D2.4 – Security Controls and Protection Profiles

Security Assurance Framework for Networked Vehicular Technology

Abstract

SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of Connected Vehicles and Vehicle-to-I (V2I) communications aiming at improving the cyber-physical security ecosystem of "connected vehicles" in Europe. The project will deliver innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of ICT related to Connected Vehicles and V2I systems, with increased connectivity of automotive ICT systems, consumer electronics technologies and telematics, services and integration with 3rd party components and applications. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

DX.X & Title:	D2.4 Security Controls and Protection Profiles
Work package:	WP2
Task:	2.4
Due Date:	28 February 2018 (30 September 2018 according to the amendment)
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR Leo Menis / AUT	**DATE** 01-June-2018
CONTRIBUTORS Onn Haran /AUT Konstantinos Maliatsos /UPRC	**DATE** 17-June-2018 17-Oct-2018
REVIEWED BY Konstantinos Maliatsos - Christos Lyvas /UPRC Panagiotis Pantazopoulos /ICCS	**DATE** 17-Oct-2018 / 20-Nov-2018 / 1-Feb-2019 02-Jul-2018 / 22-Nov-2018 / 29-Jan-2019/ 6-Feb-2019
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Document/Revision history

Version	Date	Partner	Description
V0.1	25/06/2018	AUT	First draft
V0.2	17/07/2018	AUT	Implementing comments by ICCS
V0.3	19/10/2018	AUT	Updates on Section 3 and Appendix
V0.4	11/11/2018	AUT	Implementing comments by UPRC Adjusting content to revision 1.4 of D2.3
V0.5	20/11/2018	UPRC	Internal review
V0.6	22/11/2018	ICCS	Internal review
V1.0	25/11/2018	AUT	Final version
V1.1	13/01/2019	AUT	Revised according to the reviewers' comments. The changes include: • Updated executive summary and Introduction (to align with the changes and provide clearer mapping to the DoA) • Added sub-section 1.5 to explain requirements and selection methodology (for security controls) • Added reasoning for the security controls selection in Section 3 • Added justification for each control in Section 3. • Added taxonomy of controls in Section 5.
V1.2	29/01/2019	ICCS	Internal review comments
V1.3	31/01/2019	AUT	Implementing peer review comments
V1.4	3/02/2019	AUT	Implementing peer review comments
V1.5	7/02/2019	AUT	Implementing peer review comments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Acronyms and abbreviations

Abbreviation	Description
CAN	Controller Area Network (CAN bus)
CAM	Cooperative Awareness Message
C-ITS-S	Central Intelligent Transportation System Station
DENM	Decentralized Environmental Notification Message
ECC	Elliptic-curve Cryptography
ETSI	European Telecommunications Standards Institute
FW	Firmware
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
HW	Hardware
ITS	Intelligent Transportation Systems
ITS-S	Intelligent Transportation System Station
JTAG	Joint Test Action Group
LDM	Local Dynamic Map
OBU	(Vehicle) On Board Unit – ***This term is identical to V-ITS-S***
OS	Operating System
PKI	Public Key Infrastructure
QoS	Quality of Service
R-ITS-S	Roadside Intelligent Transportation System Station
RSA	Rivest–Shamir–Adleman (encryption algorithm)
RSU	Roadside Unit -- ***This term is identical to R-ITS-S***
Rx	Receiver
SHE	Secure Hardware Extension
SPaT	Signal Phase and Time
SW	Software

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
V-ITS-S	Vehicle Intelligent Transportation System Station
TLS	Transport Layer Security
Tx	Transmitter

TABLE 1: LIST OF ABBREVIATIONS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Executive Summary

SAFERtec goal is to introduce a security assurance framework for connected vehicle technology (V2I – Vehicle to Infrastructure). One of the main building blocks of a secure system is a layered approach to security, with multiple security controls assuring mitigation of identified vulnerabilities. The controls should cover all elicited Functional Security Requirements.

In this document, the Security Functional Requirements (SFR) identified in deliverable D2.3 are explained, with its rationale provided for each one. Among others, the SFRs cover data integrity and confidentiality, as well as anonymity of the road users. Each SFR is addressed by a set of countermeasures (called controls), carefully selected in line with industry best practices for secure and private communication, and the specific V2X technology capabilities to support the automotive data dissemination.

The selected countermeasures cover a wide range of approaches, including the mitigation of wireless data injection/manipulation, device level security and protection of the vehicle internal network. Detailed discussion of their selection rationale and implementation details is provided for each countermeasure. Then, for the sake of clarity and increased usability, they are categorized using a well-known schema.

The results of D2.4 provide inputs to WP3 towards the creation of the SAFERtec modular protection profile, used as a basis of the assurance framework.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

1 Introduction

SAFERtec goals is to provide a flexible and efficient assurance framework for security and trustworthiness of V2I technology. The project will deliver innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of V2I systems. Assurance of security, safety and privacy aspects for Connected Vehicles should be measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

V2I technology opens a new wireless interface into the vehicle, with vehicle subsystem enabling V2I communication is typically connected to the vehicle internal network. Via this internal network (CAN bus), critical vehicle elements communicate. This mandates most stringent mechanisms to ensure the vehicle driver, the passengers and surrounding road users' safety is not compromised by any malicious act.

Security controls are countermeasures to mitigate security risks (related to the V2I system) and cover many aspects of the Connected Vehicle. They address the way electrical interfaces of V2I subsystem are protected, the method in which sensitive data is stored and delivered and how the sub-system elements are designed, to assure isolation, which prevents security risk propagating within the system.

The security controls are developed according to multiple industry standards and technical specifications, as well as best practices in the industry, and other industries. The secure channel is established using the latest internet technologies, such as TLS. The authentication of the road users is done via PKI (similar to common practice in banking industry), which is expected to be the biggest PKI ever deployed. The link between vehicle components may be protected using SHE specifications and latest System-On-Chip technologies are used to assure the needed performance of the security subsystem.

This document translates the output of the modelling effort done in previous deliverables (i.e., D2.2 and D2.3), into security architecture components, which can be used in a V2I system for implementation and testing. The scope of the document is limited to threats and requirements resulting from the introduction of V2I technologies into the industry and covering external wireless interfaces. It does not address existing, in-vehicle, communication networks.

In Section “1 Introduction”, the context of this document within SAFERtec is provided, including the sources of selecting the security and privacy controls described in this deliverable.

In Section “2 Requirements Overview”, the summary of the identified security requirement is provided, as they are derived to address the risks identified in risk analysis, and define the technical needs this document will cover.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

Section “3 Security Controls Overview”, lists the security controls identified for the connected vehicle use cases implemented by SAFERtec, and which can and should be implemented in a secure V2I system. The justification for the selection of each control is provided.

In Section “4 Coverage of Requirements”, the completeness of chosen security controls is shown, by explaining the coverage of the Security Requirements by the selected security controls.

In Section "5 Security Controls classification", the security and privacy controls are systematically presented under a taxonomy for the sake of clarity; it includes reasoning for selection of this specific method of classification.

In the "Appendix A: Test cases for security controls", example test cases are listed, based on which a security test program for the V2I system can be developed. An expanded set of system level test cases can be used to assure reliable implementation of security controls and be included in WP3 T3.3 – Assurance Framework Testing.

1.1 Purpose of the Document

This document details the guidelines for the implementation of countermeasures which address the security, safety and data privacy requirements presented in the deliverable D2.3 Vulnerability Analysis.

1.2 Intended readership

This deliverable is addressed to any interested reader (i.e. Public dissemination level).

1.3 Inputs from other projects

No input from other projects was considered during the compilation of this deliverable.

1.4 Relationship with other SAFERtec deliverables

This document is a bridge between Security Functional Requirements developed in deliverable D2.3, and implementation of the SAFERtec reference platform. The Security Functional Requirements are the result of a detailed modelling analysis performed on selected V2I use cases and are served as

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

input to this document. With this document, the corresponding security controls and measures to requirements are identified, in order to facilitate the definition of the SAFERtec protection profile that will be the basis of the assurance framework (WP3).

1.5 Security controls selection methodology

Security controls are selected to address Security Functional Requirements developed in deliverable D2.3. An input to this deliverable is the set of relevant documents published by organizations detailed in Table 2. As V2X technology is by nature cooperative, requiring a common "language" between communicating parties and mandating agreed upon level of security, some of the controls are dictated by the standards and regulations. In addition, semiconductor and automotive industries best practices for secure embedded devices were adopted, where applicable. For controls not mandated by regulation, and in order to support its adoption in the industry, a guiding principle was to select controls which are reasonable to implement in a consumer product in terms of cost, both unit cost and development cost.
The control selection methodology can be summarized by a sequence of steps:

- Regulatory requirements analysis and applicable controls extraction
- Relevant standard requirements analysis and security controls extraction
- Consulting industry expertise for best practices, and extraction of controls commonly adopted by system vendors

It is reasonable and expected that implementations of secure V2X system will vary between geographies and vendors, as mandatory requirements are region-dependent, and industry-recommended controls may be selectively adopted based by vendor based on broader architectural and cost considerations.

Organization	Description	Classification
C2C-CC	Car2Car Communication Consortium - consortium of European OEMs, Tier1s and suppliers collaborating to define technical specifications for V2X communication.	Industry technical steering
ETSI	European Telecommunications Standards Institute is a European standards developing organization, producing standards in the area of information and communication technologies.	Regional (EU) standards developing organization (SDO)
NIST	National Institute of Standards and Technology – non-regulatory agency within US Department of Commerce, which, among others, publish technical reports and recommendations for security implementations	Regional (US) standards developing organization (SDO)
FIPS	Federal Information Processing Standards developed by US government for computer security systems used in non-military government applications.	Standards developed by US federal government
IEEE	Institute of Electrical and Electronics Engineers develop global	International standards

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	standards in, among others, wireless technologies.	developing organization (SDO)
SAE	Society of Automotive Engineers International is a standard developing organization in various segments, with focus on automotive and (recently) connected vehicle.	International standards developing organization (SDO)
CAMP	Crash Avoidance Metrics Partnership – consortium of US OEMs, collaborating with US department of transportation on development of safety countermeasures in passenger cars	Industry technical steering
European Commission	Developed guidelines for secure V2X operation as part of the C-ITS delegated act. Any exchanged data, including V2X, should comply with the EU law of General Data Protection Regulation (GDPR)	Regulating body
NHTSA	National Highway Traffic Safety Administration, part of US Department of Transportation, specifying secure V2X implementation as part of the proposed V2X mandate (NPRM)	Regulating body

TABLE 2: INPUTS TO SECURITY CONTROLS DEFINITION

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2 Requirements Overview

As part of Deliverable 2.3, Security and Privacy Requirements were elicited. The requirements list is a result of analysis of below use-cases:

Use Case ID	Use Cases
UC-01	Optimal Driving Speed Advice
UC-02	Provision of Real-Time Traffic-Hazard Information
UC-03	Priority Request in Intersection-Crossing
UC-04	Optimal Driving Speed Advice (Cloud-based)
UC-05	Provision of Real-Time Traffic Information (Cloud-based)
UC-06	Personalised provision of driving-advices (Cloud-based)

TABLE 3: LIST OF USE CASES

In this chapter we review those requirements, as drivers for the Security Controls needed in a reference V2X system, in context of the SAFERtec project scope.

The following requirements were identified by the project team and are detailed in more length in the following chapter.

Requirement ID	Requirement	Subsystem
S1	Ensure the anonymity of stored data (in V-ITS-S)	V-ITS-S
S2	Ensure the confidentiality of stored data (in V-ITS-S)	V-ITS-S
S3	Ensure the authenticity of received data from C-ITS-S (in V-ITS-S)	V-ITS-S
S4	Ensure the authenticity of received data from R-ITS-S (in V-ITS-S)	V-ITS-S
S5	Ensure the availability of all transmitted data between Service Control, Application and communication interfaces (in V-ITS-S)	V-ITS-S
S6	Ensure the availability of all transmitted data between Service Control, Application, communication interfaces and sensor monitors (in V-ITS-S)	V-ITS-S
S7	Ensure the availability of all transmitted data from C-ITS-S to V-ITS-S (in V-ITS-S)	V-ITS-S
S8	Ensure the availability of all transmitted data from R-ITS-S to V-ITS-S (in V-ITS-S)	V-ITS-S
S9	Ensure the availability of data transmission (between V-ITS-S and C-ITS-S)	V-ITS-S
S10	Ensure the availability of data transmission (From V-ITS-S to R-ITS-S)	V-ITS-S
S11	Ensure the availability of received data from C-ITS-S (in V-ITS-S)	V-ITS-S
S12	Ensure the availability of received data from R-ITS-S (in V-ITS-S)	V-ITS-S
S13	Ensure the availability of the stored data in the service control, Application, vehicle system control and sensor monitors (in V-ITS-S)	V-ITS-S

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

S14	Ensure the availability of stored data (in V-ITS-S)	V-ITS-S
S15	Ensure the availability of transmitted data send to R-ITS-S by V-ITS-S (in V-ITS-S)	V-ITS-S
S16	Ensure the confidentiality of transmitted data send to R-ITS-S by V-ITS-S (in V-ITS-S)	V-ITS-S
S17	Ensure the confidentiality of transmitted data sent to C-ITS-S by V-ITS-S (in V-ITS-S)	V-ITS-S
S18	Ensure the confidentiality of transmitted data sent to R-ITS-S by V-ITS-S (in V-ITS-S)	V-ITS-S
S19	Ensure the integrity of all transmitted data between Service Control, Application, communication interfaces and sensor monitors (in V-ITS-S)	V-ITS-S
S20	Ensure the integrity of Software (in V-ITS-S)	V-ITS-S
S21	Ensure the integrity of Firmware (in V-ITS-S)	V-ITS-S
S22	Ensure the integrity of received data from C-ITS-S (in V-ITS-S)	V-ITS-S
S23	Ensure the integrity of received data from R-ITS-S (in V-ITS-S)	V-ITS-S
S24	Ensure the Integrity of sensor data (in V-ITS-S)	V-ITS-S
S25	Ensure the integrity of the stored data in the service control, Application, vehicle system control and sensor monitors (in V-ITS-S)	V-ITS-S
S26	Ensure the integrity of transmitted data send to R-ITS-S by V-ITS-S (in V-ITS-S)	V-ITS-S
S27	Ensure the unlikability of transmitted data sent to C-ITS-S by V-ITS-S (in V-ITS-S)	V-ITS-S
S28	Ensure the unlikability of transmitted data sent to R-ITS-S by V-ITS-S (in V-ITS-S)	V-ITS-S
S29	Only authorised users/devices can transmit data to C-ITS-S (in V-ITS-S)	V-ITS-S
S30	Only authorised users/devices can transmit data to R-ITS-S (in V-ITS-S)	V-ITS-S
S31	Only authorised users/devices can use the applications (in V-ITS-S)	V-ITS-S
S32	Ensure integrity of Software (in R-ITS-S)	R-ITS-S
S33	Ensure the authenticity of received data from C-ITS-S (in R-ITS-S)	R-ITS-S
S34	Ensure the authenticity of received data from V-ITS-S (in R-ITS-S)	R-ITS-S
S35	Ensure the availability of all transmitted data between Service Control, Application and communication interfaces (in R-ITS-S)	R-ITS-S
S36	Ensure the availability of all transmitted data between Service Control, Application, communication interfaces and sensor monitors (in R-ITS-S)	R-ITS-S
S37	Ensure the availability of data transmission (From R-ITS-S to V-ITS-S)	R-ITS-S
S38	Ensure the availability of received data from C-ITS-S (in R-ITS-S)	R-ITS-S
S39	Ensure the availability of received data from V-ITS-S (in R-ITS-S)	R-ITS-S
S40	Ensure the availability of the stored data in the service control, Application, vehicle system control and sensor monitors (in R-ITS-S)	R-ITS-S
S41	Ensure the availability of stored data (in R-ITS-S)	R-ITS-S

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

S42	Ensure the availability of transmitted data send to C-ITS-S by R-ITS-S (in R-ITS-S)	R-ITS-S
S43	Ensure the availability of transmitted data send to V-ITS-S by R-ITS-S (in R-ITS-S)	R-ITS-S
S44	Ensure the confidentiality of transmitted data send to C-ITS-S by R-ITS-S (in R-ITS-S)	R-ITS-S
S45	Ensure the integrity of all transmitted data between Service Control, Application, communication interfaces and sensor monitors (in R-ITS-S)	R-ITS-S
S46	Ensure the integrity of received data from C-ITS-S (in R-ITS-S)	R-ITS-S
S47	Ensure the integrity of received data from V-ITS-S (in R-ITS-S)	R-ITS-S
S48	Ensure the integrity of Firmware (in R-ITS-S)	R-ITS-S
S49	Ensure the integrity of the stored data in the service control, Application and communication interfaces (in R-ITS-S)	R-ITS-S
S50	Ensure the integrity of transmitted data send to C-ITS-S by R-ITS-S (in R-ITS-S)	R-ITS-S
S51	Ensure the integrity of transmitted data send to V-ITS-S by R-ITS-S (in R-ITS-S)	R-ITS-S
S52	Ensure the unlinkability of transmitted data sent to C-ITS-S by R-ITS-S (in R-ITS-S)	R-ITS-S
S53	Ensure the unlinkability of transmitted data sent to R-ITS-S by V-ITS-S (in R-ITS-S)	R-ITS-S
S54	Only authorised users/devices can transmit data to C-ITS-S (in R-ITS-S)	R-ITS-S
S55	Only authorised users/devices can transmit data to V-ITS-S (in R-ITS-S)	R-ITS-S
S56	Only authorised users/devices can use the applications (in R-ITS-S)	R-ITS-S
S57	Authenticity of C-ITS-S must be ensured (for sending data)	C-ITS-S
S58	Ensure the anonymity of stored data (in C-ITS-S)	C-ITS-S
S59	Ensure the availability of stored data (in C-ITS-S)	C-ITS-S
S60	Ensure the confidentiality of stored data (in C-ITS-S)	C-ITS-S
S61	Ensure isolation of stored data (in C-ITS-S)	C-ITS-S
S62	Ensure that malicious third parties cannot reveal who is using the C-ITS-S services (in C-ITS-S)	C-ITS-S
S63	Ensure that the data storage and data processes are aligned with the requirements introduced by GDPR (in C-ITS-S)	C-ITS-S
S64	Ensure the authenticity of received data from R-ITS-S (in C-ITS-S)	C-ITS-S
S65	Ensure the authenticity of received data from TLC (in C-ITS-S)	C-ITS-S
S66	Ensure the authenticity of received data from TMC (in C-ITS-S)	C-ITS-S
S67	Ensure the authenticity of received data from V-ITS-S (in C-ITS-S)	C-ITS-S
S68	Ensure the availability of all transmitted data between Service Control, Application, communication interfaces (in C-ITS-S)	C-ITS-S
S69	Ensure the availability of all transmitted data between Service Control, Application, communication interfaces and sensor monitors (in C-ITS-S)	C-ITS-S

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

S70	Ensure the availability of all transmitted data from V-ITS-S to C-ITS-S (in C-ITS-S)	C-ITS-S
S71	Ensure the availability of received data send to C-ITS-S by V-ITS-S (in C-ITS-S)	C-ITS-S
S72	Ensure the availability of received data from R-ITS-S (in C-ITS-S)	C-ITS-S
S73	Ensure the availability of received data from V-ITS-S (in C-ITS-S)	C-ITS-S
S74	Ensure the availability of the stored data in the service control, Application, vehicle system control and sensor monitors (in C-ITS-S)	C-ITS-S
S75	Ensure the availability of transmitted data send to V-ITS-S by C-ITS-S (in C-ITS-S)	C-ITS-S
S76	Ensure the availability of transmitted data send to R-ITS-S by C-ITS-S (in C-ITS-S)	C-ITS-S
S77	Ensure the confidentiality of transmitted data sent to V-ITS-S by C-ITS-S (in C-ITS-S)	C-ITS-S
S78	Ensure the integrity of all transmitted data between Service Control, Application, communication interfaces (in C-ITS-S)	C-ITS-S
S79	Ensure the integrity of all transmitted data between Service Control, Application, communication interfaces and sensor monitors (in C-ITS-S)	C-ITS-S
S80	Ensure the integrity of received data from R-ITS-S (in C-ITS-S)	C-ITS-S
S81	Ensure the integrity of received data from V-ITS-S (in C-ITS-S)	C-ITS-S
S82	Ensure the integrity of the stored data in the service control, Application and communication interfaces (in C-ITS-S)	C-ITS-S
S83	Ensure the integrity of transmitted data send to R-ITS-S by C-ITS-S (in C-ITS-S)	C-ITS-S
S84	Ensure the integrity of transmitted data send to V-ITS-S by C-ITS-S (in C-ITS-S)	C-ITS-S
S85	Ensure the Unlinkability of received data sent to V-ITS-S by C-ITS-S (in C-ITS-S)	C-ITS-S
S86	Ensure the Unlinkability of transmitted data sent to V-ITS-S by C-ITS-S (in C-ITS-S)	C-ITS-S
S87	Only authorised users/devices can use the applications (in C-ITS-S)	C-ITS-S
S88	Only authorised users/devices can transmit data to V-ITS-S (in C-ITS-S)	C-ITS-S

TABLE 4: IDENTIFIED SECURITY AND PRIVACY REQUIREMENTS

The applicability of each requirement to the considered use-cases is shown in following table:

Requirement ID	Category	UC-01	UC-02	UC-03	UC-04	UC-05	UC-06
S1	PRIVACY		Y	Y	Y	Y	Y
S2	SECURITY		Y	Y	Y	Y	Y
S3	SECURITY		Y		Y	Y	Y
S4	SECURITY	Y	Y	Y		Y	
S5	SECURITY	Y	Y	Y	Y	Y	Y
S6	SECURITY	Y	Y	Y	Y	Y	Y

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

S7	SECURITY		Y		Y	Y	Y
S8	SECURITY	Y	Y	Y			
S9	SECURITY		Y		Y	Y	Y
S10	SECURITY			Y			
S11	SECURITY		Y		Y	Y	Y
S12	SECURITY	Y	Y	Y		Y	
S13	SECURITY	Y	Y	Y	Y	Y	Y
S14	SECURITY	Y	Y	Y	Y	Y	Y
S15	SECURITY			Y			
S16	SECURITY			Y			
S17	SECURITY		Y		Y	Y	Y
S18	SECURITY			Y			
S19	SECURITY	Y	Y	Y	Y	Y	Y
S20	SECURITY	Y	Y	Y	Y	Y	Y
S21	SECURITY	Y	Y	Y	Y	Y	Y
S22	SECURITY		y		y	y	y
S23	SECURITY	Y	Y	Y		Y	
S24	SECURITY	Y	Y	Y	Y	Y	Y
S25	SECURITY	Y	Y	Y	Y	Y	Y
S26	SECURITY			Y			
S27	PRIVACY		Y		Y	Y	Y
S28	SECURITY			Y			
S29	SECURITY		Y		Y	Y	Y
S30	SECURITY			Y			
S31	SECURITY	Y	Y	Y	Y	Y	Y
S32	SECURITY	Y	Y	Y		Y	
S33	SECURITY	Y	Y	Y		Y	
S34	SECURITY	Y	Y	Y		Y	
S35	SECURITY	Y	Y	Y		Y	
S36	SECURITY	Y	Y	Y		Y	
S37	SECURITY	Y	Y	Y		Y	
S38	SECURITY	Y	Y	Y		Y	
S39	SECURITY			Y			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

S40	SECURITY	Y	Y	Y		Y	
S41	SECURITY	Y	Y	Y		Y	
S42	SECURITY			Y			
S43	SECURITY	Y	Y	Y		Y	
S44	SECURITY			Y			
S45	SECURITY	Y	Y	Y		Y	
S46	SECURITY	Y	Y	Y		Y	
S47	SECURITY	Y	Y	Y		Y	
S48	SECURITY	Y	Y	Y		Y	
S49	SECURITY	Y	Y	Y		Y	
S50	SECURITY			Y			
S51	SECURITY	Y	Y	Y		Y	
S52	PRIVACY			Y			
S53	PRIVACY			Y			
S54	SECURITY			Y			
S55	SECURITY	Y	Y	Y		Y	
S56	SECURITY	Y	Y	Y		Y	
S57	SECURITY	Y	Y	Y	Y	Y	Y
S58	PRIVACY		Y	Y	Y	Y	Y
S59	SECURITY		Y	Y	Y	Y	Y
S60	SECURITY		Y	Y	Y	Y	Y
S61	SECURITY	Y	Y	Y	Y	Y	Y
S62	SECURITY	Y	Y	Y	Y	Y	Y
S63	SECURITY	Y	Y	Y	Y	Y	Y
S64	SECURITY			Y			
S65	SECURITY	Y			Y		
S66	SECURITY	Y	Y		Y	Y	Y
S67	SECURITY		Y		Y	Y	Y
S68	SECURITY	Y	Y	Y	Y	Y	Y
S69	SECURITY	Y	Y	Y	Y	Y	Y
S70	SECURITY		Y		Y	Y	Y
S71	SECURITY		Y		Y	Y	Y

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

S72	SECURITY			Y			
S73	SECURITY		Y		Y	Y	Y
S74	SECURITY		Y	Y	Y	Y	Y
S75	SECURITY		Y		Y	Y	Y
S76	SECURITY		Y		Y	Y	Y
S77	SECURITY		Y		Y	Y	Y
S78	SECURITY	Y	Y	Y	Y	Y	Y
S79	SECURITY	Y	Y	Y	Y	Y	Y
S80	SECURITY			Y			
S81	SECURITY		Y		Y	Y	Y
S82	SECURITY		Y	Y	Y	Y	Y
S83	SECURITY		Y	Y		Y	
S84	SECURITY		Y		Y	Y	Y
S85	PRIVACY		Y		Y	Y	Y
S86	SECURITY		Y		Y	Y	Y
S87	SECURITY	Y	Y	Y	Y	Y	Y
S88	SECURITY		Y		Y	Y	Y

TABLE 5: APPLICABILITY OF REQUIREMENTS TO USE CASES

The requirements are aggregated into categories, for which common security controls implementation apply.

The allocation of each requirement to a certain category is given below:

Category ID	Requirement category	Requirement list
CID1	Ensure integrity of stored data	S25, S49, S82
CID2	Ensure integrity of transmitted data	S19, S26, S45, S50, S51, S78, S79, S83, S84
CID3	Ensure integrity of received data	S22, S23, S46, S47, S81, S80
CID4	Ensure availability of stored data	S13, S14, S40, S41, S59, S74
CID5	Ensure availability of transmitted data	S5, S6, S7, S8, S9, S10, S15, S35, S36, S37, S42, S43, S68, S69, S70, S76
CID6	Ensure availability of received data	S11, S12, S38, S39, S71, S72, S73,
CID7	Ensure confidentiality of stored data	S2, S60

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

CID8	Ensure confidentiality of transmitted data	S16, S17, S18, S44, S77,
CID9	Ensure only authorized users/devices have access/can use the applications or/and transmit/receive data	S29, S30, S31, S54, S55, S56, S57, S87, S88
CID10	Ensure integrity of sensor data	S24
CID11	Ensure authenticity of received data	S3, S4, S33, S34, S64, S65, S66, S67
CID12	Ensure integrity of ITS software	S20, S21, S32, S48,
CID13	Ensure isolation of stored data	S61
CID14	Ensure anonymization of the stored data regarding traffic patterns, heavy traffic routes, etc.	S63
CID15	Ensure anonymity of stored data	S1, S58,
CID16	Ensure anonymization of driver/vehicle transmitted data	S62
CID17	Ensure unlinkability of transmitted/received data	S27, S28, S52, S53, S85, S86

TABLE 6: REQUIREMENTS CATEGORIZATION

Details for each requirements category and the corresponding rationale for its introduction are provided below.

2.1 Security Requirements

Security is protection against intended incidents, i.e., incidents that happen due to a result of deliberate and planned act. Security concerns the protection of assets from threats, where these are categorised as “the potential for abuse of protected assets”. A piece of information is secure when its content is protected.

2.1.1 CID1: Ensure integrity of Stored data

Requirement: The integrity of stored data in service control, Application and communication interfaces shall be ensured.

Rationale: Data integrity is a fundamental component of information security. In its broadest use, data integrity refers to the accuracy and consistency of data stored in the ITS stations. There are multiple data types in the ITS station, integrity of which must be assured. Those data types are, just to name a few: Pseudonym certificates, Root certificates and Certificate revocation lists, Configuration files and databases. Maintaining the integrity of the stored data types assures correct operation of the ITS, such as ability to created valid digital signature.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

2.1.2 CID2: Integrity of transmitted data

Requirement: The integrity of transmitted data between ITS agents shall be ensured.

Rationale: ITS stations make joint safety decisions based on the content of V2X data received. Any modification of the transmitted data, due to an unreliable communication channel or due to manipulations from malicious users may result in compromised safety for the participating road user. For example, maliciously modified signal phase information in SPaT message (see use-cases 1 and 4) may cause the vehicle to run a red light at the intersection**.** The type of information, which is transmitted and integrity of which shall be maintained in the context of evaluated Use Cases: Traffic Light phases, real time traffic-hazard information and priority requests at intersection crossing.

2.1.3 CID3: Ensure integrity of received data

Requirement: The integrity of received data between ITS agents shall be ensured.

Rationale: The rationale is similar to CID2 (Ensure integrity of transmitted data). The requirements are separated, since the functional implementation may be asymmetrical for sending and receiving agents and different technical constraints shall apply.

2.1.4 CID4: Ensure availability of stored data

Requirement: ITS station shall satisfy the availability of the respective data for every type of communication and among every subcomponent
Rationale: ITS stations make joint safety decisions based on the content of V2X data received. ITS stations require critical data elements to be readily available within a bounded time window, to make transmitted data relevant. For example, US and EU technical requirements for ITS station mandate sensor freshness in transmitted safety message to be not older than 200ms. This requirement translates to security and safety related data types availability of several milliseconds.

2.1.5 CID5: Ensure availability of transmitted data

Requirement: ITS agents shall satisfy the availability of the wireless link for data transmission
Rationale: ITS stations are expected to periodically transmit data so other ITS stations can receive the data and make safety decisions based on it. ITS stations transmission should be performed in a timely manner to assure the freshness and relevancy of the information. Denial of Service attack may occupy the wireless link, preventing from ITS stations to transmit.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This requirement translates to protecting the ITS station from such Denial of Service attackers and detecting and potentially reporting Denial of Service attacker to other ITS stations.

2.1.6 CID6: Ensure availability of received data

Requirement: ITS agents shall satisfy the availability of the wireless link for data reception
Rationale: The rationale is similar to CID5 (Ensure availability of transmitted data) The requirements are separated, since the functional implementation may be asymmetrical for sending and receiving agent and different technical constraints shall apply.

2.1.7 CID7: Ensure confidentiality of stored data

Requirement: ITS station shall satisfy the confidentiality of the respective data for every type of communication and among every subcomponent
Rationale: Stored data is used to prove authenticity of transmitted data and to validate authenticity of received data. ITS stations assume that an authentic data is transmitted by a legitimate ITS stations. Lack of confidentially even in a single ITS station would prevent us from making this assumption and thus any received data can't be safely used.
This requirement translates to secure data, properly isolated and encrypted with tamper detection or protection. Confidentiality of C-ITS data is ensured via security design of cloud infrastructure, including secure communication channel with clients.

2.1.8 CID8: Ensure confidentiality of transmitted data

Requirement: ITS station shall satisfy the confidentiality of the transmitted data for every type of communication involving a subset of ITS stations
Rationale: Most of ITS Station transmissions are broadcast of plaintext. However, connectivity between a pair of ITS stations (unicast) or a group of ITS stations (multicast) should remain confidential by applying encryption. Entities not taking part in the connectivity should not be able to eavesdrop. This requirement translates to encrypting the link, usually securely pre-agreed or negotiated shared key. In order to establish a secure (encrypted) communication channel between any pair of system entities, each endpoint (receiving or transmitting entity) must be authenticated.

2.1.9 CID9: Ensure user authorization

Requirement: ITS station shall authorize the user or device to allow access to use a service, including application usage, transmission and reception
Rationale: ITS Station may contain multiple users, privileged and non-privileged, each may have different credentials to access different services. Unauthorized user shall not be allowed to access a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

service. For example, transmission shall not be initiated by a process potentially attempting to attach receiving ITS stations.

2.1.10 CID10: Ensure integrity of sensor data

Requirement: ITS station shall ensure the integrity of sensor data
Rationale: ITS stations make joint safety decisions based on the content of V2X data received. Sensor data is embedded inside the transmitted data. Any manipulated sensor data will not be detected by the receiving ITS stations as the data is transmitted by a legitimate ITS station. Therefore, modification of sensor data may result in compromised safety for both transmitter and receiver. For example, traffic light sensor data may transmit that light is red, while it is green, or vice versa. Vehicles transmitted data may mislead the traffic light to believe that vehicles are about to cross the intersection at red light.
This requirement translates to protecting the sensor data. If possible, data should be kept confidential (encrypted) and communicating entities should be two-way authenticated. If encryption or authentication isn't possible, for example in vehicle CAN bus, then intrusion detection or intrusion prevention schemes should be applied to alert suspicious patterns of data on the vehicle bus.
The receiving ITS station may apply plausibility checks. For example, using a camera to detect traffic light status and comparing it with the wireless communication. Or checking if the values of the sensors are coherent, meaning values are too big or follow an inconsistent movement pattern.
Sensor data integrity also includes GNSS as a data source. Thus, the system should include mechanisms that can check the integrity of the localization data – usually through plausibility checks. It is to be noted that GNSS is also used for system synchronization affecting every other system functionality.

2.1.11 CID11: Ensure authenticity of received data

Requirement: ITS station shall ensure the authenticity of all received messages
Rationale: ITS stations make joint safety decisions based on the content of V2X data received. The content of received message includes critical information for proper operation of use cases. There is a significant economic incentive to manipulate payload data to receive undeserved advantage in the interaction with other ITS stations.
Examples of manipulations:

- Elevating privileges to receive priority at intersection crossing
- Falsifying traffic information, to re-route the traffic and create free corridor for the malicious agent

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The ITS station, hence, is obligated to assure all received messages are sent from an authentic source – the source that is both authorized sending that type of message and populating it with that type of content.

2.1.12 CID12: Ensure integrity of ITS software

Requirement: ITS station shall ensure the integrity of its executed software/firmware
Rationale: ITS station behavior is driven by its SW. The entire distributed network correct behavior is relying on the fact that all ITS stations operate according to industry agreed rules, and the ITS devices are certified on a system level to comply with abovementioned rules. Each ITS station can impact behavior of nearby ITS stations, by the content of transmitted messages and the policy according to which the messages are sent. The ITS station SW is responsible for proper message generation, both in the sense of proper payload population and generation policy (rate, power, etc.). Hence, protection of executed SW from malicious or other manipulation is critical for ITS station vendor, to protect its reputation and protect itself from liability claims, in case of damage to other ITS station.

2.1.13 CID13: Ensure isolation of stored data

Requirement: ITS station shall ensure isolation of stored data between safety critical domains in the OBU and other domains (infotainment, etc.)
Rationale: Some of data flows between ITS stations are supporting safety critical use cases. Those data flows rely on data previously stored in persistent or semi-persistent data repository. An example of such semi-persistent database is LDM (Local Dynamic Map), which represents the current view of the ego vehicle of surrounding stations. Generation of driver information is based on integrity of the LDM. Hence, this and similar databases shall be isolated from system processes which are not authorized to access them. This will prevent data corruption in the data base (malicious or due to SW error).

2.2 Privacy Requirements

Privacy requirements are introduced because of privacy related concepts, namely **anonymity** of ITS network participants.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.2.1 CID14: Ensure anonymization of the stored data

Requirement: ITS station shall assure anonymity of all stored data
Rationale: ITS station tracks all users passing through an intersection. The data is analyzed and used to provide various metrics such as traffic patterns or routes. That data cannot be used to identify the drivers that have provided it. Any indication of user identity is a strict privacy violation, potentially violating the GDPR.
This requirement translates to removing station identity upon message arrival. The processing application has no notion of vehicles identity, and no ability to recover those. Further anonymization mechanism can be applied, such as providing the data to the application every 5 minutes, or other duration, to assure that the exact time of passing through the intersection is unknown. Potentially data indicating vehicle type and size can be deleted as well.
On top of that, the stored data should be kept confidential, encrypted at rest.

2.2.2 CID15: Ensure anonymity of stored data

Requirement: ITS station shall ensure that any information stored in its persistent storage about any other ITS station shall be anonymous
Rationale: Information stored about any ITS stations must not contain any information, which can be used to track ITS station and/or identify the driver identity.

2.2.3 CID16: Ensure anonymization of driver/vehicle transmitted data

Requirement: ITS station shall ensure anonymity of transmitted data
Rationale: ITS station transmission should not be used to track the vehicle. Compliance with GDPR must be assured. The ITS station shall not use any unique identifier in the transmitted message overhead or payload. Any identifier shall be frequently changed, to avoid any tracking method easier than physical surveillance.

2.2.4 CID17: Ensure driver - vehicle unlinkability

Requirement: ITS station shall assure that transmitted data can't be linked with vehicle driver identity
Rationale: ITS station transmission contains certificates and pseudonym identifiers. If either can be linked to vehicle identity, then vehicle identity can be retrieved, and driver privacy would be violated. This requirement impacts multiple aspects of vehicle enrollment in PKI, certificate distribution and storage. In the context of ITS transmission, the selection and refreshing of certificates shall be such that logging those would not expose vehicle identity.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3 Security Controls Overview

Ensuring the fulfillment of all Security and Privacy Requirements for V2X systems requires a multitude of Security Controls to be put in place. Industry best practices for implementing a Secure and Private system are detailed in this chapter. Justification arguments on the selection of each control together with appropriate references are discussed in each case. The subsequent chapter will map those security controls to the requirements.

3.1 Cryptographic Measures

3.1.1 Digital Signature

Elliptic Curve Cryptography (ECC) is one of the most powerful types of cryptography in wide use today. It is a public-key cryptography (asymmetric cryptography) method based on elliptic curves over a final field. Elliptic Curve Digital Signature Algorithm (ECDSA) is an algorithm utilizing ECC to create Digital Signature.
Each road user is enrolled by a Public Key Infrastructure and is signing outgoing messages and authenticating incoming messages using public-private key pairs. Digital Signature is generated and appended to each transmitted message using the device private key. The digital signature assures the integrity of the message content, as well as authenticity of the transmitter.
Important to mention, that to maintain privacy of the road user, each message is signed by one of the many key-pairs securely stored by the road user, and the key pair is frequently changes, thus preventing tracking road user movement by tracking the public key.
ECDSA is widely adopted in V2X industry to assure road users anonymity, authenticity and privacy.
Two elliptic curves are specified for use with ECDSA: NIST P-256 as specified in FIPS 186-4, and brainpoolP256r1 as specified in RFC 5639. SHA256 is used to create message digest to be signed. Signature generation flow is detailed in [1].

Justification
As mentioned previously, ECDSA is the de-facto control selected by V2X industry and the usage of ECDSA for V2X is standardized in US in IEEE Standard 1609.2 and in EU in ETSI TS 102 941. Both standards were covered in SAFERtec deliverable D7.4. The underlying technical reason for selecting ECDSA is the following:

- Asymmetric cryptography method is preferred when the type of communication is one-to-all (broadcast) or one-to-many (geocast), as is the case in many V2X applications (e.g. SPaT message sent by V2X enabled Traffic Light to all surrounding vehicles), and the duration of the communication is very short (may be just a second or less), reaction to data is required within fraction of seconds for safety purposes and handshake messages may fail due to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

occasionally unreliable wireless link so that establishing a common shared secret key is a prohibitive overhead in terms of time and channel bandwidth.

- Elliptic curve cryptography advantage in V2X applications over other asymmetric cryptography methods, such as RSA [2], is the smaller key size, which results in shorter over-the-air transmission and better wireless channel utilization.

3.1.2 Message Authentication Codes

Message Authentication Codes (MAC) are used to authenticate the source of a received message and assure message integrity. The method is based on shared secret key, using which the MAC is generated and verified. The method assumes the shared secret key was securely shared between communicating parties prior to the session establishment. Embedded device typically implements Secure Subsystem, which provides MAC generation and authentication capabilities.

A secure subsystem implementing MAC based authentication would consist of:

- Storage area to keep state of the cryptographic engine
- Mailbox API / HOST API to access its functionality
- Library API using the mailbox API

The main blocks of Secure Subsystem implementation in chipset are depicted below.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

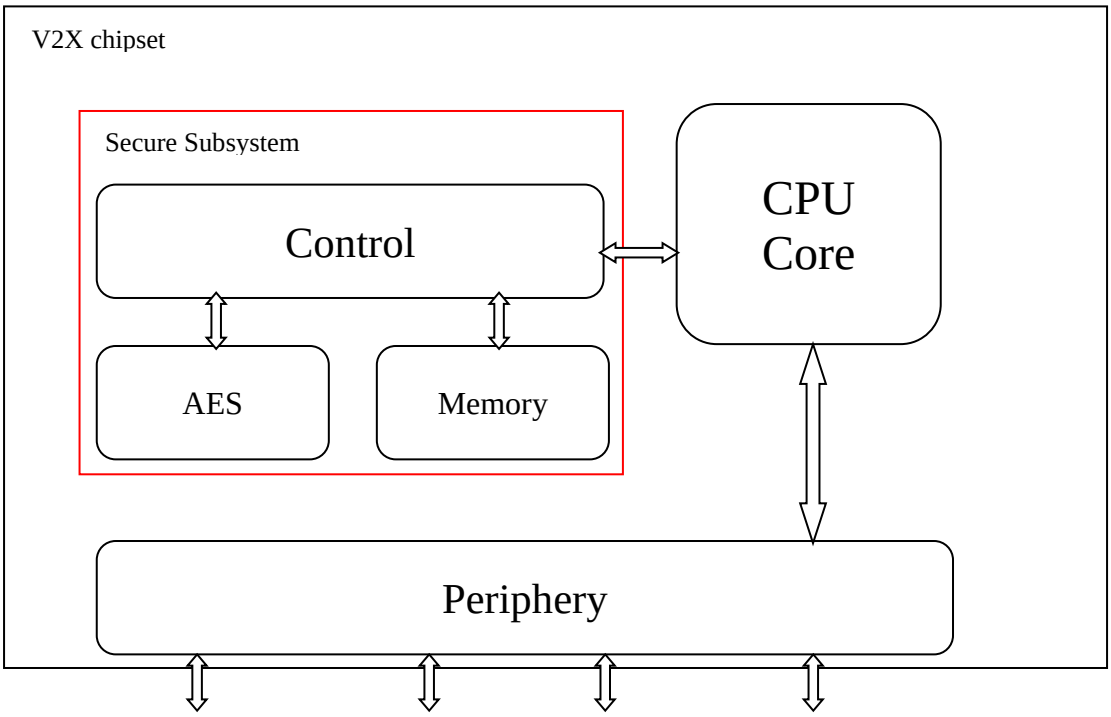


FIGURE 1: SECURE SUBSYSTEM IMPLEMENTATION

The recommended MAC generation and verification implementation is CMAC using AES-128, as specified in [3].

Justification

Authenticated and integrity protected communication utilizing MAC is a widespread practice in wireless communication industry, specifically in IEEE 802.11 (Wi-Fi) and in banking industry, for financial transactions authentication. The control is selected due to high throughput implementations available in HW, widespread use and alignment with the NIST recommendation [3].

3.1.3 Payload Symmetric Encryption

Symmetric Encryption of the Payload is used whenever road user is transmitting confidential information to a specific entity, the ECC public key of which we know. The method is not used for CAM/DENM safety messages, but in the V-ITS to R-ITS communication and in vehicle platooning use cases. V2X adopted Elliptic Curve Integrated Encryption Scheme (ECIES) for key agreement and subsequent encryption as defined in [1]. According to the adopted method, the shared secret for each message is established using Elliptic Curve Diffie-Hellman, and the payload is symmetrically

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

encrypted using AES-CCM, as recommended in [4]. Two elliptic curves are specified for use with ECIES: NIST P-256 as specified in [5], and brainpoolP256r1 as specified in [6].

Justifications

ECIES is the de-facto control selected by V2X industry and the usage of ECIES for V2X is standardized in US in IEEE Standard 1609.2 and in EU in ETSI TS 102 941. Both standards were covered in SAFERtec deliverable D7.4. Technical reasoning for selection of ECIES for authenticated and confidential communication is the high level of security, the widespread usage and the availability of fast implementations for the digital signature (ECDSA) and MAC (AES).

3.1.4 Secure Storage

V2X communication is using Elliptic Curve Cryptography and enrolment to PKI to enable mutual authentication by road users, without disclosing identity. The cornerstone of this method is the usage of private key, unique for each road user. This private key is used to generate Digital Signature (**3.1.1 Digital Signature**) for each outgoing message. The private keys of each road user are considered extremely sensitive data, and the theft of which will allow malicious user to assume attacked vehicles identity, and potentially cause disruption to the V2X network and compromise security of other road users. Secure Storage enables storing the sensitive data is such a way, that even physical access to the attacked device would not allow access to those keys.

The main objectives of secure storage:

- Allow storing of sensitive assets in such a way, that they never leave the boundaries of the Hardware Security Module in plaintext
- The size of secure storage should be such as to allow sufficient number of private keys and other sensitive assets, such as Misbehaviour reports and Certificate Revocation Lists, to be stored for prolong system operation without access to PKI infrastructure. A size of 3MB of data considered sufficient in current deployments.
  The access to the secure storage should be fast enough to allow fast signing of outgoing messages. This means in the order of several milliseconds.

There are two common methods of implementing secure storage in V-ITS:

- On HSM embedded Non-volatile memory
- On memory external to HSM

Considerations on secure storage: Storing private assets securely within the boundaries of the HSM is a convenient method, when the size of the asset data small (1-2MB), due to limited size of available storage in HSM. This method is "self-contained" and no additional memory is needed.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Alternatively, the sensitive data may be securely stored on external memory, after encryption with cryptographically strong method, such as AES-256 CCM [4] symmetric encryption. It is critical that the encryption key(s) is(are) unique for each HSM, generated randomly in the HSM and never leaves HSM boundary in plaintext format. This method requires allocation of space on external memory, however provides the secure storage space limited only by the memory physical space.

Justification

The justification for secure storage is derived directly from the fact that cryptographic methods are used, which utilize secure data stored in a persistent way on the device. The requirement for secure storage, protected by the HSM is recognized by the industry, and is mandated by C2C-CC as part of security working group defining the HSM Protection Profile (i.e., the document is not public yet, but there is a public overview of considerations available by [7]) and CAMP technical report [8] on Hardware, Software and OS security requirements of V2X system that use cryptographic private keys. Unauthorized access to the private keys is considered as the greatest security risk to V2X system.

3.1.5 Secure Communication Channel

Secure Communication Channel can be established between V-ITS/R-ITS/C-ITS using existing end-to-end cryptographic protocol, such as TLS v1.2 or higher. Recommended cipher-suites are ECDH-ECDSA, with AES-{128/SHA256/GCM or 256/SHA384/GCM or 128/SHA256/CBC or 256/SHA384/CBC}. Secure Communication Channel can address the requirement for privacy as well as data integrity. The secure session is established after initial negotiation, during which a shared secret, unique for each connection, is set. The private keys for symmetric encryption are derived from the shared secret. The negotiation, during which identity of the participating parties is authenticated and shared key is set is commonly performed using public-key cryptography.
Secure channel operation can benefit from underlying HW security blocks in the system. V-ITS embedded HSM can be used to securely establish shared secret, while embedded AES accelerators can reduce the latency and CPU load of AES decryption operations.

Justification

The suites suggested for establishing secure communication channel are in widespread usage in Internet/Wireless technologies and are commonly adopted in V2X industry for secure and reliable end-to-end communication. An example of planned TLS usage in the V2X world is as part of SCMS (Security Credential Management System), specifically to protect communication between online components of SCMS, as is proposed in [9].

3.1.6 Secure Boot

One of the main requirements of a secure system is usage of FW which has been authenticated and integrity of which has been establish before execution. This assured that any FW which has been

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

modified or somehow tampered-with would fail to execute and compromise the system and the V2X network. The main objectives of a secure boot implementation are:

- Firmware image integrity and authenticity should be verified before it is executed
  - Integrity and authenticity should be ensured using public key cryptography. Recommendation to use ECDSA with SHA-256. The vendor public key should be placed in the ITS station internal ROM.
- Facilitating firmware upgrade in case a vulnerability is detected and fixed or a feature is added, while maintaining software authenticity and integrity
  - It should be possible to prevent downgrade of a firmware image from a version that has fixed a security vulnerability to one that has that vulnerability (downgrade protection)

The secure Boot concept of operation can be summarized:

- Each loaded FW image must be digitally signed while both authenticity and integrity are verified during boot
- During boot, a chain of trust is established between the in-chip root of trust and the FW certificate
- Initial boot code is executed from the in-chip trusted ROM, each boot stage verifies subsequent loaded stages

A typical boot flow on a Secure Boot enable embedded system is depicted in the following figure:

FIGURE 2: TYPICAL SECURE BOOT FLOW

Secure boot is enabled by embedded HSM, which is the security trust anchor for the system. In V2X system implementation, software authentication and integrity check via secure boot flow is highly recommended for all embedded SW, and is required for V2X OBU stack and HSM code.

Justification

Secure boot is an automotive industry common practice for preventing SW code manipulation, leading to compromised operation. A compromised device is untrusted, and exposes the operation to high number of vulnerabilities. Significant effort in requirement specification and architectural

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

specification was done as part of EVITA (E-safety vehicle intrusion protected applications) project[1], including detailed specifications of HSM, which can support secure boot. The project goal was to propose an architecture for secure intra-vehicle network, with automotive and V2X specific requirements in mind. Specifically, an overview with references to relevant EVITA deliverables is available in [2].

3.1.7 Plausibility Checks

A set of plausibility checks is defined in V2X security standards to be applied on incoming messages, to identify and filter out potentially malicious or malfunctioning ITS transmitter. Those plausibility checks are designed to address types of attacks such as Replay Attack, where a valid message is being misused.

The critical minimal set of plausibility checks consists of [10]:

- Spatial relevance check – only messages from ITS stations within defined distance will be accepted
- Temporal relevance check – only messages generated within defined time window will be accepted
- Sensor values check – only messages with reasonable sensor values are accepted

Justification

Plausibility checks are needed as an additional protection layer in case other mechanisms have been compromised despite protection, and secure material is available to a malicious user. In addition, plausibility checks are effective to detect failures, intentional or accidental, in sensor values, such as position, speed, acceleration, and more, as fed into the V2X device, and transmitted over the air. As stated above, the minimal set of plausibility checks are industry mandated, specifically by the C2C-CC. The individual car makers are expected to enrich the set of plausibility checks for higher level of system security, by utilizing proprietary side information (e.g. information from other sensors).

[1] https://www.evita-project.org/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.2 Architecture and Policy Controls

3.2.1 Hardened OS

OS hardening is a process of reducing the size of the attack surface of the OS of a device. The process is different for each case, and the following general steps apply:

1) Identify vulnerably and assets to protect (refer to deliverable D2.3 for details).
2) Develop a robust Security Policy (the policy will be heavily influenced by the Car2car communication consortium Security WG definition of Security Gateway, which is still in progress during the writing of this document)
3) Limiting access rights, in a way which enforces the Security Policy
4) Closing all ports which do not have to remain open
5) Apply firewall where applicable

The main target of an attack is expected to be the embedded element in V-ITS due to its wide spread. There are specific measures which can and should be applied to an embedded system:

1) Disabling low level access ports, such as JTAG debug port
2) Using ROM fused bootloader
3) Use Secure Boot mechanism to authenticate the FW image (addressed separately in this document)
4) Process isolation and access control policy (addressed separately in this document)

Finally, memory protection mechanisms [11] against conventional memory corruption exploitation techniques must be applied in order to protect software, firmware and their computations integrity such as:

- Address Space Randomization for privilege (ex. Linux Kernel Mode Linux) and non- privilege processes (User Mode Linux) enforced in Operating System (OS) level
- Write Exclusive Execution policy that requires memory access permissions to be either writable but not executable (e.g., NX-bit on x86 processors and XN-bit on ARM processors) enforced in Operating System (OS) level
- Stack Protection mechanism that guards the stack memory against corruptions enforced during compilation of software

Justification

This control is generic and should be tailored specifically for application in question. There is no specific standard or recommendation on how to harden a V2X system, but a set of recommended practices from the embedded-systems world and car maker specific requirements. Automotive industry is in the process of defining common requirements as part of Automotive Grade Linux

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

(AGL), however this effort is still at its early phase at the time of writing of this document. Hardened OS reduces the ability of the attacker to use OS security weaknesses in order to take control over the system.

3.2.2 Access control policy enforcement

Process separation is a fundamental engineering framework (hardware and software) to securely design complex software systems. A layered approach to security architecture provides a scalable, maintainable, and provably effective framework to minimize security risk.

Process isolation may be achieved by a combination of several mechanisms:

- SW isolation using virtualization such as QNX hypervisor
- Mandatory Access Control (MAC) frameworks, such as SELinux (Security Enhanced Linux) [12] or Smack (Simplified Mandatory Access Control Kernel) [13]
- Physical separation: utilizing embedded HW infrastructure, such as ARM TrustZone [14] and a secure bus matrix

The separation enables limiting access of unauthorized subjects (processes/applications) to secure objects, such as secure ports. In vehicle installation, an example of secure port requiring restricted access is CAN bus interface.

The following diagram depicts an interface isolation within an embedded device:

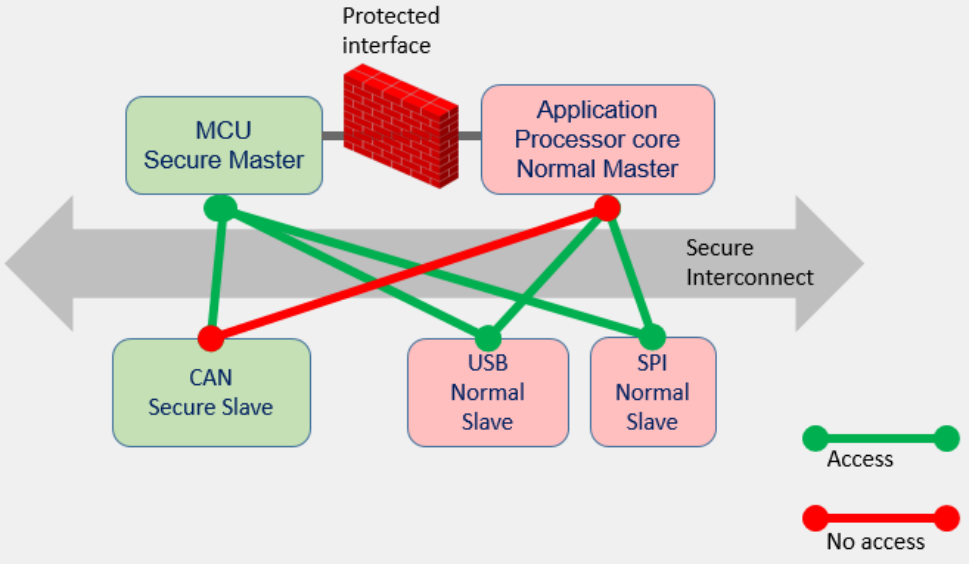


FIGURE 3: EMBEDDED DEVICES INTERFACE ISOLATION

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Justification

Access control policy is common practice in secure system design, and the automotive industry is in process of adopting it through Automotive Grade Linux security framework specification [15]. Embedded cores for automotive microcontrollers are commonly available with TrustZone architecture [16]. Access control is an additional protection measure to limit access to secure assets, such as secure storage or digital signature implementation, to authorized processes only. That serves as another layer of protection in case the SW was compromised, but still preventing it from performing critical security operation.

3.2.3 Random Identity

One of the most critical requirements on deployment of ITS network is, that by introducing it, the privacy of the road users will not be compromised. ITS station shall not transmit any information which will allow tracking it in a manner which is easier than existing methods, such as visual surveillance. Also, no information shall be transmitted, that exposes vehicle or driver unique identification. This forces the ITS station to use frequently changing random identity, as specified, for example in [10]. Usage of frequently changing pseudonyms in transmitted messages, which cannot be used to identify the driver identity[2] is hence a mandatory requirement for a privacy centric ITS station.

The pseudonym is changed:

- Every defined time interval
- On every vehicle start
- When ITS station detects a collision with a certificate digest of another ITS station
- When it's time duration is expired

In safety critical situations, such as when dangerous event is detected, the certificate change may be delayed by upper layer applications, to allow continuity of interaction between participating vehicles.

All additional identifiers, such as the network address, are changed simultaneous with the usage of random pseudonyms.

[2] Except for by several compartmentalized PKI entities working together, to revoke certificates of misbehaving actor

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Justification

Identity randomization is mandated by C2C-CC in [10] and SAE by in [17]. V2X shouldn't be capable of tracking a vehicle. Devices sold in Europe must comply with General Data Protection Regulation (GDPR) hence preventing the linking of vehicle data that reveal its identity.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4 Coverage of Requirements

In this step we show how all Security and Privacy Requirements are covered by the suite of beforementioned Security Controls. For the sake of clarity, we add all information in the following two tables.

Security Control / Requirement (V-ITS)	Digital Signature	Message Authentication Codes	Payload Symmetric Encryption	Secure Storage	Secure Boot	Secure Communication Channel	Hardened OS	Access control policy enforcement
CID1: Ensure integrity of stored data	V	V		V	V	V	V	V
CID2: Ensure integrity of transmitted data	V	V				V		
CID3: Ensure integrity of received data	V	V						
CID4: Ensure availability of stored data				V			V	V
CID5: Ensure availability of transmitted data*								
CID6: Ensure availability of received data *								
CID7: Confidentiality of Stored Data			V	V			V	V
CID8: Confidentiality of Transmitted Data						V		
CID9: User Authorization	V				V		V	V
CID10: Integrity of sensor data	V	V				V	V	V
CID11: Ensure authenticity of received data	V							
CID12: Integrity of ITS software	V				V		V	V
CID13: Ensure isolation of stored data					V		V	V

TABLE 7: SECURITY REQUIREMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Before moving to the presentation of the way we fulfill the privacy requirements, we deem appropriate to put-forward a comment on data availability. Ensuring transmit and receive data availability is not achieved by, strictly speaking, a security control. Since in the connected vehicle, the media for data delivery is wireless, it is hence inherently unreliable. There is no way to ensure the data is reliably delivered, unless employing a reliable protocol, such as TCP/IP or IEEE 802.11 with ACK based transactions. The availability of transmitted and received data can be improved by implementing state of the art mechanisms of modern communication technologies in the transceiver, such as usage of antenna array, improving link budget on Tx and Rx sides by high output signal and excellent received sensitivity and using appropriate error corrections codes. Those methods are not in the scope of this document.

Privacy Control / Requirement	Secure Storage	Random Identity
CID14: Ensure anonymization of the traffic data	V	V
CID15: Ensure anonymity of stored data	V	V
CID16: Ensure anonymization of driver/vehicle transmitted data	V	V
CID17: Ensure driver - vehicle unlinkability	V	V

TABLE 8: PRIVACY REQUIREMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5 Security Controls classification

Proposed controls can be classified according to available taxonomy schemes. The chosen classification scheme relies on the NIST special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations [18], which is:

- a comprehensive security controls catalogue
- relatively recent
- well-established (both in the academic and industrial community) as an application guidance

The chosen publication is comparable-to and more comprehensive than considered alternatives such as the ISO/IEC 27000 family - Information security management systems, as evident from controls mapping table in Appendix H of [18]. In Table 9 each SAFERtec control is classified to the most appropriate NIST 800-53 control and the applicable control family.

SAFERtec Control	NIST 800-53 control	Control family classification
Digital Signature	SC-13 CRYPTOGRAPHIC PROTECTION	SYSTEM AND COMMUNICATIONS PROTECTION (SC)
Message Authentication Codes	SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY	IDENTIFICATION AND AUTHENTICATION (IA)
Payload Symmetric Encryption	SC-13 CRYPTOGRAPHIC PROTECTION	SYSTEM AND COMMUNICATIONS PROTECTION (SC)
Secure Storage	SC-28 PROTECTION OF INFORMATION AT REST	SYSTEM AND COMMUNICATIONS PROTECTION (SC)
Secure Communication Channel	SC-13 CRYPTOGRAPHIC PROTECTION	SYSTEM AND COMMUNICATIONS PROTECTION (SC)
Secure Boot	SC-28 PROTECTION OF INFORMATION AT REST	SYSTEM AND INFORMATION INTEGRITY (SI)
Plausibility Checks	SI-10 INFORMATION INPUT VALIDATION	SYSTEM AND INFORMATION INTEGRITY (SI)
Hardened OS	SC-3 SECURITY FUNCTION ISOLATION	SYSTEM AND COMMUNICATIONS PROTECTION (SC)
Access control policy enforcement	AC-3 ACCESS ENFORCEMENT	ACCESS CONTROL (AC)
Random Identity	IA-4 IDENTIFIER MANAGEMENT	IDENTIFICATION AND AUTHENTICATION (IA)

TABLE 9: CONTROLS CLASSIFICATION

The suggested scheme is flexible and scalable to support addition of any security and privacy control, while keeping close alignment to well defined and widely used classification system. The importance of this taxonomy relates to fact that it provides direct links between ITS-specific (SAFERtec) security controls and generic families of systems' security controls.
Its usability can be extended beyond the scope of the project (especially if enhanced); implementations of connected vehicle systems can rely on such a taxonomy to ease the decision

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

making on security policies such as the identification of common controls, the application of scoping considerations or assignment of control parameter values, the selection of additional controls and control enhancements etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

6 Conclusions

Vehicle to everything communication technology brings a big promise for improved transportation safety and efficiency. It also opens a new wireless interface into the vehicle, which must be protected against intentional and unintentional manipulation by external entities. SAFERtec deliverable "D2.3 Vulnerability Analysis" elicited the main security requirements for ITS stations in the context of selected use cases. In this deliverable, a set of security controls is carefully selected (following industrial best practices, regulations and standards) and provided as a recommendation for implementation of secure- and privacy-centric ITS station. The selected security controls will serve as a bridge from the WP2 modeling work to the introduction of a modular protection profile for the connected vehicle (WP3) to serve industry-oriented needs.

The document shows, that in order to achieve true security, a multi-layered approach to security is required, protecting each critical element of the system. A combination of cryptographic methods, secure storage, isolation enabling operating system and security focused HW design are utilized in order to achieve coverage of the security requirements.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

References

[1] IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages.

[2] T. G. Marko Wolf, "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module," 14th International Conference on Information Security and Cryptology, Seoul, 2011.

[3] M. Dworkin, NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.

[4] M. Dworkin, NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality.

[5] FIPS PUB 186-4 - FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - Digital Signature Standard (DSS).

[6] rfc5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation.

[7] W. Whyte, "Hardware Security Requirements for Vehicle-to-Everything Communications," https://icmconference.org/wp-content/uploads/E11c-Whyte.pdf, 2017.

[8] CAMP, "Hardware, Software and OS Security Requirements," 2018.

[9] D. T. A. W. W. W. V. K. T. H. ,. R. G. Benedikt Brecht, "A Security Credential Management System for V2X Communications," IEEE Transactions on Intelligent Transportation Systems, 2018.

[10] Basic System Profile Release 1.3.0, CAR 2 CAR Communication Consortium.

[11] C. Song, "Preventing exploits against memory corruption vulnerabilities," Georgia Institute of Technology, 2016.

[12] http://www.selinuxproject.org/page/Main_Page.

[13] C. Schaufler, Smack in Embedded Computing.

[14] "ARM Security Technology Building a Secure System using TrustZone® Technology," ARM Limited.

[15] "Mandatory Access Control," http://docs.automotivelinux.org/master/docs/architecture/en/dev/reference/security/part-5/1-MAC.html.

[16] ARM, "How to protect Automotive systems with ARM Security Architecture," ARM, 2016.

[17] S. International, "J2945/1: On-Board System Requirements for V2V Safety," SAE International, 2016.

[18] "Security and Privacy Controls for Federal Information, NIST Special Publication 800-53 (Rev. 4)," National Institute of Standards and Technology, Gaithersburg, 2013.

[19] E. Barker, L. Chen, A. Roginsky and S. M. , Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

[20] rfc5246 - The Transport Layer Security (TLS) Protocol Version 1.2.

[21] Secure Hardware Extension Functional Specification, Version 1.1.

[22] ETSI TS 102 941 V1.2.1 (2018-05) - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.

[23] FIPS Publication 180-2: SECURE HASH STANDARD.

[24] R. L. S. A. &. A. L. Rivest, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 1978.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

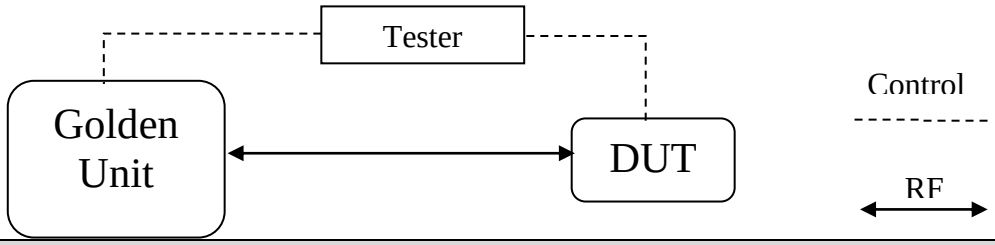
Appendices

Appendix A: Test cases for security controls

The chapter describes sample test cases for the validation of the Security Controls implementation (indicative set). For each chosen control, a Set-Up and test procedure are proposed.

Test ID	Test ID 01	**Test Name**	Digital Signature
Objective	Validate that the Safety Message is digitally signed by a valid certificate data structure.		

Set Up



Test Procedure

1) Configure the DUT to transmit 10 Safety Messages (BSM/CAM according to geography) per second (Maximal Rate)
2) Verify Safety Messages are properly structures (ASN.1 encoding, field values in range)
3) Verify Pseudonym changes according to configured interval
4) Verify all Safety Messages are properly signed with valid digital signature

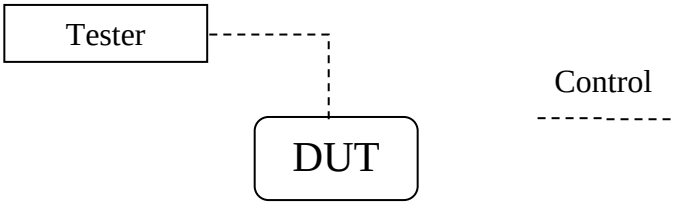
Expected Results

- All Safety Messages are properly structured
- Pseudonym change as expected
- All Safety Messages have valid digital signature

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Test ID	Test ID 02	Test Name	Secure Boot
Objective	Validate that security boot is enabled		

Set Up



Test Procedure

1) Load signed FW image to DUT
2) Power cycle, and check boot performed successfully
3) (Integrity check) Change a bit in data portion of the image
4) Power cycle, and validate boot fails
5) (Signature check) Return to original FW image and change a bit in signature portion of the image
6) Power cycle, and validate boot fails
7) (Rollback protection check) If available, load previous version of FW
8) Power cycle, and validate boot fails

Expected Results

- Step 2: Boot successful
- Step 4: Boot fails
- Step 6: Boot fails
- Step 8: Boot fails

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319