PREparing SEcuRe VEhicle-to-X Communication Systems

Deliverable 1.1

Security Requirements of

Vehicle Security Architecture

Project:	PRESERVE
Project Number:	IST-269994
Deliverable:	D1.1
Title:	Security Requirements of VSA
Version:	v1.1
Confidentiality:	Confidential, will be Public
Editors:	Jan Peter Stotz (Fraunhofer SIT), Norbert Bißmeyer (Fraunhofer SIT), Frank Kargl (University of Twente), Stefan Dietzel (University of Twente), Panos Papadimitratos (KTH), Christian Schleiffer (escrypt)
Date:	June 2011

Part of the Seventh Framework Programme

Funded by the EC - DG INFSO

Document History

Version	Status	Author	Date
0.3	Initial version	Jan Peter Stotz	2011-05-17
0.6	Threats section completed	Norbert Bißmeyer	2011-06-08
0.7	Corrections from review of all partners integrated	Jan Peter Stotz	2011-06-20
0.9	Performance requirements chapter added	Frank Kargl	2011-07-01
1.0	Corrections from final review of all partners integrated and finishing	Jan Peter Stotz	2011-07-20
1.1	Feedback from review integrated	Norbert Bißmeyer	2012-05-14

Approval		
	Name	**Date**
Prepared	Jan Peter Stotz, Frank Kargl, Jonathan Petit	2011-07-22
Reviewed	PRESERVE Partners	2011-07-26
Authorised	Frank Kargl	2011-07-28

Circulation	
Recipient	**Date of submission**
Project partners	2011-07-28
European Commission	2011-07-28

Glossary and Abbreviations

Abbreviation	Synonyms	Description	Details
API		Application Programming Interface	
AU		Application Unit	Hardware unit in an ITS station running the ITS applications
ASN.1		Abstract Syntax Notation One	
CA		Certificate Authority	
CAM		Cooperative Awareness Message	CAMs are sent by vehicles multiple times a second (typically up to 10 Hz), they are broadcasted unencrypted over a single-hop and thus receivable by any receiver within range. They contain the vehicle's current position and speed, along with information such as steering wheel orientation, brake state, and vehicle length and width.
CAN		Controller Area Network	In-vehicle bus system
CCM		Communication Control Module	Module originating from the EVITA project
CCU		Communication & Control Unit	Hardware unit in an ITS station running the communication stack
CE		Consumer Electronics	Electronic devices like smartphone or MP3 player of the vehicle driver or a passenger
CL		Convergence Layer	PRESERVE module that connects the communication stack to the PRESERVE Vehicle Security Subsystem (VSS)
CPU		Central Processing Unit	
CRC		Cyclic Redundancy Code	
CRS		Cryptographic Services	Module originating from the EVITA project
DoS		Denial of Service	
DENM	DNM	Decentralized Environmental Notification Message	A DENM transmission is triggered by a cooperative road hazard warning application, providing information to other ITS stations about a specific driving environ-ment event or traffic event. The ITS station that receives the DENM is able to provide appropriate HMI information to the end user, who makes use of these information or takes actions in its driving and

			traveling. [12]
EAM		Entity Authentication Module	Module originating from the EVITA project
ECC		Elliptic Curve Cryptography	
ECU		Electronic Control Unit	
FOT		Field Operational Test	
G5A		ITS road safety communication (802.11p)	Frequency band between 5.875 GHz and 5.905 GHz - reserved for ITS road safety communication
G5B		ITS non-safety communication (802.11p)	Frequency band between 5.855 GHz and 5.875 GHz - reserved for ITS road non-safety communication
G5C	C-WLAN	5GHz WLAN communication (802.11a)	
GNSS	GPS	Global Navigation Satellite System	Generic term for an Global navigation satellite system (GPS, GLONAS, Galileo)
HMI		Human-Machine Interface	
HSM		Hardware Security Module	
HU		Head-Unit	
I2V	I2C	Infrastructure-to-Vehicle	Communication between infrastructure components like roadside units and vehicles
I2I		Infrastructure-to-Infrastructure	Communication between multiple infrastructure components like roadside units
ICS		ITS Central Station	ITS station in a central ITS sub-system
ILP		Inter Layer Proxy	Component introduced by the SeVeCom project, that captures and allows modification of messages between different layers of a communication stack
IMT	GSM, GPRS, UMTS	Public cellular services (2G, 3G, ...)	
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). [17]

ITS-S		ITS Station	Generic term for any ITS station like vehicle station, roadside unit, ...
ITMM		ID & Trust Management Module	Module originating from SeVeCom project
IVC	ITSC, ITS Commu-nications	Inter-Vehicle Communication	Combination of V2V and V2I
IVS	OBU	ITS Vehicle Station	The term "vehicle" can also be used within PRESERVE
LDM		Local Dynamic Map	Local geo-referenced database containing a V2X-relevant image of the real world
LTC		Long Term Certificate	PRESERVE realization of an ETSI Enrolment Credential
LTCA		Long Term Certificate Authority	PRESERVE realization of an ETSI Enrolment Credential Authority
MAC		Media Access Control	
OBD		On-Board Diagnosis	
OEM		Original Equipment Manufacturer	Refers to an generic car manufacturer
OBU	IVS	On-Board Unit	
PAP		Policy Administration Point	Module originating from EVITA project
PC		Pseudonym Certificate	
PCA		Pseudonym Certificate Authority	Instance that issues pseudonym certificates
PDM		Policy Decision Module	Module originating from EVITA project
PDP		Policy Decision Point	Module originating from EVITA project
PeRA		Privacy-enforcing Runtime Architecture	Module originating from Preciosa project
PEP		Policy Enforcement Point	Module originating from EVITA project
PIM		Platform Integrity Module	Module originating from EVITA project
PKI		Public Key Infrastructure	
PMM		Pseudonym Management Module	Module originating from SeVeCom project
QoS		Quality of Service	
RSU	IRS, ITS Roadside Station	Roadside Unit	
SAP		Service Access Point	
SCM		Secure Communication	Module originating from SeVeCom

		Module	project
SEP		Security Event Processor	
SSM		Secure Storage Module	Module originating from EVITA project
TCU		Telematics Control Unit	
TOC		Transportation Operation Center	
TPM		Trusted Platform Module	
UML		Unified Modeling Language	
UTC		Universal Time Coordinated	
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)	
VIN		Vehicle Identification Number	Unique serial number of a vehicle
VSA		Vehicle Security Architecture	General outcome of PRESERVE work package 1
VSS		Vehicle Security Subsystem	Close-to-market implementation of the PRESERVE VSA
WLAN		Wireless Local Area Network	
XML		Extensible Markup Language	

Table of Contents

List of Figures

List of Tables

1 Introduction

The next generation of vehicular communication systems will enable cars and other vehicles to communicate, exchanging for example data about their current position and speed and warnings derived from their on-board sensors. Additionally, roadside units will provide a communication link to central stations monitoring traffic, collecting and distributing warnings about hazardous situations and provide traffic forecasts. However, such new Intelligent Transportation System (ITS) will become crucial for traffic safety and management. Thus, there would be significant risks and attacks could cause significant damages. Hence ITS have to integrate an appropriate security system in order to resist attacks.

In recent years, a number of projects analyzed requirements towards designing various Vehicle-to-X (V2X) communication systems. More recently, in the context of the European Telecommunications Standards Institute (ETSI), work has also been performed on the same topic. At the outset of PRESERVE, we have collected documents from prior projects, notably the constituent projects of PRESERVE, covering use cases, security requirements and threat analysis as well as functional requirements that have been identified within other projects, related literature and Field Operational Tests (FOTs). This document presents a homogenized view of this literature, enriched by the knowledge and experiences from the ETSI standardization process and other automotive activities (e.g., the Car-to-Car Communication Consortium efforts).

Based on the work presented in this document PRESERVE will develop an integrated V2X Security Architecture (VSA) and demonstrate a close-to-market implementation termed V2X Security Subsystem (VSS). This VSS will provide a sophisticated security system for use in V2X communication systems that can be used in other Field Operational Test projects.

Central part of this VSS will be a Hardware Security Module (HSM) which provides extra protection to secret key material. Additionally, the HSM will be used as cryptographic execution accelerator – especially speeding-up the Elliptic Curve (EC) signature verification.

1.1 Intelligent Transportation System

The major outcome of PRESERVE – the PRESERVE Vehicular Security System (VSS) – targets integration into different Field Operational Test (FOT) projects. Therefore, it is important to identify relevant entities, communication links, communication services, and use cases for deriving the requirements, the PRESERVE Vehicular Security Architecture (VSA) has to satisfy. Due to the different environments and focus of the different FOTs addressed by PRESERVE, the VSS should consider a large subset of different system entities, communication links and services. In order to analyze the security requirements of potential PRESERVE users in a more detail manner, we identify and describe a set of use cases which are described in Section 1.2. We selected four use cases that cover the most relevant communication forms the PRESERVE architecture can be used for.

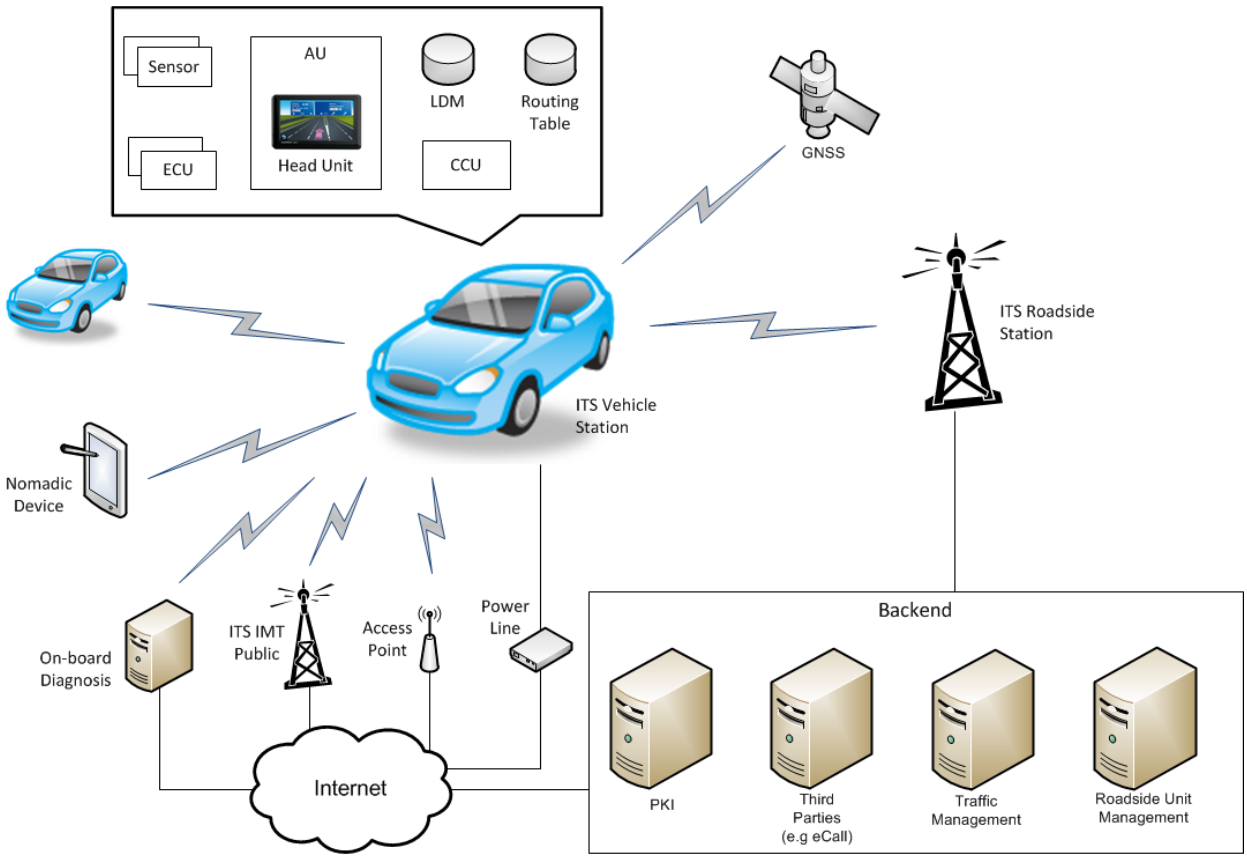

Figure 1: ITS System Overview

1.1.1 ITS Entities

The assumptions about the internal structure of an ITS and its entities is presented in this section. It is based on previous projects such as sim^{TD} [5], PRE-DRIVE [9], SEVECOM [1] and publications [17] from standardization bodies. For a recent survey, we refer the reader to [41]

1.1.1.1 ITS Vehicle Station (IVS)

- **Network layer routing table**: The routing table stores information about the location of neighboring nodes in combination with a timestamp of the node's latest update. The table entries are created based on position and time information from incoming messages. It is assumed that the geographic routing is executed on network layer of the communication stack. This also implies that the network header of the message has to contain mobility information (i.e. node ID, position, timestamp). Manipulation of the table content may cause routing attacks as wormhole or relay attacks, or possibly facilitate DoS (e.g., black- or gray-hole attacks). Such attacks could affect availability.
- **Local Dynamic Map (LDM) on facilities layer**: The LDM can be assumed to be a container that collects and manages all incoming messages. All applications running on the ITS-S can access this central storage in order to use a consistent base of data. It is assumed that this LDM is responsible for filtering duplicates or deleting outdated messages. As applications on application layer accesses this system, it is assumed that the LDM is operated on facilities layer. Manipulation of the LDM content may cause attacks related to traffic safety and traffic efficiency application.
- **Local station information on facilities layer (VIN, manufacturer, model, etc.)**: It is assumed that local station information is available and accessible to the application layer. Manipulation of this data may cause problems to the applications running at neighboring nodes. If, for example, local station dimensions at vehicle A are manipulated and subsequently broadcasted, traffic safety applications on vehicle B receiving this data

may calculate false advice, warning, or reaction. Furthermore accessing sensitive, identifying information by malicious applications can cause privacy infringements.

- **Application Unit (AU) / Head Unit (HU)**: It is assumed that the HU consists of an HMI, the navigation system and telephone applications. Additionally, it is reasonable that Consumer Electronic (CE) devices are connected to the HU. Manipulation of the HU by attacks could cause bogus advisories for the driver.
- **Communication & Control Unit (CCU)**: The CCU is a central router for different communication links such as ITS G5A/B/C and ITS IMT Public.
- **Electronic Control Unit (ECU)**: An ECU combines an on-board sensor concentrator for some components as Powertrain, Chassis & Safety or Body Electronics.
- **Sensor**: On-board sensors are controlled and managed by ECUs. Therefore, direct protection of the sensors is not considered in this document.

1.1.1.2 Roadside Unit (RSU)

A Roadside Unit consists in general of the same elements as a vehicle (see Section 1.1.1.1). The communication stack and the applications are probably very comparable with the vehicle station but the internal network may looks different. A vehicle is connected with its Powertrain, Chassis & Safety and Body Electronic whereby a RSU is connected to road sensors (e.g. induction loops, cameras) and a back-end control center.

- Network layer routing table
- Local Dynamic Map (LDM) on facilities layer
- Local station information on facilities layer (serial number, operator, …)
- Application Unit (AU)
- Communication & Control Unit (CCU)
- Electronic Control Unit (ECU) combines on-board sensor concentrator such as Powertrain, Chassis & Safety and Body Electronic
- Sensor(s)

1.1.1.3 ITS Central Station (ICS)

- Back-end systems
  - Public Key Infrastructure (PKI)
  - Traffic Management Center
  - Roadside Unit Management
  - E-call Service Center
- Third Parties (e.g. Weather information services, Parking services, …)

1.1.1.4 Nomadic Devices

Nomadic devices are stand-alone systems that can be used either in vehicles or by other traffic participants like bicyclists as a sender of regular position information and as a receiver of V2X messages. It is further assumed that such a device has no connection to the ITS-S on-board system. Here-I-Am devices would only be able to send CAMs with the current position and timestamp.

From the view point of the security, a nomadic device that is actively participating in the V2X communication may be more attractive for attackers that attempt to extract secret keys in order to use them afterwards for different attacks.

1.1.2 Communication Links

1.1.2.1 ITS G5A and ITS G5B

The ad-hoc communication between ITS-Stations via IEEE 802.11p [16] is assumed to be unstable. Frequent communication disruptions are possible due to the high mobility of ITS Vehicle Stations. The communication via G5A and G5B is reserved for ITS-S and the channel bandwidth has to be shared between all entities within communication range. Furthermore, the frequencies of G5A and G5B are reserved for traffic safety and efficiency relevant message exchange. Therefore, the protection of this communication channel has high priority in the PRESERVE VSA.

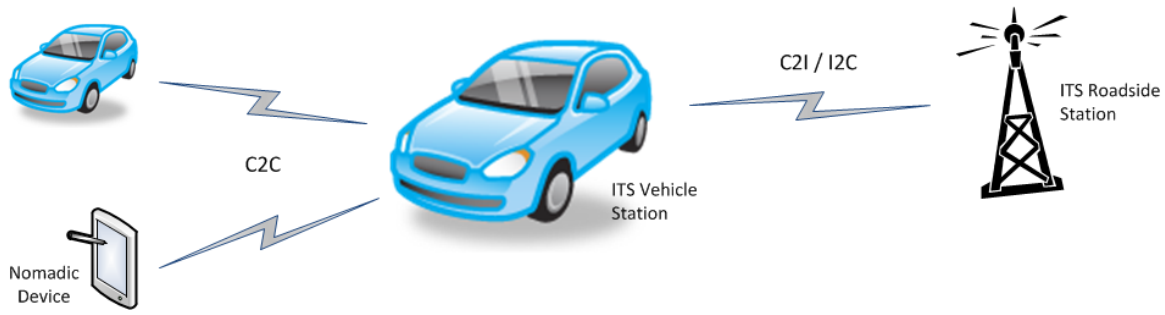

Figure 2: Communication modes and types: Car-to-car, car-to-nomadic device, Car-to-infrastructure.

The following communication links are within the scope of PRESERVE:

- **IVS** ↔ **IVS** and **IVS** ↔ **RSU**: Message exchange between vehicles is possible via broadcast or single-hop unicast. Multi-hopping is assumed to be realized by a position-based routing protocol or by store-and-forward mechanisms.
- **RSU** ↔ **RSU**: Message exchange between roadside units can be done via G5A. In most cases, it is more reasonable that an RSU is connected by a dedicated wired or wireless link to a roadside unit management center. This management center can be used in a more efficient way to exchange data between roadside units over the backend connection. Nevertheless, if mobile or moving roadside units are used, then it may be reasonable that message exchange directly between roadside units via G5A is possible. In general, we do not want to make any assumptions about density, placement, or connectivity of RSUs while at the same time we are not focusing on security of non G5A links connecting RSUs to backend systems.

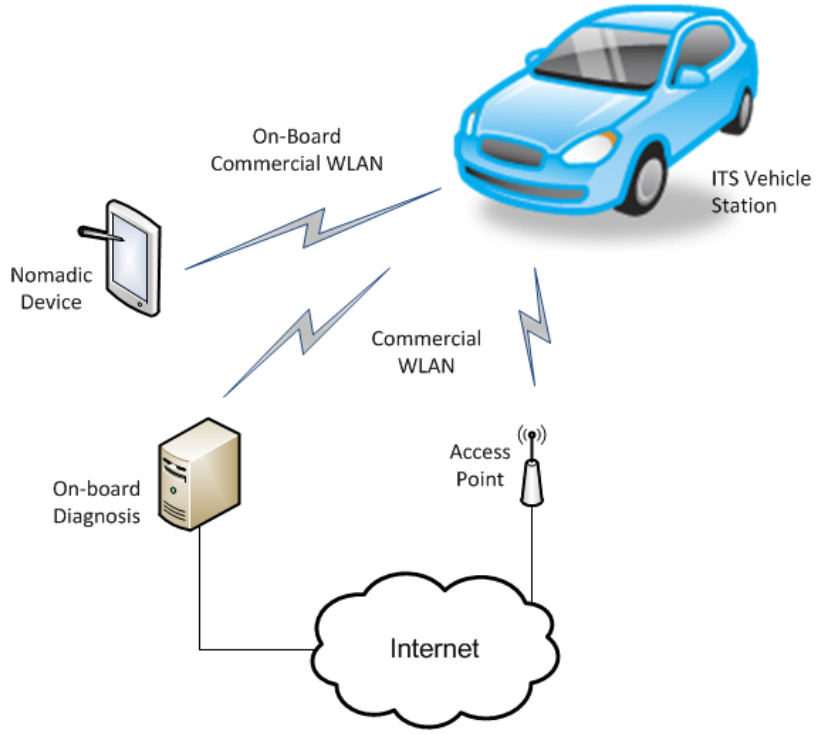

Figure 3: Communication modes and types: Wireless LAN and Cellular Data with ITS Vehicle Station

1.1.2.2 ITS G5C

The communication via Commercial W-LAN (i.e. IEEE 802.11a/b/g/n) can be used in ad-hoc mode for broadcast or unicast message exchange for non-safety critical functions. Similar to G5A the ad-hoc communication between ITS-S is assumed to be unstable. Frequent communication disruptions are possible due to the high mobility of ITS Vehicle Stations. In infrastructure mode the ITS-S may establish a connection to a public access point in order to access the internet.

The following communication links are in the scope of PRESERVE:

ITS-S ↔ ***ITS-S***:

- **IVS** ↔ **Public Access Point**: Communication between vehicles and access points in the infrastructure are assumed to be protected on Layer 2 by standard mechanisms such as WPA. Additional data protection mechanisms on higher layers are reasonable if end-to-end protection is necessary.

1.1.2.3 ITS IMT Public

If vehicles, roadside units or central stations are equipped with mobile communication systems then data exchange over this link is possible and reasonable [5]. This communication link is not limited to ITS communication but can also be used for application specific communication (e.g. Internet connection). Security mechanisms for protecting communication via ITS IMT Public are not part of the PRESERVE VSA. If specific security requirements for the data protection are identified, protection mechanisms on top of the IMT Public mechanisms can be applied.

The following communication links are relevant for PRESERVE:

- **ITS-S** ↔ **ITS-S**: For the exchange of ITS data via mobile network, the higher latency and the possibly high data volume have to be considered. Another problem may be network coverage in rural areas or tunnels.

- **ITS-S ↔ Internet**: IP communication via ITS IMT Public to the Internet **is not** in the main focus of PRESERVE and eventually can be addressed jointly with ITSSv6.

1.1.2.4 On-Board Diagnosis

The communication via On-Board Diagnosis (OBD) tools is used primarily for station updates or fault diagnosis in a garage. It is assumed for this analysis that a wired link or a wireless link over WLAN, Bluetooth or similar communication techniques between the ITS-S and the OBD tool is possible. It is assumed that the ITS-S is not directly accessible from the Internet via ITS IMT Public. Therefore, the communication via WLAN or Bluetooth can be protected by available security mechanisms of the mentioned technologies. Furthermore, it is assumed that existing secure tunnels between the OBD tool and the respective OEM are available.

The following communication link is within the scope of PRESERVE:

- ITS-S ↔ Garage / OEM

1.1.2.5 Power-Line

Battery operated vehicles require regular charging. During that time the vehicle is connected via a power cable to a charging station. Especially on public charging stations data communication is required over that cable for accounting. At private homes, the vehicle may communicate with a smart grid for using the vehicle's batteries as a power buffer for storing renewable energy.

1.1.2.6 In-Vehicle Communication

Inside the ITS-S several sensors, ECUs and at minimum one head unit can be assumed to be available. All of these components are connected via buses (e.g. CAN, MOST, FlexRay, Ethernet, etc.) in order to exchange data. The PRESERVE VSS will also be connected to the in-vehicle communication system in order to process own station information. Although roadside units will probably have a less complex network of sensors and ECUs, these networks have to be considered as well.

In the rest of the document, the entities of the on-board system are assumed to be external of the VSS from a security viewpoint. Therefore, e.g., communication stack or ECUs are not trusted by default. The VSS itself also contains SW and HW components that have to be protected.

For in-vehicle communications the following links are within the scope of PRESERVE:

- Sensor ↔ ECU
- ECU ↔ ECU
- ECU ↔ Head Unit
- ECU ↔ CCU

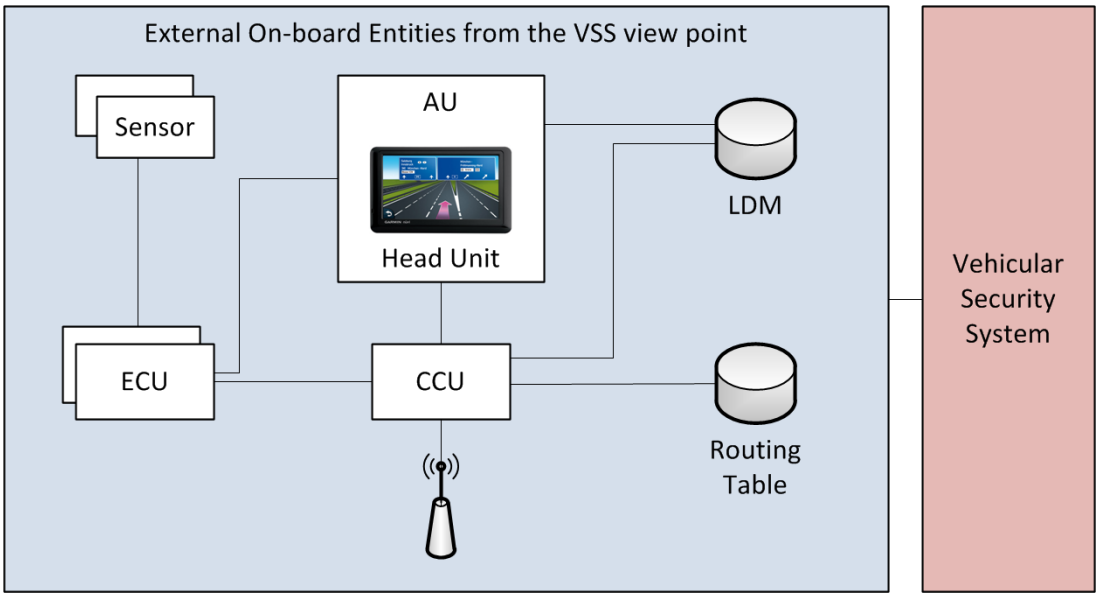

Figure 4: In-Vehicle Communication

1.1.2.7 Global Navigation Satellite System (GNSS)

Every mobile entity in the ITS must be equipped with a GNSS receiver in order to be aware of its current position. A protection of the GNSS signal is only possible if the used GNSS system provides appropriate mechanisms [42], [43]. It is not possible to enforce or introduce such additional protection mechanisms within PRESERVE.

1.1.2.8 Backend

The backend is composed by a PKI, third parties (e.g. eCall), traffic management and roadside unit management servers, all accessible via ITS Roadside station or cellular base station.

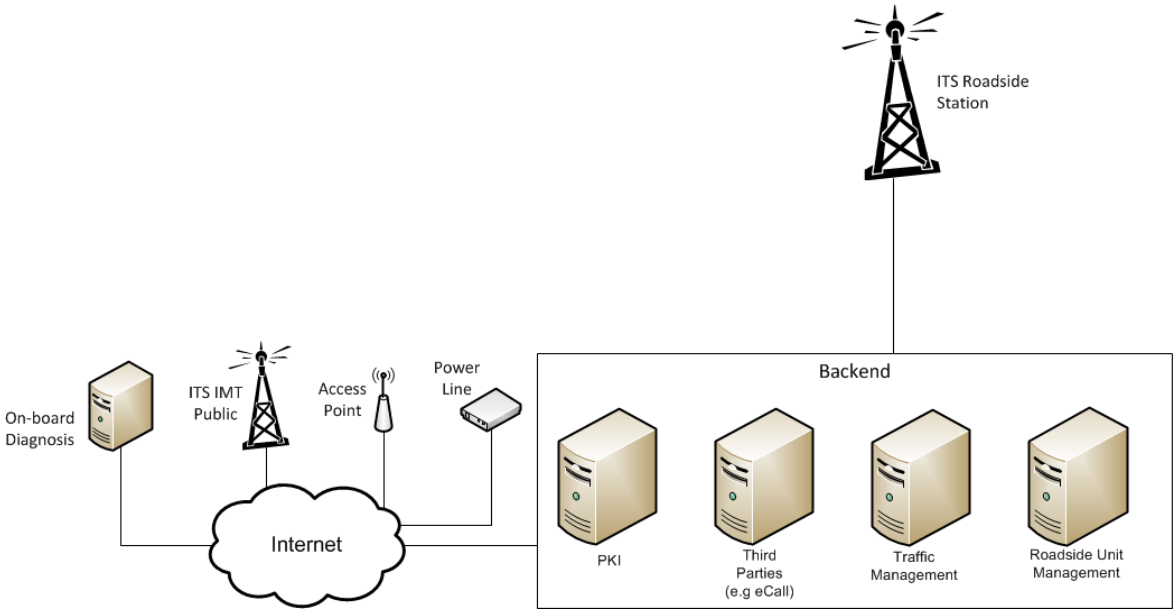

Figure 5: Intra-infrastructure and Backend Communication.

1.1.3 Communication Services

In the following section the different communication services are discussed that are related to V2X communication. The PRESERVE VSA will focus primarily on securing CAMs [11] and DENMs [12].

1.1.3.1 Network Layer V2X Packet

As the geographical routing functionality is probably realized at the network layer, mobility information has to be available there in order to create and manage the corresponding routing table. As described in sim^{TD} [6], a V2X network header is added to every message that contains the following information:

- Congestion and flow control
- Transmit power
- Traffic classes
- Hop limit
- Position vector of the sender that includes a timestamp, geographical position, speed, and heading
- Position vector of the originator that includes a timestamp, geographical position, speed, and heading

1.1.3.2 Cooperative Awareness Message

The Cooperative Awareness Message (CAM) is used as a heartbeat or a beacon message in order to provide information of presence. The ITS station has to send CAMs as soon as it becomes part of the V2X communication network. The cooperative awareness message and the proposed usage are described in more detail in ETSI [11]. As defined by ETSI the message is broadcasted regularly in the single-hop neighborhood. CAM forwarding is in general not envisioned but at intersections with bad network coverage a roadside unit may mirror CAMs in order to support affected applications (e.g. intersection collision warning). The frequency of message distribution varies from 1 Hz to 10 Hz depending on the deviation of position, heading and speed between to messages. The following data are available in each CAM:

- Generation timestamp
- Mobility data: position, speed, and heading
- Optional information: vehicle length, blue light or siren in use, open doors, etc.

1.1.3.3 Decentralized Environmental Notification Message

The Decentralized Environmental Notification Message (DENM) is used for notification about specific safety related events such as a hard breaking vehicle, detection of wrong-way driver or traffic jam detection. Furthermore, a DENM can be used for traffic efficiency use cases as described in ETSI [12]. In contrast to a CAM the DENM is not only designed to be broadcasted in the single-hop neighborhood but additionally to be forwarded to more distant nodes. Therefore, an event type, a geographical position or an area of the event, a geographical area of distribution, the detection time and duration are integral part of the DENM.

1.1.3.4 Local service announcement service

A local service announcement provides information about the availability of a local service provided by a roadside unit [13].

1.1.3.5 Internet-based service announcement service

An internet-based service announcement provides information about the availability of a service that can be accessed using an internet connection [13].

1.1.3.6 Transparent communication

At the transport layer a header may differentiate between different V2X application message types. Based on sim^{TD} [6], the V2X application payload header is defined that provides the following information:

- Unique action ID
- CancelationFlag that indicates the explicit cancelation of a message with the same action IDs from the same originator
- GenerationTime as reference for message content
- ValidityDuration defines the time span after generationTime when the message shall be deleted from all databases
- ReferencePosition that provides optionally position and heading of the originator
- ApplicationPacketType that defines the packet type in the payload

The application packet type indicates if a CAM or DENM can be found in the payload but additionally application specific messages may be defined in the V2X communication protocol. This application specific payload can be considered as transparent for the underlying communication layer and also for the security. As application specific messages can be transmitted via broadcast or unicast, the security layer should provide mechanisms for assuring authenticity and/or confidentiality also for these message types.

1.1.4 Physical Security

Physical protection can only be partly considered by the VSA. The following aspects are **not** part of the PRESERVE security requirements analysis:

- Physical protection against eavesdropping of the wireless communication channels
- Physical integrity protection of transmitted data over the air
- Physical protection against manipulation of vehicular hardware components (e.g. sensors, ECUs, communication buses). However, critical building blocks of the PRESERVE VSS have to be protected against physical access and manipulation.
- Physical resistance against premeditated destruction (e.g. vandalism)
- Protection against physical access and theft

1.2 Use Cases

The following list of use cases in Subsection 1.2.1 has been collected from the different related projects and ETSI. In Subsection 1.2.2 a subset of four use cases is selected and analyzed in a more detail way. The section of a small subset makes the verification of completeness of collected security threats, countermeasures, security requirements and functional requirements easier. The Section 1.2.2 this is done in that way that every use case covers special requirements and exhibits special behavior of V2X communications. Therefore, every use case should be a representative of a specific ITS communications cluster. Nevertheless, the PRESERVE VSA considers a broader level by selecting four use cases from Table 1.

1.2.1 List of Use Cases using V2X Communication

Name	Communication parties	Network	Relevance	Project
Emergency vehicle warning	IVS ↔ IVS IVS → RSU	G5A	High (C2C Phase 1)	ETSI [14], SeVeCom [1], PRE-DRIVE [9],

				OVERSEE [10], sim^{TD} [21]
Electronic brake lights	IVS ↔ IVS IVS → RSU	G5A	High (C2C Phase 1)	ETSI [14], EVITA [3], OVERSEE [10], sim^{TD} [21]
Stationary vehicle - accident / vehicle problem / eCall	IVS ↔ IVS IVS ↔ RSU IVS → Internet	G5A, IMT Public	High (C2C Phase 1)	ETSI [14], EVITA [3], OVERSEE [10]
Traffic condition warning, Traffic jam ahead warning, Slow vehicle warning, Hazardous Location Warning	IVS ↔ IVS RSU ↔ IVS	G5A	High (C2C Phase 1)	ETSI [14], PRE-DRIVE [9], OVERSEE [10], sim^{TD} [21]
Intersection Collision Warning (with exchange of floating car data) Collision risk warning	IVS ↔ IVS RSU ↔ IVS	G5A	High for Transmit Vehicle Mass (C2C Phase 1) rest phase 2	ETSI [14], SeVeCom [1], PRECIOSA [2], sim^{TD} [21]
Traffic information and recommended itinerary	RSU → IVS	G5A	High (C2C Phase 1)	ETSI [14], OVERSEE [10], PRECIOSA [2], sim^{TD} [21]
Enhanced route guidance and navigation (with possibly additional information exchange, e.g., booking of hotel on the road)	RSU ↔ IVS IVS ↔ ICS	G5A, IMT Public	High (C2C Phase 1)	ETSI [14], EVITA [3], sim^{TD} [21], PRECIOSA [2]
Decentralized floating car data - hazardous location, precipitations, road adhesion, visibility, wind	IVS ↔ IVS RSU ↔ IVS IVS ↔ ICS	G5A, IMT Public	High for hazardous location warning (C2C Phase 1)	ETSI [14], EVITA [3], PRECIOSA [2], sim^{TD} [21]
Roadwork warning	RSU → IVS	G5A, IMT Public	High (C2C Phase 1)	ETSI [14], SeVeCom [1], PRE-DRIVE [9], sim^{TD} [21]
Signal violation warning	IVS ↔ IVS RSU → IVS	G5A	High (C2C Phase 1)	ETSI [14], PRE-DRIVE [9]
Traffic light optimal speed advisory, Green Light Optimal Speed Advisory (GLOSA)	RSU → IVS	G5A	High (C2C Phase 1)	ETSI [14], EVITA [3], sim^{TD} [21]
Longitudinal Collision Risk Warning	IVS ↔ IVS	G5A	High (C2C Phase 1)	C2C-CC

Motorcycle approaching indication	IVS ↔ IVS	G5A		ETSI [14]
Wrong way driving warning	IVS ↔ IVS IVS ↔ RSU	G5A, IMT Public		ETSI [14], sim^{TD} [21]
Regulatory / contextual speed limits notification	RSU → IVS	G5A		ETSI [14], EVITA [3], sim^{TD} [21]
Limited access warning and detour notification	RSU → IVS	G5A		ETSI [14], EVITA [3]
In-vehicle signage	RSU → IVS	G5A		ETSI [14], sim^{TD} [21]
Point of Interest notification	RSU → IVS IVS ↔ ICS	G5A, IMT Public		ETSI [14]
Electric Vehicle Charging Spot Notification Specification	RSU → IVS ICS → IVS	G5A, IMT Public		ETSI [14]
Automatic access control and parking management	RSU → IVS Internet → IVS	G5A		ETSI [14], OVERSEE [10]
ITS local electronic commerce	RSU ↔ IVS	G5A, IMT Public		ETSI [14]
Media downloading	IVS → RSU IVS → Internet	G5A, IMT Public		ETSI [14], sim^{TD} [21]
Insurance and financial services	IVS → RSU IVS → Internet	G5A, IMT Public		ETSI [14]
Fleet management	RSU ↔ IVS	G5A, IMT Public		ETSI [14]
Loading zone management	RSU ↔ IVS	G5A		ETSI [14]
Vehicle software / data provisioning and update	RSU ↔ IVS Internet → IVS OBD → IVS	G5A, IMT Public		ETSI [14], SeVeCom [1], EVITA [3]
Vehicle and RSU data calibration	Internet → IVS OBD → IVS	G5A, Garage		ETSI [14], EVITA [3]
Toll collection	IVS → RSU	G5A		ETSI [14], EVITA [3], OVERSEE [10]
Electronic License	IVS → Special	G5A		OVERSEE [10]

Plate	IVS / RSU			
Remote Car Control	Internet → IVS	G5A, IMT Public		OVERSEE [10]

Table 1: Use cases relevant for PRESERVE using V2X Communication

1.2.2 Selected Use Cases

In this section we present selected use cases that cover the most relevant communication forms the PRESERVE architecture can be used for. Each communication form requires protection by special security mechanisms. If different use cases using the same communication form were available we preferred those which are specified by the Car-to-Car Communication Consortium as "C2C Phase 1" (first deployment phase).

The resulting use cases are:

- Intersection Collision Warning
- Emergency Vehicle Warning
- Hazardous Location Notification
- Enhanced Route Guidance and Navigation

Those four use-cases are described in detail in the following subsections. The descriptions are based on the Basic Set of Applications by ETSI [14].

1.2.2.1 Intersection Collision Warning

Use case label	Intersection Collision Warning
Actors, stakeholders	IVS, RSU
Benefits	Prevent/mitigate collision between vehicles.
Use case scenario	This use case allows vehicles present in the affected area to calculate the concrete risk for a collision with other vehicles at an intersection. • This scenario covers both controlled and uncontrolled intersections. • In both cases there may be legal issues and liability if a vehicle enters an intersection without all due driver consideration of the traffic conditions (on the crossing roadway) and accordingly increases the risk of collision. • This form of driver behavior may be a violation of local laws and it may require identification of the vehicle and driver by the appropriate authority.
Main requirements	• The capability of vehicles to **broadcast** V2X cooperative awareness messages and accordingly to receive and process V2X **CAM**. • A roadside unit to be installed if line-of-sight between vehicles is obstructed. RSU needs to be capable to **relay** CAMs or to detect and signal a collision risk. • Accurate positioning of vehicles on digital maps. • Minimum frequency of the periodic message: 10 Hz. • Critical time requirement: Latency time less than 100 ms.

Involved components	Sender • Communication stack • VSS Receiver • Communication stack • VSS • Intersection Collision application that calculates intersection collision risk • HMI

Security aspects	• Signing of outgoing CAM
	• Verification of incoming CAM
	• Plausibility check of the CAM mobility data
	• Consideration of high channel load due to:
	  ○ High CAM frequency at intersections,
	  ○ Mirroring of CAMs by the RSU that may cause reception of duplicate CAMs,
	  ○ Possible large intersections with several lanes per direction.
	• Consideration of low latency requirements
	• Possible lock of pseudonym change in the vicinity of intersections (unless this is not needed or not possible due to other functionality, e.g., if mix-zones are placed at intersections [44].)

Table 2: Use Case Description of Intersection Collision Warning

1.2.2.2 ***Emergency Vehicle Warning***

Use case label	Emergency Vehicle Warning
Actors, stakeholders	IVS, RSU with traffic light
Benefits	• Vehicles, equipped with a V2X communication receiver, can warn the driver about an approaching emergency vehicle. • Traffic lights that are connected to an RSU are able to change the traffic light status according to the approaching emergency vehicle
Use case scenario	This use case allows an active emergency vehicle to announce early its presence in a precise manner. In many countries, the presence of an emergency vehicle imposes an obligation for vehicles in the path of the emergency vehicle to give way (yield) and to free an emergency corridor.
Main requirements	• Capability for an emergency vehicle to **broadcast** V2X **CAMs** with relevant emergency signs being activated. • Capability for all vehicles and relevant roadside units to receive and process V2X cooperative awareness messages. • Minimum frequency of V2X cooperative awareness messages issued by the emergency vehicle: 10 Hz. • Critical time requirement: Latency time less than 100 ms.
Involved components	Sender

	• Facilities layer with connection to the CAN bus in order to request status of vehicle (light bar or siren in use) to generate appropriate CAMs • Communication stack • VSS Receiver • Communication stack • VSS • Emergency vehicle application that processes relevance • HMI
Security aspects	• Special authorization of the sender (emergency vehicle) necessary • Pseudonym change at activation of emergency status. It is reasonable that police cars are signing their V2X messages with regular pseudonyms as long as their light bar is not in use. In case of blue light driving the pseudonym has to be changed with the first message with relevant emergency signs. • Consideration of low latency requirements

Table 3: Use Case Description of Emergency Vehicle Warning

*1.2.2.3 **Hazardous Location Notification***

Use case label	Hazardous Location Notification
Actors, stakeholders	IVS, RSU
Benefits	Reduce the risk of accident which could be caused by a hazardous location.
Use case scenario	This use case informs vehicles of any hazardous location either temporary or permanent.
Main requirements	• Capability for a vehicle, from detecting a hazardous location, to **broadcast**/**geocast** in V2X **DENMs** the hazardous location notification. • Capability for concerned vehicles (on the same road, and same heading of the cars having detected a hazardous location) to receive and process V2X and I2V decentralized environmental notification messages. • Capability for all vehicles crossing the vehicle that signals a hazardous location to **store and forward** received DENMs according to their geo-casting parameters. • Minimum frequency of the periodic message: 10 Hz.
Involved components	Sender • Application that detects the hazard and generates a DENM • Communication stack • VSS Receiver • Communication stack • VSS

	• Application processing the DENM
Security aspects	• Signing of outgoing DENM • Verification of incoming DENM • Check plausibility of sender's mobility data • Consideration of multi-hop security

Table 4: Use Case Description of Hazardous Location Notification

1.2.2.4 ***Enhanced Route Guidance and Navigation***

Use case label	Enhanced Route Guidance and Navigation
Actors, stakeholders	IVS, RSU
Benefits	Optimize planned route according to personal preferences, including preferred landscape, road types, and overnight stays.
Use case scenario	A vehicle passes a roadside unit, which has the capability to access the Internet and enable any passing by vehicle or parked vehicle to access an Internet server. The vehicle then requests an optimized itinerary (new waypoints, possibly hotel rooms for overnight stay) according to some personalized requirements. The enhanced routing service charges a fee per request. Likewise, the booked hotel rooms are charged to the requestor [14] [2].
Main requirements	• Encryption of destination (region, address) • Encryption of personal information (address, credit card) • Binding of sent data to user-specified purposes • Circumvention of data linking and aggregation
Involved components	Sender • Application requests privacy-relevant information from the on-board vehicle system and generates application specific V2X messages. • Communication stack • VSS Receiver • Communication stack • Application on roadside unit or backend server that calculates new waypoints and possibly books hotel rooms.
Security aspects	This interaction involves two types of personal information, which need to be protected by privacy policies: • The destination needs to be sent to the RSU and may not be related to a unique identifier. Likewise, the returned route may not be stored and correlated with unique identifiers of individuals. • Personal information, such as address and credit card details, which is exchanged for payment purposes, may not be used for unauthorized purposes, including, but not limited to, collection of address databases and linking of address data and route data.

Table 5: Use Case Enhanced route guidance and navigation

2 Security Requirements Analysis

The following risk analysis is a collection of information from the related work of ETSI [15] and the C2C-CC as well as the related projects SeVeCom [1], EVITA [3], sim^{TD} [7], PRECIOSA [2] and OVERSEE [10]. Performing a new analysis of risk and threats in vehicular communication networks is not part of the PRESERVE security requirements analysis because the relevant threats have been already analyzed in detail in corresponding projects. Therefore, we refer to the risk analysis of the related projects in order to check the correctness of the defined risk. In this security requirements analysis at first the potential attackers are listed followed by their possible motivations. Subsequently, the threats linked to their risk and possible counter-measures are listed in five tables that consider the classical security protection classes:

- Availability
- Integrity, Authenticity and Authorization
- Confidentiality
- Privacy with Anonymity and Pseudonymity
- Accountability, Auditability and Non-repudiation

Figure 6 presents the process of the security requirements analysis that has been performed within PRESERVE (see [20] for a detailed description of the approach). In the first step, all relevant security requirements that are derived from the use cases described in related work are collected. Within this process, SeVeCom [20] simply collected all security requirements without evaluation of specific relevance. In the second step, related attacks and threats against the listed security requirements are identified. In the third step the threats are clustered based on their attack methods and possible undesirable consequences. Furthermore, the affected networks and assets have been listed in the clustered threat tables. In step 4, risks are identified and assigned to the threats. In the SeVeCom security requirements analysis, three groups of risk have been used that are assigned based on values from 0 to 6. A description of the group of risks can be found in the subsection Risk Analysis. This classification and evaluation of risks for the threats is primarily based on:

- ETSI TVRA [15] Section 10.3
- EVITA D2.3 [3] Appendix C and the paper “Security Requirements for Automotive On-Board Networks” [22]
- SeVeCom D1.1 [1] Section 7
- sim^{TD} D21.5 [7] Section 4.3.3.3
- PRECIOSA D1 [2]

In step 5 possible countermeasures are assigned to the tables of clustered threats based on the collection in table Possible Countermeasures. Additionally, available solutions and components from related projects have been identified. In the last step of the security requirements analysis process, the relevance of the threat for PRESERVE is evaluated. This evaluation is based on the definition of the main PRESERVE focus and possibilities to consider the specific threat with technical solutions.

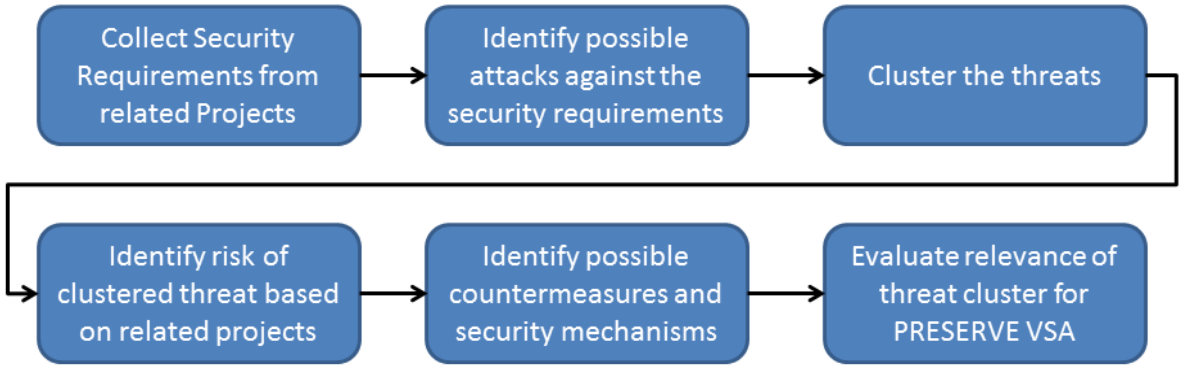

Figure 6: Work steps, leveraging existing literature, towards identifying risks and mechanisms.

Also the possible countermeasures that are listed in the last table (Table 26) of this chapter have been integrated into the threat tables. Finally, modules and concepts of related projects have been considered in these tables.

2.1 Potential Attackers and Attack Types

The threat coming from an attacker depends on the attacker's abilities, technical knowledge and methods on accessing the attack target. For this security analysis we clustered the set of potential attack types and attackers into different groups.

2.1.1 Attacker Types

2.1.1.1 External Attacker

- External attackers from the Internet
- External attacker within communication range of ITS G5A
- External attackers with physical access to ITS Stations

2.1.1.2 Internal Attacker

Internal attackers have more access privileges and are therefore able to gain direct or physical access to certain systems. Regarding ITS we assume internal attackers with valid credentials and access to one or more (simultaneously) of the following entities:

- ITS Vehicle Station
- Roadside Unit
- ITS Central Station
- On-Board Diagnosis

2.1.2 Attack Variants

2.1.2.1 Active Attack

For an active attack the attacker actively intervenes into the attacked system. This includes injection or alteration of software or data stored on an ITS Station as well as injection or alteration of data that is transmitted between ITS Stations or from a sensor in a vehicle to the on-board unit.

2.1.2.2 Passive Attack

In a passive attack, the attacker limits itself to methods that do not actively change anything within the attacked system. A common passive attack is eavesdropping protected information like key material. In ITS, passive attacks are also relevant, regarding the collection of wireless transmitted messages for attacking user privacy for example.

Passive attacks are very difficult to detect as they do not change the system behavior.

2.1.3 Attack Situations

2.1.3.1 Offline Attack

For performing an offline attack, the attacker requires direct access to the hardware to be attacked. As the attack type indicates the attacked system is offline, its regular software environment is not active. The attacker accesses the storage components of the system using a different operating system or by transplanting certain hardware components into a system controlled by the attacker. Both ways allow overriding Access Control Lists (ACLs) of file-systems, database systems for accessing and modifying sensitive data like credentials, account data and cryptographic keys that are not protected by appropriate mechanisms (unauthorized data access).

In addition, the implementation code of applications or the operating system can be modified by the attacker allowing him to disable certain parts of the software or significantly change the way how the software operates at runtime (unauthorized data and software manipulation).

2.1.3.2 Online Attack

For attacking a system using an online attack one exploitable vulnerability in the operating system or an application running on that system is required at least. This vulnerability is used to bypass a security enforcement system and inject for example code defined by the active attacker that is then executed by the system. This may result is a temporary or permanent change of the system behavior. Depending on the vulnerability an attacker can get up to full control of the attacked system.

2.2 Attacker Motivation

Understanding the attacker's motivation is very important in a security analysis. Based on the different types of attacks, motivation classes can be determined.

- Physical harm, vandalism, terrorism and organized crime
  - Impersonation of a victim in order to perform actions with stolen identities
  - Denial of use/service
  - Causing an accident
- Obtaining information about the driver
  - Global attacker may try to get access to mobile profiles
  - Companies may calculate individual risk related to drivers
  - Criminals could use mobility profiles in order to steal or hijack cars or even abduct people (e.g., for ransom)
- Financial incentives
  - After an accident, the car owner could try to manipulate the data stored in the vehicle to obscure liable behavior
  - Insurance fraud
  - Spam
  - Vehicle manufacturer intellectual property infringement
  - Harm the economy of ITS and road traffic, e.g. provoke traffic congestion
  - Manipulate vehicles of competitors, e.g., making them inefficient or disabling part of their functionality, in order to
    - Destroy public reputation
    - Blackmailing
- Personal motivation and utility
  - Gain reputation as a scientist/hacker
  - Get ability to run own SW on parts of the system installed in the car
  - Enhancement of own traffic conditions (may regard vehicle drivers or residents)

- Restore anonymity/location privacy at the level before the introduction of ITS systems

2.3 Risk Analysis

The risk situation of Vehicle-to-Vehicle communication systems as well as the risk of vehicle internal systems has been analyzed within the previous projects [3], [1], [7], [2], [9], [10] and ETSI [15]. For PRESERVE we use those documents and extract the identified threats, join them and subsume to a joined risk situation.

The following subsections contain the joint results including a classification of risks according to severity level. The calculation of severity is based on the following factors:

- Potential of an attacker
  - Time of disruption of the system after attack
  - Expertise of the attacker
  - Opportunity
  - Equipment needed by the attacker
- Likelihood of the attack
- Impact

Table of severity levels	
Severity	**Description**
Minor	Based on the risk analyses of the related projects, the potential of the attack, the impact and the likelihood is not very high. Therefore, this threat and the responsible countermeasures need not be considered in PRESERVE with highest priority.
Major	Based on the risk analyses of the related projects, the potential of the attack, the impact and the likelihood is high. Therefore, this threat and the responsible countermeasures must be considered in PRESERVE.
Critical	Based on the risk analyses of the related projects, the potential of the attack, the impact and the likelihood is very high. Therefore, this threat and the responsible countermeasures must be considered in PRESERVE with highest priority.

Table 6: Severity levels

Further to the severity classification we have rated each threat according to its relevance for PRESERVE. The rating ranges from “low” for threats that are not directly addressed by PRESERVE via “medium” to “high” for threats with a major or critical severity and that are in the main scope of PRESERVE.

2.3.1 Availability and Denial of Service Threats

“Protocols and services should remain operational even in the presence of faults, malicious or benign. This implies not only secure but also fault-tolerant designs, resilience to resource depletion attacks, as well as self-stable protocols, which resume their normal operation after the ’removal’ of the faulty participants” [45].

“Some applications, particularly safety applications, require high availability of the communication system. For example, a post-crash/breakdown warning requires that the radio channel is available such that approaching cars can receive the warning message in time. If the medium is

jammed e.g. by an attacker and therefore such messages don't arrive at the receivers in a very short time, the application gets useless" [20].

2.3.1.1 *Jamming of signals*

Name of Threat	**Jamming of signals**
Description	Generation of signals that intentionally introduce interference into a communication channel, to prevent error-free reception
Network	ITS G5A GNSS, On-Board
Asset	Communication
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3]
Identified Risk	Major
Possible Countermeasures	• Implement frequency agility – CDMA/spread-spectrum system • Integrate multiplicity of links or media, e.g. ITS-IMT Public
Available solution / component	
Relevance in PRESERVE	**Low** • Security on layer 2 is not focus of the PRESERVE VSA
Measurements for Evaluation (Testing)	No testing necessary

Table 7: Threat: Jamming of signals

2.3.1.2 *Denial-of-Service of V2X communications*

Name of Threat	**Denial-of-Service of V2X communications**
Description	Methods: • Flooding: Generating a high volume of invalid messages (single hop, multi hop) • Malware, manipulating the sending or receiving capabilities • Black-hole attack (message dropping) • Selective message forwarding / dropping • Exploitation of flaws in the production design • Message manipulation by forwarders that cause information loss • Sabotage, destruction of communication equipment (e.g. break external antennas) Undesirable Consequences: • DoS on incoming messages • DoS on outgoing messages • DoS on internal resources
Network	ITS G5A
Asset	Communication
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3], SeVeCom [1], PRE-DRIVE [9]
Identified Risk	Critical

Possible Countermeasures	• Reduce frequency of V2X messages • Entity authentication by using platform integrity mechanisms • Enable location authentication by signing GNSS data • Software authenticity and integrity is certified • Use an Intrusion Detection System • Remote deactivation of misbehaving ITS-S • Hardware-based identity and protection software; Attestation of HW and SW
Available solution / component	• A plausibility check in the communication stack of the geographic routing should avoid message flooding • The plausibility check implemented in sim^{TD} (Java, OSGi) [8] checks the message frequency of incoming V2X messages • Security Watch Dog module of EVITA could be used to check the message frequency of incoming V2X messages • Platform Integrity Module of the EVITA project could be used to verify the integrity of installed software. It is responsible for chaining and unchaining of data into a platform configuration. An ITS-S platform with modified software in the communication stack should not be allowed to send messages. • Selective message forwarding / dropping is considered in scientific papers with a watch-dog mechanism that overhears the communication of the neighbors in promiscuous mode. Probably it may not be an appropriate mechanism for geographic multi-hop communications in VANETs.
Relevance in PRESERVE	**Medium** • DoS should generally be addressed by the PRESERVE VSA • Frequency of incoming messages can be checked before the message verification is performed in order to omit DoS of VSA and flooding of LDM. • The integrity of the VSA hardware and software components can be protected by the Platform Integrity Module. The integrity of external components (e.g. communication stack) is protected by the VSA as long as the on-board components are EVITA HSM enabled. Nevertheless, malicious or high frequent invocation of the VSS cannot be avoided which may result to a DoS of own ITS-S.
Measurements for Evaluation (Testing)	• Test whether maximum CAM message frequency defined by ETSI [11] is violated • Manipulate SW of the PRESERVE VSS • Manipulate SW that uses the security services of the PRESERVE VSS • Test update of on-board SW on ECUs that are EVITA HSM enabled and the update of respective platform integrity modules on these ECUs.

Table 8: Threat: Denial-of-Service of V2X communications

2.3.1.3 Denial-of-Service of on-board units and internal busses

Name of Threat	**Denial-of-Service of on-board units and internal buses**
Description	Methods: • Malware injecting high message volume into the internal buses (e.g. flash malicious code) • Exploit implementation flaws • Sabotage, destroying of ITS-S
Network	On-Board
Asset	CCU, ECU, Communication
Source (Project)	EVITA [3]
Identified Risk	Minor
Possible Countermeasures	• Hardware-based identity and protection software; Attestation of HW and SW
Available solution / component	• Security Watch Dog module of EVITA could be used to check the message frequency of internal messages • Platform Integrity Module of EVITA could be used to verify the integrity of installed software. It is responsible for chaining and unchaining of data into a platform configuration. It has to be considered that probably only a small number of internal ECUs are equipped with an HSM or compatible security implementations.
Relevance in PRESERVE	**Medium** • DoS of on-board units can only be considered as long as the on-board components are EVITA HSM enabled. Assuming only very few ECUs are equipped with security add-ons (e.g. Security Watch Dog, Platform Integrity Module) the risk of DoS attacks cannot be fully eliminated with classical ECUs on-board.
Measurements for Evaluation (Testing)	No testing necessary

Table 9: Threat: Denial-of-Service of on-board units and internal buses

2.3.1.4 *System infection with malware*

Name of Threat	**System infection with malware**
Description	Methods: • Unauthorized SW update (e.g. via remote access, ODB, or by exploit implementation flaws) Undesirable consequences: • Integration of inconsistent software that is not following standardized ITS communication behavior. • Deleting or manipulating of service information, security parameters, local station data or LDM data • DoS on incoming messages • DoS on outgoing messages • DoS on internal resources
Network	On-Board, OBD, Backend
Asset	Communication, CCU, Head Unit
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3], PRE-DRIVE [9]
Identified Risk	Critical
Possible Countermeasures	• Entity authentication by using platform integrity mechanisms • Software authenticity and integrity verified • Hardware-based identity and protection software; Attestation of HW and SW • Using sandboxes, firewalls, checkpoints in combination with a policy decision module • Implement a Privilege Management Infrastructure (PMI)
Available solution / component	• In sim^{TD} the verification of software components of the ITS-S is not considered • Platform Integrity Module of EVITA could be used to verify the integrity of installed software, SW updates and configuration files. It is responsible for chaining and unchaining of data into a platform configuration. An ITS-S platform with modified software in the communication stack is not allowed to send messages.
Relevance in PRESERVE	**Medium** • Protection of on-board SW should be considered by the PRESERVE VSA. o Basically, the SW and HW of the PRESERVE VSS itself should be protected by platform integrity mechanisms o Protection of users of the PRESERVE VSS (e.g. communication stack) may be considered by PRESERVE but cannot be guaranteed without a trusted operating system [10]. o Protection of other on-board SW and HW is considered by the PRESERVE VSA as long as the

	ECUs are EVITA HSM enabled.
Measurements for Evaluation (Testing)	• Manipulate SW of the PRESERVE VSS • Manipulate SW of ECUs which are EVITA HSM enabled

Table 10: Threat: System infection with malware

2.3.2 Integrity and Masquerade (Authenticity and Authorization) Threats

Trust is crucial in safety-related applications, in which vehicles react according to legitimate messages they receive. Authentication ensures that the sender of a message is correctly identified. With **ID authentication**, the receiver is able to verify a unique ID of the sender. The ID could be the license plate or chassis number of the vehicle. Yet, in many cases, the actual identity of nodes does not play an important role – receivers are satisfied if they are able to verify that the sender entity has a certain attribute. Hence, **entity authentication** is a security requirement that allows verifying attributes of the sender, e.g. that the sender is a car, a traffic sign etc. For applications using location information, **location authentication** allows to verify that the sender is actually at the claimed position, or that the message location claim is valid.

Applications require that the transported information must not be altered between sender and receiver.

"Access control and entity authorization is necessary for applications that need fine-grained definition of the rights that a user or infrastructure component has. For instance, an authorized garage may be allowed to fully access wireless diagnostics, whereas other parties may only be granted limited access. Another form of access control can be the exclusion of misbehaving nodes (e.g. by an intrusion detection system using a trust management scheme) from the VANET by certificate revocation or other means" [20].

The access to specific services, provided by the infrastructure or other nodes, is determined locally by policies. Access to the vehicular network and messages is mandated by default open to all nodes for applications such as those designed for safety. Assignment of distinct roles to different types of nodes is assumed. As part of access control, authorization establishes what each node is allowed to do in the network, e.g., which types of messages it can insert in the network, or more generally the protocols it is allowed to execute [45].

2.3.2.1 Manipulation of the routing table, LDM or application behavior of other ITS station

Name of Threat	**Manipulation of the routing table, LDM or application behavior of other ITS stations**
Description	Methods: • Sending messages with bogus information, e.g., position data in order to create for example a black-hole or bogus application information (e.g. faked emergency alerts) • Spoofing or jamming GNSS positioning signals • Use GNSS radio signal generator to manipulate local time of ITS station in order to enable replay attacks • Forging of messages • Impersonation, e.g., masquerading an ITS-S, or its network or on-board sensor, or Sybil attacks • Replay of "expired" messages Undesirable Consequences:

	• Influence routing and decisions of applications • Use other identities in order to send messages that need specific authorization (e.g. emergency vehicle messages) • Corrupt or inject fake sensor data • Replay V2X messages at a similar location but a different time • Replay V2X messages at a different location and a different time (Wormhole)
Network	ITS G5A, GNSS, IMT Public, On-Board
Asset	CCU, ECU, HU, Communication
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3], SeVeCom [1], PRE-DRIVE [9]
Identified Risk	Critical
Possible Countermeasures	• Sender identification and/or authentication. Receivers in some cases should be able to verify the unique ID of the sender • Digitally sign each message at the sender • Include an authoritative identity in each message • Using secure storage module • Perform plausibility and consistency tests on incoming messages • Perform trustworthiness evaluation of incoming messages • Enable location authentication by signing GNSS data • Use broadcast time (UTC or GNSS) • Use Inertial Navigation System (INS) or dead-reckoning • Implement differential monitoring on the GNSS

Available solution / component	• Secure Communication Modules from SeVeCom can be used to secure CAM and DENM. This module of SeVeCom uses a Crypto Module in order to sign and verify with hardware support. As described in IEEE 1609.2 [19] the own timestamp in the security header or external timestamp in the network or facilities layer has to be verified in order to avoid replay of expired messages.
	• In sim^{TD}, the security header is added at the network layer. This implies that every data on the network layer and above is protected:
	  ○ Originator position vector on network layer
	  ○ Position vector of V2X common header
	  ○ Payload on application layer
	• The Pseudonym Manager of SeVeCom could be used in combination with a HSM in order to use only own certificates.
	  ○ It should not be possible for a user of the security stack to spoof, impersonate or masquerade other ITS-S.
	  ○ Only one pseudonym can be used for a specific type of application and at any given time, in order to avoid Sybil attacks.
	• The Entity Authentication Module in combination with the Policy Decision Module of EVITA could prevent unauthorized access to the security manager or directly to the se-

	curity modules that are responsible for message signing. In order to manage the access the Policy Decision Modules of EVITA could be used. Integrity protection of external SW components, which use the VSS, can only be guaranteed with presence of a trusted OS. • Plausibility checks could be used to verify position data of incoming messages. In sim^{TD} an implementation in Java / OSGi is available. The Security Watchdog Module could also be used to make these checks. Furthermore, the Trust Manager of SeVeCom could be adopted by such a mobility data plausibility check. • Providing an Inertial Navigation System or dead-reckoning is not part of the PRESERVE VSA.
Relevance in PRESERVE	**High** • Authenticity and integrity of message payload as well as protection of originator node information have to be considered by the PRESERVE VSA • Protection against unauthorized invocation of the VSS is not considered. As the integrity of external entities cannot be guaranteed due to the absence of a trusted operating system, the authentication of the invoking entity cannot be verified.
Measurements for Evaluation (Testing)	• Send messages with invalid signature • Send message with invalid/expired certificate • Send message with invalid certificate signer, e.g. untrusted certificate issuer • Send message with invalid timestamp, position or mobility data • Send message with unauthorized payload

Table 11: Threat: Manipulation of the routing table, LDM or application behavior of other ITS stations

2.3.2.2 *Manipulation and Corruption of relayed data en route*

Name of Threat	**Manipulation and Corruption of relayed data en route**
Description	Methods: • Alter / Tamper • Inject Undesirable Consequences: • Providing false or misleading information to other ITS-S • Forging of message content
Network	ITS G5A
Asset	Communication
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3], SeVeCom [1], PRE-DRIVE [9]
Identified Risk	Major
Possible Countermeasures	• Sender authentication and possibly identification. Receiver should be able to verify the unique ID of the send-

	er • Digitally sign each message at the sender / forwarder • Mutable fields of a forwarded message could be modified by an intermediate node en route can be protected by an additional digital signature • Include an authoritative identity in each message • Perform plausibility and consistency tests on incoming messages for the last forwarder / sender
Available solution / component	• For every message a signature of the generator / originator protects the application payload. Additionally, at every forwarder a second signature and pseudonym certificate is added that protects the mutable fields on network layer. • In sim^{TD} it is decided to protect only single-hop messages (CAM & DENM). Multi-hop messages are appended by only one security header (signature + certificate) of the originator. Mutable fields in the network header (routing data and sender position vector) are not protected by an additional security header. The additional overhead in the message is not acceptable.
Relevance in PRESERVE	**Low** • Only authenticity and integrity of message payload that is generated at the originator have to be considered by the PRESERVE VSA. Additional verification and signing operations for mutable fields produces high overhead and latency but have only limited risk. Protection of sender information in the forwarded message should be considered in the PRESERVE VSA with low severity.
Measurements for Evaluation (Testing)	No testing necessary

Table 12: Threat: Manipulation and Corruption of relayed data en route

*2.3.2.3 **Sensor (data) manipulation***

Name of Threat	**Sensor (data) manipulation**
Description	Methods: • Spoof • Physical access (external manipulation of input) • Input controlling attacks [45] • Interface access • Corrupt code or data • Access via internal short range communication interfaces (Bluetooth, Wi-Fi, USB, …)
Network	On-Board
Asset	ECU, Communication, HU
Source (Project)	EVITA [3], PRE-DRIVE [9]
Identified Risk	Major
Possible Countermeasures	• Source identification and authentication

	• Property authentication by using platform integrity mechanisms • Hardware-based identity and protection software; Attestation of HW and SW • Using sandboxes, firewalls, checkpoints in combination with a policy decision module
Available solution / component	• The Platform Integrity Module (PIM), Entity Authentication Module (EAM) and the Communication Control Module (CCM) of EVITA could be used to protect the on-board communication between Sensor, ECU, HU and PRESERVE VSS as long as the external components are EVITA HSM enabled.
Relevance in PRESERVE	**Medium** • Sensible on-board entities such as ECUs can be protected by secure communication modules and platform integrity methods • Probably most on-board entities are not equipped with an EVITA HSM and which makes a protection by PRESERVE impossible. Therefore, the PRESERVE VSA considers the protection of on-board ECUs with lower priority.
Measurements for Evaluation (Testing)	• Manipulation of sensor / ECU SW which is EVITA HSM enabled • Manipulation of sensor / ECU HW which is EVITA HSM enabled

Table 13: Threat: Sensor (data) manipulation

*2.3.2.4 **Integration of Malware***

Name of Threat	**Integration of Malware**
Description	Methods: • Malware delivered by mobile devices, remote update, OBD, etc. • Exploit vulnerability or implementation error • Flash malicious code to firmware Undesirable Consequences: • Components are not following standardized ITS communication behavior • Manipulation of local service information, security parameters and configurations, local station data or LDM data on the ITS-S
Network	On-Board, OBD, Backend
Asset	CCU, ECU, HU, Communications
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3], SeVeCom [1], PRE-DRIVE [9]

Identified Risk	Critical
Possible Countermeasures	• Source identification and authentication • Property authentication by using platform integrity mechanisms • Digitally sign SW updates • Include an authoritative identity in each SW update • Software authenticity and integrity can be certified if trusted OS available • Hardware-based identity and protection software; Attestation of HW and SW • Implement a Privilege Management Infrastructure
Available solution / component	• The Platform Integrity Module (PIM), Entity Authentication Module (EAM) and the Communication Control Module (CCM) of EVITA could be used to protect the integrity of in-vehicle software and possible update processes as long as the components are EVITA HSM enabled.
Relevance in PRESERVE	**Medium** • Protection of on-board SW should be considered by the PRESERVE VSA. o Basically, the SW and HW of the PRESERVE VSS itself should be protected by platform integrity mechanisms o Protection of users of the PRESERVE VSS (e.g. communication stack) may be considered by PRESERVE but cannot be guaranteed without a trusted operating system. o Protection of other on-board SW and HW is considered by the PRESERVE VSA as long as the ECUs are EVITA HSM enabled.
Measurements for Evaluation (Testing)	• Manipulate SW of the PRESERVE VSS

Table 14: Threat: Integration of Malware

2.3.2.5 Access to cryptographic private key material and credentials

Name of Threat	**Access to private key material and credentials**
Description	Methods: • Manipulation • Insertion • Deletion • Unauthorized use of private keys • Physical access using side channel attack methods • Illegal acquisition, modification or breaking of keys Undesirable Consequences: • Authorization violation: an unknown application uses security services in order to sign correctly bogus message content.

	• Extraction of private keys
Network	On-Board
Asset	CCU, Remote Update
Source (Project)	sim^{TD} [7], EVITA [3], SeVeCom [1], PRE-DRIVE [9], [25]
Identified Risk	Major
Possible Countermeasures	• Using Entity Authentication Module from EVITA project • Using secure storage module • Using sandboxes, firewalls, checkpoints in combination with a policy decision module

Available solution / component	• The Pseudonym Manager of SeVeCom could be used in combination with a Secure Storage Module (SSM) of EVITA in order to use only one of the own certificates.
	  ○ It should not be possible for a user of the security stack to spoof, impersonate or masquerade other ITS-S.
	  ○ Only one pseudonym can be used at any point in time (for a given type of application) in order to avoid Sybil attacks.
	  ○ It must not be possible that an unauthorized entity overwrites or add root CA certificates
	• The Entity Authentication Module in combination with the Policy Decision Module of EVITA could be used in order to avoid unauthorized access to the security stack and security modules that are responsible for message signing. In order to manage the access the Policy Decision Modules of EVITA could be used. Integrity protection of external SW components, which use the VSS, can only be guaranteed with presence of a trusted OS.
	• The Secure Communication Module of SeVeCom in combination with security formats as described in IEEE 1609.2 [19] should be used.

Relevance in PRESERVE	**High**
	• Sensible data such as private short-term and long-term keys have to be protected by the VSS against manipulation and extraction.
	  ○ Offline attacks are considered in order to avoid extraction of private keys from secure storage
	  ○ Protection against online attacks will not be considered in the VSA
	• Unauthorized substitution or insertion of Root CA certificates must be avoided by the PRESERVE VSS.
	• Protection against unauthorized deletion of keys or certificates is not critical as accountability on the vehicles in is not considered in the PRESERVE VSA.
	• Side channel attacks against the HSM have to be considered in the PRESERVE VSA
	• Unauthorized access and usage of the security services cannot be avoided in the PRESERVE VSA due to missing trusted operating system.

Measurements for Evaluation (Testing)	• Simple key store access must not be possible • Side channel attacks may be possible

Table 15: Threat: Access to private key material and credentials

2.3.2.6 *Manipulation of communication recording system*

Name of Threat	**Manipulation of communication recording system**
Description	Methods: • Manipulate received messages • Insert received messages • Delete received messages
Network	ITS G5A, ITS IMT Public
Asset	CCU
Source (Project)	ETSI [15], SeVeCom [1]
Identified Risk	Minor
Possible Countermeasures	• Using entity authentication module • Using secure storage module • Using sandboxes, firewalls, checkpoints in combination with a policy decision module
Available solution / component	
Relevance in PRESERVE	**Low** • The integration of an in-vehicle recording system that stores for example incoming messages will not be considered in the PRESERVE VSA
Measurements for Evaluation (Testing)	No testing necessary

Table 16: Threat: Manipulation of communication recording system

2.3.2.7 *Manipulation of backend databases*

Name of Threat	**Manipulation of back-end databases**
Description	Methods: • Send fake intrusion detection alerts to the PKI Undesirable Consequences: • Blackmailing in order to provoke possible revocation
Network	Backend
Asset	PKI
Source (Project)	ETSI [15]
Identified Risk	Major
Possible Countermeasures	• Source identification and authentication • Encryption of personal and private data

	• Perform plausibility and consistency tests on incoming messages • Using sandboxes, firewalls, checkpoints in combination with a policy decision module
Available solution / component	
Relevance in PRESERVE	**Low** • Intrusion detection and automated revocation processes will not be considered in the first design of the PRESERVE VSA
Measurements for Evaluation (Testing)	No testing necessary

Table 17: Threat: Manipulation of backend databases

2.3.3 Confidentiality Threats

"Some applications require that only the sender and the intended receiver can access the content of a message, e.g. instant messaging between vehicles. Confidentiality specifies that transported information cannot be eavesdropped on its way between sender and receiver" [20].

*2.3.3.1 **Eavesdropping of privacy relevant data***

Name of Threat	**Eavesdropping of privacy relevant data**
Description	Methods: • Listen / Eavesdropping • Intercept data • Data traffic analysis Undesirable Consequences: • Get information about vehicles traces, destinations, names, addresses, credit card numbers, etc.
Network	ITS G5A, ITS IMT Public, On-Board
Asset	Communication
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3], SeVeCom [1]
Identified Risk	Critical
Possible Countermeasures	• Encryption of private data in transmission • Use of pseudonyms that cannot be linked to long term ID or user • Using a Secure Storage Module • Using the Entity Authentication Module (EVITA)
Available solution / component	• Secure Communication Module (SCM) from SeVeCom can be used to encrypt unicast DENM. The ID & Trust Management Module of SeVeCom stores and manages the certificates of neighboring ITS-S that are needed for encryption. The SCM further uses the Cryptographic Services (CRS) of EVITA in order to encrypt and decrypt with

	hardware support. • The Entity Authentication Module in combination with the Policy Decision Module of EVITA could be used in order to avoid unauthorized access to the security manager or directly to the security modules that are responsible for message signing. In order to manage the access the Policy Decision Modules of EVITA could be used. Integrity protection of external SW components, which use the VSS, can only be guaranteed with presence of a trusted OS.
Relevance in PRESERVE	**High** • Encryption of personal and private data on transmission is necessary and required also by the PRESERVE VSA itself (e.g. pseudonym request) • Encryption of DENM payload is controlled by security classes that are used by the Secure Communication Module. • Access and usage of the encryption service directly by applications should be possible to encrypt / decrypt their specific message payload
Measurements for Evaluation (Testing)	• Send encrypted messages and try to intercept them on the transmission • Stress encryption by using changing pseudonym keys • Access the encryption security service by different applications. If the PRESERVE VSS is only accessible by the communication stack then the request for encryption has to be delegated from the application to the communication stack.

Table 18: Threat: Eavesdropping of privacy relevant data

2.3.3.2 *Interception and eavesdropping of confidential SW*

Name of Threat	**Interception and eavesdropping of confidential SW**
Description	Methods: • Intercept remote diagnosis • Intercept update processes • Eavesdrop internal communication Undesirable Consequences: • Monetary loss • Intellectual loss
Network	On-Board
Asset	Remote Update, Communication
Source (Project)	EVITA [3], SeVeCom [1]
Identified Risk	Major

Possible Countermeasures	• Encryption of software update on transmission
Available solution / component	• Communication Control Module from EVITA can be used to decrypt software updates for ECUs. This module uses the Crypto Support Module which accesses the Cryptographic Services (CRS) of EVITA in order to encrypt and decrypt with hardware support.
Relevance in PRESERVE	**Medium** • As remote updates the PRESERVE SW should be considered, the corresponding data packets must be encrypted on transmission • SW update of other on-board entities is not protected by the PRESERVE VSS in the first draft • In a second step, the VSA can be enhanced by mechanisms that consider secure SW updates of other on-board entities
Measurements for Evaluation (Testing)	• Send encrypted SW updates and try to intercept them on the transmission

Table 19: Threat: Inception and eavesdropping of confidential software

2.3.4 Privacy (Anonymity and Pseudonymity) Threats

"Privacy is an important factor for the public acceptance and successful deployment of VANETs. It means that the driver is able to keep and control the information related to the vehicle (e.g. identity of the driver, the driving behavior, the past and present location of the vehicle etc.) from other parties. Without privacy protection, VC provides a convenient way for an observer to track and identify the vehicle and its passengers, hence makes the Big Brother surveillance scenario more a reality than a fiction. But safety-related applications in VC also require trust between the communication partners, so total anonymous for privacy reason is not feasible. There are different security requirements for privacy, in this way the information of the vehicle and the driver can be protected as much as possible. For example, in "vehicle-based road condition warning", a car does not need to reveal its identity, but needs to provide its location information so that other cars can estimate e.g. the relevance of received warning messages. ***ID privacy*** *specifies how much the identity of the sender should be kept secret. Depending on the applications,* ***location privacy*** *has different levels, which range from distributing location information freely throughout the network to totally keeping it private. Although privacy requirements apply for normal communications, public authorities wishing to have access to the identity or location information of cars may have* ***jurisdictional access****"[20].*

"Privacy protection is a general requirement that relates to the protection of private information stored off-line. In the context of communication, which is the object of SeVeCom, we are interested in anonymity for the actions (messages and transactions) of the vehicles. We elaborate on the VC-specific aspects that we seek to address next.

For privacy, along with security, we focus on private vehicles (e.g., excluding emergency vehicles, buses, etc.). This is so, as the operation of all other VC nodes, including RSUs, does not raise any privacy concerns, and all those other nodes should be readily identifiable. A primary concern for VC systems is to provide location privacy, that is, prevent others (any observer) from learning past or future locations of a VC system user (vehicle driver or passenger). With

our focus on VC, we can safeguard location privacy by seeking to satisfy a more general requirement, anonymity for the vehicle message transmissions.

Ideally, it should be impossible for any observer to learn if a specific vehicle transmitted or will transmit in the future a message (more generally, take an action, that is, be involved in a VC protocol), and it should be impossible to link any two or more messages (in general, actions) of the same vehicle. Even if an observer tried to guess, that should leave only a low probability of linking a vehicle's actions or identifying it among the set of all vehicles, the anonymity set. We will elaborate on this notion when we discuss below the management of identities and credentials for VC system entities.

Rather than aiming for this strong anonymity, we require a relatively weaker level of protection: messages should not allow the identification of their sender, and two or more messages generated by the same vehicle should be difficult to link to each other. More precisely, messages produced by a vehicle over a protocol-selectable period of time, τ, can always be linked by an observer that received them. But messages m_1, m_2 generated at times t_1, t_2 such that $t_2 > t_1 + \tau$ cannot. In terms of the observer, we assume that its physical presence is bounded, as stated earlier for the adversary." [46]

*2.3.4.1 **Collect privacy sensitive data***

Name of Threat	**Collect privacy relevant data**
Description	Methods: • Data traffic analysis • Location tracking • Create vehicles traces Undesirable Consequences: • Create links between a persons and its destinations at specific time
Network	ITS G5A, ITS IMT Public
Asset	Communication
Source (Project)	sim^{TD} [7], ETSI [15], EVITA [3], SeVeCom [1], PRE-DRIVE [9]
Identified Risk	Major
Possible Countermeasures	• Use of pseudonyms that cannot be linked to long term ID, user or other pseudonyms • Using secure storage module that prevents unauthorized disclosure
Available solution / component	• Secure Communication Modules from SeVeCom can be used to sign outgoing CAM and DENM with changing pseudonym certificates. This module of SeVeCom uses the Pseudonym Manager that accesses the Cryptographic Services (CRS) of EVITA in order to access the private key of the own pseudonym certificates. • The Entity Authentication Module in combination with the Policy Decision Module of EVITA could be used in order to avoid unauthorized access to the security manager of SeVeCom or directly to the security modules that are responsible for private key management. In order to manage the access the Policy Decision Modules of EVITA

	could be used. Integrity protection of external SW components, which use the VSS, can only be guaranteed with presence of a trusted OS.
Relevance in PRESERVE	**High** • Due to requirements from PRECIOSA, changing pseudonyms are considered in the PRESERVE VSA
Measurements for Evaluation (Testing)	• Collect communication data and try to create traces • Evaluation of pseudonym change mechanisms • Try to map recorded traces to personal information (e.g. location of living and location of work)

Table 20: Threat: Collect privacy relevant data

*2.3.4.2 **Resolution of pseudonyms***

Name of Threat	**Resolution of pseudonyms**
Description	Methods: • Intercept/prevent pseudonym refill process • Get access to the PKI • Data traffic analysis • Location tracking • Create vehicle traces Undesirable Consequences: • Linking between Long Term ID and Pseudonyms • Linking between different pseudonyms from the same owner
Network	ITS G5A, ITS IMT Public, Backend
Asset	Communication
Source (Project)	sim^{TD} [7], EVITA [3], SeVeCom [1], PRE-DRIVE [9]
Identified Risk	Major
Possible Countermeasures	• Encryption pseudonym request on transmission • Using secure storage module that prevents unauthorized disclosure on the ITS-S and PKI • Split of power in the backend. A PKI entity alone is not able to disclose the link between pseudonyms and long term ID
Available solution / component	• Pseudonym Manager of SeVeCom could be adapted to request new pseudonym certificates from the PKI CA. • The public and private keys of the pseudonyms should be generated on the ITS-S and stored in the HSM. • The Entity Authentication Module in combination with the Policy Decision Module of EVITA could be used in order to avoid unauthorized access to the security manager of SeVeCom or directly to the security modules that are responsible for private key management. In order to man-

	age the access the Policy Decision Modules of EVITA could be used. Integrity protection of external SW components, which use the VSS, can only be guaranteed with presence of a trusted OS. • For the request of new pseudonym certificates privacy preserving mechanisms from PRECIOSA (V-TOKEN) [18] could be used to protect the Long Term Certificate of the ITS-S. • Splitting the PKI into Long Term CAs and Pseudonym CAs in order to avoid linking possibilities between different pseudonyms and the long term ID of an ITS-S
Relevance in PRESERVE	**High** • Due to requirements from PRECIOSA changing pseudonyms are considered in the PRESERVE VSA
Measurements for Evaluation (Testing)	• Intercept messages for the pseudonym refill on transmission. Try to create mapping between single pseudonyms • Try to create mapping between single pseudonyms at the Pseudonym CA • Try to get access to the Pseudonym CA in order to read database entries that are used for pseudonym resolution (i.e. create link between pseudonym ID and long term ID)

Table 21: Threat: Resolution of pseudonyms

*2.3.4.3 **Integration of Malware***

Name of Threat	**Integration of Malware**
Description	Methods: • Integration of malware that has access to privacy relevant data • Exploit vulnerability or implementation error
Network	On-Board, Backend
Asset	CCU, PKI
Source (Project)	EVITA [3]
Identified Risk	Minor
Possible Countermeasures	• Property authentication by using platform integrity mechanisms • Software authenticity and integrity is certified • Hardware-based identity and protection software; Attestation of HW and SW • Using sandboxes, firewalls, checkpoints in combination with a policy decision module • Implement a Privilege Management Infrastructure
Available solution / component	• Using an HSM in order to protect the private keys. • The Platform Integrity Module (PIM) of EVITA could be used to protect the integrity of the VSS software

Relevance in PRESERVE	**Medium**
	• Protection of on-board SW should be considered by the PRESERVE VSA.
	  ○ Basically, the SW and HW of the PRESERVE VSS itself should be protected by platform integrity mechanisms
	  ○ Protection of users of the PRESERVE VSS (e.g. communication stack) may be considered by PRESERVE but cannot be guaranteed without a trusted operating system.
	  ○ Protection of other on-board SW and HW is not considered by the PRESERVE VSA

Measurements for Evaluation (Testing)	• Manipulate SW of the PRESERVE VSS

Table 22: Threat: Integration of Malware

2.3.5 Accountability, Auditability and Non-repudiation Threats

"Certain application needs to track and reconstruct what was going on in the past. In our project, the non-repudiation requirement is also called auditability, by which senders or receivers can prove that messages have been received or sent respectively. For some applications, messages may only be stored for a very limited time (e.g. the last 10 seconds in a ring buffer) and made permanent only in case of an incident (e.g. crash)" [20].

2.3.5.1 Manipulation of data in the ITS Central Station

Name of Threat	**Manipulation of data in the ITS Central Station**
Description	Methods: • Manipulate database of Pseudonym CA • Manipulate traffic management in order to provoke bogus message distribution • Manipulate link between Long Term Certificate and Pseudonym Certificate in the PKI in order to avoid prosecution for motoring offences or for mounting security attacks • Exploit vulnerability or implementation error • Integration of Malware
Network	Backend
Asset	Storage
Source (Project)	sim^{TD} [7], ETSI [15]
Identified Risk	Critical
Possible Countermeasures	• Identification and authentication at access to the backend • Using sandboxes, firewalls, checkpoints in combination with a policy decision module • Implement a Privilege Management Infrastructure • Authenticity and integrity of software update is certified
Available solution / component	

Relevance in PRESERVE	**Medium**
	• Access the ICS has to be protected in general
	  ○ PRESERVE VSA considers access control for the PKI
	  ○ Access control to other third parties is not part of the PRESERVE VSA

Measurements for Evaluation (Testing)	• Try to get access to the Pseudonym CA in order to read database entries that are used for pseudonym resolution

Table 23: Threat: Manipulation of data in the ITS Central Station

2.3.5.2 *Access to key material and certificates*

Name of Threat	**Access to key material and certificates**
Description	Methods: • Extraction of private keys • Manipulation • Insertion • Deletion Undesirable Consequences: • Integrate new Root CA certificates • Substitute own private keys in order to obfuscate own vehicle behavior (i.e. in case of an accident) • Extract pseudonyms in order to cover traffic violations (e.g. start a Sybil attack)
Network	On-Board
Asset	CCU, Remote Update
Source (Project)	sim^{TD} [7], EVITA [3]
Identified Risk	Minor
Possible Countermeasures	• Authenticity and integrity of certificate update is certified • Using entity authentication module • Using secure storage module • Maintain audit log

Available solution / component	• Using the Secure Storage Module (SSM) of EVITA in order to protect the private keys.
	  ○ Import of private keys may result in higher risk for the accountability and non-repudiation
	  ○ Creating the private keys in the secure storage and ensure that these keys never leave this module would be more secure
	• Use only ECC as described in IEEE 1609.2 in order to use strong keys
	• Use Entity Authentication Module and Policy Decision Module of EVITA in order to avoid unauthorized access by entities that may overwrite or add root CA certificates

Relevance in PRESERVE	**Medium** • Access to the private keys on all ITS-S has to be protected by HSM. • Extraction of private keys from other ITS-S. Extraction of own private keys is not considered in the first draft of the VSA. • The use of cryptographic security services is not protected by the VSA. Authentication and authorization of components, modules or applications cannot be verified due to missing trusted OS.
Measurements for Evaluation (Testing)	• Verify that the private keys on the ITS-S cannot be substituted or exchanged remotely.

Table 24: Threat: Access to key material and certificates

2.3.5.3 *Repudiation of message transmission and receipt*

Name of Threat	**Repudiation of message transmission and receipt**
Description	Methods: • Manipulate and spoof GNSS positioning signal • Spoofing • Impersonate • Masquerade Undesirable Consequences: • Manipulate a communication recording system in order to cover traffic violations
Network	ITS G5A, ITS IMT Public, GNSS
Asset	Communication
Source (Project)	ETSI [15], SeVeCom [1]
Identified Risk	Major
Possible Countermeasures	• Using entity authentication module • Using secure storage module • Maintain audit log (communication recording system) • Enable location authentication by signing GNSS data • Use broadcast time (UTC or GNSS) • Use Inertial Navigation System (INS) or dead-reckoning • Implement differential monitoring on the GNSS
Available solution / component	
Relevance in PRESERVE	**Low** • The integration of an in-vehicle communication recording system will not be considered in the first design of the PRESERVE VSA

Measurements for Evaluation (Testing)	No testing necessary

Table 25: Threat: Repudiation of message transmission and receipt

2.4 Problem Areas

- Intrinsic high density of ITS message traffic due to broadcasting and beaconing in V2V systems.
- Lack of flow control in V2V broadcast messaging.
- Absence of addressing in broadcast messages meaning source cannot be identified so malicious and irrelevant messages can only be rejected by the application, not at the network layer in the ITS stack.
- The sub-optimal use of the available bandwidth caused by the random re-attempt period in the "Listen before send" message transmission method.
- Inability of the ITS-S (Vehicle) to quickly detect and isolate interference on radio channels.
- CAM and DENM messages do not include any form of identification information.
- Vehicle-to-Vehicle messages include no validation or legitimacy checks.
- Uncertainty regarding how timestamps are created and how to use them to check the validity of messages.
- ITS-S (Vehicle) memory can be modified by information received over the air interface.
- Broadcast messages are in general intended for all ITS-S within range.

2.5 Possible Countermeasures

Description of countermeasure	Considers ITS problem area	Source (Project)
Reduce frequency of V2X messages	High density of V2X messages (DoS)	ETSI [15]
Node identification and authentication. Receiver should be able to verify the unique ID of the sender / originator / forwarder	Spoofing, Impersonation, Masquerade	ETSI [15], SeVeCom [1]
Property authentication by using platform integrity mechanisms	Distinct functions / actions need authorization of the sender	SeVeCom [1]
Enable location authentication by signing GNSS data	Manipulation of GNSS signal in order to enable replay attacks	SeVeCom [1]
V2X Message exchange via infrastructure only if in communication range	Flow control in V2V broadcast messaging and high density of V2X messages (DoS)	ETSI [15], SeVeCom [1]
Implement frequency agility – CDMA/spread-spectrum system	Jamming of G5A	ETSI [15]
Integrate ITS-IMT Public	Jamming of G5A, misbehavior detection	ETSI [15]
Digitally sign each message - Symmetric - Asymmetric	- Prevent false message injection - Remove misbehaving ITS stations - Avoid presentation of personal data as ID	ETSI [15], SeVeCom [1], PRE-DRIVE [9]
Include a non-cryptographic	Reduces the risk of unnoticed	ETSI [15]

checksum	message corruptions (accidentally modifications en route)	
Include an authoritative identity in each message	- Check authenticity of messages - Ability to record message in order to present the message to authority afterwards	ETSI [15], SeVeCom [1], PRE-DRIVE [9]
Use broadcast time (UTC or GNSS)	Addresses relay attacks. If time is not cryptographically bound then replay attacks are still possible	ETSI [15]
Include sequence numbers in each message	Addresses replay attacks. If sequence number is not cryptographically bound then replay attacks are still possible	ETSI [15]
Use Inertial Navigation System (INS) or dead-reckoning	Removes the possibility of GNSS spoofing	ETSI [15]
Implement differential monitoring on the GNSS	Aid to check validity of messages and to synchronize the source of the timestamp creation	ETSI [15]
Encryption of personal and private data on transmission	Protects data in unicast transmissions	ETSI [15], SeVeCom [1], PRE-DRIVE [9]
Implement a Privilege Management Infrastructure (PMI)	Protects against the installation of malware and malicious modification of configurations	ETSI [15]
Software authenticity and integrity is certified	Restriction which SW can run on the ITS-S	ETSI [15]
Use of pseudonyms that cannot be linked to long term ID or user.	- User cannot be identified by analysis of V2X messages - Association of service use with users becomes challenging	ETSI [15], SeVeCom [1], PRE-DRIVE [9]
Maintain audit log (communication recording system)	Makes non-repudiation for sent and received V2X messages possible	ETSI [15], SeVeCom [1]
Perform plausibility and consistency tests on incoming messages.	- Restricts possibilities for malicious message injection - Reduce the risk of wormhole attacks - May reduce the risk of Sybil attacks	ETSI [15], SeVeCom [1]
Revocation Remote deactivation of misbehaving ITS-S	Eviction of misbehaving or unregistered ITS-S	ETSI [15], SeVeCom [1]
Hardware-based identity and protection software. Attestation of HW and SW	Secure storage and maintenance of software, OS and platform configuration Extraction of long term and short term IDs	ETSI [15], SeVeCom [1], PRE-DRIVE [9]
Using sandboxes, firewalls,	Authorization violation	ETSI [15],

checkpoints in combination with a policy decision module		SeVeCom [1]
Using secure storage module that prevents unauthorized disclosure, detects any unauthorized data manipulation and detects any replay attacks	Authorization violation against stored key material	EVITA [3], PRE-DRIVE [9]
Using entity authentication module using user, roles and device identification and authentication	Authorization violation against usage of cryptographic services	EVITA [3]

Table 26: Countermeasures

3 Requirements

3.1 Performance Requirements

There are no simple answers to the question what the requirements are as V2X provides a very challenging and complex environment. At the moment, you can only make a well educated guess about many values as large-scale measurements are missing. It is expected that the on-going FOTs and pilots will provide results to refine the basic requirements discussed herein. Until then, we will base our work on reasonable and well-motivated assumptions derived from theoretical models, simulations, and simple measurements as presented here.

For ITS communication there are currently 3 frequency channels specified and in principle a suitable dual- or multiple-radio OBU can send or receive in parallel on all those frequencies. In the worst case, this linearly scales the number of packets that can be sent or received and that need to be processed by the VSS. However, due to the different nature of communication on different channels (safety vs. efficiency vs. comfort), the profiles will not be comparable. It is likely that the large amount of broadcast communication on the control channel will create the highest load (from a security perspective) there. We focus our following discussion on a one-channel scenario with control-channel communication where mostly only CAM and DENM messages are sent.

3.1.1 Metrics

In this section we first list a number of performance metrics going from general and more communication oriented metrics to more security specific requirements where one can ideally derive the later directly from the former. Those will be the metrics by which we specify the performance requirements.

*3.1.1.1 **System Configuration Parameters***

3.1.1.1.1 Certificate Cache Lookup Effectiveness

CLE (0 ≤ CLE ≤ 1): The effectiveness of the certificate lookup, determined by the cache size.

*3.1.1.2 **Packet Processing Rates***

3.1.1.2.1 Outgoing Packets per Second

OPPS (1/s): Here we measure the number of packets per second that are sent by an ITS station and that need to be processed by the VSS.

3.1.1.2.2 Packet Signature Generations per Second

SGPS (1/s): For every packet send, one needs to generate a suitable signature, i.e. SGPS = OPSS. Note that we assume that every packet needs to be signed, which is true at least for CAMs and DENMs, if we don't apply omission schemes as outlined in [26] [33] [34] [39].

3.1.1.2.3 Incoming Packets per Second

IPPS (1/s): Here we consider the number of packets per second that are received by an ITS station and that need to be processed by the VSS.

3.1.1.2.4 Packet Signature Verifications per Second

SVPS (1/s): For every signed packet received, one needs to verify the signature plus (potentially) the certificate. Assuming that a certain fraction of packets contain yet unverified certificates, we get:

SVPS = (1 + CLE) IPSS, 0 <= CLE <= 1

*3.1.1.3 **Packet Processing Delays***

3.1.1.3.1 Transmission Delay

TD (ms): The "airtime" of a packet measured in ms.

3.1.1.3.2 Outgoing Communication Delay

OCD (ms): The time that the stack needs to transmit a packet. Note, again, that because of the reasons given above, this can only be a statistical value.

3.1.1.3.3 Signature Generation Delay

SGD (ms): The delay for generating one packet signature. This includes calculating a hash (HD) plus performing the actual digital signature generation operation.

SGD = HD + SD

HD = Hash Delay, SD = Signing Delay

Both values include all internal delays of the VSS, e.g., the times to load keys and the time to transfer messages or other data into the HSM or out of it.

3.1.1.3.4 Outgoing Packet Delay

OPD (ms): To satisfy overall delay requirements (which are application specific), an outgoing packet should be sent by an ITS station within a bounded delay measured from the time the application submits the data to a SAP to the time the last bit of a packet is sent out. As we are not assuming a real-time system to be in place and as network access is only probabilistic, this can only be a statistical measure providing a certain confidence interval. For security, we consider the delay only for packets that need to be processed by the VSS, e.g., in order to attach security payload. We get:

OPD = OCD + SGD

3.1.1.3.5 Incoming Communication Delay

ICD (ms): The delay needed by the communication stack (without security processing) to deliver a message to the application or facilities SAP where it is ready for processing.

3.1.1.3.6 Signature Verification Delay

SVD (ms): The delay for verifying one packet signature. This includes calculating a hash (HD) plus performing the actual digital signature verification operation. Furthermore, for a certain fraction CLE of packets, one needs to verify the certificate which is assumed to take the same amount of time as verifying the signature itself. Therefore, we get:

SVD = (1 + CLE)(HD + VD) + (1 - CLE) CLD

HD = Hash Delay, VD = Verification Delay, CLD = Certificate Cache Lookup Delay

3.1.1.3.7 Incoming Packet Delay

IPD (ms): To satisfy overall delay requirements (which are application specific), an incoming packet should be available to an ITS application within a bounded delay measured from the time the last bit of the packet is received from the radio link to the time the packet is accessible to the application. For security, we consider the delay only for packets that need to be processed by the VSS, e.g., in order to verify security payload. We get:

IPD = ICD + SVD

3.1.1.3.8 Packet Delay

PD (ms): The overall delay of a packet sent from an application or facility until it is received by a corresponding application or facility in a receiving vehicle measured from SAP to SAP. We get:

PD = OPD + TD + IPD

*3.1.1.4 **Other Metrics***

3.1.1.4.1 Pseudonym Change Delay

PCD (ms): The additional delay introduced when the ITS station switches from one pseudonym to another. Measured as additional time added to a packet stream sent at maximum rate.

3.1.2 Approach

When trying to come up with specific values for the metrics listed above, one could take different approaches. One could, for example, aim for average or worst-case values or could derive data from theoretical analysis, simulations, or measurements.

For the purpose of this report, we will first provide different worst-case estimations. As our VSS should scale well and also operate reliably under high-load situations, we need to identify what maximum load will occur under operation. Maximum load usually occurs in dense traffic and situations where a lot of communications take place and the communication channel is saturated (e.g., maximum CAM rate + DENMs triggered by events). We assume that if the VSS and HSM can handle maximum load in terms of packet rates and delay requirements, it will also adapt to scenarios with lower load requirements. Where system dimensioned for a maximum load does not seem implementable or too costly, we will discuss separately why we have chosen a different value as requirement. If proposing adaptive schemes, one should ensure that this adaptation works reliably in the full range of scenarios.

Note that in this version of the document we are not considering load control mechanisms like Transmit Power Control (TPC), adaptive beaconing, or Clear Channel Assessment (CCA) threshold adaptation [35] [36], which again will influence the load experienced by the VSS.

To approach the problem from different angles, we first start with a theoretically derived maximum channel load scenario that defines the upper boundary that an IEEE 802.11p with a 6 MHz channel can process. Next, we discuss various publications in literature that discussed the issue of broadcast bandwidth in IVC. We also provide an own load estimation for a standard scenario and a maximum load scenario for urban and highway traffic where similar scenarios are also used in the project sim^{TD} for their load analysis. Finally, we provide some simulation results and look at preliminary load measurements performed in some FOT projects.

3.1.3 Worst-Case Estimate

Schoch, e.a. [26] give a worst case approximation of the number of packets that two stations can exchange via IEEE 802.11p. According to them, a theoretical of roughly 2200 packets per second can be received, if one vehicle sends to exactly one other vehicle and no collision occurs. This assumes packets with a payload of 221 bytes (30 bytes application payload, 181 bytes security payload). As no single sender in a V2X scenario would send 2200 packets per

second, this rate will not be achieved in practice, as one definitely has to consider collisions and other effects. Still, it is an interesting upper bound.

3.1.4 Theoretical Analysis

[27] provides a formal Markov-chain-based model discussing broadcast delivery in a VANET setting. Unfortunately, their evaluation does not fix various parameters so that no direct results can be derived for our purposes. However, it at least underlines the assumption from the previous section that a larger number of senders will inevitably lead to packet loss and that for typical settings, a number of 200 senders may lead to 80% of the packets being lost.

[28] also discusses achievable packet rates, comparing an analytical model with simulations. Unfortunately, the authors focus on 24 and 54 Mbps data rates, which are not in line with our assumed data rate of 6 Mbps. Still, it can be derived that typical delay for transmitting a packet (OCD + TD) is below 2 ms and should thus be negligible. We also see a significant drop in packet reception rates as node density increases.

Vinel also conducted various studies on broadcast in VANETs together with various co-authors. [29] provides “a simple analytical model for the periodic broadcasting in vehicular ad-hoc networks”. Based on this work and assuming 50 senders, one can expect for a higher load (2,000 packets/s) a packet reception probability of 50 to 80% (depending on bit error rate). The actual packet rates are thus between 1,000 and 1,600 packets/s. For even higher load (3,000 packets/s), the actual received packets stay at this level as collisions destroy all additional packets being sent. Higher numbers of senders (above 50) will likely even decrease this value. [29] also analyses typical transmission delay and founds it to be below 3 ms in the analyzed scenarios.

[30] additionally looks at the saturation case with higher numbers of vehicles. For a set of vehicles between 50 and 75, it shows that the packet reception rate quickly drops to zero, independent of the bit error rate. Likewise, transmission delay reaches 8.1 ms.

[37] describes another interesting effect. With high traffic density and under high channel load, the possible communication range can get reduced by up to 90%. So while communication remains possible with close-by vehicles, vehicles hardly receive any packets from more remote vehicles. This of course also effectively reduces the number of packets that are received and need to be processed. Simulations in [37] show that a vehicle only reliably receives data packets of 200 Bytes size up to 300 m. At larger distances, the reception probability drops sharply to values of 40% or below. Similar analysis in [38] shows the effect that communication range has on update delay. The probability of informing vehicles reliably about positions of other vehicles within a delay of one second or less is below 10% for dense traffic and beacon rates of 8 Hz. This all indicates that the communication system can easily get overloaded and would react with sharp increase in packet drops. However, this does not reliably answer the question whether packet rates in the order of 1,000 to 1,600 can realistically be expected or not.

In the next section we want therefore to analyze, whether the packet rates discussed above can actually occur in realistic driving scenarios, to see whether this performance is really required.

3.1.5 Load Scenarios

In order to discuss functional requirements it is useful to define different load scenarios that should be considered by PRESERVE. In the following list a standard scenario and a maximum load scenario is discussed. Similar scenarios are used in the project sim^{TD}. The functional use-cases described in Section 1.2 are not related to specific load scenarios. However, some functions related to urban traffic such as Intersection Collision Warnings will not be transmitted in highway load scenarios.

3.1.5.1 Standard urban load scenario (SUL)

- ITS-S station drives with 60 km/h in an urban environment

- 10 other ITS-S are inside the communication range
- ITS-S station sends 5 CAMs per second (assuming 60 km/h and some speed/direction changes and considering CAM generation rules of ETSI TS Annex-B [11])
- No special events
- 50 incoming V2X messages per second have to be processed
- 5 outgoing V2X messages per second have to be processed
- Processing time per packet: 18 ms

3.1.5.2 Maximum urban load scenario (MUL)

- ITS-S station drives with 60 km/h in an urban environment
- 50 other ITS-S are inside the communication range
- ITS-S station sends 10 CAMs per second (assuming 60 km/h and heavy speed/direction changes and considering CAM generation rules of ETSI TS Annex-B [11])
- Several special events that result generation and reception of different DENMs
- ITS-S station sends 5 DENMs per second
- 750 incoming V2X messages per second have to be processed
- 15 outgoing V2X messages per second have to be processed
- Processing time per packet: 1.3 ms

3.1.5.3 Standard highway load scenario (SHL)

- Highway with two lanes per direction
- ITS-S station drives with 100 km/h on a highway with traffic density of 1800 vehicles per hour per lane (about 0.5 vehicles per lane per second)
- 80 other ITS-S are inside the communication range
- No special events
- ITS-S station sends 6 CAMs per second (assuming 100 km/h and few speed/direction changes and considering CAM generation rules of ETSI TS Annex-B [11])
- 480 incoming V2X messages per second have to be processed
- 6 outgoing V2X messages per second have to be processed
- Processing time per packet: 2 ms

3.1.5.4 Maximum highway load scenario (MHL)

- Highway with three lanes per direction
- ITS-S station drives with 100 km/h on a highway with traffic density of 2600 vehicles per hour per lane (about 0.7 vehicles per lane per second)
- 150 other ITS-S are inside the communication range
- ITS-S station sends 10 CAMs per second (assuming 100 km/h and heavy speed/direction changes and considering CAM generation rules of ETSI TS Annex-B [11])
- Several special events that result generation and reception of different DENMs
- ITS-S station sends 5 DENMs per second
- 2250 incoming V2X messages per second have to be processed
- 15 outgoing V2X messages per second have to be processed
- Processing time per packet: 0.4 ms

3.1.6 Simulations and Measurements

We also conducted some simulations to analyses expected packet reception rates. For this, we use the UUlm distribution of JiST/SWANS in version 1.2. The scenario consists of a 353m x 353m empty field and a variable number of vehicles positioned in a grid covering the entirety of the field. We use simulated 802.11p class C radio units (transmission power of 20 dBm), which

yields a delivery rate of approximately 99.9% when communicating between any two nodes in the grid with a free channel. We further configured the simulation to use additive noise, Rayleigh fading, and the two-ray ground reflection model to simulate signal propagation. The application we run in this setup is a simple CAM broadcasting scheme at 10 Hz with a jitter of up to 100 ms. The size of each CAM is 191 bytes. The nominal transmission rate is set to 6 Mbps. Each simulation runs for one minute simulation time and we repeat each setup 30 times with different random seeds. Instead of using averages we selected the maximum number of successfully delivered packets in a single vehicle because we are interested to find an approximation of peak values. The nodes were positioned statically without any mobility during the entire simulation run. Figure 7 shows a peak packet rate slightly above 950 packets per second at around 120 nodes and afterwards the effectively received packets decline again due to collisions. So this seems to indicate that the actually achievable packet rate is more at the lower bound of the range discussed in Section 3.3.

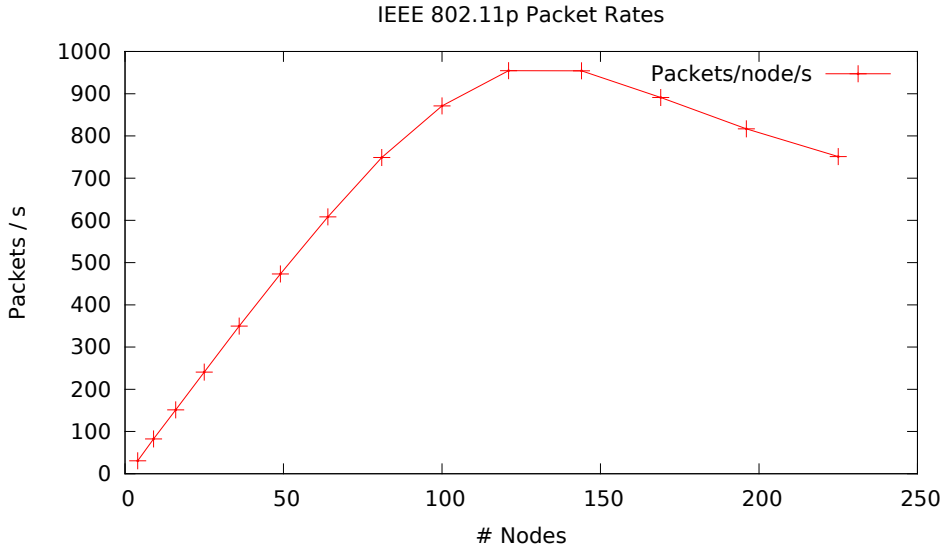

Figure 7: Packets received per node and second

We are currently also conducting first measurements with a small number of units that were not ready by the time of writing this report. A later update will be provided. Meanwhile, [14] indicates that results from simulations in [37] can also be transferred to real-world communication scenarios at least with a small number of units.

3.1.7 Cryptographic processing

We also want to take into consideration existing work on cryptographic performance in OBUs. Petit [31] directly investigates the impact of cryptographic on communication. Based on experiments with ECDSA libraries, signature generation takes between 2.5 and 3.3 ms and verification between 5 and 6.6 ms (depending on key size). This is found to be considerably larger than the transfer delay which can be neglected. However, this 10 ms crypto delay is found to be a relevant factor that can significantly delay a warning to a driver and translates to an additional braking distance of around 30%. One should also note that crypto delay was measured on a rather powerful desktop computer (Pentium D 3.4 GHz), which is likely not representative to what can be expected in the first generation of vehicular OBUs.

[32] extends this analysis and also discusses the effect of higher vehicle densities. Due to the high number of packets to be processed, delays for processing a specific packet can easily reach an order of one second, which is clearly unacceptable as packets queue up waiting to be processed.

In SAE-2011-01-0584 [33], Krishnan and Weimerskirch present some cryptographic measurements performed on a realistic OBU (Denso WSU). For two WSUs communication at 10 beacons / second, signature generation delays for ECC-256 is 6.6 ms while verification is

measured at 28.5 ms (on a system also running safety applications). Again, this will likely increase significantly if packets have to be queued.

Regarding delays, D21.4 of sim^{TD} [6] describes in section 2.5.4 different traffic classes in order to let the applications select the appropriate level of relevance, reliability and latency. For latency three different general classes are offered: *latency < 50 ms*, *latency < 100 ms* and *best effort*. As the communications security is integrated on senders and receivers side the delay introduced by the PRESERVE crypto should matching the traffic classes. As discussed in the PRE-DRIVE security architecture [9], the performance of the ITS-S processing may not be equal. This needs to be taken into consideration when integrating the PRESERVE VSS on a host platform.
As defined in ETSI TS 102 637-2 [11] the latency of CAM generation must not exceed 100 ms. The latency for data acquisition must be lower than 50 ms and the distribution process must be faster than 50 ms, which includes the security processes on both the receiving and the sending side.
As defined in ETSI TS102 637-4 [13] the "maximum end to end latency time measured at the receiving ITS station facilities layer shall be less than 100 milliseconds" - this includes signing, sending, receiving, verifying and passing the communication stack in both directions.

It is therefore safe to assume 50 ms as an upper bound transmission delay that for most messages while the share available for cryptographic processing remains to be confirmed.

3.1.8 Performance Conclusions and Requirements

What can be deduced from this discussion for our VSS requirements? From a worst-case perspective, one should assume around 2,200 packets per second as a maximum, given a packet size of around 200 bytes payload and one 6 Mbps radio.

Based on the theoretical models that we looked at, one should expect incoming packet rates between 1,000 and 1,600 packets per second; however the simulation results clearly indicate that the result is probably closer to 1000 or even below. Note that we have not looked yet at effects that adaptive beaconing rate, transmit power control, and CCA threshold adaptation can have on these numbers.

The different driving scenarios we looked into indicate that in most driving situations (SUL, MUL, and SHL) the packet rates do not exceed 750 packets per second. Only the maximum highway scenario (MHL) goes well beyond this value (2,265 packets per second). However, in this case the limits of the communication channel will limit the achievable rate to a value well below this.

For the further discussion, we assume a preliminary maximum value of 1,000 signature generations / verifications to be realistic, as higher numbers will likely not be achieved in FOTs and pilot tests due to limits in equipped vehicles and equipment rate in general. We clearly note that the focus of PRESERVE lies on FOTs and pilots. For a later deployment of products, one might have to adjust this value upwards. However, it is one objective of the testing to be performed in PRESERVE WP3 to identify exactly what this higher value might be by contributing actual measurements.

Delay for processing a single packet is composed of a transmission delay (below 2 ms on a non-saturated channel) and a cryptographic delay between 10 ms and 33 ms (depending on the cryptographic software/hardware in place). This seems to be well in-line with requirements of application that have a delay requirement of 50 ms or higher. However, if packets need to be queued for transmission or cryptographic processing, the delay can get much long and be even in the order of seconds. To prevent such queues from building up, one needs to cryptographically process at wire speed, leaving about 1 ms per incoming or outgoing packet.

Processing 1,000 packets per second and processing each in 1 ms can hardly be met by current hardware. As discussed in [32], a Pentium D 3.4 GHz processor needs about 5 times as long for a verification (which is the most time-consuming operation in cryptographic processing overhead) and a typical OBU even 26 times as long. This is a good indication that a dedicated

cryptographic co-processor is likely to be necessary. Alternatively, one has to apply efficiency strategies like the ones presented in [26] or [33].

The testing of PRESERVE WP3 will analyze this question in a more detail and provide a more definitive answer on the requirements for future products. For now, let's come back to the initial metrics and try to derive some design requirements for WP2.

Metric	Requirement	Explanation
CLE	0.05 /s	*Certificate Cache Lookup Effectiveness:* We don't have reliable analysis here. This needs to be looked into. For the time being, having about 5% of the certificates come from new vehicles and requiring an extra certificate check seem reasonable.
OPPS	≤ 15 /s	*Outgoing Packets Per Second:* Based on the MUL/SHL load scenario provided.
SGPS	15 /s	*Signature Generations per Second:* OPSS
IPPS	1.000 /s	*Incoming Packets per Second:* As motivated in the conclusions.
SVPS	1.050 /s	*Signature Verifications per Second: SVPS = (1 + CLE) IPSS*. Note that, e.g., the EVITA FPGA solution is able to perform around 400 signature operations per second [4].
PD	50 ms	*Packet Delay:* delay for end-to-end transmission of a packet. See discussion in Section 3.1.7
TD	1 ms	*Transmission Delay:* Actual transmission is very fast. Maximum airtime of short packets is below 1 ms.
OCD	7 ms	*Outgoing Communication Delay:* Assuming no or only very short queuing of packets.
SGD	7 ms	*Signature Generation Delay:* This is what remains available for verification.
OPD	14 ms	*Outgoing Packet Delay: OPD=OCD+SGD.* We assume majority of delay created on recipient side.
ICD	1 ms	*Incoming Communication Delay:* No queuing involved here, so processing the packet in the stack should be instantaneous.
SVD	34 ms (1 ms)	*Signature Verification Delay:* *SVD = (1 + CLE)(HD + VD) + (1 - CLE) CLD* Specific measurements to be performed will provide actual measurements on the values of Hash Delay (HD), Verification Delay (VD), and Certificate Cache Lookup Delay (CLD). See also note on IPD.
IPD	35 ms	*Incoming Packet Delay:* We assume majority of delay created on recipient side. Note that while this is ok for a packet to meet application delay requirements, the average processing time per packet must not exceed 1 ms if sequential processing is assumed. On the other hand, only a fraction of traffic will be highest traffic class, so this will be a little more relaxed in practice. Exact value determines on the traffic mix.

PCD	50 ms - IPD-OPD	*Pseudonym Change Delay:* Pseudonym changes should not lead to a violation of overall delay requirements. We suggest using a pseudonym change strategy that changes pseudonyms only in situations of low load and circumvents this problem.

A combination of analytical modeling, detailed simulation evaluation, and experimentation has been presented in a line of work that goes beyond the basic cryptographic protection. The cost of cryptographic operations, the effect on channel reception, and the overall effect of security and privacy enhancing solutions on the effectiveness of the vehicular communication applications has been investigated in [48], [47], [34]. Initially, considering cost reduction techniques and safety applications, it was shown that secured systems can support nearly as effectively safety applications [48], [47]. The framework of investigation was extended with analytical models that allow estimating how to provision processing power for future systems depending on future cryptographic primitives and their (increasing) cost [34]. Moreover, data floating applications, on top of the safety ones, were investigated [34]. An experimental investigation for secure geo-cast [50], followed by an extended one with analysis and simulations, corroborates the usefulness of overhead reduction schemes and the role of on-board processing power for scalability [49]. The dissemination of information across multiple hops can impose overhead on nodes that do not necessarily benefit or are immediately relevant to the received messages; strategies to adaptively reduce this overhead without compromising security has been investigated in [51]. [52].

3.1.9 Metrics not considered herein

There are a couple of other metrics that could be considered and discussed, but that left out of the discussion for brevity.

The pseudonym system considered by current proposals requires the regular generation of new ECC key-pairs when requiring new pseudonyms. The secret keys need to be generated and stored by the HSM. So the rate and delay with which keys can be generated becomes relevant. In the US PKI approach [23], the pseudonyms must change every 5 minutes. Therefore, 288 pseudonym certificates would be needed per day and thus approximately 60 seconds would be needed for key generation every day assuming a key generation time of 5 ms. The C2C-CC [24] proposes a less strict concept which does not need as much as pseudonym certificates per day. In general, one should aim at an approach where verification of safety messages has priority and other operations are performed only in situations of low load.

If the HSM includes a Trusted Computing device that performs integrity measurements of the system, one should furthermore specify, how should address the delay created by these measurements.

3.2 Requirements from the PRESERVE VSS

The following table shows the requirements of the PRESERVE VSS. Therefore those requirements have to be fulfilled for being able to use the PRESERVE VSS. The security itself needs for example access to the ITS stations status information or to the communications. The security use cases in Table 27 are not related to V2X communication use cases presented in Table 1 that aims to enhance traffic safety and efficiency. However, in WP2 these requirements have to be considered in order to allow the VSS to exchange security related data.

Requirement	Description of requirement	Source (Project)
ITS G5A	Data connection to the backend. The security system needs access to the communication stack in order to send and receive V2X messages (DENMs)	OVERSEE [10]

	Security Use Cases: • Pseudonym refill • Update of security profiles / policies	
ITS IMT Public	Data connection to the backend. The security system needs access to the communication stack in order to send and receive IP messages. • It must be possible to establish the connection from the external entity • Vehicle cannot be accessed from external. The vehicle has to establish the connection. Security Use Cases: • Pseudonym refill • Update of security profiles / policies • Software update	OVERSEE [10]

On-Board,	Own mobility data has to be accessible. The security needs reading access to the vehicles internal bus communication. In IEEE 1609.2 v2-d6 SAPs are described for this data exchange.
	
	• Vehicle's geographical position with latitude, longitude and elevation
	  ○ GNSS (GPS)
	  ○ Enhanced by vehicle movement (enhanced positioning)
	• Consistent and synchronized time as absolute value in milliseconds
	
	Security Use Cases:
	
	• Enable strategies for pseudonym change based on own vehicle behavior
	• Verification of pseudonym validity that have geographical restrictions
	• Verification of mobility data of received messages
		OVERSEE [10], IEEE 1609.2 v2-d6 [19]

Table 27: Requirements from the PRESERVE VSS

3.3 Requirements for the PRESERVE VSS

3.3.1 Technical and Functional Requirements

In this section the requirements from applications and systems regarding the PRESERVE VSS are collected. Non-technical requirements should be neglected in the following table.

Requirement	Important for	Project
Signing of outgoing V2X messages • In [4], Section 4.2.3.1 it is stated that the ECDSA engine is able to generate / verify around 200 signatures (ECC-256) per second → approximately latency of 5 ms per message.	Applications running on the ITS-S	EVITA [4], PRE-DRIVE [9], C2C-CC
Verification of incoming V2X messages • Although verification of incoming messages is more critical than signing, EVITA has not stated the maximum number of verification tasks per second.	Applications running on the ITS-S	PRE-DRIVE [9], C2C-CC
Generation of ECC keys • In [4] section 4.2.3.1 it is stated that the asymmetric cryptographic engine is able to generate / verify around 200 signatures per second. As generation of ECC keys is the first step of ECDSA, it may need 200 generations of ECC keys per second. • In the US PKI [23] approach the pseudonyms must change every 5 minutes. Therefore, 288 pseudonym certificates would be needed per day → approx. 60 seconds would be needed for key generation every day assuming a key generation time of 5 ms. • The C2C-CC [24] proposes a less strict concept which does not need as much as pseudonym certificates per day.	PRESERVE security architecture	EVITA [4], US DoT [23], C2C-CC [24]
Minimum overhead • Minimum security sacrifice, maximum overhead saving	G5A communication link	C2C-CC, PRE-DRIVE [9]
Low latencies • Signing • Verification • Encryption • Decryption • Pseudonym refill process	Applications running on the ITS-S	sim^{TD} [6], PRE-DRIVE [9], ETSI [11], ETSI [13]

• Interface access (Authorization of interface users) As described in D21.4 of sim^{TD} in section 2.5.4 different traffic classes are provided by the communication stack in order to let the applications select the appropriate level of relevance, reliability and latency. For latency three different general classes are offered: *latency < 50 ms*, *latency < 100 ms* and *best effort*. As the communications security is integrated on senders and receivers side the delay introduced by the PRESERVE crypto should matching the traffic classes. As discussed in PRE-DRIVE the performance of the ITS-S processing may not be equal. Therefore, minimum system requirements of the host should be defined in PRESERVE. As defined in [11] the latency of CAM generation must not exceed 100 ms. The latency for data acquisition must be lower than 50 ms and the distribution process must be faster than 50 ms, which includes the security processes. As defined in [13] the "maximum end to end latency time measured at the receiving ITS station facilities layer shall be less than 100 milliseconds" - this includes signing, sending, receiving, verifying and passing the communication stack in both directions.		
Simple to integrate and use • Certification, bootstrapping and decommissioning of needed crypto HW is important for supplier and manufacturer • Plug and play	Communication stack and applications running on the ITS-S	Audi, Denso
Flexibility of integration • Integration on network layer or facilities layer possible • The PRESERVE-API shall grant access to all PRESERVE facilities independently of their concrete implementation and location in the vehicular system. • Solutions can be easily deployed and flexibly tailored • Low package requirements • Support e.g. "here I am" (HIM) devices	Communication stack and applications running on the ITS-S	OVERSEE [10], C2C-CC, Audi, Denso

or iPhone, Android, navigation device, etc. (not all devices will have the same security capabilities) • Must fit into design, production, maintenance, administrative processes of OEMs, suppliers, administrations, workshops, ...		
Security management • Management of security processes • Error handling	Deployment and re-usability	OVERSEE [10]
Temperature resistance and shock resistance according to automotive requirements • Considering industry standards • *Automotive grade* crypto hardware	Deployment and FOTs	OVERSEE [10], Daimler
Dimensions of the HW should consider automotive requirements • Considering industry standards	Deployment	OVERSEE [10]
Ability to test VSS	Deployment	

Table 28: Technical and Functional Requirements for the VSS

3.3.2 Non-Technical and Non-Functional Requirements

Requirement	Important for	Project
Cost effective • Expensive solutions will not make it to the market • Efficient solutions keep economic aspects in mind	Deployment	ETSI, C2C-CC [24], Audi, Daimler, Denso
Compatibility regarding a global security solution (US/EU/JP) • Make security and privacy an *integral part of ITS* • VSA/VSS must align with existing and on-going standardization	Deployment and re-usability	Audi, Denso
Legal issues • Exporting crypto • IPRs	Deployment	Denso

Privacy • Protection and obfuscation of drivers location • Protection against collection of vehicle traces	Deployment	ETSI, C2C-CC

Table 29: List of non-functional and non-technical requirements that should be considered by the PRESERVE security architecture

4 Conclusions and Outlook

Based on the different project results we were able to derive the security and functional requirements that our PRESERVE Vehicle Security Architecture (VSA) has to satisfy. Additional performance requirements regarding the Hardware Security Module (HSM) were estimated – based on the usage scenarios. The performance assumptions for the HSM are crucial requirements regarding the development process of this custom Application-Specific Integrated Circuit (ASIC).

Based on the collected requirements in the next step the architecture of the Vehicle Security Solution (VSS) will be created.

5 References

[1] R. Kroh, A. Kung, and F. Kargl, "SEVECOM - D1.1 - VANETS Security Requirements," 2006.

[2] T. Benz, et al., "PRECIOSA D1 V2X Privacy Issue Analysis," 2009.

[3] A. Ruddle, et al., "EVITA - D2.3 - Security requirements for automotive on-board networks based," 2009.

[4] B. Weyl, et al., "EVITA - D3.2 - Secure On-board Architecture Specification," 2011.

[5] H. Stübing, et al., "simTD - D21.2 - Spezifikation der IT-Sicherheitslösung," Delivable, 2009.

[6] A. Hiller, et al., "simTD - D21.4 - Spezifikation der Kommunikationsprotokolle, Appendix 3: Functional Description and Base Specification of SIM-NET," 2009.

[7] M. Mattheß, et al., "simTD - D21.5 - Spezifikation der IT-Sicherheitslösung," 2009.

[8] J. Schütte, et al., "simTD - D22.3 - Fahrzeugseitige IT-Sicherheitsarchitektur," Deliverable, February 2010.

[9] M. Gerlach, et al., "PRE-DRIVE C2X - D1.3 - Security Architecture," 2009.

[10] G. Rafael and A. Crespo, "OVERSEE - D1.4 - Functional Requirements Analysis," 2010.

[11] ETSI TS 102 637-2, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service V1.1.1," ETSI Technical Specification ETSI TS 102 637-2, April 2010.

[12] ETSI TS 102 637-3, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service V1.1.1," ETSI Technical Specification ETSI TS 102 637-3, 2011.

[13] ETSI DTS 102 637-4, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 4: Operational Requirements," 2010.

[14] ETSI TR 102 638, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," June 2009.

[15] ETSI TR 102 893, "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)," 2010.

[16] ETSI ES 202 663, "European Profile Standard for the Physical and Medium Access Control Layer of Intelligent Transport Systems Operating in the 5 GHz Frequency Band," in *European Telecommunications Standards Institute*, Sophia Antipolis, France, 2010.

[17] ETSI EN 302 665, "Intelligent Transport Systems (ITS); Communications Architecture," ETSI European Norm ETSI EN 302 665, September 2010.

[18] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for Conditional Pseudonymity in VANETs," in *IEEE WCNC 2010*, Sydney, Australia, 2010.

[19] Intelligent Transportation Systems Committee, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE Vehicular Technology Society Standard 1609.2™-2006, 2006.

[20] F. Kargl, Z. Ma, and E. Schoch, "Security Engineering for VANETs," 2006.

[21] C. Paßmann, G. Schaaf, and K. Naab, "simTD D11.2 - Ausgewählte Funktionen," Deliverable, 2009.

[22] O. Henninger, et al., "Security Requirements for Automotive On-board Networks," in *9th International Conference on Intelligent Transport System Telecommunications (ITST 2009)*, Lille, France, 2009.

[23] S. Pietrowicz, T. Zhang, and H. Shim, "Short-Lived, Unlinked Certificates for Privacy-Preserving Secure Vehicular Communications," in *17th ITS World Congress*, Busan, Korea, 2010.

[24] Car-2-Car Communication Consortium, "C2C-CC Public Key Infrastructure Memo," Report, February 2011.

[25] G. Steel, "Towards a Formal Security Analysis of the SeVeCom API", in *9th ESCAR Embedded Security in Cars Conference*, Germany, November 2008.

[26] E. Schoch, and F. Kargl, "On the Efficiency of Secure Beaconing in VANETs", ACM Conference on Wireless Security (ACM WiSec '10), 03/2010.

[27] A. Rao, A. Kherani, and A. Mahanti, “Performance Evaluation of 802.11 Broadcasts for A Single Cell Network with Unsaturated Nodes”, Networking 2008, Springer LNCS 4982, 2008

[28] X. Ma and X. Chen, “Delay and Broadcast Reception Rates of Highway Safety Applications in Vehicular Ad Hoc Networks,” Proceedings of IEEE INFOCOM, MObile Networks for Vehicular Environments Workshop, May, 2007

[29] A. Vinel, V. Vishnevsky, Y. Koucheryavy “A Simple Analytical Model for the Periodic Broadcasting in Vehicular Ad-hoc Networks”, IEEE GLOBECOM 2008, 4th workshop on BWA, November 2008, New Orleans, USA.

[30] Vinel, A., Staehle, D., Turlikov, A., “Study of Beaconing for Car-to-Car Communication in Vehicular Ad-Hoc Networks”, Communications Workshops, IEEE International Conference on ICC, 2009

[31] Jonathan Petit, “Analysis of ECDSA authentication processing in VANETs”, NTMS'09 Proceedings of the 3rd international conference on New technologies, mobility and security, IEEE Press Piscataway, NJ, USA, 2009

[32] Petit, J., Mammeri, Z., “Analysis of authentication overhead in vehicular networks”, Third Joint IFIP Wireless and Mobile Networking Conference (WMNC), 2010

[33] Krishnan, H., Weimerskirch, A., “Verify on Demand – A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication”, SAE-2011-01-0584, SAE International 2011.

[34] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, Antonio Lioy, "On the Performance of Secure Vehicular Communication Systems," IEEE Transactions on Dependable and Secure Computing, to appear (preprint at IEEExplore)

[35] Robert K. Schmidt, Tim Leinmüller, Bert Böddeker, and Günter Schäfer, “Adapting the Wireless Carrier Sensing for VANETs”, 7th International Workshop on Intelligent Transportation (WIT 2010), Hamburg, Germany, March 23th - 24th, 2010.

[36] Robert K. Schmidt, Achim Brakemeier, Tim Leinmüller , Frank Kargl, Günter Schäfer, “Advanced Carrier Sensing to Resolve Local Congestion”, The Eighth ACM International Workshop on VehiculAr Inter-NETworking (VANET 2011), Las Vegas, USA, September 2011

[37] Robert K. Schmidt. T. Köllmer, T. Leinmüller, B. Böddeker, G. Schaefer, “Degradation of Transmission Range in VANETs caused by Interference”, Praxis der Informationsverarbeitung und Kommunikationstechnik (PIK), Special Issue on Mobile Ad-hoc Networks, 4(2009).

[38] Bernhard Kloiber, Thomas Strang, Fabian de Ponte-Mueller, Cristina Rico Garcia, Matthias Roeckl, “An Approach for Performance Analysis of ETSI ITS-G5A MAC for Safety Applications”. ITST 2010, 09-11 Nov. 2010, Kyoto, Japan.

[39] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmüller, "Secure and Efficient Beaconing for Vehicular Networks (Short Paper)", 5th ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2008), San Francisco, USA, ACM, 09/2008.

[40] Robert K. Schmidt, Bernhard Kloiber, Florian Schüttler, Thomas Strang, Degradation of Communication Range in VANETs caused by Interference 2.0 - Real-World Experiment, 3rd International Workshop on Communication Technologies for Vehicles (Nets4Cars), Oberpfaffenhofen, Germany, 23.-24. März 2011.

[41] P. Papadimitratos, A. de La Fortelle, K. Evensen, R. Brignolo, and S. Cosenza, “Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation,” IEEE Communications Magazine, Vol. 11, No. 1, pp. 84-95, November 2009

[42] P. Papadimitratos and A. Jovanovic, "GNSS-based positioning: Attacks and Countermeasures," IEEE MILCOM, San Diego, CA, USA, November 2008

[43] P. Papadimitratos and A. Jovanovic, "Protection and Fundamental Vulnerability of Global Navigation Satellite Systems (GNSS)," IEEE International Workshop on Satellite and Space Communications (IEEE IWSSC), Toulouse, France, October 2008

[44] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," ACM Workshop on Wireless Networking for Intelligent Transportation Systems (ACM WiN-ITS), Vancouver, BC, Canada, August 2007

[45] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," Workshop on Embedded Security in Cars (ESCAR), Berlin, Germany, November 2006

[46] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communications Magazine*, November 2008

[47] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, and A. Lioy, "Impact of Vehicular Communication Security on Transportation Safety," IEEE INFOCOM MOVE, Phoenix, Arizona, USA, April 2008

[48] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET," The Fourth ACM MobiCom International Workshop on Vehicular Ad Hoc Networks (ACM VANET), Montréal, QC, Canada, September 2007

[49] A. Festag, P. Papadimitratos, and T. Tielert, “Design and Performance of Secure Geo-cast for Vehicular Communication,” *IEEE Transactions on Vehicular Technology* (*IEEE TVT*), Vol. 59, No. 5, pp. 1-16, June 2010

[50] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," IEEE VTC-Fall Conference, Baltimore, MD, USA, October 2007

[51] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux and J.-Y. Le Boudec, “Adaptive Message Authentication for Multi-Hop Networks,” *IEEE/IFIP International Conference on Wireless On-demand Network Systems and Services (IEEE/IFIP WONS)*, Bardonecchia, Italy, January 2011

[52] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-Y. Le Boudec and J.-P. Hubaux, "Adaptive Message Authentication for Vehicular Networks," Short paper, *ACM MobiCom VANET*, Beijing, China, September 2009