PREparing SEcuRe VEhicle-to-X Communication Systems

Deliverable 5.4

Deployment Issues Report V4

Project:	PRESERVE
Project Number:	IST-269994
Deliverable:	D5.4
Title:	Deployment Issues Report V4
Version:	1.2
Confidentiality:	Public
Editor:	N. Bißmeyer
Cont. Authors:	N. Bißmeyer, M. Feiri, A. Giannetsos, F. Kargl, B. Lonc, M. Moser, M. Khodaei, S. Gisdakis, H. Jin
Date:	2016-01-31

Part of the Seventh Framework Program
Funded by the EC-DG INFSO

Document History

Version	Date	Main author	Summary of changes
v0.1	2014-10-09	N. Bißmeyer (Fhg SIT)	Initial version
v0.2	2014-10-10	M. Moser (escrypt)	Contents regarding ASIC cost model added to Chapter 2
v0.3	2014-10-13	N. Bißmeyer (Fhg SIT)	Contents in Chapter 4 added
v0.4	2014-10-13	M. Feiri (UT)	Model of Certificate Omission and Certificate Pre-Distribution
v0.5	2014-10-30	N. Bißmeyer (Fhg SIT)	Content of Chapter 4 exchanged by a short version.
v0.6	2014-10-31	M. Feiri (UT)	Reduce sections 3.1 and 3.2 to short versions
v0.7	2014-11-13	A. Giannetsos and M. Khodaei (KTH)	Updated Sections 3.3. and 5
v0.8	2014-11-25	B.Lonc (Renault) and N. Bißmeyer (Fhg SIT)	Contributions for Section 2.5 added
v0.9	2014-11-28	A. Giannetsos and M. Khodaei (KTH)	Content of Sections 2.2 created
v0.10	2014-12-02	N. Bißmeyer (Fhg SIT)	Update of Section 2.2 and introduction added
v0.11	2014-12-28	F. Kargl (UT)	Complete revision, adding conclusion
v0.2	2015-01-10	F. Kargl (UT)	Preliminary version for submission
v0.3	2015-06-10	A. Giannetsos and M. Khodaei (KTH)	Content of Sections 2.3 created
v0.9	2015-06-10	F. Kargl (UT)	Review version prepared
v1.0	2015-06-25	N. Bißmeyer (Fhg SIT)	Final version
v1.1	2015-12-01	F. Kargl (UT), M. Moser (escrypt)	Update incorporating reviewer comments (cost model, conclusion)
v1.2	2015-12-08	M. Khodaei and H. Jin (KTH)	Updating the overview of the survey

Approval		
	Name	Date
Prepared	F. Kargl & N. Bißmeyer	2014-12-28
Reviewed	All Project Partners	2015-01-10
Authorized	Frank Kargl	2015-01-16
Updated	Frank Kargl	2015-12-08

Circulation	
Recipient	Date of submission
Project Partners	2015-12-08
European Commission	2016-01-31

Contents

List of Figures

List of Tables

Glossary

Abbrev	Synonyms	Description	Details
CA		Certificate Authority	A CA is an entity that issues digital certificates.
CC		Common Criteria	Well-known international framework for assurance in the IT industry.
CCMS		Cooperative Credential Management System	A cooperative security credential management system generates and handles digital credentials such as keys and certificates.
CPU		Central Processing Unit	
ECC		Elliptic Curve Cryptography	ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
ECU		Electronic Control Unit	
FOT		Field Operational Test	
HSM		Hardware Security Module	
IPR		Intellectual Property Right	
ITS		Intelligent Transportation Systems	Intelligent Transport Systems (ITS) are systems to support transportation of goods and humans with information and communication technologies in order to efficiently and safely use the transport infrastructure and transport means (cars, trains, planes, ships).
ITS-S		ITS Station	Generic term for any ITS station like vehicle station, roadside unit, ...
IVS	OBU	ITS Vehicle Station	The term "vehicle" can also be used within PRESERVE

Abbrev	Synonyms	Description	Details
LTC		Long-Term Certificate	PRESERVE realization of an ETSI Enrolment Credential. The long-term certificate authenticates a stations within the PKI, e.g., for PC refill and may contain identification data and properties.
LTCA		Long-Term Certificate Authority	PRESERVE realization of an ETSI Enrollment Credential Authority that is part of the PKI and responsible for issuing long-term certificates.
MPCUP		Media Independent Pseudonym Certificate Protocol	A protocol that allows vehicles equipped with different communication technologies to obtain certificates of their pseudonym keys.
OEM		Original Equipment Manufacturer	Refers to an generic car manufacturer
OBU	IVS	On-Board Unit	An OBU is part of the V2X communication system at an ITS station. In different implementations different devices are used (e.g. CCU and AU)
PC	Short Term Certificate	Pseudonym Certificate	A short term certificate authenticates stations in G5A communication and contains data reduced to a minimum.
PCA		Pseudonym Certificate Authority	Certificate authority entity in the PKI that issues pseudonym certificates
PKI		Public Key Infrastructure	A PKI is a set of hardware, software, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
PP		Protection Profile	
RA		Resolution Authority	Entity within the SCMS or PKI to resolve pseudonymous IDs and certificates if necessary.
RSU	IRS, ITS Roadside Station	Roadside Unit	A RSU is a stationary or mobile ITS station at the roadside acting as access point to the infrastructure.

Abbrev	Synonyms	Description	Details
SCMS	PKI	Security Credential Management System	A security credential management system generates and handles digital credentials such as keys and certificates. A CSMS could be a PKI with additional functionalities.
SPCURO		Secure Pseudonym Certificate Update via Road-side Unit	SPCURO is a protocol used to update pseudonym certificate via roadside units in a secure and efficient way.
TAL		Trust Assurance Level	
V2I	C2I	Vehicle-to-Infrastructure	Direct vehicle to roadside infrastructure communication using a wireless local area network
V2V	C2C	Vehicle-to-Vehicle	Direct vehicle(s) to vehicle(s) communication using a wireless local area network
V2X	C2X	Vehicle-to-Vehicle (V2V) and/or Vehicle-to-Infrastructure (V2I)	Direct vehicle(s) to vehicle(s) or vehicle(s) to infrastructure communication using a wireless local area network
VSS		V2X Security Subsystem	Close-to-market implementation of the PRESERVE VSA that is the outcome of PRESERVE work package 2

1 Introduction

Work Package 5 investigates the major security and privacy related aspects in ITS that have not been taken into account previously, and thus, have not been sufficiently addressed. These aspects also include issues related to the market introduction of V2X security systems. This deliverable presents the results of the project's year 4 both with respect to research and deployment challenges.

The chapters and sections of this document contain only a short introduction of the different topics in order to keep the main document clear. Details that have been published in literature are referenced and provided separately to the reviewers.

Topics related to the deployment of the PRESERVE solutions and components are presented in Chapter 2. Here, we investigate what is necessary to deploy the PRESERVE platform integrated on ITS stations as Vehicular Security Subsystem (VSS) and in the infrastructure as security credential management system.

An overview of the plans for the deployment of the VSS are given in Section 2.1 and aspects for PKI business models are discussed in Section 2.2. In Section 2.4 a brief introduction is given into the cost model of the ASIC chip. The validation and certification of ITS stations, which is introduced in Section 2.5, is a very relevant topic that is related to the VSS deployment and the PKI operation. In the same way, the secure acquisition of pseudonym certificate valid for different domains is introduced in Section 2.6. The protocol proposed in this section is able to transmit certificate signing requests and responses over different channels which allows to equip ITS stations on demand with certificates.

In the remainder of the document, we address various open research challenges for ITS and the results that PRESERVE produced to address them.

In Chapter 3 solutions are introduced that focus on the scalability aspect of secure V2X communications. A formal model for certificate omission is provided in Section 3.1 followed by a proposal for certificate pre-distribution in Section 3.2 that aims at making secure V2X communication more efficient. In Section 3.3 a mechanism is introduced that increases privacy, robustness, and scalability of existing PKI designs.

In Chapter 4 we address reactive security solutions and specifically misbehavior detection for V2X. With our solution, we aims to detect attacks and the responsible attackers in the network in order to exclude them permanently from active participation.

Chapter 5 introduces a secure solution for a smartphone-based traffic information system which extends the scope of PRESERVE's research work more towards generic cooperative ITS and ITS application.

Finally, in Chapter 7 we provide a conclusion of this document and a conclusion of the research we did in PRESERVE altogether.

2 Deployment of PRESERVE

2.1 Plans for Deployment of VSS

The VSS Kit is composed of software and hardware components. This section will mainly focus on the deployment of software components and the ASIC will be discussed in Section 2.4.

2.1.1 Availability

Trialog and the University of Twente have decided to release the software created for the VSS Kit under an open source license (i.e., LGPL2). Since the consortium is still developing some features (e.g., pseudonym update through RSU, compliance with last ETSI standard versions), the code is still available on the PRESERVE repository only. Trialog has planed the following actions:

- Provide the PRESERVE library on the project website. The sources are not provided yet, but the software can be downloaded free of charge by anyone with just a small registration.
- Set up a bug tracker tool. A Mantis server will be setup in order to collect the bugs and provide a good traceability.
- Set up a public repository. The sources will be released on a public repository such as github where other developers can contribute.

2.1.2 Plans for Deployments in European and National Projects

During the project life cycle, PRESERVE has provided the VSS kit to the SCORE@F project and to other selected partners like Hitachi (for ETSI compliance testing) or DRIVE C2X. Further deployment and integration is planned with the following projects:

- **Compass4D**. This European pilot project works on three ITS services: Red Light Violation Warning (RLW), Road Hazard Warning (RHW), and Energy Efficient Intersection (EEI). They have decided to the PRESERVE VSS kit for ensuring the security in these services. Trialog and Escrypt will provide support during and after the PRESERVE project. A memorandum of understanding has been signed.

- **ISE and ELA**. These two National projects are funded by SystemX (officially created on February 1st, 2012 as part of the “Investment for the Future” program put in place to support innovation in France). The ISE (ITS Security) project (see http://www.irt-systemx.fr/project/ise/?lang=en) aims at providing secure building blocks and certification solutions applied to ITS. ISE is also in relations with ELA (Automotive Electronics and Software) project (see http://www.irt-systemx.fr/project/ela/?lang=en). ISE has selected Trialog as partner in order to contribute to the secure building block embedded in vehicles. The PRESERVE VSS kit will be reused and new features will be developed in this context.

PRESERVE partners will continue to advertise availability of the VSS Kit through different channels (ETSI, C2C-CC, IEEE, National and European projects, etc) in order to find new projects.

2.1.3 Plans with Hitachi

The VSS library provides an API and has to be connected to the communication stack. Since the integration work with SCORE@F, we are in good contact with Hitachi and continue integration during version updates. This is useful and necessary as it allows us a joint participation to ETSI plug tests.

2.1.4 Plans with ETSI

The VSS kit conforms to ETSI standards, in particular TS 103 097. For this reason, the project participates to the periodic ETSI plug tests. The next session will be organized in March 2015. The project is also involved in the validation of the compliance tool developed by ETSI. Actually, ETSI is developing a compliance tool for checking the conformance of secure building blocs with ETSI documents. In order to validate the tool, PRESERVE provides the VSS kit as a reference platform.

2.1.5 Participations to the EIP Smart Cities and Communities (EIP-SCC)

PRESERVE is focusing mostly on ITS. However, the ITS domain is also linked to the topic of smart cities. In this context, a commitment has been submitted by TRIALOG to the EIP-SCC. The commitment has been accepted and can be found at this address: http://eu-smartcities.eu/commitment/7926.

TRIALOG has participated to the kick-off meeting organized on the 9th of October in Brussels. TRIALOG plans to promote the VSS kit as a building block of the SCC platform. For this reason, TRIALOG is involved in the further conference calls and will participate to the next plenary meeting (not yet scheduled).

2.2 PKI Structure and Business Model

2.2.1 World-wide Vehicular PKI Harmonization

Results presented in this section are partly based on work of the EU-US ITS International Standards Harmonization Task Group number 6 (HTG#6) were PRESERVE participated in and provided significant contributions.

The foundational element of any crypto-system is the functionality that enables security processes, namely the system that serves as trust anchor and the basis for crypto-processes such as trust verification, integrity protection, encryption, etc. The connected vehicle environment requires a foundational trust element that serves these needs: it must, at minimum, provide crypto-material that enables trust, both in the contents of messages, and the protection of data from unintended readers. The chosen solution depends on a public-key infrastructure; however the systems currently under development in the US and the EU are somewhat different in their approach. Since the modern car market is global, and since the operable systems may indeed be different in at least two political environments, an understanding of just what the implications of differing trust anchors is warranted. For the purpose of this analysis, the foundational trust anchor is referred to as a Cooperative Credential Management System, or CCMS. At minimum the CCMS serves as root trust authority and provider of security credentials.

CCMS comprises a set of *authorities* or *components* with distinct roles that will be operated either by *federal agencies* or *private corporations*. In figure 2.1 the components are listed with processes that are relevant for the operation of the credential management. A detailed description of the processes, related use cases, and necessary inter-CCMS interfaces are described in the deliverables of HTG#6 [1]. The components of the CCMS are

- the Root Certification Authority (RCA),
- the intermediate CA which might be optional,
- the enrolment component which is also known as Long-Term Certification Authority (LTCA),
- the authorization component which is also known as Pseudonym Certification Authority (PCA),
- the misbehavior component,
- and the revocation component.

The LTCA, governed by federal or private agencies, is responsible for issuing Long-Term certificates (LTCs), in principle one per vehicle. The PCA, possibly non-governmental and commercially deployed, issues sets of pseudonyms to each vehicle registered with an LTCA. A *domain* - geographic regions or applications - is defined as the set of vehicles registered with one or multiple LTCAs, subject to the same administrative regulations

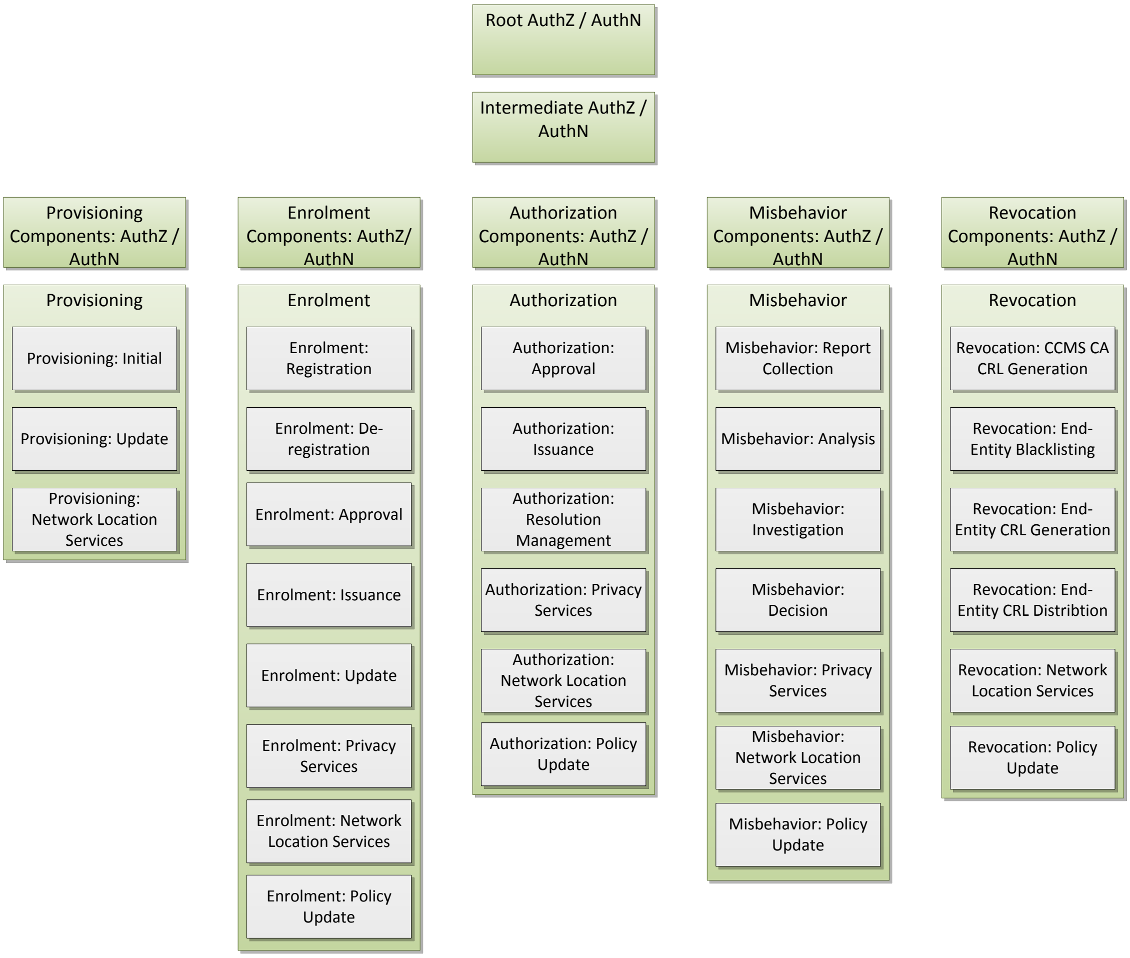

Figure 2.1: CCMS components

and policies. When necessary, e.g., for investigation purposes, the resolution management of the authorization component can initiate a process to reveal linking information of pseudonym certificates or the long-term identity of an ITS station, based on a set of pseudonymously authenticated messages. Moreover, across different domains, trust is established with the help of a higher-level authority, RCA, or a set of such authorities and cross-certification. Furthermore, it is possible that CCMS across multiple domains established trust on different levels. As further detailed in the HTG#6 documents [1] four different CCMS federation scenarios are identified.

- No trust between CCMS of different domains
- Trust on registration (canonical ID) level
- Trust on enrolment certificate level
- Trust on pseudonym certificate level

The different levels of cooperation and inter-CCMS communication requires different levels of policy harmonization. Based on theses levels each ITS station can have unique or multiple memberships as well as registrations to one or multiple domains.

2.2.2 Security for Service-Oriented Vehicular Networks

As vehicles become more automated, integrating more consumer devices [2] and featuring powerful embedded platforms and antennas, a new trajectory of commercial applications and services will emerge. Indeed, there is a growing demand for accessing the Internet and personalized services (tailored to the specific interests of individuals) from vehicles. This transformation is driven by the concept of leveraging “car as a platform” capable of running a gamut of services and performing numerous transactions for their users. The envisioned ecosystem of applications will range from simple infotainment services [3] and content distribution [4] to Internet access and the development of an “Application Store for automotive applications” [5, 6]. Such multi-service environments are expected to provide clear customer benefits and motivate commercial operators to invest in large-scale deployments of ITS systems.

Of course, security and user privacy still remain key pillars (as is the case for current Vehicular PKIs); however, the anticipated transplantation of commercial services into the ITS domain calls for comprehensive solutions that bring closer the worlds of ITS networks and Internet-based services, giving birth to a *service-oriented* vehicular ecosystem. Addressing the diverse requirements of vehicle operators and Service Providers (SPs) for identity management and fine-grained access control across multiple domains, is the main challenging task[1]. Furthermore, since existing Internet business models already entail a plethora of commercial SPs, it would be best if stakeholders from the vehicular domain tried to lure them in providing ITS-tailored services instead of looking for new ones. This calls for a synthesis of ITS-specific security and privacy (notably the security infrastructure) standards with widely accepted Internet technologies such as Web Services (WS) [7].

Therefore, there is a need for a model that provides authentication, authorization, accountability and user privacy along with a comprehensive set of services for identity management in multi-service automotive ecosystems. Service discovery and registration should support the provision of various personalized services and motivate SPs to enter the vehicular market. Moreover, the establishment of trust relations (*federations*), among different system entities, should facilitate access control across multiple domains. Of course, it goes without saying that such a model should encompass existing vehicular communications standards and the underlying CCMS by leveraging long-term credential and identity managing entities (expected to be deployed in ITS systems). All these functionalities should be provided in a *standard-compliant* and *platform-neutral* manner to ensure interoperability and scalability.

Overall, the merging of vehicular networks and web technologies (already envisioned in the real world) can yield numerous advantages for ITS. This convergence is compounded

[1] Direct applications of existing security solutions from the Internet domain is not desired as they cannot meet ITS security and privacy requirements

by the desire to access the Internet and personalized services from vehicles. As the need for security services such as authentication, data confidentiality and integrity, and non-repudiation are already established as critical enablers to meet those objectives, the focus must turn to an implementation plan that can best support the success of such a service-oriented vehicular ecosystem. PKIs present a cohesive framework within which service discovery and registration, access control across multiple domains can be conducted with the required trust.

2.3 Broadening Awareness on the PRESERVE Platform

There is a consensus being formed, in terms of basic technological aspects for *security* and *privacy* in ITS. Nonetheless, many questions concerning the actual deployment of these systems are not addressed yet. In addition, issues such as product life-cycles and costs for ITS products and services have to be defined, so that vehicular communication solutions can be brought to market. These are (indeed) important factors for the PRESERVE project and more generally for the ITS community.

Towards this direction, to better understand the realities of today's VC security landscape and to gauge the perception of the broader ITS community regarding the PRESERVE architecture, we have designed and disseminated a questionnaire that seeks answers to the above-described issues. In what follows, we provide an overview of the structure of our survey along with the methodology used for formulating the included questions. More information regarding the questionnaire can be found on the PRESERVE website[2].

2.3.1 Overview of the Survey

Our survey is designed in a way that no prior knowledge of the participants is presumed. We begin by asking the contributors to provide us with input on their background. This helps us to better analyze their responses and weight them accordingly. Each response reflects the opinion of the individual who completed the survey and not of the institution he/she represents. Moreover, all provided data are reported in aggregate with that of other participants to ensure anonymity and confidentiality.

We use three types of questions; *multiple choice*, *free text* and *matrix questions*. For the latter, we utilize a scale from 0 (low) to 4 (high) to indicate the confidence of the response. The questionnaire comprises six sections:

- **Introductory Questions**: This section contains general questions focusing on the background of the participant with respect to security and privacy issues of ITS. In addition, we try to capture his/her understanding on the PRESERVE architecture.

[2] http://www.preserve-project.eu/node/43

- **Questions on Safety Applications**: These questions focus on the security and privacy requirements for specific safety applications as defined in the survey. We also make inquiries on the suitability of the PRESERVE architecture for protecting such applications.
- **Questions on Infotainment and Miscellaneous Applications**: These two sections focus on infotainment and miscellaneous applications. Similarly to the previous section, we are interested in (*i*) the security and privacy requirements of these types of applications, and (*ii*) the applicability of PRESERVE's VSS.
- **Questions Regarding Financial Aspects**: These questions target participants whose role in the institutions they represent is of managerial nature.
- **Questions Regarding Technical Aspects**: This section pertains to participants with adequate technical expertise to give us their insights on some security- and privacy-related questions.

2.3.2 Survey Dissemination

We have created an on-line version of our survey utilizing tools that allow vast dissemination and in-depth data processing. The survey was broadcasted to various entities such as standardization bodies and experts in the area of ITS. We advertised it to possible contributors during the ITS World Congress held in Vienna from 22 to 26, October 2012. In addition, we disseminated our survey during the proceedings of C2C-CC Forum held in Göteborg (Sweden) on 13 and 14, November 2012 and in the EIT-ICT Safe Mobility chapter [3]. We have continued with collaborating FOT projects, with a US-EU Harmonization Working Group, and selected researchers in the broader ITS area.

2.3.3 Analysis of Aggregated Results

2.3.3.1 Introductory Questions

As aforementioned, this section contains general questions regarding the participant's background. Besides some *optional* fields (for anonymity reasons) related to some personal info including name, email, etc., we are mostly interested ($Q1$ and $Q2$) in the type of organization (e.g., University, Research Institute, etc.) he/she is employed and the actual type of employment. Based on these answers, we can extract a better understanding on the participant's background, knowledge and technical expertise.

[3] http://www.eitictlabs.eu/action-lines/intelligent-mobility-and-transportation-systems/

Question 3 In *Q3*, we ask the participants about their familiarity with the PRESERVE project and various standardization bodies active in the area of ITS (IEEE 1609.2-WG[4], ETSI-WG5[5] and C2C-CC [8]). If the participant's confidence level is high, she is considered to be a specialist when it comes to technical aspects for ITS and the answers will be analyzed accordingly. The following figure illustrates the received responses.

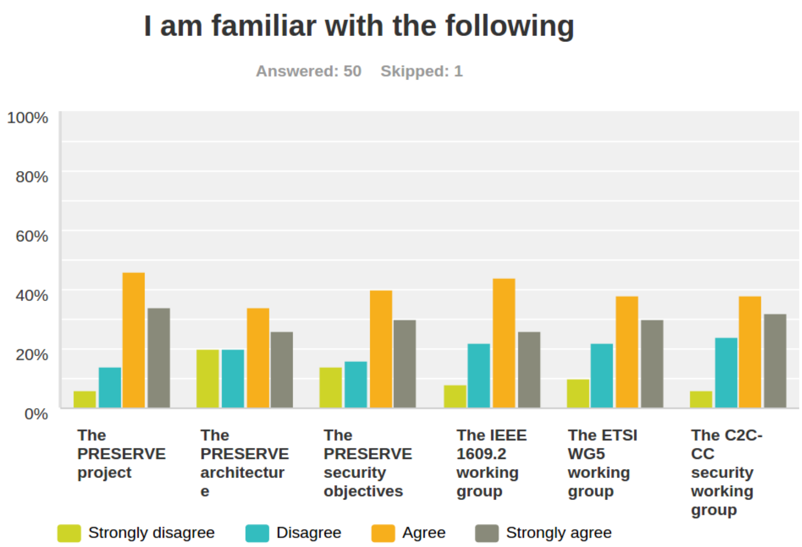

Figure 2.2: Question 3

What we can infer is that the majority of participants were familiar with the PRESERVE project (90%), the PRESERVE architecture (60%) and the project's security objectives (70%). Furthermore, 70% were familiar with the aforementioned standardization bodies and working groups. For the ETSI-WG5 and the C2C-CC, the percentages are 68% and 70%, respectively. The numbers show that successful projects can be more visible and raise awareness towards adoption of cutting technologies, more than consortia and standardization bodies.

Question 4 *Q4* focuses on *how* important, the participants, consider security and privacy requirements to be. These requirements are extracted from the state-of-the-art research and (relevant) technical literature.

[4] http://vii.path.berkeley.edu/1609_wave/
[5] http://www.etsi.org/website/technologies/intelligenttransportsystems.aspx

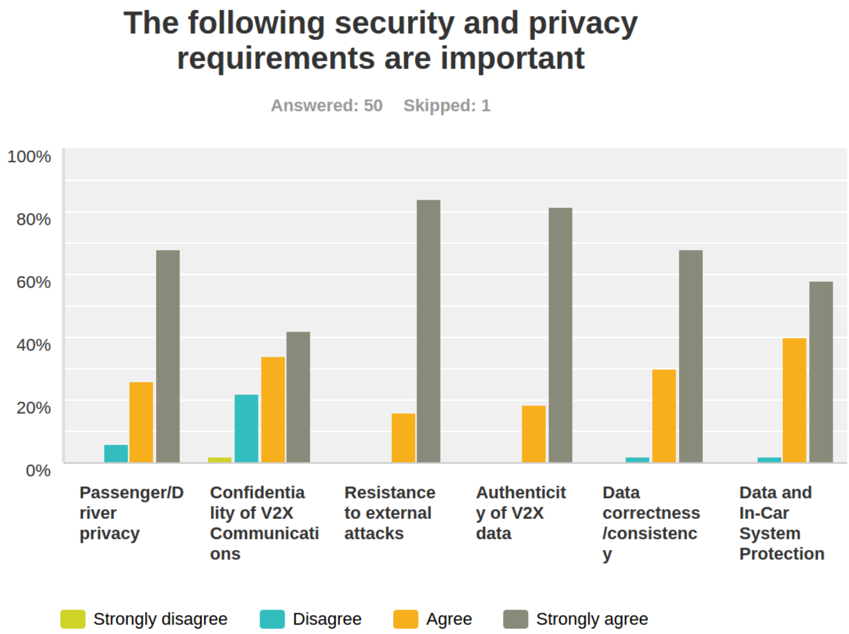

Figure 2.3: Question 4

As the above figure shows, the majority of participants consider “driver and passenger privacy” to be of paramount importance (94%). This high percentage reflects the strong research interest for privacy-preserving vehicular communications. The same holds for the rest of the requirements: More specifically, 76% of the responders believe that ensuring the authenticity of V2X communications is a critical requirement. All responders agree that resilience against external attacks is also pivotal. Finally, the same consensus holds in the case of communication authenticity (100%) and in-Car protection (98%). There are responses that confidentiality is not important resonating with old modelling and requirements [9].

Question 5 *Q5* tries to identify whether the broader ITS community considers applications which are built on top of collaborative, ad-hoc communication protocols (IEEE 802.11p) to require stronger security guarantees than the ones relying on the more resilient cellular networks (e.g., 2G/3G/LTE).

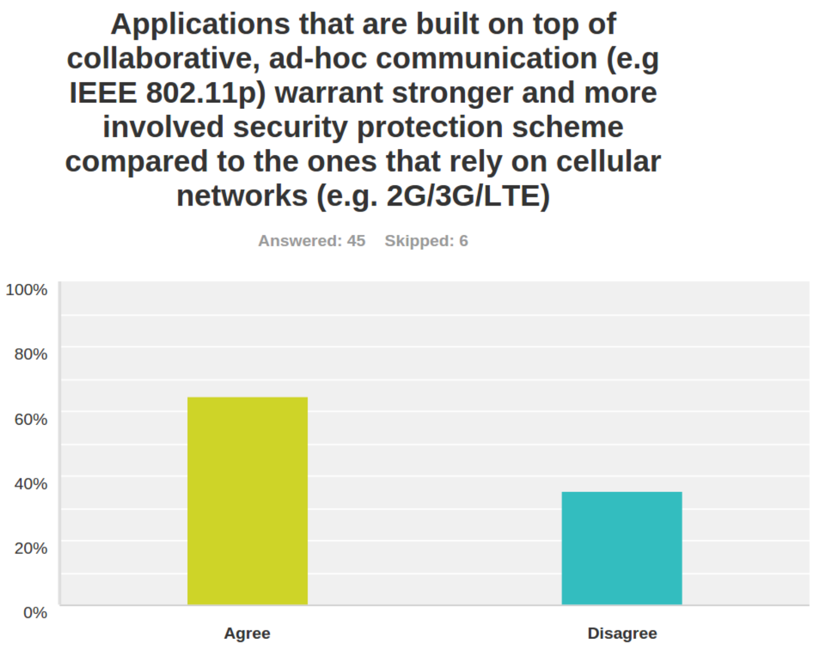

Figure 2.4: Question 5

As we can see, indeed, the majority of participants believe that applications built on top of ad-hoc communication schemes require stronger security protection compared to applications that rely on cellular networks. This result came to verify the thoughts that were brought forth in a panel discussion that took place during the IEEE VNC 2011[6]

Question 6 In *Q6* we ask the participants whether they think that PRESERVE architecture can be applied to ITS applications that are built on top of cellular networks. As it can be seen in the following figure, 97.5% of the responders agree that PRESERVE's architecture is applicable to applications built on top of 802.11p. Although this percentage decreases in the case of cellular networks (e.g., 3G, LTE), still the overall majority agrees that PRESERVE can ensure the security and privacy of such applications. It is interesting to point out that the standards for cellular systems, notably 3GPP, take fundamentally different approaches than VC systems security. Of course, one can be agnostic to the network and apply the PRESERVE solution transparently, but this does not leverage the cellular security architectures. [10, 11]

[6] http://www.ieee-vnc.org/2011/talks/panel.pdf

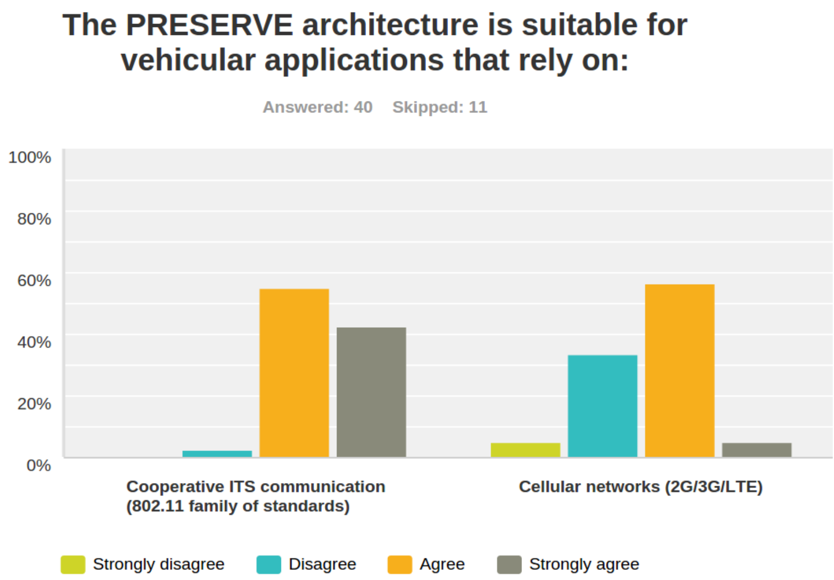

Figure 2.5: Question 6

Question 7 *Q7* asks the opinion of participants about the applicability of PRESERVE to applications specific to various different domains.

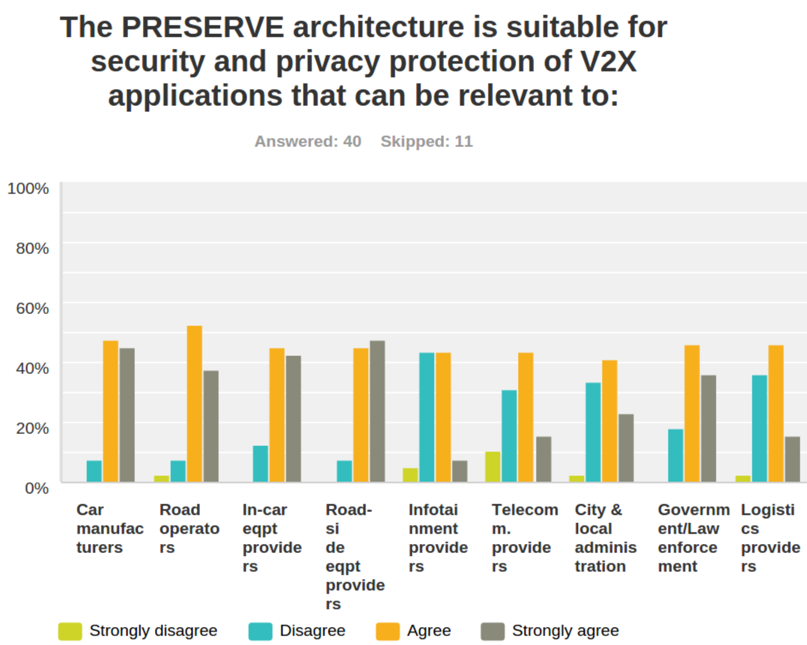

Figure 2.6: Question 7

Indeed, the majority of the participants believe that PRESERVE can meet the security and privacy requirements of a wide gamut of applications. The only exception is for applications relevant to *Telecommunication Providers* (41%) and providers of infotainment services (50%). This can address the concern of unsuitability of PRESERVE architecture for some of the vehicular applications. For example, there is not a high consensus on the suitability of the PRESERVE architecture for the security and privacy of infotainment providers, telecommunication providers and city and local administrations [10, 11].

2.3.3.2 Safety Applications Questions

This part of the survey focuses on safety applications. We consider the following application-specific list:

- **Road Hazard Warning**: Sudden slow-down warning, vehicle safety function (out of normal condition warning).
- **Cooperative Awareness**: Emergency vehicles notification, slow vehicle notification, motorcycle notification.
- **Cooperative Collision Avoidance**: Vulnerable user warning.
- **Traffic Hazard Warning**: Wrong way driving notification, stationary vehicle notification, traffic jam notification, signal violation notification.

We created four (4) questions in order to get a better insight *if* and *how* PRESERVE's VSS can be utilized to guarantee the security and privacy requirements of the four safety applications presented above.

Questions 8, 9 *Q8* and *Q9* probe the familiarity of the participants regarding the security and privacy requirements of safety applications. As the core focus of PRESERVE is on safety applications, it is critical to understand the opinion of the ITS community concerning the suitability of PRESERVE for these types of applications. The following figure illustrates the answers provided in the context of *Q8*.

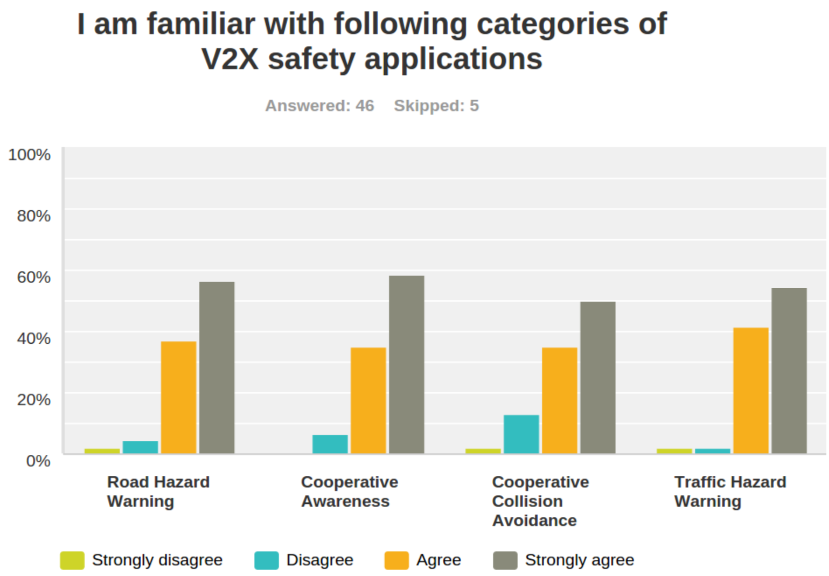

Figure 2.7: Question 8

As we can see, the majority of the responders are familiar with different types of safety applications. Furthermore, they concur that security and privacy are of paramount importance for safety applications, as the following figure shows. There are strong agreement on the importance of security and privacy for road/traffic hazard warnings; at the same time, there are more disagreement on the importance of security and privacy for the road/traffic hazard warnings. This confliction might be due to different viewpoints on considering security and privacy for these applications. One can argue that in a critical situation, e.g. safety application, the privacy of users should not be taken into account for the sake of human safety.

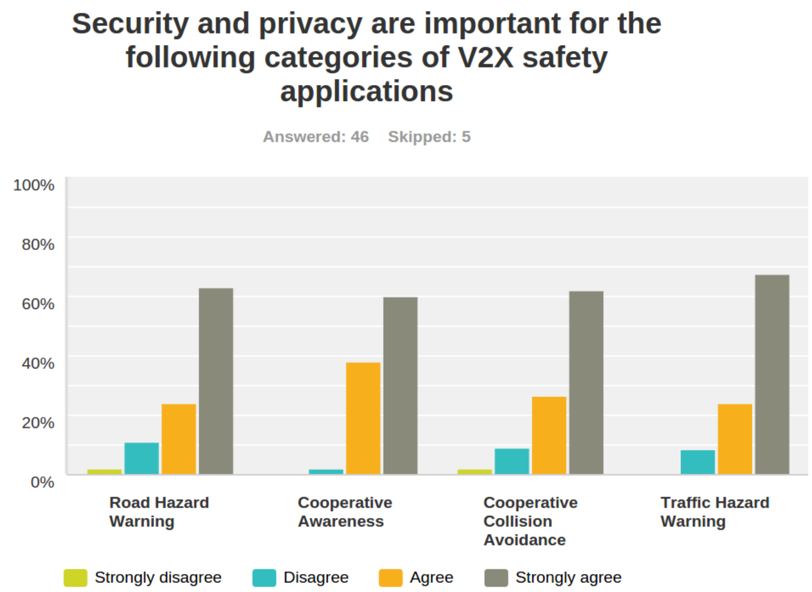

Figure 2.8: Question 9

Questions 10 *Q10* illustrates that the majority of participants (97%) agree that the PRESERVE architecture is suitable for different safety applications. Such a high agreement shows the suitability of the architecture for the safety applications.

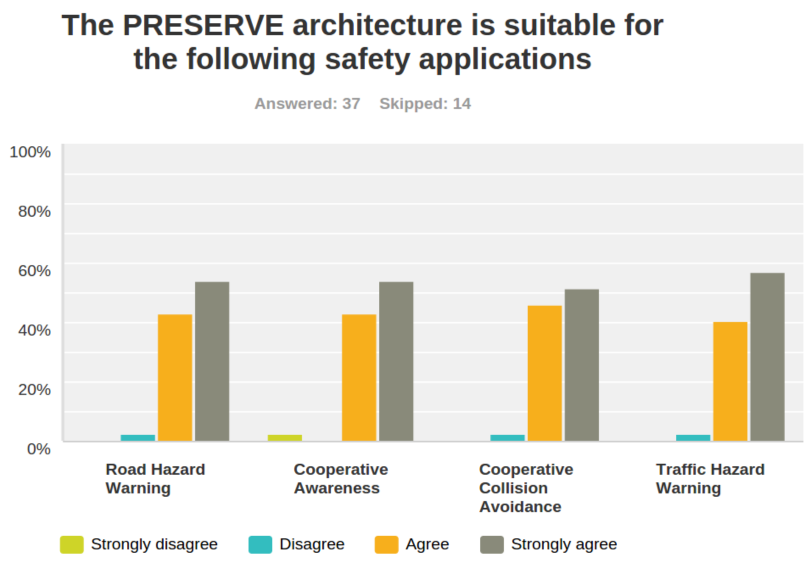

Figure 2.9: Question 10

Questions 12 *Q12* aims at identifying the negative influence of the security properties on the performance of the safety applications. As we can see, the majority (60%) of the responders believe that the privacy protection can highly affect on the performance of the safety applications. That is why there are also disagreement in *Q9* on the security and privacy consideration for the safety applications. As shown, there are disagreement on the influence: 52.5% believe that it does not have a performance influence on the authenticity for V2X, 60% agree that there is no performance degradation for V2X data consistency and 70% of the participants reflect that there is no performance influence on the in-car system integrity.

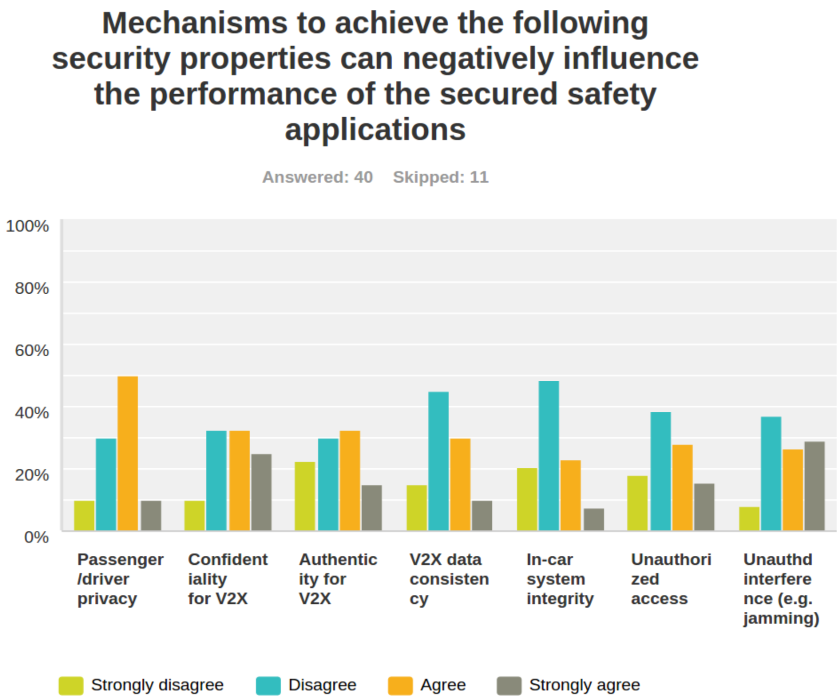

Figure 2.10: Question 12

2.3.3.3 Traffic Efficiency Questions

Question 13, 14, 16 In *Q13*, around 93% of the responders (strongly) agree that privacy is important for traffic efficiency applications and around 94% of the participants (strongly) agree the PRESERVE architecture could satisfy security and privacy requirements in these applications.

Q16 investigates the influence of security requirements on the performance of traffic efficiency applications. Overall, the responses are similar to those in *Q12*, but with a small shift towards disagreement. This is due to less time criticality in traffic efficiency applications than in secured safety applications.

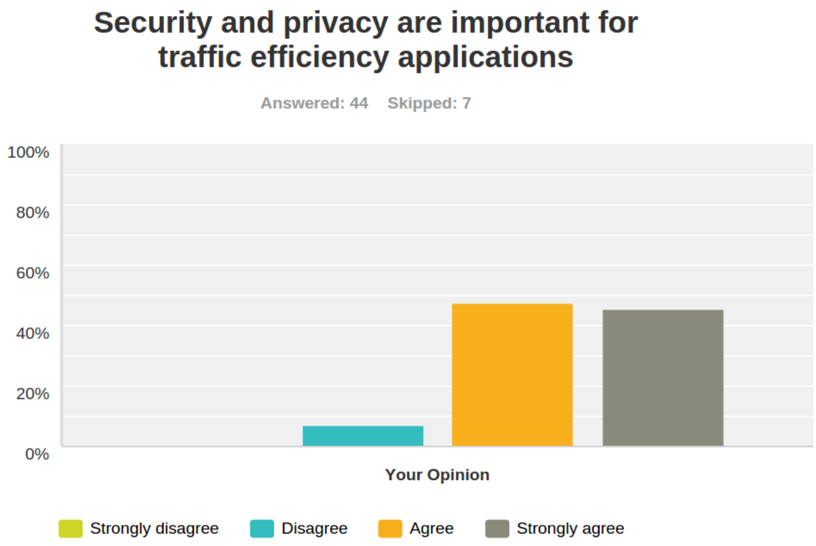

Figure 2.11: Question 13

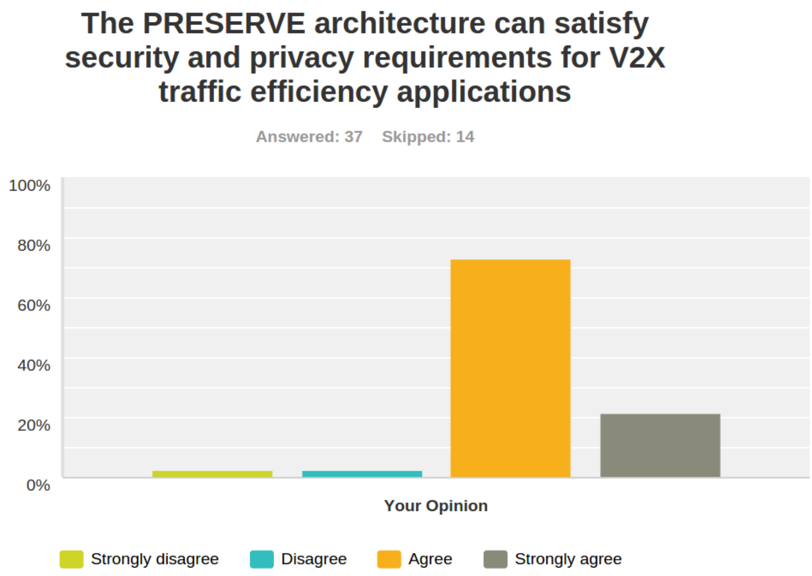

Figure 2.12: Question 14

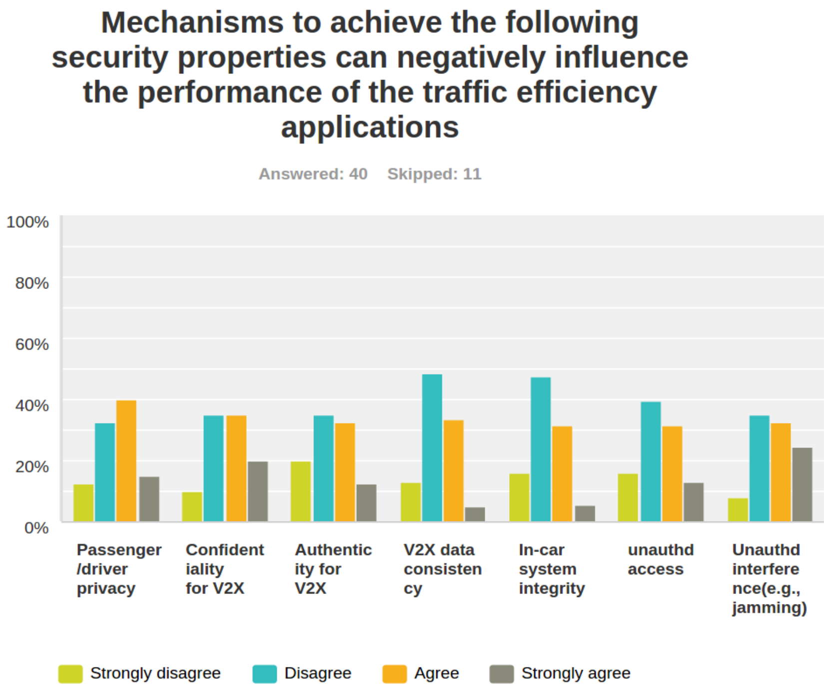

Figure 2.13: Question 16

2.3.3.4 Infotainment Applications Questions

Question 17, 18 Apart from traffic efficiency applications, most responders consider that security and privacy are also important in other applications (*Q17*). Especially, 40% of the responders strongly agree that security and privacy are important for vehicle life cycle management. In *Q18*, a vast majority of them agree that the PRESERVE architecture can satisfy security and privacy requirements in such applications. However, a few of them strongly agree with those, considering the purpose of the PRESERVE architecture is to secure V2V and V2I communication.

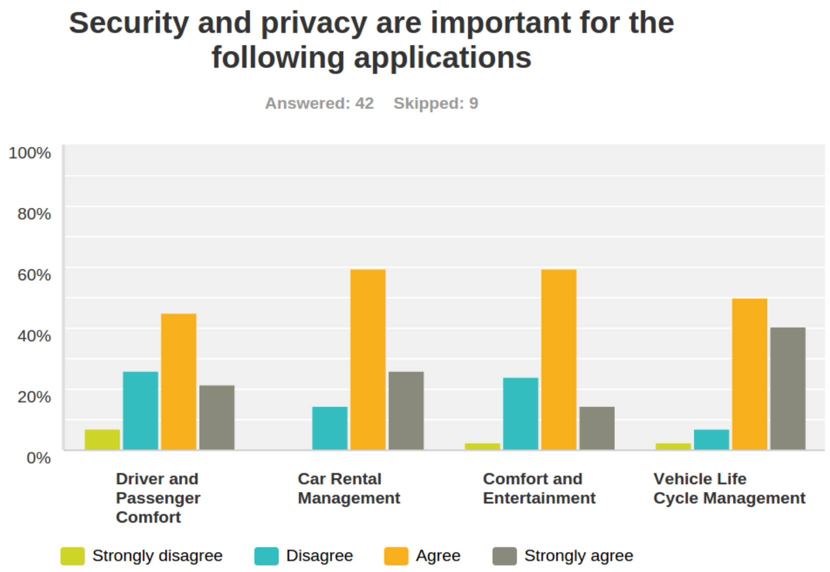

Figure 2.14: Question 17

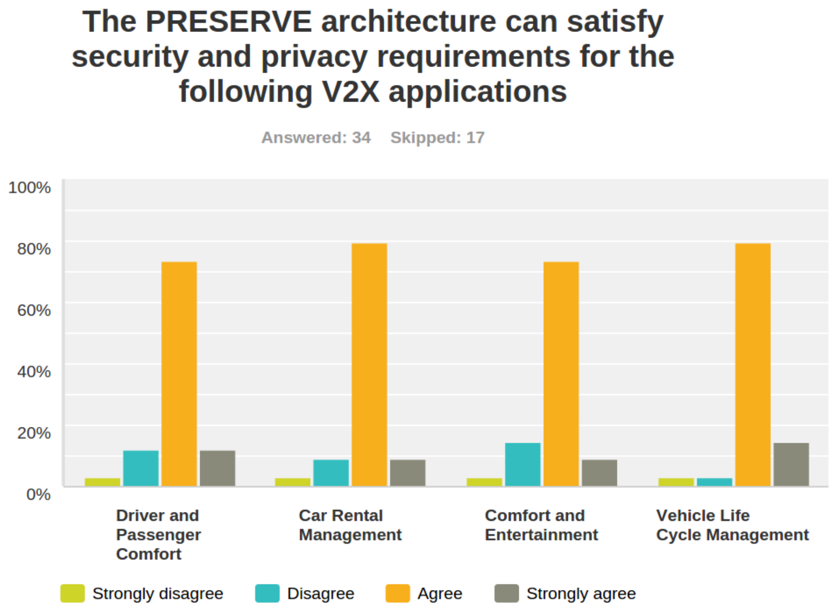

Figure 2.15: Question 18

2.3.3.5 Financial Aspects Questions

This section of the survey targets participants whose role in the company or the institution they represent is of managerial/business (non-technical) nature.

Question 21 *Q21* tries to infer the understanding of participants on the particular business aspects of ITS systems. As the following figure shows, the majority of the responders (70%) has either a substantial experience or a good understanding of such business aspects.

Figure 2.16: Question 21

Question 22 *Q22* focuses on the participant's opinion on the potential commercial value of the PRESERVE ITS solution. As we can see, the majority of responders (53.1%) agree that PRESERVE is a viable solution in the ITS domain.

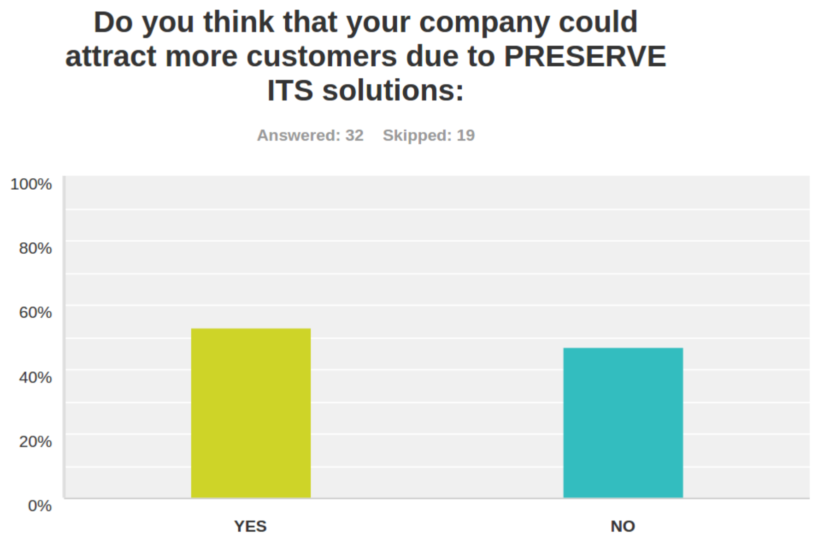

Figure 2.17: Question 22

Question 23 *Q23* asks for the participant's perception on the motives and incentives that drive organizations and institutions to introduce security and privacy solutions into their ITS-related products and services.

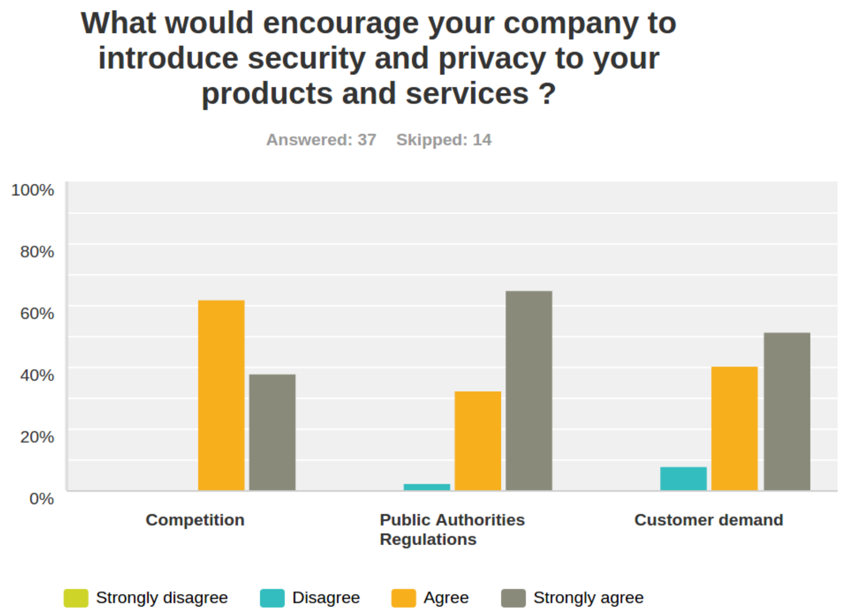

Figure 2.18: Question 23

As it can be seen from the figure, all of the responders believe that their organization will incorporate security and privacy in their products mostly due to the ongoing competition. In addition, 97% and 91% of the responders highlighted the importance of the regulations provided by various public authorities and customer demand respectively.

Question 24 *Q24* asks to identify the level of security and privacy that the corporations are willing to consider in their products and services. As we can see, the majority of the participants, i.e. 77%, consider the comprehensive security and privacy protection in their products while 23% reflect their view on applying base-level security and privacy according to the corresponding regulations. Interestingly, everyone agrees on security and privacy consideration in their products and services.

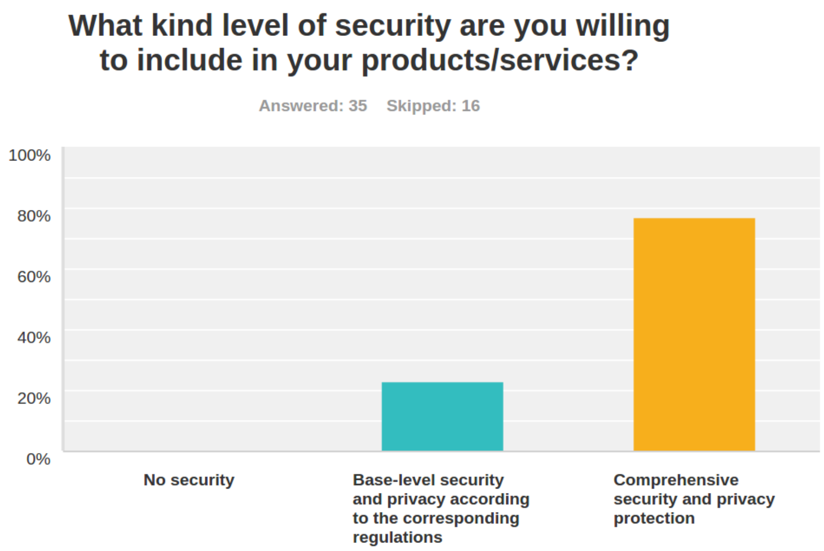

Figure 2.19: Question 24

Question 25 *Q25* tries to identify the estimated amount that the participants' companies can afford by applying security and privacy consideration to the products and services. Only 9% of the participants believe that their companies can afford low amount of money for security and privacy consideration. 33% of them reflect their perspective on a medium amount to be afforded by the company. 39% and 18% of the participants expressed that the estimated amount afforded by their companies is high and very high, respectively.

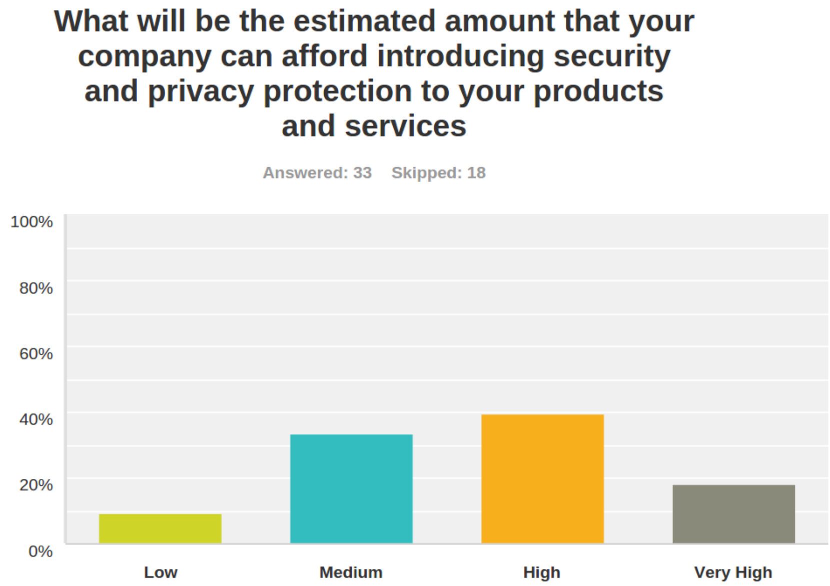

Figure 2.20: Question 25

Question 26 *Q26* asks to figure out the participants' view on the estimated product life-cycle cost of ITS related products. 9% of them agree that the cost would be low whereas 33% of them believe that the cost would be medium. 39% of the responders reflect their estimation to be high while 18% of them agree that the cost for a company to afford introducing security and privacy protection would be very high.

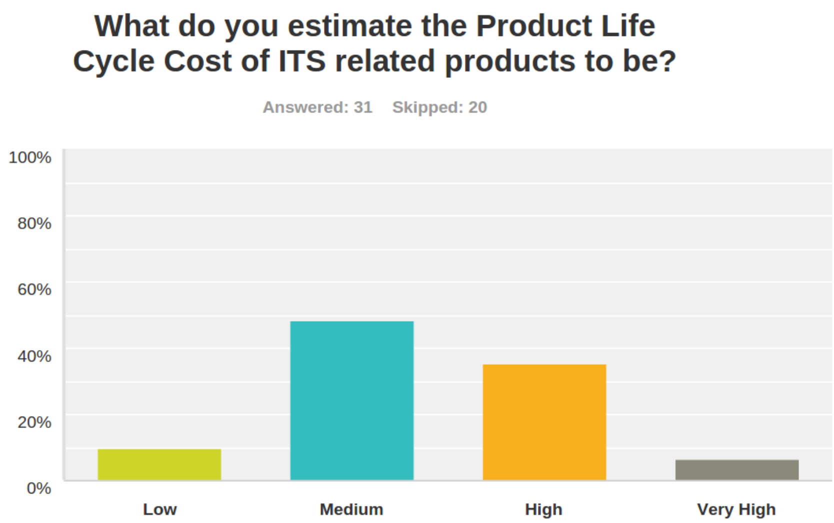

Figure 2.21: Question 26

Question 27 *Q27* asks to figure out the responders' perspective on the cost distribution among the ITS facilities. The majority of the participants, i.e., 65%, believe that the cost required for the ITS hardware would be the highest whereas the lowest cost required for the ITS facilities are product certificate and validation.

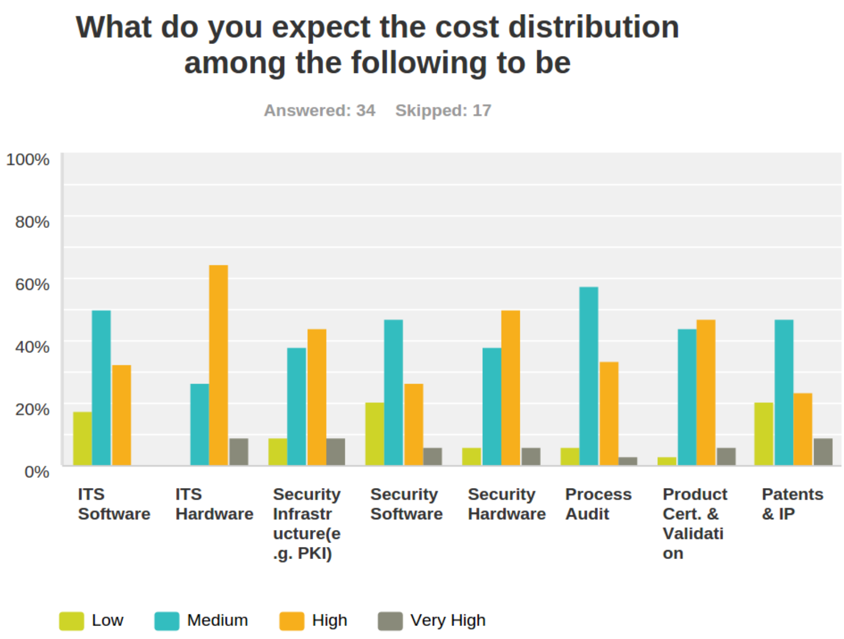

Figure 2.22: Question 27

Both answers from *Q26* and *Q27* imply that security and privacy solutions should be efficient enough to be deployable with affordable devices.

Question 28, 29 *Q28* asks to identify the value of security and privacy protection for the safety applications. As expected, the majority of the responders (67.5%) believe to be very high. 25% and 7.5% of the participants agree that the value of security and privacy protections for the safety applications are high and medium, respectively. No one agrees that it is of low value due to the criticality of the safety applications. For *Q29*, 67.5% of them agree that the value of security and privacy protection for traffic efficiency applications is high or very high.

It is worth to mention that the percentage of responders who consider security and privacy protections for safety applications very high is the same as the percentage who consider security and privacy protections for traffic efficiency applications is high or very high. This implies that although security and privacy protection is important in both applications, it is considered more critical in safety-related applications.

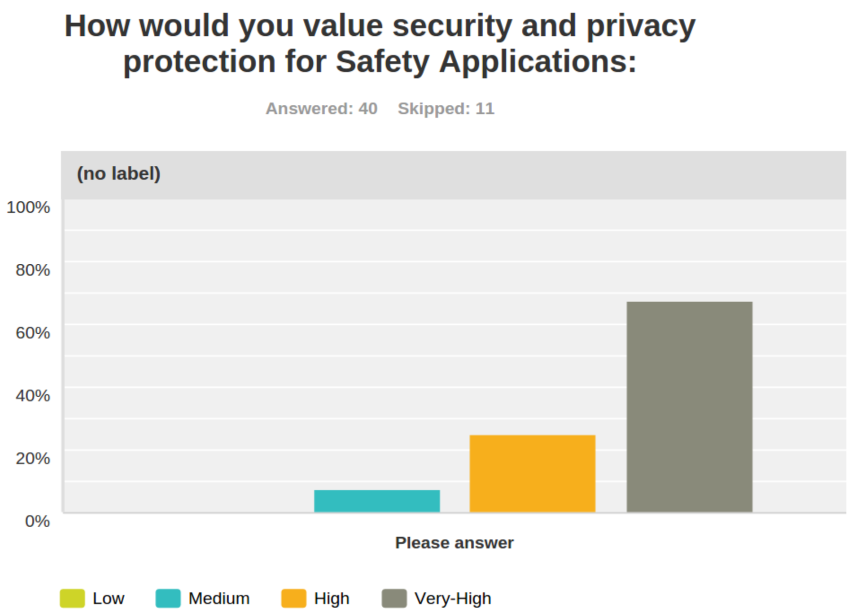

Figure 2.23: Question 28

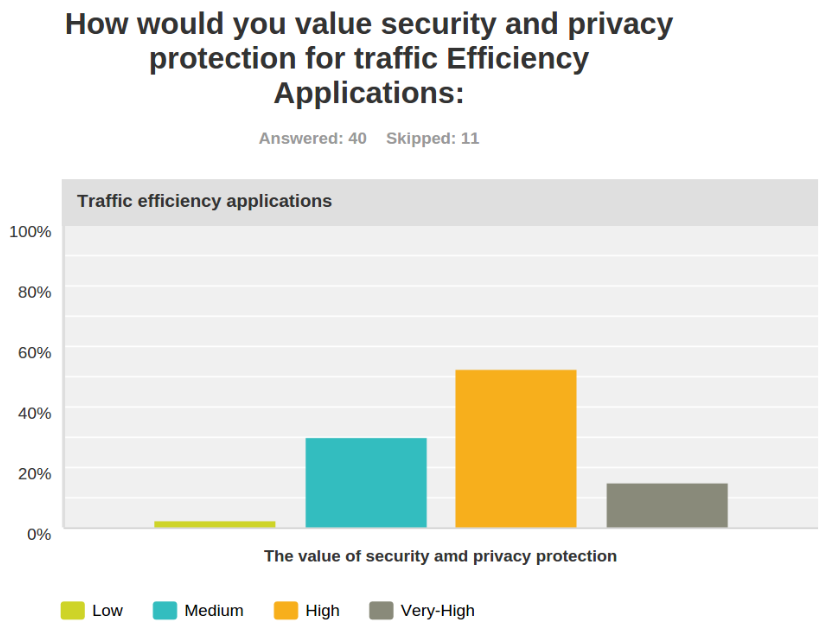

Figure 2.24: Question 29

Question 30 *Q30* asks to identify who should pay the cost for the security and privacy considerations. 64% agree that the customers, to the degree they are willing to, have to pay the cost; 51% believe that the authorities and governmental organizations are the responsible authorities. 52% and 68% also reflect that the telecommunication providers and car manufacturers are the corresponding entities to pay the cost for security and privacy.

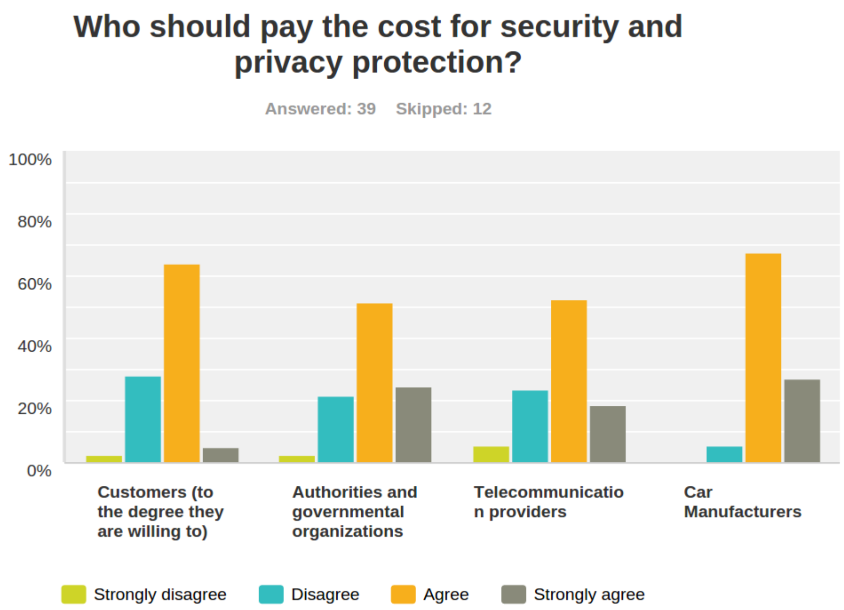

Figure 2.25: Question 30

Question 31 *Q31* asks to identify who should mainly invest in roadside infrastructure. The majority agree that public authorities (64%) and traffic management service providers (63%) are the main investors in the roadside infrastructure. Road operations also strongly agreed by 36% of the participants to invest in this area.

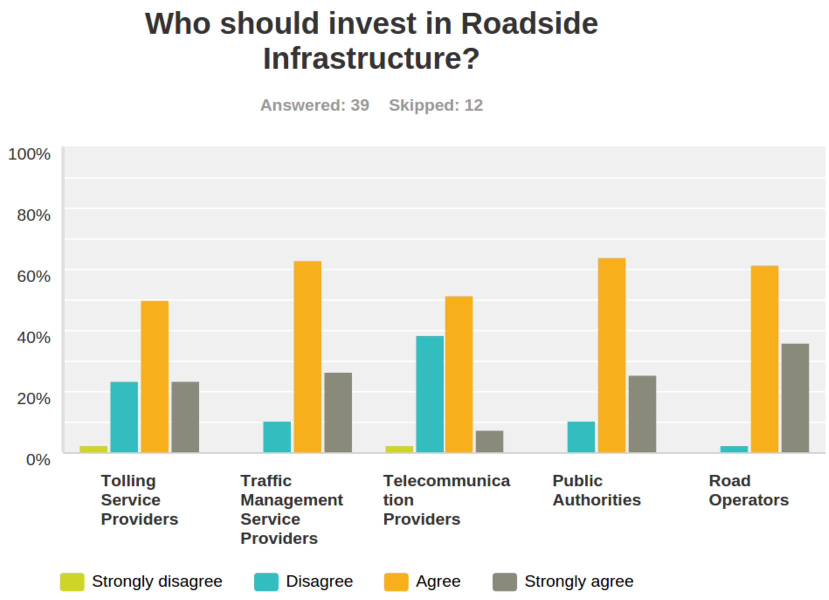

Figure 2.26: Question 31

2.3.3.6 Technical Aspects Questions

Question 32, 33 In *Q32*, around 72% of responders claim that they have substantial research and/or development experience. Essentially, the responders agree that all the attacks listed in *Q33* could bring negative impact, while they consider compromised roadside infrastructures or onboard equipment as two most fatal attacks. It is reasonable since the administrators and users will lose control over the infrastructures and devices once they are compromised, and cannot guarantee that they will work as expected. In-transit V2X traffic tampering incurred relatively lower concern. It might be due to the consideration of the responders for integrity protection of V2X communication.

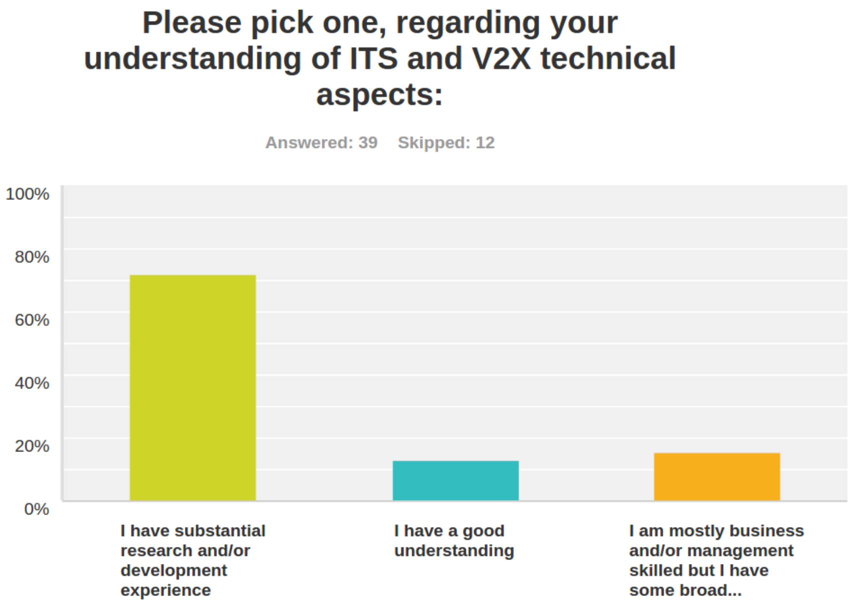

Figure 2.27: Question 32

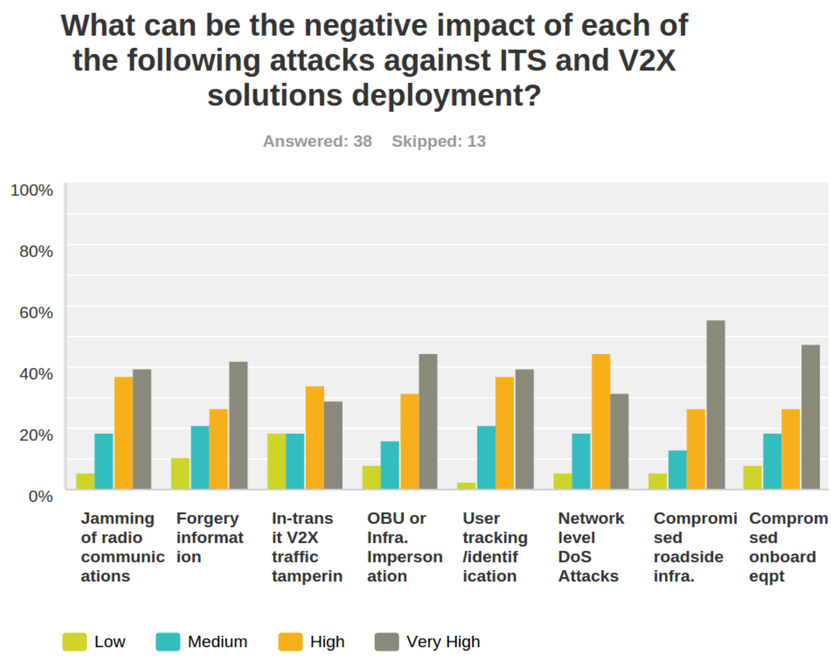

Figure 2.28: Question 33

Question 34, 35, 36 In *Q34*, *Q35* and *Q36*, most of the responders suggest ECDSA as the main cryptographic primitive for different types of applications. This complies with IEEE 1609.2, ETSI and C2C-CC standards. Moreover, they strongly suggest ECDSA-256 as a proper key size, although ECDSA-224 could be suitable as well.

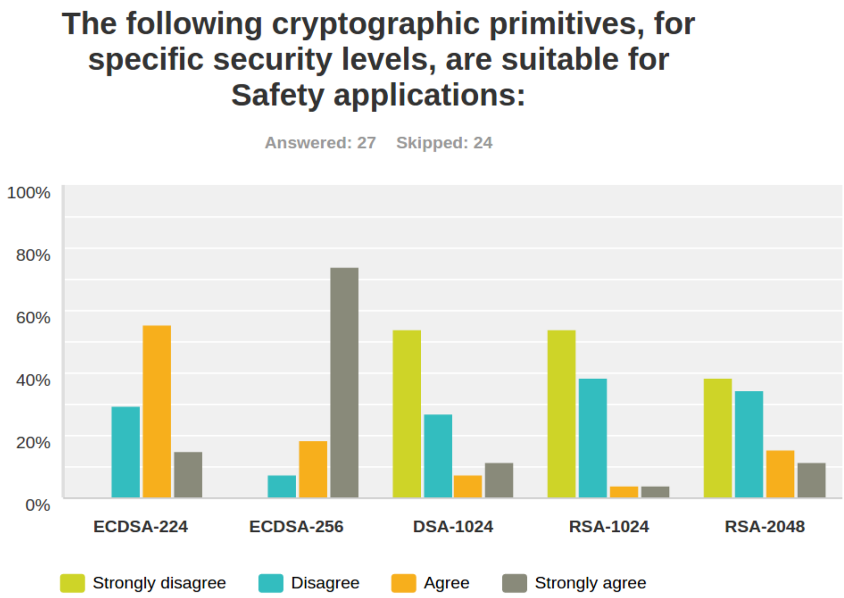

Figure 2.29: Question 34

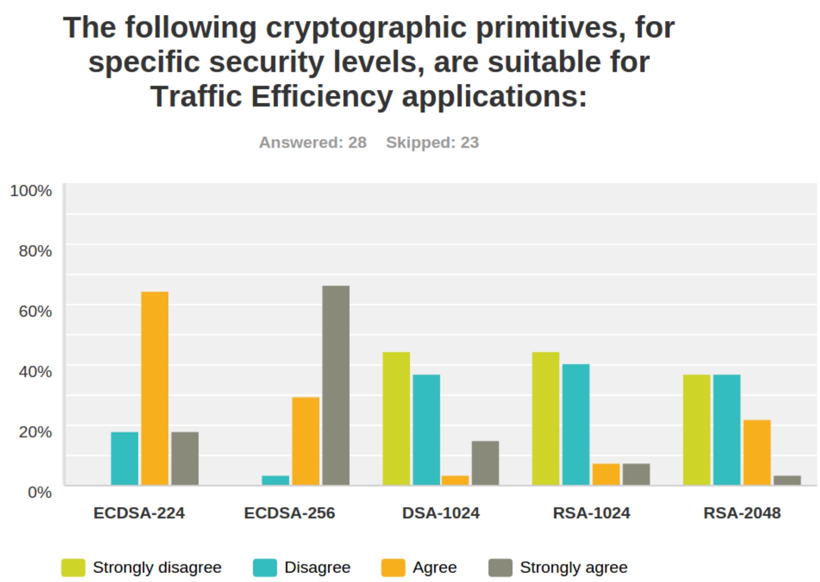

Figure 2.30: Question 35

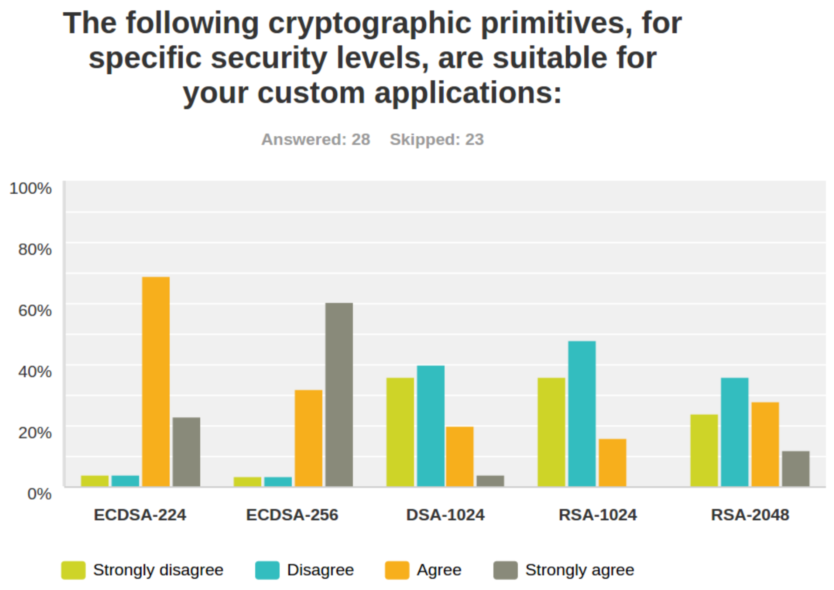

Figure 2.31: Question 36

Question 37 *Q37* investigates the major technical challenges towards the deployment of secure and privacy preserving V2X solutions. From security and privacy perspective, identity management, trust management and security updates are considered as the major challenges. In addition, standardization and interoperability are considered as two important aspects towards manufacturing and deployment phases. OBU processing power and OBU software complexity are considered less challenging considering the improving hardware specification of off-the-shelf OBUs.

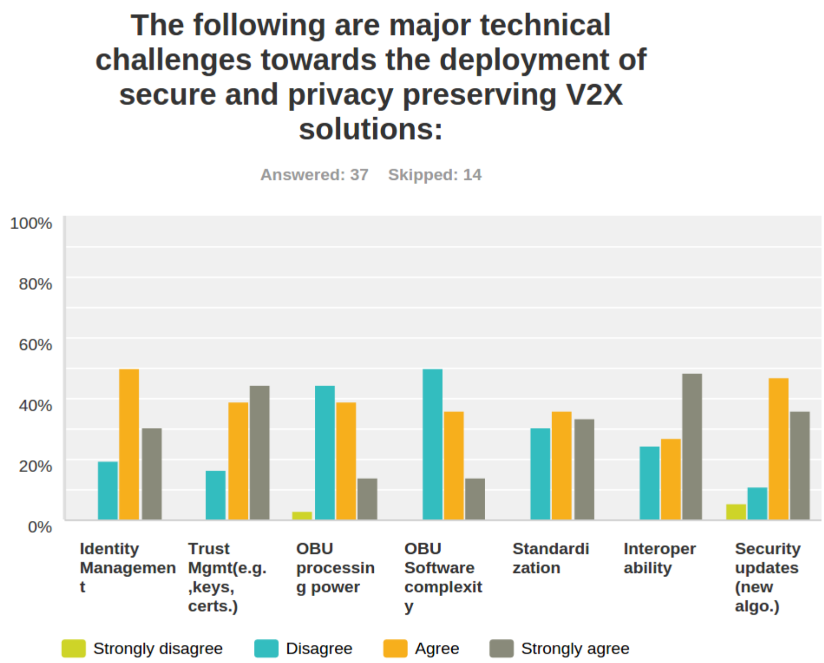

Figure 2.32: Question 37

2.3.4 Remarks

In conclusion, what we can deduce from the provided feedback is that the community definitely values the security and privacy aspects of vehicular communications and considers PRESERVE as a valid proposal that meets all the core requirements for secured safety applications and traffic efficiency applications. Nonetheless, it is yet not clear whether or not the presence of PRESERVE will create added value for companies that will adopt such solutions.

We can observe that PRESERVE architecture is suitable for vehicular applications to be deployed by both cooperative ITS communication (802.11 standards) and cellular networks. Although the majority (97.5%) agree to rely on cooperative ITS communication rather than cellular networks, there is no consensus on that front. Recent research show that the cellular security architectures are also converging towards this direction.

For some of the questions, we need further investigations. For example, both *Q25* and *Q26* did not explicitly list the cost in terms of numbers, and this may result in incorrect impression for the investigators since the responders may have different interpretations on the choices.

2.4 ASIC Cost Model

In PRESERVE, a cost model was created to relate the functionality of an ASIC to its costs which is very useful during early phases of the chip development. However, creating such a cost model for the production of an ASIC-based C2C-HSM is a difficult task, as it is based on two parameters which are in principle unknown:

- **Performance**: the performance of an ASIC chip can only be estimated until an ASIC is actually produced. Such estimations of the performance depend on many different factors, but may be given based on previous experience with similar technologies. As the number of ECC signature verifications per second is the key performance factor for ASICs in a C2C environment, we will use the verification speed as an indicator for the overall performance of the ASIC (note that this is a strong simplification, as other functionality of the chip may perform differently).
- **Absolute costs**: absolute costs of ASIC production depend on many factors such as produced quantities, design size, supported features, technologies, customer-supplier relationship and many more. In short, an OEM ordering an ASIC highly specialized for a certain use-case in large quantities (millions) for series production will get a totally different price than a smaller organization producing only small quantities of research ASICs. Hence, a cost model including absolute costs is not really meaningful and we will concentrate on relative costs instead.

Considering these difficult preconditions and leveraging on the experience gained during the design of the PRESERVE HSM ASIC, we try to give numbers and estimations for the given parameters to the best of our knowledge in the following.

2.4.1 Performance

Assuming that only one ECC core is implemented, the key factor for the verification speed is the technology (node size) in use. Generally speaking, a smaller gate size allows higher clock rates of the chip and thus better performance in terms of verification speed.

The verification speed can also be improved by implementing more than one ECC core in the chip design which can be used in parallel. However, the overall number of verifications measured outside of the chip does not scale linearly with the number of ECC cores, as there are several other limiting factors (bottlenecks), e.g.:

- Busload on the AHB bus
- AHB bus frequency
- System software complexity
- External communication (e.g., SPI, USB, Ethernet...)

The more ECC cores are running in parallel, the more influence these limiting factors will have. If, e.g., the maximum data rate of the bus is already fully consumed, adding additional ECC cores will not add any additional verification performance. The number of ECC cores that can be implemented is also limited by the number of gates available on the chip. Using a smaller technology will result in a higher number of gates on a chip of the same size. For example, on a chip of size 4mm x 4mm we can estimate the following numbers:

- ASIC 180nm: approx. 1.4 million gates
- ASIC 90nm: approx. 3 million gates
- ASIC 55nm: approx. 8 million gates

Depending on the system that is implemented, the 180nm technology may only yield enough space for one ECC core, whereas 90nm will allow for up to ten ECC cores and 55nm will allow for even more. Of course, this also depends heavily on the remaining components on the chip (e.g. CPU, RAM, ROM, interfaces, other cores) and how much chip space they require. Furthermore, we assume that more than 10 ECC cores are not reasonable with respect to the limiting factors.

Based on these numbers, we estimated the maximum numbers of verifications per second that can be achieved with a highly specialized and optimized chip design. As mentioned, these are only estimations and concrete numbers can only be given once an ASIC is produced and tested. The results can be seen in Table 2.1.

Technology	**Max clock rate**	**Verifications per second with**		
		1 ECC	**5 ECC**	**10 ECC**
ASIC 180nm	100 MHz	100	-	-
ASIC 90nm	200 MHz	200	750	1100
ASIC 55nm	350 MHz	320	1200	1760

Table 2.1: ASIC performance estimation

2.4.2 Relative costs

The costs stated in this section are relative costs based on evaluations done within the PRESERVE project. They are useful to compare different options/technologies and show, how different performance requirements on the one hand are reflected in the costs/prices on the other hand.

At the center of the cost estimation is the slowest option (option 1), i.e. the 180nm technology with only one ECC. The costs of the other options are then given as additional costs relative to option 1. We distinguish the following categories of costs for the ASIC production:

- Fixed costs: only applicable once in the production process which are mostly given by the following two items
  - Design costs (frontend and backend design)
  - Prototyping costs (production of prototype/silicon mask and first shuttle)
- Costs per item: costs for each additional unit that is being produced

Altogether, the considerations result in the following cost model described in Table 2.2.

Opt.	**Verifications/s**	**Technology**	**ECCs**	**Cost relative to option 1**		
				Design	**Prototype**	**Item Costs**
1	100	180nm	1	0	0	0
2	200	90nm	1	+ 9 %	+ 175 %	+ 83 %
3	320	55nm	1	+ 22 %	+ 175 %	+ 116 %
4	750	90nm	5	+ 30 %	+ 175 %	+ 83 %
5	1100	90nm	10	+ 51 %	+ 175 %	+ 83 %
6	1200	55nm	5	+ 43 %	+ 175 %	+ 116 %
7	1760	55nm	10	+ 64 %	+ 175 %	+ 116 %

Table 2.2: ASIC cost model

Analyzing the above cost model, one will find many interesting aspects. Of course, option 1 is the cheapest, but offers also the weakest performance. This is only an option for validation purposes, but not for applications in realistic C2C environments. The other options offer more possibilities in these terms. However, moving to a smaller technology will increase all costs items. While prototype costs will be equal for 90nm and 55nm, design costs and costs per item will increase significantly for a smaller gate size. The number of ECCs does only influence the design costs, as more ECCs result in a bigger design and thus in higher design efforts.

An interesting aspect can also be found by comparing options 5 and 6, since both result in a similar performance, but different prices. While option 5 uses a bigger technology and a bigger design, option 6 makes use of a higher clock rate. With the lower design costs and slightly better performance, option 6 is a good choice for a research environment. Yet on the other hand, it also comes with higher costs per item and thus option 5 is more suitable for a mass production environment.

One also needs to consider that option 5 requires a higher degree of parallelism to achieve the same absolute performance which increases software and overall system complexity and may not even be possible to reach.

2.4.3 Target costs

As stated above, absolute target costs are difficult to come by in contrast to the evaluation of relative costs in the previous section. This has multiple reasons, the most important one is the variety of factors having significant impact on the absolute costs of a chip production. Those factors include:

- Production factors
  - Quantities ordered (total per run/per year)
  - Production type / technology used
  - Required lead time
- Technical factors
  - Functionality of the SoC besides V2X security
  - Chip size / area consumption
  - Node size / clock rate
  - Number of outgoing pins
  - Power consumption boundaries
  - Temperature boundaries

As these are only examples, the decisive factors are too manifold to give a concrete target cost estimation without detailed analysis of the SoC setting, including negotiations with potential partners and IC manufacturers as well as discussions with target customers about quantities and requirements. As any of such discussions take place under strict confidentiality, it is not possible to publish the results.

2.5 Validation and Certification

For the security of a V2X communication system, assurance about the in-vehicle security of participants is vital: The receiver of a message has to be able to rely on the fact that the sender has generated the message correctly. Hence, a security breach on the sender side would have impact on the receiver of a message. Therefore, only vehicles with a reasonable “level of security” should be able to obtain certificates from the C2X PKI that authorize them to sign messages. Security assurance addresses the question how to determine (with appropriate confidence) whether a product provides the required security properties or not.

A wide-spread approach to assurance is the (methodical) security evaluation of a product by an independent third party. Based on such an evaluation, vendors can obtain certificates for their products stating the evaluation result. For V2X systems, it would be desirable to have a (minimum) standard, according to which all products have to be evaluated before being deployed. Successful evaluation and certification could be the basis for Enrolment Authorities to issue enrolment credentials to vehicles. From a technical point of view, it is irrelevant if such an evaluation would be required by legal regulations or obtained by consensus within the automotive industry. However, care must be taken that the costs of security evaluation and certification do not become prohibitive.

A well-known international framework for assurance in the IT industry is **Common Criteria (CC)**, which is widely-used, e.g., for security evaluation of smartcards. CC provides a catalogue of standardized security requirements and security evaluation requirements, as well as a methodology to structure the evaluation process and its documentation. CC not only addresses the security assessment of the product itself, but it includes the product life-cycle, including development and (at least to some extent) operation. After successful evaluation, a product can be certified. CC enables the definition of **Protection Profiles (PPs)** that describe a class of products and the related security requirements. For a concrete product, a vendor can then write a Security Target (essentially an instantiation of the PP, fixing the details that were left open by the PP authors) that claims conformance to the PP. After successful evaluation, the vendor receives a certificate for the product which states that the product conforms to the specified PP. Conformance to a PP enables customers to check that the security of different products (from different vendors) at least have been evaluated according to some common set of requirements.

The Car-to-Car Consortium (C2C-CC) – a consortium of the (European) automotive industry – is considering the adoption of an approach similar to the CC. Currently, it is not yet sure whether the C2C-CC would make evaluation and certification by (existing) CC evaluators and authorities according to existing procedures mandatory. However, the CC framework could be used as a basis for evaluation (and certification) by either an entity like an industry consortium, or by self-certification of the manufacturer. In any case, the C2C-CC introduced Trust Assurance Levels (TALs) that should be included in the authorization tickets (pseudonym certificates) of vehicles. Currently, an informal description of TALs exists, and a Common Criteria Protection Profile is being drafted that might be used for the (yet to be defined) certification process.

The C2C-CC proposed the following Trust Assurance Levels (TALs) (see Figure 2.33):

- **TAL 0:** No evaluation.
- **TAL 1:** Only the software of the C2X box is evaluated.
- **TAL 2:** In addition to TAL 1, the C2X box hardware, including dedicated hardware security and tamper evidence, is evaluated
- **TAL 3:** In addition to TAL 2, “private” ECUs and a “private” network directly connected to the C2X box are evaluated. Moreover, basic tamper resistance of the HSM is required.
- **TAL 4:** In addition to TAL3, all relevant in-vehicle sensors and ECUs are evaluated. Moreover, moderate to high tamper resistance of the HSM is required.

Trust Ass. Level (TAL)	Requirements			Implications		
	Minimum Target of Evaluation (TOE)	Minimum Evaluation Assurance Level (EAL)	Minimum (Hardware) Security Functionality	Prevented (Internal) Attacker acc. to CC	Potential Security Implications	C2X Use Case Examples
0	None	None	None	None	Not reliable against security attacks in general	Some limited,e.g. using trusted C2I infrastructures
1	+ V2X box software	EAL 3	Only software security mechanisms	Basic	Not reliable against simple hardware attacks (e.g., offline flash manipulation)	Non-safety, but most privacy relevant use cases
			Minimum Level			
2	+ V2X box hardware	EAL 4	+ dedicated hardware security (i.e., secure memory & processing) + tamper evidence	Enhanced Basic	Not reliable against more sophisticated hardware attacks (e.g., side-channel attacks)	C2C-CC day one use cases (e.g., passive warnings and helpers)
3	+ private ECU & private network	EAL 4+ (AVA_VAN.4 vulnerability resistance)	+ basic tamper resistance	Moderate	C2X box secure as stand alone device, but without trustworthy in-vehicle inputs	Safety relevant relying not only on V2X inputs
4	+ relevant in-vehicle sensors and ECUs	EAL 4+ (AVA_VAN.5 vulnerability resistance)	+ moderate – high tamper resistance	Moderate – High	C2X box is trustworthy also regarding all relevant in-vehicle inputs	All

Figure 2.33: Overview of the proposed trust assurance levels (Source: internal C2C-CC report on Trust Assurance Levels)

According to the current proposal, not only the extent of the evaluation (What is evaluated and what requirements are mandatory?), but also its depth (How thoroughly is the evaluation performed?) increases with each TAL. However, this proposal might still be changed in future versions.

The current consensus is that TAL 2 would be the appropriate minimum level for the Day 1 use cases. Therefore, a PP is currently being drafted on behalf of the C2C-CC with the goal to define TAL 2 in the terms of the CC. However, future applications will require higher TALs.

The work on TALs in C2C-CC has not been finished yet and is still a matter of discussion and changes. We thank Hans Löhr (Bosch, C2C-CC) who has provided contributions to this section.

2.6 Pseudonym Certificate Signing Request

ITS standards have introduced the V2X Public Key Infrastructure (PKI) and the pseudonym certificates to protect security and privacy of ITS stations. In a PKI, certificate management raises significant challenges especially regarding solutions for renewing certificates in the embedded ITS-S vehicle. A reliable updating process of certificates can only be guaranteed if a update over the air service is provided. Indeed, for an embedded and connected vehicular system like ITS-S vehicle, security management services should be done without user interaction. It is further required to design a secure and efficient protocol to a perform certificate acquisition process for practical ITS. The protocols designed in [12] take into consideration the PKI specifications especially the role separation for the various PKI authorities (LTCA and PCA). The certificate update protocol is adapted to the different connectivity patterns and modes between a vehicle and the PKI authorities. These security protocols with the PKI are agnostic of the communication system. In the proposal of a new protocol for updating pseudonym certificates over the air [12] different possible connectivity options with the PKI are considered, i.e. different media and protocol stacks (see Figure 2-3). Additionally, the application protocols do not assume nor prevent the use of a transport security layer below, e.g. TLS.

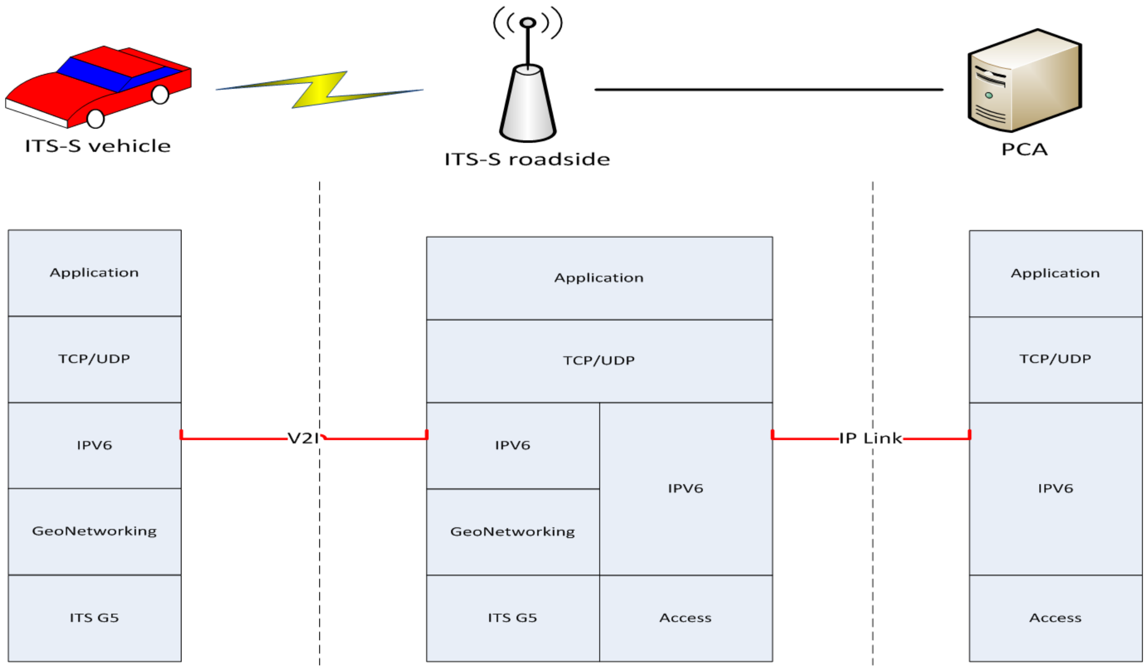

Figure 2.34: Communication stacks between vehicle and PCA if V2I communications based on IPV6 over GeoNetworking protocol

In fact, permanent connection to the PKI authorities is not expected to be available for ITS-S vehicles. Therefore, a pull or push model is taken into account concerning the connectivity between a vehicle and PKI authorities. Furthermore, two major connectivity patterns for pseudonym certificates updates are considered:

- In a mono technology pattern between vehicle and PCA, the ITS-S vehicle has cellular network access (3G for example) and establishes a direct connection to PKI authorities in order to download new pseudonym certificates.
- In a multiple, heterogeneous technology pattern the vehicle uses the free ITS G5 (or other Wi-Fi technology) to establish a connection to PKI authorities. In this case, ITS-S vehicle has no direct access to the PKI authorities.

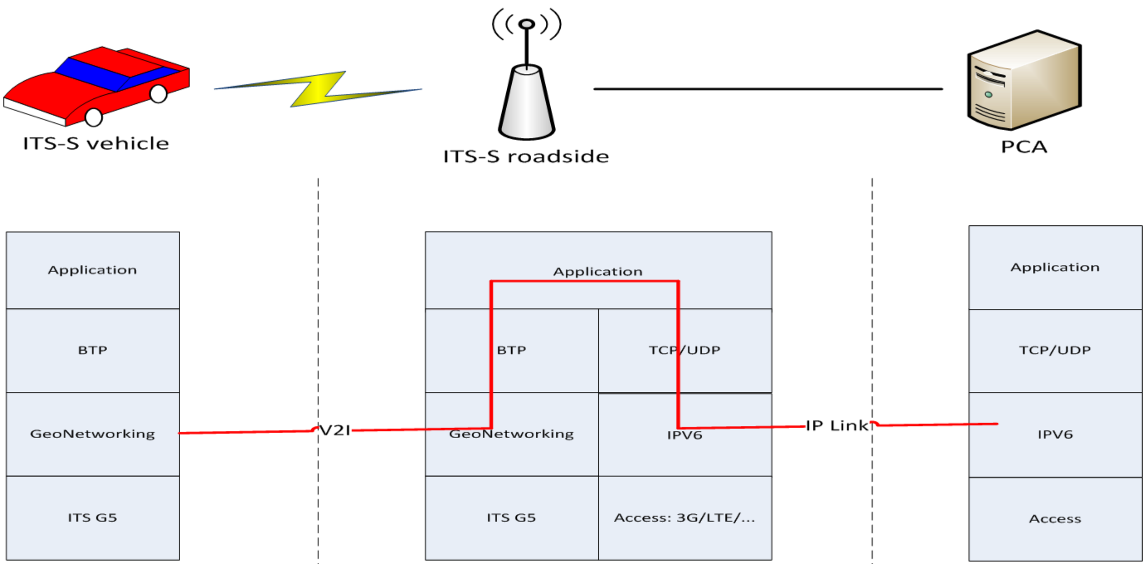

Figure 2.35: Communication stacks between vehicle and PCA if V2I communications based on GeoNetworking protocol

A detailed description of the proposed protocols MPCUP and SPCURO is given in [12]. MPCUP is a media independent pseudonym certificate protocol that follows the pull connectivity mode. This protocol allows vehicles equipped with 3G technology to obtain certificates of their pseudonym keys.

SPCURO is the protocol used to update pseudonym certificate via roadside units in a secure and efficient way. Aiming at being interoperable with actual ITS standards, the protocols focus on the ETSI ITS PKI model presented in [13]. A first implementation of the pseudonym certificate update protocol using ITS G5 was done in the frame of this research. In order to provide a proof of concept this protocol was implemented using the Score@F platform for OBU and RSU. This concept implementation used a simulator for the remote PKI services and for the access of security services. The integration and test of the protocols with the PRESERVE VSS is on-going in PRESERVE WP2 and WP3.

3 Scalability of secure communication

3.1 A Formal Model for Certificate Omission

To prevent injection of messages by external attackers, vehicles sign every beacon with a private key and append the accompanying certificate to the message. Any receiver then has to verify the certificate and the signature of the beacon before further processing of the message. Hence, security creates a communication overhead (i.e., packet size increases) and a computational overhead (i.e., time to process the packet). One approach to reduce communication overhead is to omit certificates, decreasing the beacon packet size by 140 bytes [14]. Benefits of the certificate omission schemes described below were proven by simulation in [15–17].

- No omission of certificates (NoOm): This scheme serves as a baseline as it performs no omission.
- Periodic omission of certificates (POoC) [18]: The idea of POoC is to add the certificate every n beacons.[1] Certificate periods of 3 seconds and 10 seconds are often considered.
- Neighbor-based certificate omission (NbCO) [19]: This scheme considers the context of a vehicle in the omission decision. The idea of NbCO is to only attach the certificate to beacons if there is a change in the neighbor table.
- Congestion-based certificate omission (CbCO) [16]: This scheme considers the load of the communication channel as the guiding metric. If the communication channel is free, there is no need to omit certificates to reduce the load on the channel. If the communication channel is congested, then the communication load is reduced by aggressively omitting certificates.

The benefits of certificate omission schemes in VANET have been so far proven by simulation. However, the research community is lacking of a formal model that would allow implementers and policy makers to select the optimal parameters for such schemes. In /citefeiri:2014:formalmodel, we lay the foundations of the formal model for certificate omission schemes in VANET. We apply the model to 'No Omission' and 'Periodic Omission', which validates the previous simulation and helps to identify and optimize influencing parameters for these schemes.

[1] called *certificate period* in the original paper

To remain independent of the intricacies of signal propagation details in specific scenarios, we restrict our assumptions about the communication channel to an abstract packet delivery probability function $D_s(d)$ for a given scenario s with the distance d between sender and receiver as input. Additionally we use c to denote the rate of certificate inclusions. With these inputs we combine the probability of already having received a certificate (CPL) with the probability of receiving a packet at all (NPL) to obtain a a formula for the likelihood successful packet reception from a new neighboring vehicle.

$$(1 - ((1 - D_s(d) * c)^n)) * D_s(d) \tag{3.1}$$

The results are in line with simulation models that have served as validation for the introduction of omission schemes in previous works. However our current model only considers the NoOm and POoC omission schemes. Alternative omissions schemes, such as CbCO and NbCO, rely on context sensitive mechanisms. Building models for such schemes remains as future work. The availability of precise analytical models for the relevant omission schemes will enable rigorous selection of schemes and parameters with the most beneficial trade-offs for overall packet delivery success.

3.2 Certificate Pre-Distribution

Adding security through the pervasive use of digital signatures does have a significant impact on the usage of bandwidth and computational resources. To this end, applications should use a digital signature scheme that minimizes the increase of bandwidth usage. However, bandwidth overhead not only depends on the choice of a digital signature scheme but more importantly on the distribution method of certificates. A deficiency in optimizing bandwidth usage leads to an increase of packet collisions in the wireless channel, and thus, can cause degradation of service quality for all applications, including safety-of-life applications.

Typically, a sender is expected to bundle all relevant certificates of a trust chain with each signed message. This allows recipients to fully validate the message. However, this creates a significant bandwidth overhead. Alternatives are on-demand requests of missing certificates or omission schemes that determine a frequency of omitting certificates. The fundamental trade-off, however, is the introduction of cryptographic packet loss in the form of unverifiable packets [16]. Omission schemes need to balance the intended decrease of network packet loss (NPL) as a result of fewer collisions in the communication channel against the unintended introduction of cryptographic packet loss (CPL).

In [20] and an upcoming publication at IEEE VTC 2015, propose a technique that combines certificate omission and certificate pre-distribution in order to reduce communication overhead and to minimize cryptographic packet loss. Pre-distribution anticipates the need for certificates and disseminates them proactively. Needs for certificates arise through the

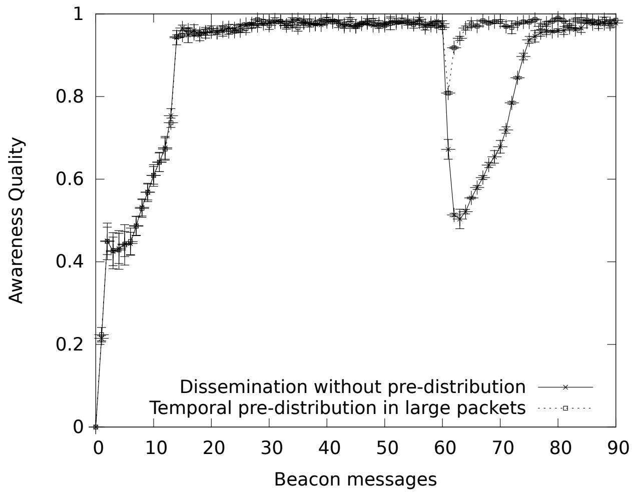

Figure 3.1: Awareness quality without and with temporal pre-distribution

arrival of new vehicles in a geographic region, or through a switch of cryptographic identities with the intention of breaking linkability of vehicle movements over extended periods of time.

Figure 3.1 shows that this technique does not cause any negative effects during the pre-distribution period before the pseudonym changes. A major improvement is, however, visible in the reduced drop of Awareness Quality (AQ) at the point of a synchronized pseudonym change. AQ falls to only about 0.8 compared to 0.5 when not applying temporal pre-distribution. The AQ then reaches the previous level within only one or two beacon cycles, performing much better than the pseudonym change without pre-distribution.

Simulation results demonstrated that pre-distribution of certificates does not eliminate cryptographic packet loss entirely. However, this technique can significantly reduce cryptographic packet loss caused by pseudonym changes while driving. Moreover, the introduction of certificate pre-distribution should be possible without requiring deep changes to existing architectures for certificate management in vehicular communication. As such we expect to see further practical evaluations of this technique to minimize service quality reductions due to the addition of security and privacy in vehicular communication.

As we limited the pre-distribution techniques to one-hop dissemination, the first future work is the evaluation of multi-hop dissemination. This will require more careful scoping rules to avoid wasteful usage of bandwidth, and a close investigation of privacy aspects. Indeed, wide-scale pre-distribution might improve tracking capabilities of attackers that would otherwise have gaps and uncertainties in their coverage. One more opportunity for enhancements is the selection of certificates for pre-distribution. Improved strategies could aim to maximize expected utility for neighboring vehicles based on knowledge of vehicle trajectories and position histories.

Another future work is the investigation of out-of-band channels, as we exclusively considered certificate pre-distribution in-band within the same 802.11p communication channel.

Alternative communication channels, possibly with different performance attributes, could be used to predictively maintain caches of certificates needed by vehicles.

3.3 Towards Deploying a Scalable & Robust VPKI

With basic concepts understood, there are few works that crisply define Vehicular Public-Key Infrastructure (VPKI) components. The SeVeCom project [21], and its continuation, PRESERVE, have led to a VPKI instantiation compliant to the C2C-CC framework. Because of direct PCA - LTCA communication (at the time of pseudonym provision), the LTCA knows the pseudonym providing PCA, thus it can easily link messages. Similarly, the SCMS [22] requires that the identity provider forwards requests to PCAs, thus being prone to the same inference[2].

SEROSA [23] proposed a general *service-oriented* security architecture seeking to bridge the Internet and the VC domains. However, the identity provider can still infer the identity of the service provider based on the protocol design. Moreover, the multi-domain environment explicitly addressed by SEROSA leaves space for Sybil-based misbehavior. The infrastructure cannot prevent multiple spurious requests to different PCAs. Of course, an HSM (ensuring all signatures are generated under a single valid pseudonym at any time) can be a general remedy to the problem [24].

On that front, we advance the state-of-the-art (enhancing our earlier work for a *multi-domain* VPKI [25, 26]) with a more complete system[3]. Our protocols and their novel features render the VPKI more robust to misbehaving vehicles. In particular, even in a future environment with a multiplicity of Long Term Certification Authority (LTCA) and Pseudonym Certification Authority (PCA) servers, it is impossible for a compromised vehicle to obtain multiple credentials valid simultaneously (i.e., set the ground for Sybil-based [9] misbehavior), and thus harm the Vehicular Communication (VC) operations. Moreover, we propose a generic pseudonym lifetime determination approach to enhance message unlinkability, thus user privacy.

So far, it has been assumed (often implicitly) that the VPKI servers are fully trustworthy. Nonetheless, the prospect of having multiple such servers commercially deployed (in diverse environments under different regulations), makes this assumption less realistic. In fact, one cannot preclude servers that are *honest*, i.e., follow specified protocols and protect their private keys, but they may be *curious*, i.e., tempted to trace clients (vehicles) if given the opportunity. For example, to offer customized services or optimize own operations. The experience from other mobile applications and location-based services hints this is a realistic threat to user privacy. To address this challenge, we extend our adversary model by considering *honest-but-curious* servers and design our VPKI to be resilient against such behaviors.

[2] Unlike the PRESERVE system, SCMS allows multiple simultaneously valid pseudonyms held by the vehicle, thus not being concerned with Sybil-based misbehavior.

[3] The linking of the pseudonym request (and thus long-term identity) to a specific PCA and the request timing (and thus an easy to guess set of pseudonyms and signed messages) is possible for VeSPA.

Last but not least, very few works provided detailed experimental validation of their VPKI designs to show the performance and availability of their systems. Towards that, we develop a *standard-compliant* full-fledged, refined, cross-platform VPKI and present an extensive experimental evaluation. Using the similar setup as in the literature, to have a meaningful and direct comparison, we find that our system achieves very significant improvement over prior art. With contributions on these three dimensions, we advance towards a more robust and scalable concrete VPKI system.

Overall, we seek to improve the protection achieved by strengthening the robustness of the VPKI to adversarial attacks, notably in the light of a multi-domain setup. Moreover, we seek to improve the VPKI in rendering it more resilient to *honest-but-curious* servers. The motivation for the latter stems from experience in other areas of mobile computing: service providers tend to amass information in an attempt to profile clients. Although recent VPKI proposals separate duties among servers, no design explicitly sought to prevent such tracking. Compounding these issues, we wish to maintain standard-compliant functionalities, but at the same time protect privacy. Results of this work have been published in [27].

4 Reactive Security Mechanisms

The objective of reactive security in the context of PRESERVE is to detect misbehavior in vehicular ad hoc networks and to identify the responsible attackers or faulty nodes in order to exclude them from active network participation. Vehicles and roadside units use wireless ad hoc communication in VANETs to increase traffic safety and efficiency by exchanging cooperative awareness information and event-based messages. Considering both presence and status of vehicles moving in a defined range drivers can be notified instantly about upcoming potentially dangerous situations such as a sudden braking action of a vehicle driving in front or the tail end of a traffic jam ahead. VANET nodes frequently broadcast mobility-related information (i.e. absolute values for position, time, heading, and speed) within a communication range of several hundred meters to establish a cooperative awareness of single-hop neighbors. Due to the ad hoc communication between network nodes traffic safety applications become feasible that have low latency requirements. This new kind of communication is therefore target of attackers who try to misuse the system and get an advantage at the expense of other network nodes.

The protection against external attackers in VANETs is provided by applying cryptographic methods. Only registered nodes of the VANET are equipped with valid keys that are certified by a trusted certificate authority. Internal attackers who possess appropriate hardware, software, and valid certificates must be considered as a dangerous threat. Attackers who either extract valid keys and certificates from a communication unit or install a malware on VANET devices on board of vehicles or on roadside units are able to send bogus messages that are accepted by unsuspecting vehicles. We demonstrate in [28] that the processing of fake information may affect the safety and efficiency of the overall traffic in the attackers' single or multi-hop communication range.

Most existing solutions in the context of misbehavior detection in VANETs are based on data-centric plausibility and consistency checks. We propose in [28] new methods and frameworks to evaluate the behavior of VANET nodes based on cooperatively exchanged location-related information. Since privacy protection plays an essential role in VANETs, the design of a mechanism for long-term attacker identification has to consider different privacy preserving requirements. In order to protect the driver privacy, vehicles use temporary pseudonymous identifiers in the wireless ad hoc communication that are changed randomly. This privacy protection mechanism aims to hinder internal and external attackers to create long-term traces and traffic profiles based on recorded communication traffic. In the same way, single central entities should not be able to link pseudonymous identifiers to long-term vehicle identifiers. A credential provider, for example, should not be able to link on its own pseudonymous identifiers from wireless communications to a number plate or a vehicle identification number. Likewise, the measures for misbehavior detection and attacker identification must not weaken the driver privacy.

Figure 4.1 shows our proposed general strategy for misbehavior detection and long-term attacker identification in VANETs as detailed in [28]. The attacker vehicle A and the be-

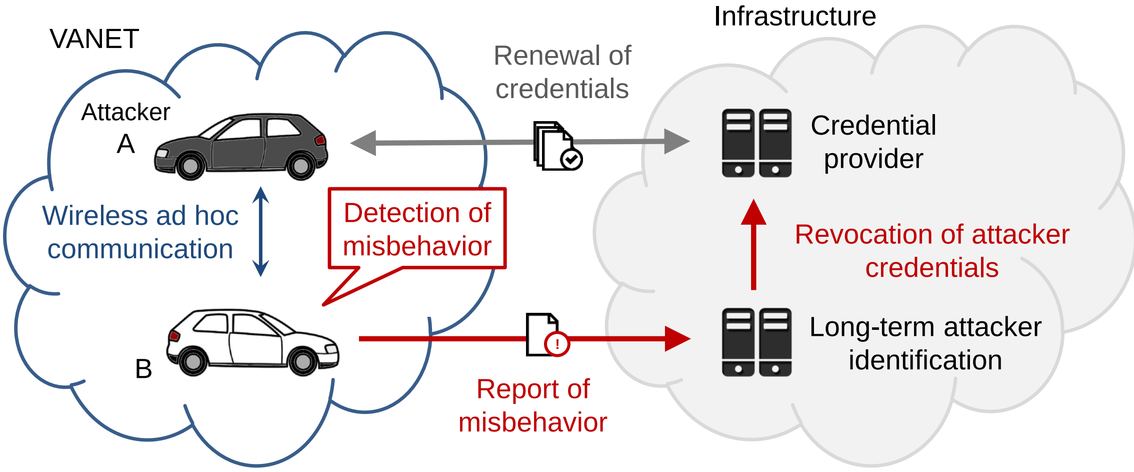

Figure 4.1: Strategy for misbehavior detection and attacker identification in VANETs

nign vehicle B communicate through a VANET using cryptographic credentials such as asymmetric keys and certificates that ensure the authentication and authorization of the sender as well as the message integrity. After a while, vehicle B detects a potential misbehavior of vehicle A based on mobility data consistency and plausibility checks. As soon as the suspicion is substantiated vehicle B reports the misbehavior to the infrastructure for attacker identification. It has to be considered that vehicles can frequently change their pseudonymous identifiers in order to preserve drivers' privacy. Therefore, it may be necessary to involve the credential provider such as a public key infrastructure (PKI) in order to identify the source of misbehavior. After the identification of the attacker, the credential provider revokes the attacker's credentials or rejects certificate renewal requests originating from the identified attacker. The disturbing network nodes should be prevented to actively participate in VANET communications until their correct behavior can be ensured. Furthermore, it has to be ensured in this process that attackers are not able to discredit benign nodes with faked misbehavior reports. We developed a novel strategy that follows the strategy shown in Figure 4.1. It consists of three main contributions: local misbehavior detection, local short-term identification of potential attackers, and central long-term identification of attackers.

The concept for *local misbehavior detection on VANET nodes* is based on different information sources such as received packets or sensor measurements to perform data consistency and data plausibility checks. In case of detected inconsistencies or implausible movement characteristics the suspicious node is observed and its trustworthiness is locally evaluated.

The contributions for *local short-term identification of potential attackers* consider explicitly the frequent change of neighbor node identifiers as stipulated by European standards and international industrial regulations. Based on test results gained from a simulations and experiments with test vehicles a concept for the local misbehavior evaluation of neighbor nodes is proposed. The resulting node trustworthiness is further used to generate misbehavior reports that are transmitted to a central evaluation authority. Consequently, the central authority is informed about suspicious nodes and hence potential attackers of the VANET.

The third main contribution is the processing of misbehavior reports for *central long-term identification of attackers*. If sufficient evidence is reported by a significant number of independent VANET nodes the central misbehavior evaluation authority is authorized to request information whether different pseudonymous IDs contained in related misbehavior reports belong to the same suspicious node. This process is supported by the central certificate authorities which ensure the consideration of drivers' privacy while processing critical information. After the assessment of the reported suspects the central misbehavior evaluation authority is able to identify the attacker and exclude his or her from active participation in any VANET communication.

Based on the knowledge gained from our practical experiments with test vehicles we developed an effective concept to enable the secure and reliable long-term operation of VANETs. Attackers and faulty nodes can reactively be excluded from the network after independent network nodes have locally detected their misbehavior and a central authority has identified the offenders. This approach is more effective in terms of long-term attacker exclusion and minimization of false-positive detections compared to related approaches that are only deployed on VANET nodes. Consequently, the proposed concept will help to minimize the motivation of potential attackers to aim on VANETs. Due to the detection of abnormal node behavior even novel attack methods that may emerge in the future should be effectively counteracted by applying these concepts.

Beyond the work presented in [28], PRESERVE partners have addressed various aspect of misbehavior detection. In [29] we discuss open research issues in MBD with a special emphasis on generic frameworks that allow flexible and dynamic combination of different detection mechanisms.

First ideas towards such a framework are presented in [30] where we use subjective logic as the basis for combining results from different detection mechanisms. Finally, [31] reports our results on how to exploit redundancy in multi-hop C2X protocols in order to identify and filter out incorrect information. The paper puts a special emphasis to aggregation protocols but also addresses various other V2X information dissemination protocols.

5 Smartphone-based Traffic Information Systems

Traffic congestion deteriorates the quality of life of citizens and contributes significantly to environmental pollution and economic loss. Traffic Information Systems (TISs) aim at solving this problem by collecting traffic data and providing drivers with location-specific information (e.g., traffic estimates). The increasing smartphone penetration, along with the wide coverage of cellular networks, defines an unprecedented large-scale network of sensors (with extensive spatial coverage) able to serve as traffic probes for TISs.

To unleash the benefits of smartphone-based TISs, users must participate in large numbers. Ideally, anyone possessing a smartphone should contribute to the TIS. Nevertheless, this very openness of such systems renders them vulnerable to adversaries and malicious users. It is thus necessary to secure the collection of data and render the contributing users (smartphones) accountable. This is a task that cannot be achieved only by relying on the security of the mobile-to-cellular infrastructure communication.

At the same time, as TISs require fine-grained location information, the privacy of the contributing participants must be protected. Smartphones already reveal a great deal of, possibly sensitive, information to the cellular operators (e.g., user identity, coarse grained location and calling/messaging actions among others).

These points define a challenging trade-off; although users should be able to participate in the system in an anonymous manner, they should be held, at the same time, fully accountable of their actions. Furthermore, the introduction of security and privacy-protection mechanisms should neither deplete the user platform resources (i.e., computation resources, battery and bandwidth) nor should it come at the expense of the TIS's efficiency and accuracy. This sets the challenge ahead: *Can we leverage smartphones and build efficient, secure, privacy-preserving TISs of unprecedented spatial coverage?*

More specifically, the system should satisfy the following security and privacy requirements in the presence of both *external* (i.e., unauthorized entities that try to harm the system operation) and *internal* (i.e., user devices or TIS entities that exhibit malicious behavior) adversaries:

- **Authentication & Authorization**: Only authorized devices shall be able to submit traffic reports or retrieve traffic status updates from the TIS.
- **Anonymity**: Transactions should be performed in a privacy-preserving manner. More specifically, the TIS should receive guarantees for the eligibility of the device with respect to the TIS service. No information concerning the real identity of the

device, and consequently of the subscriber, should leak. Moreover, traffic reports should not be traced back to devices.

- **Report Unlinkability**: Ideally, the TIS should not be able to link reports originating from the same device. However, inference techniques can (with some probability) link anonymous reports from the same device [9]. To this end, the TIS system should render such inference attacks hard.
- **Confidentiality/Integrity**: The confidentiality/integrity of the communications between the system entities (i.e. infrastructure and smartphones) should be ensured.
- **Accountability**: User devices should be held liable for actions disrupting the system operation. The system should provide the necessary means for the identification (de-anonymization) and the eviction of faulty devices. After their eviction (revocation of their credentials), offending devices should no longer be able to participate .

For the infrastructure components we consider *honest-but-curious* system entities that correctly execute protocols but try to harm the privacy of users, possibly using inference and filtering techniques to reconstruct the whereabouts of vehicles.

For our system detailed in [32], we employ the architecture, first presented in [10], based on the Generic Bootstrapping Architecture (GBA) proposed by the 3GPP consortium. When the user launches our mobile application, the device initiates the authentication process with the GBA gateway. If this process is successful, the mobile device gets authorized by the Group Signature Center (GSC) and it receives anonymous credentials to protect its privacy. Then, the device can participate in the traffic estimation process by submitting or requesting information.

Our goal is to provide authentication while ensuring unlinkability and anonymity of traffic reports. An honest-but-curious TIS server, or an outsider getting access to the accumulated data, should not be able to map location information to users. Moreover, the mobile operator, which administers the GBA gateway and has access to the user identities, should not be able to retrieve their fine-grained location data.

Our results confirm it is feasible to build accurate and trustworthy smartphone-based TIS. Nevertheless, there are still challenges ahead: security and privacy cannot, alone, incentivize users to participate in large numbers. Towards this, it is interesting to provide fair and privacy-preserving incentive mechanisms.

6 Contributions to other research topics

In 2014, PRESERVE partners also made scientific contributions in a number of other research topics. This includes especially privacy protection for ITS.

In [33], we have published an extensive survey on pseudonym mechanisms for V2X and cooperative ITS. The paper (currently in pre-print) was already provided to various stakeholders (incl. C2C-CC and HTG#6) and proved a valuable source as such a comprehensive overview on research results and standardization efforts in this area was missing. Such surveys are of especial value for the harmonization activities as often HTG members are not familiar with the research results that researchers world-wide have created in the past.

A similar survey was created on the topic of in-network aggregation in vehicular communication systems [34]. Both surveys have been published at one of the most high-impact journals in our field, IEEE Communications Surveys and Tutorials. A third survey on the topic of misbehavior detection for vehicular communication is currently under preparation.

In [35], we have revisited the assumptions of privacy requirements in V2X. We especially highlight the fact that unlinkability protection against a local attacker may be next to impossible to achieve and that current pseudonyms do not really protect against such attacks. We also discuss that such a protection may not really be necessary, as a all-seeing local attacker may not really be realistic. Instead, we propose to focus on more relevant attacker models and on strong anonymity guarantees from pseudonym protocols. Similar considerations are presented in [36].

Those thoughts are taken up in [37] where we design a pseudonym scheme that is compatible with current V2X protocols and standards and at the same time deliberately provides full anonymity against any malicious entity that wants to breach privacy. So it can be considered the most far-reaching privacy protection mechanism for V2X proposed so far. This includes protection against law-enforcement and other authorities who have no means to identify vehicles based on pseudonymously signed messages.

A drawback is that revocation (which requires linking of pseudonyms) is only possible with the cooperation of the legitimate owner of a vehicle (which may happen if a vehicle is stolen or an OBU is compromised by an attacker). This proof-of-concept work highlights the full-spectrum of privacy choices available in V2X.

7 Conclusion

With this deliverable, we conclude the work on deployment issues (Work Package 5) of PRESERVE. As presented in deliverables 5.1 to 5.4, WP5 has covered a broad range of topics related to open challenges in deployment and research of V2X security and privacy. In this conclusion, we will summary major lines of works and their achievements in WP5 throughout the full duration of PRESERVE.

WP5 work started with D5.1 which presented Y1 work focused on privacy protection as well as architectural, life-cycle, and management aspects. A major part of this deliverable discusses privacy protection in V2X via pseudonyms. This discussion was later extended to a comprehensive survey on privacy protection and pseudonyms that was published in 2015 in IEEE Communications Surveys and Tutorials [33] and made our results accessible to a broad community. It is the first paper to discuss pseudonym use in such extent. Together with our research presented throughout PRESERVE, we can consider the use of pseudonyms as a privacy protection method the de-facto standard that every IVC standard should build upon and integrate. Research provides a broad variety of options to implement regarding pseudonym resolution, pseudonym revocation, and pseudonym change. Final decisions on implementation have now to be taken in standards and by implementers.

D5.1 also presented substantial work on many other topics, for example, it discusses architectural considerations regarding position of the security layer in the protocol stack. It can now be said, that our proposed solution (network layer instead of facilities or application layer) is fully in-line with the proposed approach from ETSI which emerged after intensive discussions with both Car2Car-CC and ETSI WG5.

D5.2 then focused deeper on life-cycle management and initial cost model for our ASIC development on the deployment side. Regarding security life-cycle management, it provided detailed descriptions of processes and interfaces for V2X PKI operation in-line with developments in C2C-CC and ETSI and provides (together with respective WP1 and WP2 deliverables) a thorough treatment of that topic that is helpful to everyone implementing or setting a V2X PKI.

D5.2 also introduced our effort on broadening awareness of the PRESERVE platform and also soliciting industry requirements by running a survey. This survey was evaluated and results described in later WP5 deliverables. Likewise, the cost model for ASIC development was also a first step towards later results.

Another focus in D5.2 were misbehavior detection schemes both inside vehicles and in central entities. This topic is continued in D5.3 and substantially provided more research results in this area. Misbehavior detection (MBD) can be considered the third fundamental pillar of V2X security (besides ID management/message integrity and privacy protection using pseudonyms) and can be considered the least mature. Therefore, the substantial amount of research on MBD in PRESERVE constitutes a highly relevant effort that advanced the state of the art towards a point where later efforts can derive concrete system descriptions for standardization and implementation.

At the end of year 3, D5.3 presented results from our survey that investigated requirements and awareness of ITS security solutions. As project, we needed to realize that the survey approach did not solicit feedback in a mass number as initially hoped for when starting this activity, therefore, results described in D5.3 and later updated in D5.4 are of a more qualitative than quantitative nature.

D5.3 also provided substantial additional results on misbehavior detection by presenting a framework to integrate outputs from different singular detection mechanisms that were described earlier. By this integration, we can increase the accuracy of MBD and cover broader sets of scenarios. Another major contribution in D5.3 is the presentation of test results of one of the first real-world studies of MBD in driving experiments.

D5.3 continued with major sections on identify management proposing new directions for vehicular PKI design and pseudonym management and security architecture taking up results from our V2X architecture workshop.

With this deliverable, we concluded D5.4 work by discussing multiple issues related to deployment of PRESERVE. This includes initial investigations of business models for different economic activities in the field of V2X security, final survey results and a discussion on the ASIC cost model.

The second major topic covered is the scalability of secure communication, especially with respect to certificate omission. While this was addressed in various earlier WP5 deliverables, we were now able to provide concluding notes in this regards.

Summarizing the work conducted in PRESERVE, its members contributed during its conduction to a total of so far 47 peer-reviewed publications related to V2X security and privacy and has thus evidently provided a vast body of input and material to the advancement of our field. WP5 provided overviews and new contributions to all major areas of V2X security: 1.) ID management/integrity protection, 2.) privacy protection and pseudonym management, and 3.) misbehavior detection. As a practically oriented project, we not only looked at the pure technical aspects of these topics, but also considered industry-relevant aspects like life-cycle management, cost issues, and business opportunities despite the project's partners being exclusively being composed of technical experts. We therefore hope that the results will be taken up and refined by other experts in the respective fields when finally rolling out V2X communication.

Bibliography

[1] EU-US ITS Intergovernmental Standards Harmonization Working Group, “Public key infrastructure (PKI) architecture analysis and recommendations for harmonization,” EU-US ITS Task Force, Tech. Rep., 2014.

[2] P. Papadimitratos, “ "On the Road" - reflections on the security of vehicular communication systems,” *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*, pp. 359–363, sept. 2008.

[3] “Intelligent Transport Systems (ITS), Vehicular Communications (VC), Basic Set of Applications, Definitions,” ETSI TR 102 638 V1.1, Tech. Rep., Jun. 2009.

[4] H. Zhu, R. Lu, X. Shen, and X. Lin, “Security in service-oriented vehicular networks,” *IEEE Wireless Communications*, vol. 16, no. 4, pp. 16–22, Aug. 2009.

[5] S. Mollman, “From Cars to TVs, Apps are Spreading to the Real World,” Oct. 2009. [Online]. Available: http://www.cnn.com/2009/TECH/10/08/apps.realworld/

[6] A. Goodwin, “Ford Unveils Open-Source Sync Developer Platform,” Oct. 2009. [Online]. Available: http://reviews.cnet.com/8301-13746_7-10385619-48.html

[7] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, “SEROSA: SERvice Oriented Security Architecture for Vehicular Communications,” in *proceedings of the IEEE Vehicular Networking Conference (VNC)*, Dec. 2013.

[8] “Car2car communication consortium manifesto,” http://www.car-2-car.org/.

[9] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “Securing Vehicular Communications - Assumptions, Requirements, and Principles.” in *Proceedings of 4th Workshop on Embedded Security in Cars (ESCAR)*, Berlin, Germany, 2006, pp. 5–14.

[10] V. Manolopoulos, P. Papadimitratos, T. Sha, and A. Rusu, “Securing smartphone based its,” in *11th International Conference on ITS Telecommunications (ITST)*, August 2011, pp. 201–206.

[11] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, “Secure and privacy-preserving smartphone-based traffic information systems,” 2014.

[12] B. Lonc and C. Jouvray, “Specification of pseudonym certificates update protocols (ota),” PRESERVE, Tech. Rep., 2014.

[13] ETSI - European Telecommunications Standards Institute, “Intelligent transport systems (ITS); security; trust and privacy management,” ETSI, Technical Report TR 102 941, June 2012.

[14] ——, “Intelligent transport systems (ITS); security; security header and certificate formats,” ETSI, Technical Report TR 103 097, April 2013.

[15] M. P. Feiri, J. Y. Petit, and F. Kargl, “Congestion-based certificate omission in vanets,” in *Ninth ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2012, Low Wood Bay, Lake District, United Kingdom*. New York: ACM, June 2012, pp. 135–138.

[16] ——, “Evaluation of Congestion-based Certificate Omission in VANETs,” in *Vehicular Networking Conference*. IEEE, 2012, pp. 101–108.

[17] M. Feiri, J. Petit, R. K. Schmidt, and F. Kargl, “The impact of security on cooperative awareness in VANET,” in *Fifth IEEE Vehicular Networking Conference (VNC ’13)*, December 2013, pp. 127–134.

[18] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “On the performance of secure vehicular communication systems,” *Dependable and Secure Computing, IEEE Transactions on*, vol. 8, no. 6, pp. 898–912, 2011.

[19] E. Schoch and F. Kargl, “On the efficiency of secure beaconing in vanets,” in *Proceedings of the third ACM conference on Wireless network security*, ser. WiSec ’10. New York, NY, USA: ACM, 2010, pp. 111–116. [Online]. Available: http://doi.acm.org/10.1145/1741866.1741885

[20] 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. [Online]. Available: http://www.vehicularlab.uni.lu/wp-content/uploads/2014/03/Proceedings_FG_IVC_2014.pdf

[21] R. Kroh, A. Kung, and F. Kargl, “SEVECOM (D1.1) VANETs Security Requirements Final Version,” 2006. [Online]. Available: http://www.sevecom.org

[22] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A security credential management system for V2V communications,” in *2013 IEEE Vehicular Networking Conference, Boston, MA, USA, December 16-18*, 2013.

[23] S. Gisdakis, M. Lagana, T. Giannetsos, and P. Papadimitratos, “SEROSA: service oriented security architecture for vehicular communications,” in *2013 IEEE Vehicular Networking Conference, Boston, MA, USA, December 16-18*, 2013.

[24] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, “Architecture for secure and private vehicular communications,” in *In Proceedings of the 7th International Conference on ITS Telecommunications*, Sophia Antipolis, France, June 2007.

[25] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, “VeSPA: Vehicular Security and Privacy-preserving Architecture,” in *ACM Workshop on Hot Topics on Wireless Network Security and Privacy (ACM HotWiSec)*, Budapest, Hungary, Apr. 2013.

[26] N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos, "Towards a secure and privacy-preserving multi-service vehicular architecture," in *proocedings of the 4th International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN)*, Madrid, Spain, Jun. 2013.

[27] 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.

[28] N. Bißmeyer, "Misbehavior detection and attacker identification in vehicular ad hoc networks," Ph.D. dissertation, Technical University Darmstadt, November 2014.

[29] 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. [Online]. Available: http://www.vehicularlab.uni.lu/wp-content/uploads/2014/03/Proceedings_FG_IVC_2014.pdf

[30] 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.

[31] 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 (VNC 2014)*. Paderborn, Germany: IEEE, December 2014.

[32] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Secure and privacy-preserving smartphone-based traffic information systems - to be published," *IEEE Transactions on Intelligent Transportation Systems*, 2015.

[33] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. PP, no. 99, pp. 1–1, 2014. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6873216

[34] 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. [Online]. Available: http://dx.doi.org/10.1109/COMST.2014.2320091

[35] 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. [Online]. Available: http://www.vehicularlab.uni.lu/wp-content/uploads/2014/03/Proceedings_FG_IVC_2014.pdf

[36] 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.

[37] 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.