouane, H. Kopp, R.W. van der Heijden, D. Le Metayer, F. Kargl: Formal Verification of Privacy Properties in Electric Vehicle Charging"	Publication	University of Twente	Dissemination of research results of PRESERVE (submitted)

2014-09-18	Participation F. Kargl at Daimler Road Privacy Workshop in Stuttgart, Germany	Dissemination	University of Twente	Dissemination of research results of PRESERVE
2014-09-22 - 2014-09-26	Hosting and participation to ITS HTG#6 working group meeting at Fraunhofer SIT in Darmstadt	Liaison	Fraunhofer SIT	Dissemination of research results of PRESERVE
2014-09-24	Organization, hosting and participation to C2C-CC Security Working Group Meeting at Fraunhofer SIT in Darmstadt	Liaison	Fraunhofer SIT, escrypt,	Updating C2C-CC on current PRESERVE status
2014-09-25	Organization, hosting and participation to ITS HTG#6 public stakeholder day at Fraunhofer SIT in Darmstadt	Dissemination	University of Twente, Renault, Fraunhofer SIT	Dissemination of research results of PRESERVE
2014-09-25	Consultation confcall with Toyota ITC on ITS security and privacy	Dissemination	University of Twente	Dissemination of research results of PRESERVE
2014-09-26	Participation of P.Papadimitratos at Seminar at Renault	Dissemination	KTH	Dissemination of research results of PRESERVE
2014-09-28	Submission to IEEE VTC-Spring 2015: "S. Dietzel, A. Peter, F. Kargl: Secure Cluster-based In-network Information Aggregation for Vehicular Networks"	Publication	University of Twente	Dissemination of research results of PRESERVE (submitted)
2014-09-29	Presentation of PhD Thesis by Rim Moalla on 'Securing Future Cooperative ITS Applications' was delivered in Télécom ParisTech, Paris.	Presentation	Renault	Dissemination of research results of PRESERVE
2014-09-30	Participation of T. Giannetsos in KTH-SAAB meeting, Stockholm	Dissemination	KTH	Dissemination of research results of PRESERVE
2014-07 - 2014-09	Acceptance at IEEE Communications Surveys & Tutorials: "J.Petit, F.Schaub, M.Feiri, F.Kargl: Pseudonym Schemes in Vehicular Networks: A Survey"	Publication	University of Twente	Dissemination of research results of PRESERVE
2014-07 - 2014-09	Submission to IEEE VNC 2014: "Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure"	Publication	KTH	Dissemination of research results of PRESERVE
2014-07 - 2014-09	IEEE Transactions on Intelligent Transportation Systems: "Secure and Privacy-Preserving Smartphone based Traffic Information Systems"	Publication	KTH	Dissemination of research results of PRESERVE
2014-10 - 2014-12	Participation to monthly C2C-CC security working group confcalls	Liaison	Escrypt, Fraunhofer SIT	Updating C2C-CC on current PRESERVE status.
2014-12-08	WP6: participation to the Advisory Board in Munich.	Dissemination and Exploitation	Escrypt, Renault, Fraunhofer SIT/AISEC, KTH, UT	Updating advisory board members on current PRESERVE status.
2014-10-13	VTC2015 Spring: M.Feiri, R.Pielage, J.Petit, N. Zannone, F.Kargl "Pre-distribution of Certificates for Pseudonymous Broadcast Authentication in VANET"	Reviewed Publication	UT	Submitted
2014-12-03	IEEE VNC2014: M.Feiri, J.Petit, F.Kargl "Formal Model of Certificate Omission Schemes in VANET"	Reviewed Publication	UT	Published and Presented
2014-10-23	Presentation on data protection and privacy in automobiles at 16th VDI-Forum in Böblingen, Germany	Dissemination	UT	Presentation
2014-11-12	Meeting with Vector Informatik to update on status of PRESERVE	Dissemination	UT	Presentation
2014-12-03	IEEE VNC2014: S. Dietzel, J. Gürtler, R. van der Heijden, F. Kargl "Redundancy-based statistical analysis for insider attack detection in VANET aggregation schemes"	Reviewed Publication	UT	Published and Presented
2014-12-03	IEEE VNC2014: D. Förster, F. Kargl, H. Löhr "PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET)"	Reviewed Publication	UT	Published and Presented

2014-12	IEEE Communication Surveys and Tutorials: S. Dietzel, J. Petit, F. Kargl, B. Scheuermann "In-Network Aggregation for Vehicular Ad Hoc Networks"	Reviewed Publication	UT	Final publication
2014-10-06/09	Keynote speech at IEEE Nets4Cars, P. Papadimitratos	Dissemination	KTH	Presentation
2014-10-27/31	CySEP Winter School organized by NSS group, KTH, Posters Presented "Deploying a Vehicular Credential Management System: Challenges Ahead" (M. Khodaei), "Secure and Privacy Enhancing Location Based Services" (H. Jin)	Dissemination	KTH	Published and Presented
2014-11-27	KTH & SAAB Meeting at KTH, T. Giannetsos, P. Papadimitratos	Dissemination	KTH	Presentation
2014-12-2/2	IEEE VNC 2014: M. Khodaei, H. Jin, P. Papadimitratos "Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure"	Reviewed Publication	KTH	Published and Presented
2014-12	IEEE Transactions on Intelligent Transportation Systems: S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, P. Papadimitratos "Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems "	Reviewed Publication	KTH	Published
2014-10-09	Participation to the EIP Smart cities Kickoff	Other	Trialog	PRESERVE commitment is accepted
2015-03-19/20	Feiri, Petit, Kargl; "The case for announcing pseudonym changes"; 3rd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication	Other Publication, Presentation	UT	Published and presented
2015-01 - 2015-03	Participation to monthly C2C-CC Security Working Group Confcalls	Liason	Escrypt, Fraunhofer SIT	Updating C2C-CC on current PRESERVE status.
2015-01 - 2015-03	Final update of HTG#6 deliverales with information based on PRESERVE technical documents	Liason	Fraunhofer SIT	Updating HTG#6 documents based on PRESERVE
2015-02-15	IEEE VT Magazine: M. Khodaei, P. Papadimitratos "Identity and Credential Management in Vehicular Communication Systems"	Publication	KTH	Paper submitted
2015-02-11	Participation to the EIP SCC meeting in Brussels	Dissemintation	Trialog	Dissemination of the PRESERVE results (possibility to reuse PRESERVE in the platform)
2015-03-04/06	Fazouane e.a.; “Formal Verification of Privacy Properties in Electric Vehicle Charging”; International Symposium on Engineering Secure Software and Systems (ESSOS’15)	Publication, Presentation	UT	Published and presented
2015-03-19/20	Participation to the ETSI Plugtest	Demo, Other	Trialog, Fraunhofer SIT	PRESERVE VSS Kit is compliant with standards and interoperable with other solutions
2015-03-26	Presentation on C2X security at Bosch Workshop in Renningen, Germany	Presentation	UT	Dissemination of PRESERVE results
2015-05-21	Presentation of PRESERVE by N. Bissmeyer (Fraunhofer SIT) at the CAST-Workshop on Mobile und Embedded Security in Darmstadt, Germany	Presentation	Fraunhofer SIT	Dissemination of PRESERVE results
2015-06-17/18	PRESERVE Final Event at KTH Stockholm including workshops of C2C-CC, ETSI, and HTG#6	Presentations and Demos	All	Dissemination of PRESERVE results.

4 Plan for Dissemination and Exploitation Activities beyond End of the Project

In this chapter, we will discuss our dissemination and exploitations plans beyond the end of the project, 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 Plans of Different Partners for Dissemination and Exploitation

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

4.2 Demonstration at ITS World Congress 2015 in Bordeaux

Various PRESERVE partners are committed to present the project results at the ITS World Congress in October 2015 in Bordeaux. We have requested space at the EU exhibition area for this.

5 Overall Summary

This deliverable is the final WP6 deliverable. PRESERVE dissemination and exploitation activities proved highly successful. PRESERVE was a central part of the ITS security and privacy community. During its lifetime, PRESERVE members were active in the C2C-CC security working group, in ETSI TC ITS working group 5 on security (here even as (co-)chair), in two harmonization task groups and in various other groups. By this broad engagement, we contributed to an exchange of know-how between academic and industrial partners.

Events organized and hosted by PRESERVE were attended by a large number of experts from industry and academia and include:

- The Vehicular Networking and Intelligent Transportation Systems Summer School in September 2012: https://www.preserve-project.eu/summer-school-2012
- The International ITS Harmonization Workshop in November 2012: https://www.preserve-project.eu/harmonization-workshop
- The Security Architecture Workshop in June 2013: https://www.preserve-project.eu/security-architecture-workshop
- The Harmonized Cooperative ITS Security Policy Public Workshop in November 2014: https://www.preserve-project.eu/harmonization-workshop-2014
- The PRESERVE Final event in June 2015: https://www.preserve-project.eu/final-event

Beyond, PRESERVE partners hosted many individual meetings of the working groups. PRESERVE partners also presented results at many occasions including industry events.

PRESERVE partners also made a significant impact on the scientific state to the art. With a total of sixty scientific publications, it by far exceeded initial expectations. This is extended by more than 60 presentations and demos on the topic of ITS security and privacy at various occasions.

Three young scientists involved in PRESERVE managed to conclude their PhD during the lifetime of the project.

As a lasting legacy, PRESERVE provides an open-source version of the VSS Kit 2 (software-only version) that can be downloaded free of charge from the PRESERVE website. So far, it has been downloaded already by 50 different parties.