



# 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:** 1.0  
**Confidentiality:** Public  
**Editor:** N. Bißmeyer  
**Cont. Authors:** N. Bißmeyer, M. Feiri, A. Giannetsos, F. Kargl, B. Lonc, M. Moser, M. Khodaei  
**Date:** 2015-01-10



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)	A Formal 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. Link to publication (dissertation)
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
v1.0	2014-01-10	F. Kargl (UT), N. Bißmeyer (FhG SIT)	Finalizing integrating partner comments.

## Approval

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

## Circulation

Recipient	Date of submission
Project Partners	2015-01-21
European Commission	2015-01-21

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Deployment of PRESERVE</b>	<b>6</b>
2.1	Plans for Deployment of VSS . . . . .	6
2.1.1	Availability . . . . .	6
2.1.2	Plans for Deployments in European and National Projects . . . . .	6
2.1.3	Plans with Hitachi . . . . .	7
2.1.4	Plans with ETSI . . . . .	7
2.1.5	Participations to the EIP Smart Cities and Communities (EIP-SCC) . . . . .	7
2.2	PKI Structure and Business Model . . . . .	8
2.2.1	World-wide Vehicular PKI Harmonization . . . . .	8
2.2.2	Security for Service-Oriented Vehicular Networks . . . . .	10
2.3	ASIC Cost Model . . . . .	11
2.3.1	Performance . . . . .	11
2.3.2	Relative costs . . . . .	12
2.4	Validation and Certification . . . . .	14
2.5	Pseudonym Certificate Signing Request . . . . .	16
<b>3</b>	<b>Scalability of secure communication</b>	<b>18</b>
3.1	A Formal Model for Certificate Omission . . . . .	18
3.2	Certificate Pre-Distribution . . . . .	19
3.3	Towards Deploying a Scalable & Robust VPKI . . . . .	21
<b>4</b>	<b>Reactive Security Mechanisms</b>	<b>23</b>
<b>5</b>	<b>Smartphone-based Traffic Information Systems</b>	<b>26</b>
<b>6</b>	<b>Contributions to other research topics</b>	<b>28</b>
<b>7</b>	<b>Conclusion</b>	<b>29</b>

# List of Figures

2.1	CCMS components . . . . .	9
2.2	Overview of the proposed trust assurance levels (Source: internal C2C-CC report on Trust Assurance Levels) . . . . .	15
2.3	Communication stacks between vehicle and PCA if V2I communications based on IPV6 over GeoNetworking protocol . . . . .	16
2.4	Communication stacks between vehicle and PCA if V2I communications based on GeoNetworking protocol . . . . .	17
3.1	Awareness quality without and with temporal pre-distribution . . . . .	20
4.1	Strategy for misbehavior detection and attacker identification in VANETs . .	24

# List of Tables

2.1	ASIC performance estimation . . . . .	12
2.2	ASIC cost model . . . . .	13

# 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
<b>LTC</b>		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.
<b>LTCA</b>		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.
<b>MPCUP</b>		Media Independent Pseudonym Certificate Protocol	A protocol that allows vehicles equipped with different communication technologies to obtain certificates of their pseudonym keys.
<b>OEM</b>		Original Equipment Manufacturer	Refers to an generic car manufacturer
<b>OBU</b>	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)
<b>PC</b>	Short Term Certificate	Pseudonym Certificate	A short term certificate authenticates stations in G5A communication and contains data reduced to a minimum.
<b>PCA</b>		Pseudonym Certificate Authority	Certificate authority entity in the PKI that issues pseudonym certificates
<b>PKI</b>		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.
<b>PP</b>		Protection Profile	
<b>RA</b>		Resolution Authority	Entity within the SCMS or PKI to resolve pseudonymous IDs and certificates if necessary.
<b>RSU</b>	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
<b>SCMS</b>	PKI	Security Credential Management System	A security credential management system generates and handles digital credentials such as keys and certificates. A SCMS could be a PKI with additional functionalities.
<b>SPCURO</b>		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.
<b>TAL</b>		Trust Assurance Level	
<b>V2I</b>	C2I	Vehicle-to-Infrastructure	Direct vehicle to roadside infrastructure communication using a wireless local area network
<b>V2V</b>	C2C	Vehicle-to-Vehicle	Direct vehicle(s) to vehicle(s) communication using a wireless local area network
<b>V2X</b>	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
<b>VSS</b>		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 2.3 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 2.4, 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 2.5. 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 aim 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 2.3.

#### 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 planned 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) where 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 [?]. 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

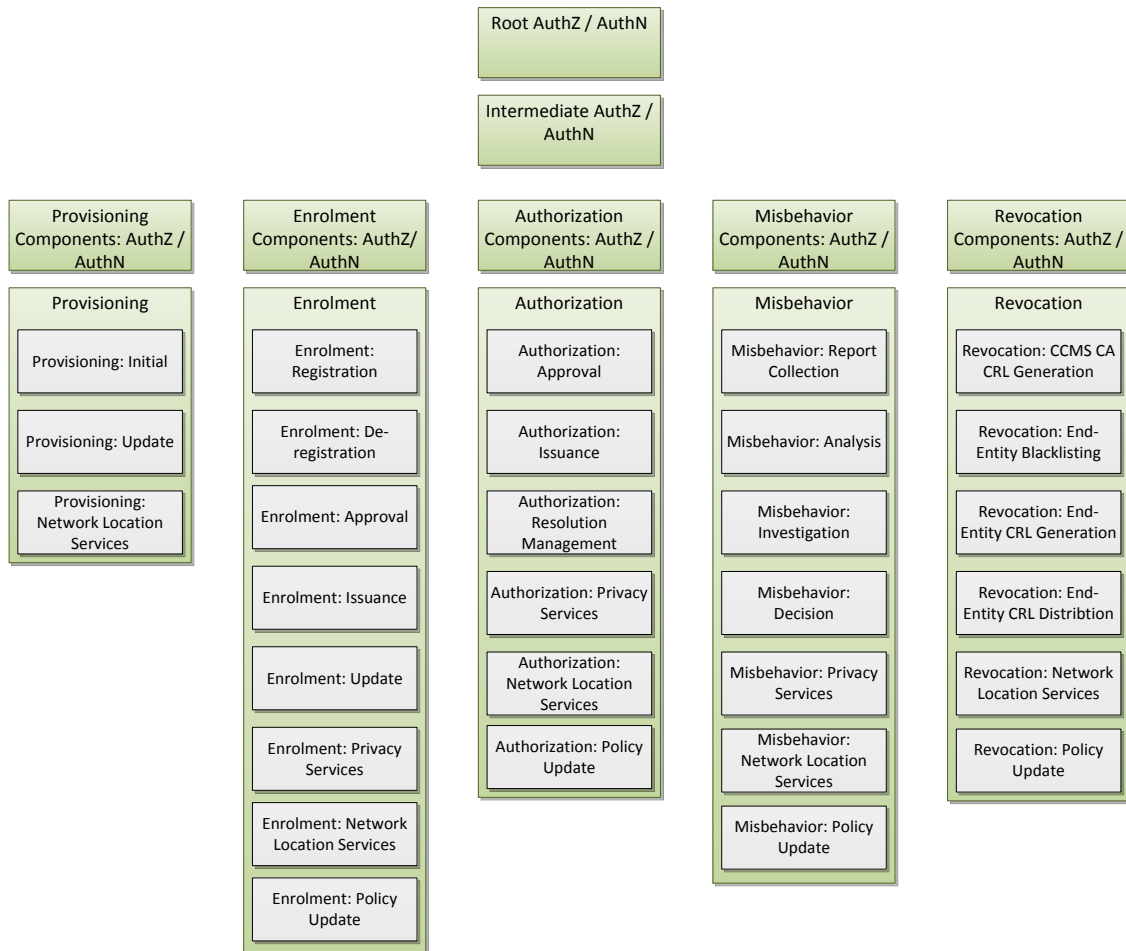


Figure 2.1: CCMS components

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 [?] 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 these 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 [?] 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 [?] and content distribution [?] to Internet access and the development of an “Application Store for automotive applications” [?, ?]. 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<sup>1</sup>. 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) [?].

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

<sup>1</sup> 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 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.

### 2.3.1 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

### 2.3.2 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 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 2.2):

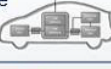




Trust Ass. Level (TAL)	Requirements			Implications		
	Minimum Target of Evaluation (TOE)	Minimum Evaluation Assurance Level (EAL)	Minimum (Hardware) Security Functionality	Prevented (Internal) Attacker acc. to CC	Potential Security Implications	C2X Use Case Examples
0	None 	None	None	None	Not reliable 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
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 2.2: Overview of the proposed trust assurance levels (Source: internal C2C-CC report on Trust Assurance Levels)

- **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.

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 Löhner (Bosch, C2C-CC) who has provided contributions to this section.

## 2.5 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 perform certificate acquisition process for practical ITS. The protocols designed in [?] 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 [?] 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.

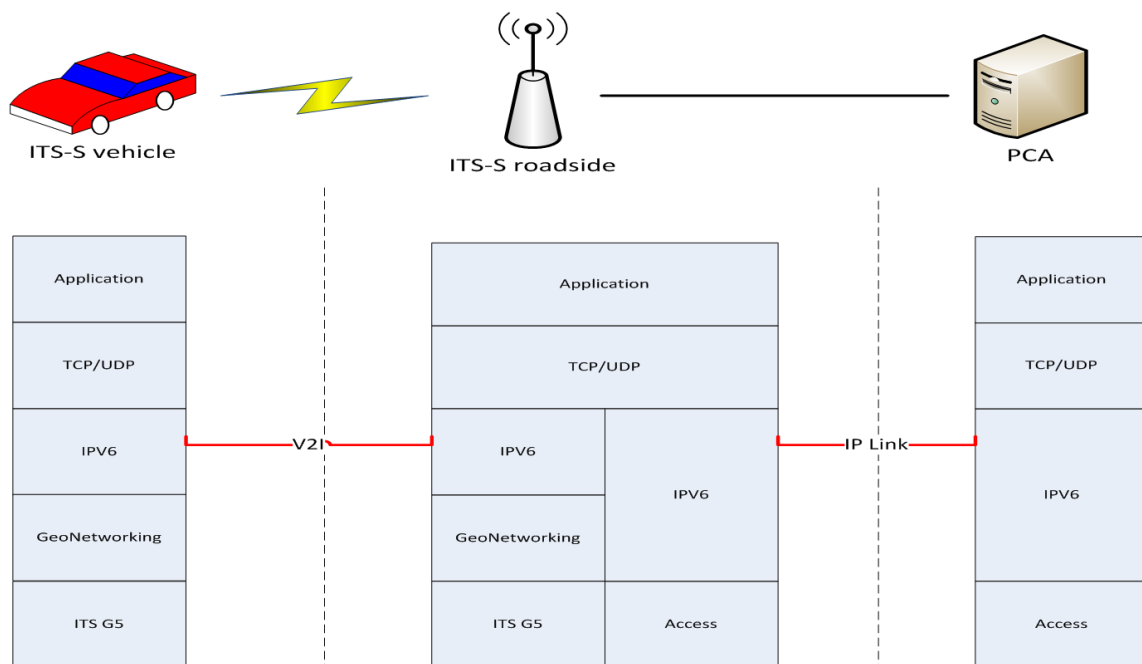


Figure 2.3: Communication stacks between vehicle and PCA if V2I communications based on IPV6 over GeoNetworking protocol

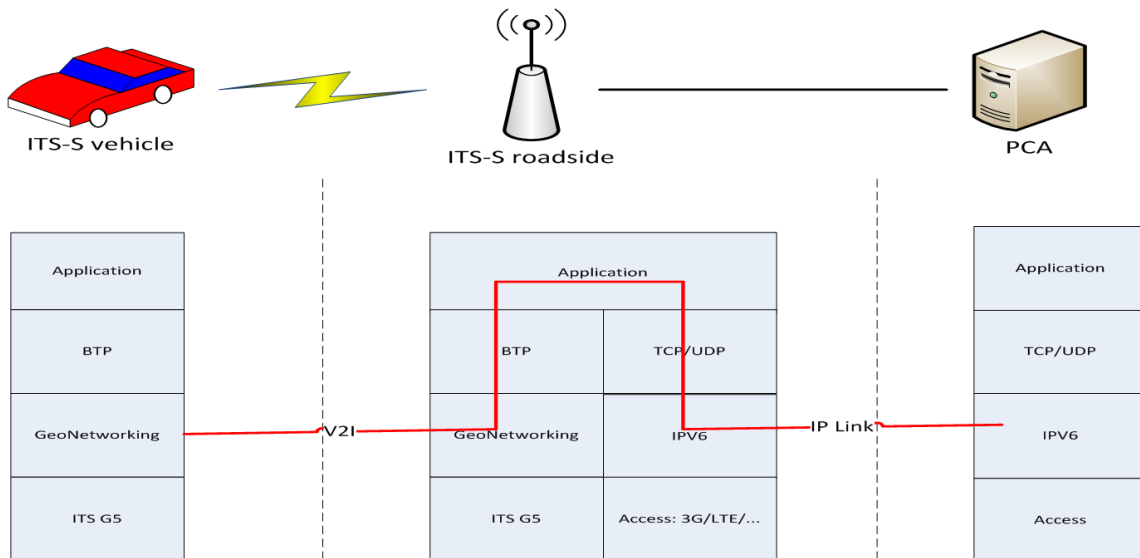


Figure 2.4: Communication stacks between vehicle and PCA if V2I communications based on GeoNetworking protocol

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.

A detailed description of the proposed protocols MPCUP and SPCURO is given in [?]. 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 [?]. 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 [?]. Benefits of the certificate omission schemes described below were proven by simulation in [?, ?, ?].

- No omission of certificates (NoOm): This scheme serves as a baseline as it performs no omission.
- Periodic omission of certificates (POoC) [?]: The idea of POoC is to add the certificate every  $n$  beacons.<sup>1</sup> Certificate periods of 3 seconds and 10 seconds are often considered.
- Neighbor-based certificate omission (NbCO) [?]: 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) [?]: 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.

---

<sup>1</sup>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 formula for the likelihood successful packet reception from a new neighboring vehicle.

$$(1 - ((1 - D_s(d) * c)^n)) * D_s(d) \quad (3.1)$$

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 [?]. 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 [?] 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



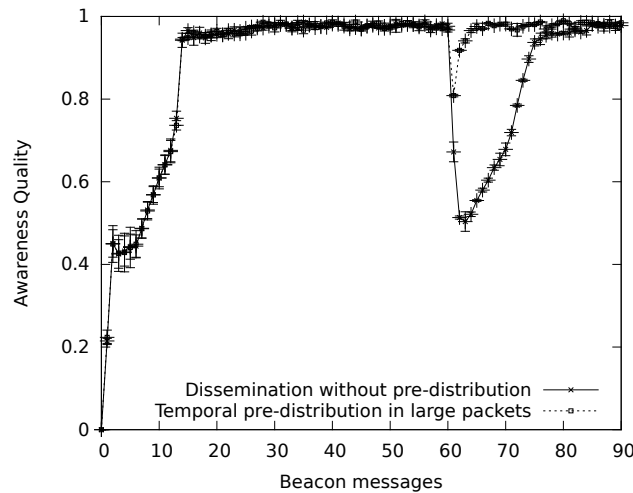


Figure 3.1: Awareness quality without and with temporal pre-distribution

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 [?], 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 [?] requires that the identity provider forwards requests to PCAs, thus being prone to the same inference<sup>2</sup>.

SEROSA [?] 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 [?].

On that front, we advance the state-of-the-art (enhancing our earlier work for a *multi-domain* VPKI [?, ?]) with a more complete system<sup>3</sup>. 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.

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

<sup>3</sup>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 [?].

## 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 [?] 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 [?] 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 [?]. The attacker vehicle *A* and the benign

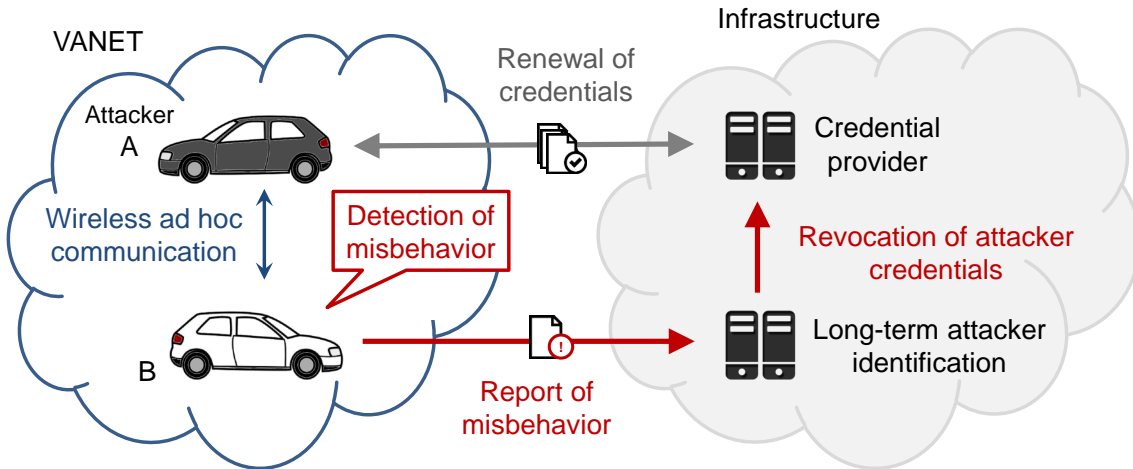


Figure 4.1: Strategy for misbehavior detection and attacker identification in VANETs

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 [?], PRESERVE partners have addressed various aspect of misbehavior detection. In [?] 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 [?] where we use subjective logic as the basis for combining results from different detection mechanisms. Finally, [?] 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 [?]. 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 [?], we employ the architecture, first presented in [?], 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 [?], 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 [?]. 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 [?], 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 [?].

Those thoughts are taken up in [?] 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 WP5 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.

This started with D5.1 presented Y1 work which focused on privacy protection as well as architectural, life-cycle, and management aspects. D5.2 then focused deeper on life-cycle management and initial cost model for our ASIC development on the deployment side. Research focus was put on misbehavior detection and initial works performance aspects. D5.3 presented results from our survey that investigated requirements and awareness of ITS security solutions. We also investigated business models for different economic activities in the field of V2X security. On the research side, misbehavior detection and identity management played a major role. We also presented results from our final architecture workshop.

We want to stress that PRESERVE 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.