D7.5 –Contribution, Extensions and/or Recommendation to Standards

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:	D7.5 –Contribution, Extensions and/or Recommendation to Standards
Work package:	WP7 - Dissemination and Standardization
Task:	T7.3 Standardization Plan and Activities
Due Date:	M39
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR Sammy HADDAD / OPPIDA	**DATE** 30-March-2020
CONTRIBUTORS Andras Varadi / Commsignia Christos Kalloniatis / UPRC Costas Lambrinoudakis / UPRC Kostas Maliatsos / UPRC	**DATE** 05 April 2020 07 April 2020 07 April 2020 08 April 2020
REVIEWED BY Panagiotis Pantazopoulos / ICCS Mattia Zeni / TomTom	**DATE** 13 April 2020 13 April 2020
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

Document/Revision history

Version	Date	Partner	Description
V0.1	31/03/2020	OPP	First draft
V0.2	05/04/2020	Commsignia	Inputs to Section 4, 5 and Appendix B
V0.3	07/04/2020	UPRC	Inputs to Section 3
V0.4	08/04/2020	ICCS	Inputs to Section 10, 11, edits in the introduction and conclusions
V0.5	08/04/2020	Commsignia	Edits in Section 9 and Table 1
V0.6	09/04/2020	OPP	Version sent for internal review
V0.7	13/04/2020	ICCS	Internal review comments
V0.8	13/04/2020	TomTom	Internal review comments
V1.0	14/04/2020	OPP	Corrections in line with internal review comments - final version

Table of Contents

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

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
AFT	Assurance Framework Toolkit
ANSSI	Agence nationale de la sécurité des systèmes d'information (National Cybersecurity Agency of France)
CR	Comment Resolution
C-ITS	Cooperative Intelligent Transport Systems
C2C	Car-to-Car Communication Consortium
EN	European Norm
ETSI	European Telecommunications Standards Institute
GNSS	Global Navigation Satellite System
ICT	Information & Communication Technologies
ID	Identifier
ITS	Intelligent Transport Systems
ITS-S	ITS Station
MD	Misbehavior Detection
MoU	Memorandum of Understanding
MS Windows	Microsoft Windows
NTP	Network Time Protocol
PoTi	Position and Time management (ETSI EN 302 890-2)
PP	Protection Profile
SAP	Service Access Point
SAF	Security Assurance Framework
SF	Security Function
STF	Specialist Task Force
SOG-IS	Senior Official Group Information Security Systems
TVRA	Threat, Vulnerability and Risk Analysis (ETSI TR 102 893)
VCS	Vehicle C-ITS System

V2X	Vehicle-to-Everything
WI	Work Item
WG	Working Group
WG SEC	Security Working Group of C2C

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

This deliverable is concluding the work under the project's Task 7.3 on standardization. In deliverable 7.4 (first deliverable of the task) we have produced and updated a standardization plan in order to identify the relevant standardization opportunities and gaps (either de facto or official). Standardization bodies, ITS consortia and working groups were pointed by the plan which also included a timeline of actions carefully designed to maximize the likelihood of a SAFERtec contribution.

In this document we present the results of the execution of the above plan by the consortium partners. The achievements are discussed against the aforementioned targets. The relevant work-items that have been submitted to the attention of standardization bodies and relevant working groups, are detailed.

The project has managed to go further than the original plans and has addressed standardization opportunities that were not identified in D7.4. All those results are presented in this document.

With the work and achievements presented here, SAFERtec fulfilled one of its central objectives i.e., the significant contribution to relevant automotive security standards.

1 Introduction

1.1 Purpose of the Document

This document presents the result of the execution of the standardization plan defined during the project.

Different goals and action points have been set in the Standardization plan defined in deliverable 7.4. In order to efficiently execute this plan, we defined different standardisation working groups (i.e., groups of SAFERtec's partners to be involved on a specific standardization task) for which we defined action plans (i.e., actions and timeline to be achieved).

The final standardization objectives and the (originally) estimated likelihood of their fulfilment is depicted in Table 2.

Title	Likelihood
ETSI TR 102 893 - ITS TVRA	• Very likely
ETSI TR 103 460 – Malicious behaviour detection	• Likely
Protection Profiles (ETSI)	• Likely
SAF	• De facto / regulation ○ Likely
ETSI TR 103 415 - Pre-standardization study on pseudonym change management	• Unlikely
Vulnerability tests (NEW) (ETSI)	• ETSI ○ Unlikely • De facto / regulation ○ Unlikely

Table 2 The SAFERtec standardization plan (latest version)

In this document we present for each of those objectives the final results obtained. For each standardization target we present: the relevant SAFERtec working group, the originally planned actions and then, the (latest) activities and achieved results.

Furthermore, we discuss contributions made beyond the original plan. In fact, we managed to identify new opportunities that emerged in the course of the project that helped us to go beyond the initial plans. We present our PoTi EN contribution in Section 9 and detailed in Appendix B: The SAFERtec proposal for EN 302 890-2.

In Section 9 we present (possible) future opportunities and the standardization potential of the SAFERtec-developed AFT which is planned to be promoted to standardization in view of a large identified gap.

1.2 Intended readership

Besides the project reviewers, this deliverable is addressed to any interested reader (*i.e.*, Public dissemination level).

1.3 Inputs from other projects

This deliverable does not use any inputs from other projects.

1.4 Relationship with other SAFERTEC deliverables

This deliverable presents the result of the execution of the standardisation plan defined in D7.4 “SAFERtec Standardization Plan”.

2 Identification of partners representatives

In deliverable 7.4 we defined the following partners interfaces for standardization activities. The following abbreviations are used in the rest of the document:

Partner	Abbreviation
Matthieu Gay (CCS)	MGA
Guillemette Massot (CCS)	GMA
Kostas Maliatsos (UPRC)	KOM
András Váradi (COMM)	AVA
Sammy Haddad (OPP)	SHA
Leo Menis (AUT)	LME

Table 3 Partners' names abbreviations

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

3 ETSI TR 102 893 - ITS TVRA

3.1 Identified working group

Standardization	SAFERtec working group
ETSI TR 102 893 - ITS TVRA	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ UPRC (KOM) ▪ CCS (MGA) ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA) ▪ Commsigna (AVA)

It is to be noted that the above SAFERtec working group has been extended to include security and privacy experts to complete the required expertise to address TVRA needs. Dr Christos Kalloniatis and prof. C. Lambrinoudakis (both UPRC members) heavily contributed to the SAFERtec work submitted to the TVRA working group.

3.2 Initially planned actions points

ID	Action point description	Partners involved	Date
AP1.1	• Identify and contact ETSI working item responsible • Ask for possible inputs and their formats	Oppida Commsigna ICCS	31/01/2019
AP1.2	Formalize SAFERtec standardization inputs for the TVRA based on D2.3 and SAFERRtec privacy requirements (studied in WP2)	UPRC CCS	27/02/2019 -
AP1.3	Send standard modification request to the ETSI	CCS Autotalks	08/03/2019
AP1.4	Updates of the modification request in line with the iterative discussions with ETSI experts (that work was undertaken along the last semester of the project)	UPRC	Winter 2019

3.3 Activities and obtained results

One of the SAFERtec's goals was to provide flexible and efficient assurance framework for security and trustworthiness of connected vehicles in Europe. The project has delivered innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of ICT related Connected Vehicle and V2X systems. The cornerstone of SAFERtec was to provide assurance for security, safety and privacy aspects of Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

To achieve such goals, SAFERtec has begun with the definition of several use cases based on the stakeholders' experience. We have selected the most relevant of them for the project and we have built a new methodology based on three well-established methodologies EBIOS [1], Secure Tropos [2] and PriS [3] to formalize and address their safety, security and privacy issues. Our methodology helped us to define for each of those use cases potential threats, define security objectives and requirements to enforce appropriate countermeasures and protection mechanisms. We then generalized those results to a reference ITS architecture (based mainly on ETSI references).

More specifically, regarding privacy issues, the SAFERtec project has contributed to the development of the ETSI ITS TVRA document (TR 102 893). To this respect, and considering that:

- *A piece of information is secure when its content is protected, whereas it is private when the identity of its owner is protected*
- *In information society, privacy is adopted as a fundamental right of the individual and is related to issues like: the type of the information collected, how and for what purpose is this information used, how is it protected, shared, rented, sold or, otherwise, disseminated*
- *Privacy concerns the protection of the assets' owner identity from users that do not have the owner's consent to view/process their data*

the following assumption have been made:

<u>Participating Actors in the studied Use Cases:</u>

- **Vehicle and Nearby Vehicles**
  - *Pseudonym-ID*; It can be linked to the vehicle only through collaboration of the enrollment and authorization authorities (mainly for legal issues)
  - *Car-ID*; Directly identifies the car
- **RSUs**
- **Road User**
  - Pedestrians
  - Cyclists
  - etc.

<u>Privacy Requirements that should be satisfied:</u>

- **Anonymity of involved Road Users**

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

- **RSUs to Vehicles (I2V) - Broadcasting**
  - Assuming that the RSU does not relay a message received by a vehicle, there are no privacy requirements
- **Vehicle to Nearby Vehicles (V2V), Vehicle to RSU (V2I) and RSU relaying a vehicle's message to nearby Vehicles (I2V) - Broadcasting**
  - Unlinkability between pseudonym-id and car-id
  - Unlinkability between pseudonym-id and location data
- **Vehicle to Vehicle (V2V), RSU to Vehicle (I2V), Vehicle to RSU (V2I) - Unicast/Multicast**
  - Unlinkability between pseudonym-id and car-id
  - Unlinkability between pseudonym-id and location data
  - If the RSU offers Internet Access involving IPv6 addresses (like Media Downloading, Fleet Management etc.) the authentication / authorization of the vehicle by the service provider (e.g. Media server) will be realized through the IPv6 address which should be unlinkable with the car-id

Based on the above, we have studied the ETSI TS 102 940 [4] and ETSI TS 102 941 [5] standards and more specifically the privacy requirements set for the specified use cases (application classes).

Then, the use cases defined in the ETSI ITS TVRA document (TR 102 893) that do not appear in ETSI TS 102 940 have been classified into the appropriate "Application Class", thus inheriting the privacy requirements set for the specific application class (if any).

From the aforementioned analysis it can be noted that privacy requirements have been clearly specified by ETSI for only six use cases. SAFERtec has proceeded proposing Privacy requirements for all use cases (ETSI and TVRA) in alignment with the ones already proposed by ETSI. This information can be found in the right-most column of the sheet appearing in the Appendix C: Privacy requirements proposed to TVRA (associated with the ETSI 940/94 applications and TVRA use-cases).

This work has been carried over many months with different means. As ETSI full member Airbus allowed the SAFERtec consortium to be involved in the workgroup 5 which is dedicated to ITS security (ITSWG5).

CCS (Airbus) has participated on behalf of the consortium to many conference calls in the context of this work group, the first one with the TVRA rapporteur, M Scott CADZOW originally planned on the 2nd May 2019 postponed on the 10th May promoting the SAFERtec contribution on privacy aspects. This first call led us to participate to a face-to-face meeting on the 10th July 2019 at Sophia Antipolis to discuss about the improvements SAFERtec could provide to the TVRA standard.

Several calls have followed this physical meeting, on the 3rd of September 2019, the 9th of October, the 14th of January 2020 at the occasion of the ITS week, the 5th of March 2020 with the TVRA rapporteur and the whole SAFERtec consortium to specifically discuss about the SAFERtec contribution and the ways to improve it and finally, a last session on the 12th of March 2020 with the TVRA rapporteur was planned but has been postponed to a future date.

Nevertheless, Scott CADZOW, the TVRA rapporteur for ETSI, acknowledged our work carried out during all this last months and even though our work will stay anonymous in the TVRA standard, he kindly expressed his acknowledgment through an mail (see Appendix A: The ETSI rapporteur acknowledging the SAFERtec contribution to the ETSI TR 102 893).

4 ETSI TR 103 460 – Malicious behaviour detection

4.1 Identified working group

Standardization	SAFERtec working group
ETSI TR 103 460 – Malicious behaviour detection	• Leader ○ Oppida (SHA) • Participants ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA)

4.2 Initially planned actions points

ID	Action point description	Partners involved	Date
AP2.1	• Identify and contact ETSI working item responsible • Ask for possible inputs and their formats	Oppida Commsigna ICCS	31/01/2019
AP2.2	Identify from D 2.3 (Vulnerability analysis), D3.2 (PPs) and D5.2 potential plausibility checks to be potential inputs for the standard	UPRC CCS	31/06/2019
AP2.3	Send inputs to the ETSI via the ETSI member portal	CCS Autotalks	08/03/2019

4.3 Activities and obtained results

ETSI WG5 responsible for the initial study on Misbehaviour detection was contacted early on (during the ETSI workshop held in March 2019) about the SAFERtec project goals and links to misbehaviour detection.

During the project, the standard ETSI TR 103 460 was used to support the specifications of threats as well as to define foreseen standard compliant behaviour in terms of protection against such types of threats ("foreseen" as the standard is still in a draft stage).

Although SAFERtec did not push any direct contribution into the ETSI working group, the results obtained in Q4 2019 – Q1 2020 are considered as a potential contribution to be delivered to ETSI after the project; partners ICCS, UPRC and Commsignia has expressed interest to continue this progress after the project and deliver the outcome[1] once all internal verification has reached a certain maturity level (at each individual partner).

[1] ETSI members have already been informed about that intention during the SAFERtec final event.

SAFERtec has spent significant effort in order to include Misbehaviour Detection as part of the modular PP. Since the pre-standardization study on the subject is currently ongoing, the SAFERtec work was performed taking into account that the proposed security controls should: (i) suggest no modification in the current ITS stack, (ii) not require the exchange of extra ITS messages beyond the already used set, (iii) not require any extra data sets besides the information that already exists in the vehicle, (iv) not require any hardware modification.

The results of the procedure were the following:

- Definition of a set of seven plausibility checks as Misbehaviour Detection Information Flow Policy, that will help the V-ITS-S identify possible misbehaviour.
- Definition a set of Security Functional Requirements (SFRs) for the V-ITS-S modular PP that impose the application of the policy – as well as relevant audit and test SFRs.
- Definition a methodology for the determination of thresholds for some plausibility checks and application of the methodology through simulation.
- Testing and validation of some implemented plausibility checks with the use of the SAFERtec test-bench, after the modification of the Communication Unit images by the SAFERtec development team.

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

5 Protection Profiles (ETSI)

5.1 Identified working group

Standardization	SAFERtec working group
Protection Profiles	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ UPRC (KOM) ▪ CCS (MGA) ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA) ▪ Commsigna (AVA)

5.2 Initially planned actions points

ID	Action point description	Partners involved	Date
AP3.1	Request a time slot to the C2C WG SEC for SAFERtec PPs presentation during the C2C week to held place 11th to 14th of March 2019 in Guyancourt, France	Oppida Commsigna Autotalks	15/02/2019
AP3.2	Contact the ANSSI to present the SAFERtec project, the PPs and the SAF	Oppida CCS	15/02/2019
AP3.3	Present the SAFERtec PPs and propose to the C2C consortium to study the possibility to standardize the PP	Oppida Commsigna Autotalks	11/03/2019

5.3 Activities and obtained results

The modular PP has been presented together with the SAF at the C2C Week which took place in Renault premises in Guyancourt (France), from the 11th to the 14th of March 2019.

As identified in D7.4, the need for internationally recognize PP is important. Formally identified as mandatory by the Delegated Act on ITS systems, the need of such document is still strongly expressed by many actors of the ITS domain (existing activities in the C2C, the French automotive platform, C-Roads project, etc.). However, such document is rarely directly standardized via international standardization bodies such as ISO, CEN or ETSI. It is usually written and validated by the industry together with the certification entities (which is currently an ongoing C2C work) and only then possibly proposed to standardization bodies.

That's why we choose to exploit the C2C as a central dissemination point in the industrial community to promote our work and explore the standardization potential of the SAFERtec PP.

The modular approach drew the attention of the participants. Several discussions followed on the complexity of writing such a document and the differences with the current C2C PPs.

The C2C is not willing to go towards standardization yet for PPs. The point has been discussed, but they do not want to lose ownership of their documents. In fact, so far, the C2C PPs belongs to the C2C consortium, thus it allows them to update and manage this document at their will. This would not be the case if there was an agreement to have PPs standardized by the ETSI, even if C2C experts recognized the advantage to have a document more widely and actively managed (updated) over time, as happens with the ETSI's regular review and updates.

Currently, the C2C is running a work item to update their Vehicle C-ITS System (VCS) PP. Thanks to the MoU signed with the C2C, SAFERtec members have been allowed to have access and comment the document. Thus, a communication was initiated between the WG3 SAFERtec partners and the C2C VCS work item, discussing the various issues. Through this channel, SAFERtec is trying to help C2C to update their PP, invest on SAFERtec's results and also refine the SAFERtec PP by monitoring the new trends and policies in the ITS ecosystem.

Since the VCS PP is currently under discussion, until now, the main input was given by previous PP attempts – like C2C Vehicle Gateway [10] and the PFA PP [11]. SAFERtec contributed with the performance of a comparative study between the modular PP, [10], [11] and the preliminary results of the C2C VCS PP. In addition, SAFERtec has made comments and remarks on user roles, remote connection possibility, threats, threat agents, user identification/authentication, user access and information control policies. Besides the various suggestions, SAFERtec has adopted some identified good policies identified by the other PPs and performed some relevant requirements.

SAFERtec contribution is provided through communications undertaken by Oppida - SHA. The work is still on going.

As such, even if no standards will be produced or updated thanks to SAFERtec, the C2C VCS PP which should become a European reference (to get support from the SOG-IS) will benefits from SAFERtec's input and work results.

6 SAF

6.1 Identified working group

Standardization	SAFERtec working group
SAF	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ Oppida (SHA) ▪ UPRC (KOM) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA & MGA) ▪ Commsigna (AVA)

6.2 Initially planned actions points

ID	Action point description	Partners involved	Date
AP4.1	Request a time slot to the C2C WG SEC for SAF presentation during the C2C week to held place 2nd to 4th of July 2019 in Guyancourt, France	Oppida Commsigna Autotalks	17/05/2019
AP4.2	Contact the ANSSI to present the SAFERtec project, the PPs and the SAF	Oppida CCS	15/02/2019
AP4.3	Present the SAF to the SOG-IS with the ANSSI support define a European alternative to the regular CC certifications.	Oppida Commsigna Autotalks	December 2019

6.3 Activities and obtained results

SAF has been presented together with the PP at the C2C Week which took place in Renault premises in Guyancourt (France), from the 11th to the 14th of March 2019.

The presentation led to long and interesting discussions with the C2C members. Even if full support was not obtained to propose the SAF approach to the SOG-IS, the C2C WG SEC members agreed to open a new work item (WI) on the definition of a dedicated assurance framework for ITS and take SAF as one input (among others) to the study.

The WI is still ongoing at the time this deliverable is finalized. Oppida is participating to this WI and regularly promotes the SAF approach and its real adaptation to ITS needs.

The ANSSI has also been contacted several times. Different e-mail exchanges and unformal discussion with ANSSI members allowed us to make the ANSSI aware of the approach we propose. However, during the project it was not possible to meet them in a dedicated meeting. They cancelled the participation to SAFERtec’s plenary that took place in CCS premises in Elancourt on the 15th and the 16th of May 2019.

7 ETSI TR 103 415 - Pre-standardization study on pseudonym change management

7.1 Identified working group

Standardization	SAFERtec working group
ETSI TR 103 415 - Pre-standardization study on pseudonym change management	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ UPRC (KOM) ▪ CCS (MGA) ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA)

7.2 Initially planned actions points

ID	Action point description	Partners involved	Date
AP5.1	Contact working group coordinator to present SAFERtec project and identify possible collaborations or inputs to provide.	Oppida	15/02/2019

7.3 Activities and obtained results

The work done in the project was not mature enough to become a proposition for standardization. Discussions have been initiated with responsible of the ETSI WI in order to identify opportunities to collaborate.

SAFERtec's members that are also ETSI members have been invited to participate to the ETSI WI and make propositions, but by the end of the WI no SAFERtec results were ready to be pushed and proposed to be included in the ETSI study.

8 Vulnerability tests (ETSI)

8.1 Identified working group

Standardization	SAFERtec working group
Vulnerability tests (NEW)	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ CCS (MGA) ▪ Oppida (SHA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ CCS (GMA & MGA))

8.2 Initially planned actions points

ID	Action point description	Partners involved	Date
AP6.1	Formalize a vulnerability test plan based on the security requirement provided in the PPs (D3.2) and the actual vulnerability tests run in WP3 and 5. Contact the ANSSI in order to present the vulnerability test plan to their experts.	Oppida CCS	27/09/2019
AP6.2	Present the SAFERtec vulnerability test plan to the ANSSI and discuss possible collaboration with other SOG-IS members to define standardized tests plan to be used under the C-ITS Delegated act.	Oppida CCS	10/2019
AP6.3	Present the SAFERtec test plan to the SOG-IS members.	Oppida CCS	December 2019

8.3 Activities and obtained results

The maturity of the results provided by WP3 and WP5 tests did not allow us to formalize a real proposition. That's why we did not manage to fully achieve AP6.1.

Even if several vulnerability test-campaigns have been run, by several partners and many different interfaces have been tested, the obtained tests were in the end too specific to become standardization inputs.

In fact, the products tested were only one instance of ITS products developed in the context of a research project. They were neither fully mature (TRL9) nor fully standardized products (not all interfaces conformant to one identifiable standard). Thus, most of the tests done are not directly reusable for other products and further studies need to be done before trying to propose standardized vulnerability tests suites.

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

9 Activities outside D7.4 standardization plan

9.1 ETSI EN 302 890-2 - Position and Time management (PoTi)

9.1.1 Identified working group

The following group has been defined when the opportunity aroused to contribute to this standard.

Standardization	SAFERtec working group
ETSI EN 302 890-2 - Position and Time management (PoTi)	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ UPRC (KOM) ▪ CCS (MGA) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Commsigna (AVA) ▪ CCS (GMA)

9.1.2 Initially planned actions points

There were no planned actions for this work item since the possibility for SAFERtec to contribute to this standard emerged after the last update of our standardization plan defined in D7.4.

9.1.3 Activities and obtained results

SAFERtec partners have performed several iterations of review on the various versions of the draft EN standard during its drafting stage. After the standard reached 40-60% progress, changes have been delivered in two iterations (one at approximately 40% and one at 60%).

The first iteration focused on providing the STF key areas to cover in the EN. This input was sent in an informal way as no contribution (text) was foreseen (at phase AP2.2), rather comments were targeting missing aspects from the standard, mainly on the security concept and requirements. These general remarks were reflected by the security statements that have been included mainly in chapter 5.5.1.

The second iteration consisted of the SAFERtec proposed text (see Appendix B: The SAFERtec proposal for EN 302 890-2) to be inserted into the standard as a dedicated chapter for security. Most of the proposals relate directly to the SAFERtec PPs. This change was submitted and the SFT accepted the contribution for consideration. ETSI submission was performed on behalf of the project by Matthieu Gay (CCS). The next phase was the Comment Resolution meeting held on October 2 2019. The official meeting minutes of this meeting is not public (available only for ETSI members), however SAFERtec was represented by Andras Varadi. The text proposed as change during the CR meeting has already been processed by the STF with some modifications. The general response to the proposal was

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

positive[2], however the CR team did not agree on the scope and the lack of consensus meant that the contribution was not accepted. The reason for the refusal was that the contribution dealt with security issues, while currently the PoTi work item is basically concerned with the technical and functional architecture of the module. Although the group agreed that the PoTi module would benefit from such requirements, it claimed that the composition of the group has no security expertise in order to evaluate our proposal. Nevertheless, the ETSI WG5 (security) would need to propose a solution (develop a new standard) for applying the same security / privacy requirements for any of the respective modules (instead of editing every published or draft standard). In this context, the SAFERtec proposal would remain relevant, when the ETSI WG5 deals with the security and privacy requirements for the PoTi. SAFERtec partners that are also ETSI members have made some contacts exploring the possibility for a work item addressing PoTi-related security issues.

Despite the contribution being not accepted, the standard evolved to have a small subset of the security requirements (at chapter 5.5.1).

9.2 The SAFERtec AFT (Assurance Framework Toolkit) and its standardization potential

The standardization potential of the AFT developed in the WP6 of the project is reflected along two axes.

The first one relates to the shortage of relevant tools: CCMODE tool is a solution which allows to produce all the necessary CC documents and supplementary documents [6] but requires a certain environment management (EMT). In [7] a generator of security target templates, named "GEST" automatically generates security target templates from already evaluated and certified products. "TL SET", was introduced by Trusted Labs [8] as a smart editor for Security Targets and Protection Profiles using predefined libraries for identifying CC functional and assurance requirements; however, it is not available online anymore. Finally, "CC Toolbox" was a MS Windows application sponsored by the National Information Assurance Partnership (NIAP, the US government initiative) to assist users in writing security targets but is no longer supported and available. (Version 6.0f, 12 March 2001) [9]. None of the above tools has similar features to AFT (e.g., it is platform-independent).

The second axis is the lack of standardization attempts of such tools; to the best of our knowledge there is no relevant technical report/WI to specify the functionality of online tools that support automated CC-based evaluations inputs design. Yet, evaluation input content is strongly structured by the CC requirements and mandatory elements have to be produced to fulfil them. If many formats are possible, they are constrained by CC and greatly impacted by the used technologies; then, it is not easy for a (product) developer to know if the information he provides is conformant to these constraints. Defining standardized tools and inputs formats that fulfil both CC and ITS technologies constraints would greatly help developers to produce their mandatory evaluation input documents

[2] The PoTi rapporteur kindly declined to offer an unofficial letter to the SAFERtec consortium acknowledging our contribution but did mention that the proposal has been written down in the minutes and most notably, that has been considered as very interesting.

and ease the evaluator work thanks to the standardization of the elements to be evaluated. This would greatly lower evaluation costs and difficulties for all actors.

These points together with the commitment of the involved partners, ICCS (as the AFT designer and developer) and OPP (as an AFT consultant and an accredited CC laboratory), to explore opportunities beyond the SAFERtec lifetime suggest the strong potential of AFT to reach standardization fora and be favourably considered.

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

10 Conclusions

The SAFERtec project has successfully met one of its core objectives i.e., to make a contribution (or recommendation) to one or more relevant standards in the area of automotive cyber-security. The relevant achievements have been detailed in the document at hand.

The SAFERtec work has found its (direct) way to one standard on risk analysis of ITS communications (i.e., TVRA) and has exercised influence on one more on position and time service (i.e., PoTi). Furthermore, the project has carried-out experimental work on misbehaviour detection and is about to bring the relevant results to the attention of the ETSI experts working on a relevant pre-standardization study. On a more ambitious note, the project partners seek to invest effort on SAFERtec WP6 work-items and pursue the standardization opportunities for the AFT software developed in the project.

Given that the TVRA has been and remains one flagship document in the area of collaborative ITS risk analysis, the SAFERtec project has already managed to leave a very important footprint on the relevant state-of-the-art and influence future standardization research to be carried-out by both industry and academia.

11 References

[1] EBIOS 2010 Expression of Needs and Identification of Security Objectives. [Online]. Available: https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/

[2] H. Mouratidis and P. Giorgini, "Secure tropos: a security-oriented extension of the tropos methodology." Int'l Journal of Software Engineering and Knowledge Engineering, vol. 17, no. 2, pp. 285–309, 2007.

[3] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the PriS method," Requirements Engineering, vol. 13, no. 3, pp. 241–255, Sep 2008.

[4] ETSI ITS communications security architecture and security management (ETSI TS 102 940 V1.3.1 2018-04) [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

[5] ETSI Intelligent Transport Systems (ITS); Security; Trust and Privacy Management (ETSI TS 102 941 V1.3.1 2019-02) [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v010301p.pdf

[6] D. Rogowski, "Software Implementation of Common Criteria RelatedDesign Patterns," 2013 Federated Conference on Computer Science and Information Systems, Krakow, 2013, pp. 1147-1152.

[7] D. Horieet al.,"GEST: A generator of ISO/IEC15408 Security Targettemplates". Computer and Information Science 2009, pp 149-158.

[8] Trusted Labs Accredited CC Evaluator https://www.trusted-labs.com/

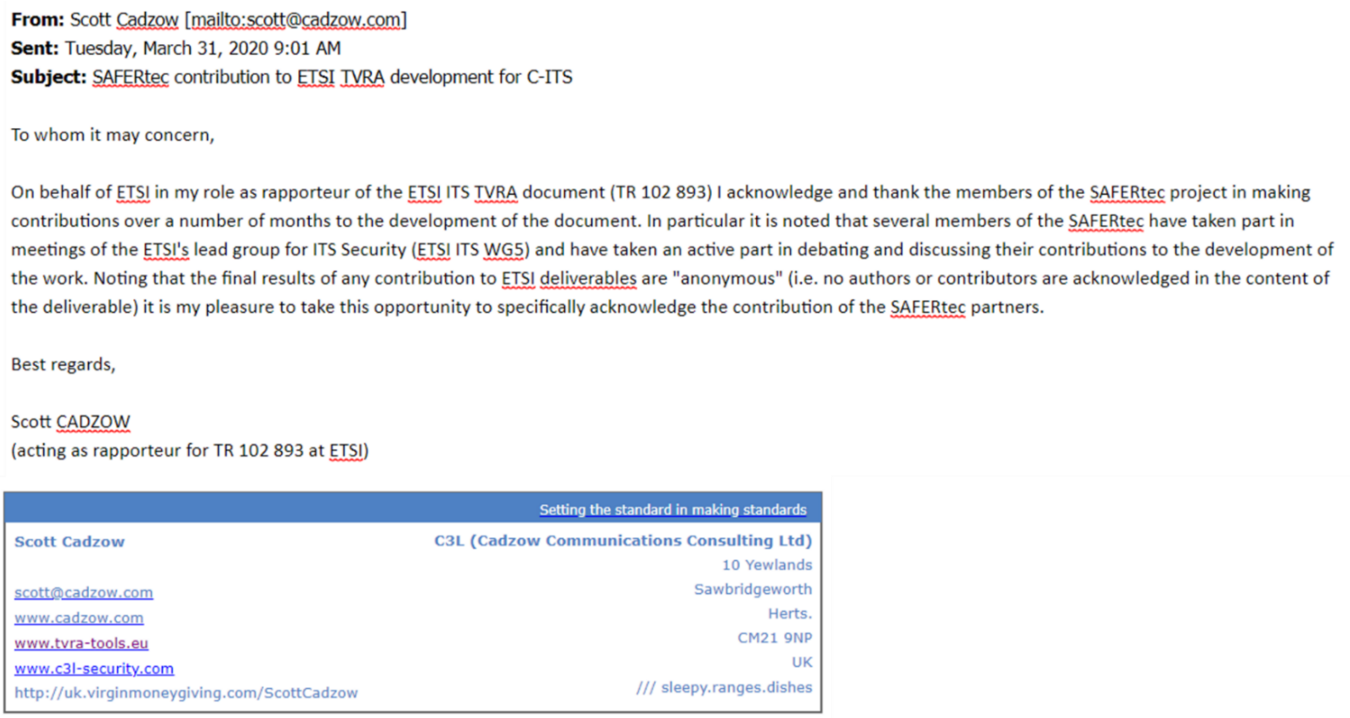
[9] CC Toolbox [Online]. Available: http://pagenotes.com/writings/ccToolbox6f/

[10] Protection Profile V2X Gateway CAR 2 CAR Communication Consortium – Working Group Security (WG SEC).

[11] PlateForme Automobile (PFA), "Protection Profile V2X Gateway", 04/12/2018

Appendices

A: The ETSI rapporteur acknowledging the SAFERtec contribution to the ETSI TR 102 893



From: Scott Cadzow [mailto:scott@cadzow.com]
Sent: Tuesday, March 31, 2020 9:01 AM
Subject: SAFERtec contribution to ETSI TVRA development for C-ITS

To whom it may concern,

On behalf of ETSI in my role as rapporteur of the ETSI ITS TVRA document (TR 102 893) I acknowledge and thank the members of the SAFERtec project in making contributions over a number of months to the development of the document. In particular it is noted that several members of the SAFERtec have taken part in meetings of the ETSI's lead group for ITS Security (ETSI ITS WG5) and have taken an active part in debating and discussing their contributions to the development of the work. Noting that the final results of any contribution to ETSI deliverables are "anonymous" (i.e. no authors or contributors are acknowledged in the content of the deliverable) it is my pleasure to take this opportunity to specifically acknowledge the contribution of the SAFERtec partners.

Best regards,

Scott CADZOW
(acting as rapporteur for TR 102 893 at ETSI)

Setting the standard in making standards

Scott Cadzow	C3L (Cadzow Communications Consulting Ltd)
	10 Yewlands
scott@cadzow.com	Sawbridgeworth
www.cadzow.com	Herts.
www.tvra-tools.eu	CM21 9NP
www.c3l-security.com	UK
http://uk.virginmoneygiving.com/ScottCadzow	/// sleepy.ranges.dishes

B: The SAFERtec proposal for EN 302 890-2 - PoTi entity security requirements

The PoTi entity should have the following security-privacy objectives:

- Authenticity
- Integrity
- Privacy
- Anonymity
- Accountability

The role of the PoTi in the ITS-S does not indicate the need for a confidentiality objective. Confidentiality should be imposed, depending on the use case, by the overlaying application using the positioning and time information extracted by the module.

As a service PoTi should be protected against security threats that may compromise the achievement of the aforementioned objectives.

The attack surface for the PoTi consists of the defined interfaces defined in Sec. 5.5, as well as debugging/programming or proprietary interfaces used for installing, updating and activating the PoTi service. In the following security and risk analysis, the following assumptions on the operation of the PoTi have been made:

- Sources of information for the PoTi include:
    - GNSS.
    - Vehicle sensors related to vehicle motion and dynamics.
    - Time servers.
    - Raging service announcement from the ITS network or the overlaying cellular.
    - Position and time information from other stations of the ITS-S constellations.
    - Overlaying applications providing augmented estimated.
- PoTi facilities may be used by:
    - Other facilities that require position and time information.
    - ITS Applications that require position and time information.
    - Network and radio protocols that require timestamping or position information.

Threats:

The following threats have been identified. They can possibly cause harm in the PoTi functionality and consequently in the operation of the ITS-S:

- **Spoofing**
    - An attacker is disguised as a legitimate source of position and timing references (e.g. GNSS, NTP server, etc.) and sends messages with the intention to trick the PoTi in producing inaccurate estimates.

- **Unauthorized access:**
  - Users, applications or services try to access PoTi functions and information not allowed to them, to modify, delete data or mispresent vehicle actions and activities.
- **Malicious Code Injection – Application Modification :**
  - The specific threat involves the malicious injection or introduction of code into the PoTi software. An attacker could also alter the code to take root permissions of the device that hosts the PoTi. In this way an attacker achieves abnormal operation and handles the system resources.
- **Extreme Solicitation:**
  - An attacker could perform a DoS attack, by flooding the service and thus making the system unavailable to legitimate applications and users or blocking the service access to updated and accurate sources of position/timing information.
- **Data Leakage:**
  - Attackers could try to leak data from the PoTi to third parties who should not receive this data. The specific threat includes disclosure of functional, location, personal information and software details.
- **Intentional or unintentional data tampering:**
  - An application, service or user intentionally or unintentionally tampers position and timing information that are either provided to the PoTi as input or ate originated by PoTi.

Security Policies for the PoTi:

The following polices regarding authorization, access and information flow are recommended in order to minimize impact and the likelihood of an attack implementing a threat:

- Authorized users, services and application that access the PoTi resources shall be held accountable for actions within the system.
- All users/applications/services gaining access to the PoTi services and resources shall have a unique identifier not to be shared with other users.
- The role of the Administrator with the right to update, upgrade or modify the PoTi system (code, interfaces, functionalities) shall be separate and distinct from other users. The administrative authority shall be given only to trusted entities and it should be as restricted as possible supporting only the administrative duties the use has.
- The role of the user (a) providing information sources for the PoTi and the user (b) of the PoTi services should be distinguished. User (a) shall be held accountable for the quality of provided information.
- All users shall be required to update credentials and change passwords at intervals defined by the adopted password management policy.
- The PoTi may use the security services through the SF-SAP provided by:
  - The hardware and software security modules of the ITS-S.
  - The misbehavior detection module (it is assumed part of the security vertical ITS layer)

- The security services are considered trusted, if the link of the SF-SAP is isolated (physically, or virtually) – i.e. not shared with any other entity. The SF-SAP link should be encrypted, requiring authenticity to allow information exchange over the SF-SAP. The ITS-S shall protect the SF-SAP from spoofing and manipulation either by physical or logical methods.
- The ITS-S shall cryptographically verify the integrity and validity of all applications/users interacting with the PoTi as sources using digital signatures prior to installation. No validated sources of information will be used by the PoTi.
- An incoming message is taken into account only if it is digitally signed. The policy shall include:
  - GNSS messages – e.g. under the Galileo Public Regulated Service.
  - NTP messages and network time synchronization protocols.
  - Ranging messages
  - ITS messages from other ITS stations of the ITS constellation.
- All digitally-signed sources of information regarding time or position shall retain an updated quality/confidence metric that will allow the PoTi system to properly weight the validity and the immediacy of the piece of information. If no metric (or method to extract one) is provided the piece of information should not be used.
- The PoTi system shall take measures against NTP-related distributed denial of service attacks (use security countermeasures, non-public NTP servers, etc.)
- The PoTi service shall retain a service for self-check (possibly in communication with the misbehaviour protection module) and it shall enter a secure state in case of a detected functional/operational failure (e.g. failing systematically to provide accurate time stamps or/and position estimates).
- The PoTi service shall ensure that the ID of the ITS-S is not made available to any external attacker/observer.
- The PoTi service shall ensure that no external attacker/observer is able to associate the user location or/and route with the actual ID of the ITS-S.
- Records of user access details and log of modifications are kept in order to provide evidence for security incident investigations.
- Any unauthorised access shall be reported to the system administrator, to the ITS management entity.
- The PoTi service shall contain validated services that perform conversions between time systems and reference coordination systems in respect to the ITS-S reference positions and confidences. The PoTi service shall only use information if the reference system is known, and if there is a validated, available function able to perform transformation if needed.
- The PoTi service should be able to self-test, benchmark and take into account the processing latency imposed by the application of the applied security protocols and controls in order to minimize the station clock deviation.

The aforementioned policy rules shall be taken into account during the design, development and operation of the PoTi module of the ITS-S. The development/administration entity shall enforce security controls and countermeasures that impose the policies.

C: Privacy requirements proposed to TVRA (associated with the ETSI 940/94 applications and TVRA use-cases)

ETSI 940/941			USE CASES DEFINED IN ETSI 940 AND TVRA THE ONES HIGHLIGHTED IN GREEN APPEAR ONLY IN TVRA and they have been allocated BY SAFERtec to the appropriate APPLICATION CLASS	PRIVACY REQUIREMENTS PROPOSED BY SAFERtec
Application Class	**Application**	**Privacy Requirements according to ETSI 940**	**Use Cases**	**Proposed Privacy Requirements (aligned with the ones proposed by ETSI 940 - column C)**
Active road safety	Driving assistance - Co-operative Awareness (CA)	Unlinkability between CAM messages and Personal Identity	Emergency vehicle warning	-
			Slow vehicle indication	Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data
			Lane Change Manoeuvre	
			Traffic condition warning	
			Across traffic turn collision risk warning Merging Traffic Turn Collision Risk Warning	
			Co-operative merging assistance Intersection collision warning Co-operative forward collision warning Lane Change Manoeuvre	
	Driving assistance - Road Hazard Warning (RHW) In the ETSI 940 standard three different categories have been	-	Emergency electronic brake lights Wrong way driving warning (infrastructure based)	Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data
			Merging Traffic Turn Collision Risk Warning	
			Co-operative forward collision warning	
			Intersection collision warning	
			Stationary vehicle - accident	
			Stationary vehicle - vehicle problem Traffic condition warning	

ETSI 940/941			USE CASES DEFINED IN ETSI 940 AND TVRA THE ONES HIGHLIGHTED IN GREEN APPEAR ONLY IN TVRA and they have been allocated BY SAFERtec to the appropriate APPLICATION CLASS	PRIVACY REQUIREMENTS PROPOSED BY SAFERtec
Application Class	**Application**	**Privacy Requirements according to ETSI 940**	**Use Cases**	**Proposed Privacy Requirements (aligned with the ones proposed by ETSI 940 - column C)**
	identified: **Static**: with no need for Privacy Reqs **Interactive:** with Privacy Requirements which are not however specified since they were considered to be out of the scope of the standard **Area HWs:** with no need for Privacy Reqs		Vulnerable road user Warning	Anonymity of the Involved Road User **For V2V case:** Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data
			Wrong way driving warning (infrastructure based)	-
			Signal violation warning	-
			Roadwork warning	-
			Decentralized floating car data - Hazardous location	Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data
			Decentralized floating car data - Precipitations	
			Decentralized floating car data - Road adhesion	
			Pre-crash sensing warning (Indication)	
			Pre-crash sensing warning (Data exchange)	
			Co-operative glare reduction	
			Decentralized floating car data - Visibility	

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

ETSI 940/941			USE CASES DEFINED IN ETSI 940 AND TVRA **THE ONES HIGHLIGHTED IN GREEN APPEAR ONLY IN TVRA and they have been allocated BY SAFERtec to the appropriate APPLICATION CLASS**	**PRIVACY REQUIREMENTS PROPOSED BY SAFERtec**
Application Class	**Application**	**Privacy Requirements according to ETSI 940**	**Use Cases**	**Proposed Privacy Requirements (aligned with the ones proposed by ETSI 940 - column C)**
			Decentralized floating car data - Wind Vulnerable road user Warning Pre-crash sensing warning Co-operative glare reduction	
Cooperative traffic efficiency	Co-operative Speed Management (CSM)	-	Regulatory/contextual speed limits notification	-
		-	Curve Warning	-
		-	Traffic light optimal speed advisory	-
	Co-operative Navigation (CN)	-	Traffic information and recommended itinerary	-
		-	Public transport information **(Only for 'service', not for 'advertisement')**	Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data
		-	In-vehicle signage	-
Co-operative local services	Location Based Services (LBS)	-	Point of Interest notification **(Only for 'service', not for 'advertisement')**	Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data
		-	Automatic access control and parking management **(Only for 'service', not for 'advertisement')**	
		-	ITS local electronic commerce	
		-	Media downloading	
		-	Insurance and financial services	

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

ETSI 940/941			USE CASES DEFINED IN ETSI 940 AND TVRA **THE ONES HIGHLIGHTED IN GREEN APPEAR ONLY IN TVRA and they have been allocated BY SAFERtec to the appropriate APPLICATION CLASS**	**PRIVACY REQUIREMENTS PROPOSED BY SAFERtec**
Application Class	**Application**	**Privacy Requirements according to ETSI 940**	**Use Cases**	**Proposed Privacy Requirements (aligned with the ones proposed by ETSI 940 - column C)**
Global internet services	Communities Services (CS)	-	Fleet management	
		-	Loading zone management	
		-	Theft related services/After theft vehicle recovery	
	ITS station Life Cycle Management (LCM)	-	Vehicle software/data provisioning and update	Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data Unlinkability between IPv6 address and car-id
		-	Vehicle and RSU data calibration	Unlinkability between pseudonym-id and car-id Unlinkability between pseudonym-id and location data
	Transport related electronic financial transactions	-		-