White Paper on Misbehaviour Detection and Reporting to Misbehaviour Authority

CAR 2 CAR Communication Consortium

About the C2C-CC

Enhancing road safety and traffic efficiency by means of Cooperative Intelligent Transport Systems and Services (C-ITS) is the dedicated goal of the CAR 2 CAR Communication Consortium. The industrial driven, non-commercial association was founded in 2002 by vehicle manufacturers affiliated with the idea of cooperative road traffic based on Vehicle-to-Vehicle Communications (V2V) and supported by Vehicle-to-Infrastructure Communications (V2I). The Consortium members represent worldwide major vehicle manufactures, equipment suppliers and research organisations.

Over the years, the CAR 2 CAR Communication Consortium has evolved to be one of the key players in preparing the initial deployment of C-ITS in Europe and the subsequent innovation phases. CAR 2 CAR members focus on wireless V2V communication applications based on ITS-G5 and concentrate all efforts on creating standards to ensure the interoperability of cooperative systems, spanning all vehicle classes across borders and brands. As a key contributor, the CAR 2 CAR Communication Consortium and its members work in close cooperation with the European and international standardisation organisations.

Disclaimer

The present document has been developed within the CAR 2 CAR Communication Consortium and might be further elaborated within the CAR 2 CAR Communication Consortium. The CAR 2 CAR Communication Consortium and its members accept no liability for any use of this document and other documents from the CAR 2 CAR Communication Consortium for implementation. CAR 2 CAR Communication Consortium documents should be obtained directly from the CAR 2 CAR Communication Consortium.

Document information

Number:	2092	**Version:**	1.0	**Date:**	2021-12-17
Title:	Misbehaviour Detection and Reporting to Misbehaviour Authority			**Document Type:**	WP
Part of release	N.a.				
Release Status:	Public				
Status:	Final				

Table 1: Document information

Changes since last release

Date	Changes	Edited by	Approved
2021-12-17	Initial release	Release Management	Steering Committee

Table 2: Changes since last release

Table of contents

List of Tables

List of Figures

Abbreviations

AA	Authorization Authority (synonym to PCA)
AD	Autonomous Driving
ADAS	Advanced Driver Assistance System
AI	Artificial Intelligence
AP	Access Point
AT	Authorization Ticket (synonym to PC)
CAM	Co-operative Awareness Message
CCMS	Cooperative-ITS Security Credential Management System
C-ITS	Cooperative Intelligent Transport Systems
CP	Certificate Policy
CPA	Certificate Policy Authority
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
DCC	Decentralized Congestion Control
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority (synonym to LTCA)
EC	Enrolment Credential (synonym to LTC)
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System Station
LTC	Long Term Certificate (synonym to EC)
LTCA	Long Term Certificate Authority (synonym to EA)
MA	Misbehaviour Authority
MR	Misbehaviour Report
ML	Machine-Learning
OBU	On-Board Unit
PC	Pseudonym Certificate (synonym to AT)
PCA	Pseudonym Certificate Authority (synonym to AA)
PKI	Public Key Infrastructure
RCA	Root Certificate Authority
RSU	Road-Side Unit
SAP	Service Access Point

SCM	Secure Communication Module
SCMS	Security Credential Management System
SEP	Security Event Processor
SOC	Security Operations Center
TLM	Trust List Manager
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to everything
VCS	Vehicle C-ITS Station
VSA	V2X Security Architecture
VSS	V2X Security System

1. Introduction

1.1 Abstract

This white paper presents the results of projects, in their Research and Development phase, and Testbeds on security architectures, on-board misbehaviour detection mechanisms, and reporting to a Misbehaviour Authority. The focus of the survey conducted in this paper was Day1 C-ITS applications.

The paper also lists existing standards that specify misbehaviour framework architectures and identifies future work to be done on Day2+ C-ITS applications to propose further privacy-friendly local misbehaviour detection mechanisms and reporting protocol.

1.2 Survey of document

The survey conducted in this paper covers EVITA, SEVECOM, PRESERVE, SCA, nIoVE H2020, SecForCARS projects.

2. Overview of Existing Work on Misbehaviour Detection and Reporting via a Central Authority

2.1 EVITA, PRESERVE and FOTs on V2X

2.1.1 EVITA Project

EVITA (E-safety Vehicle Intrusion protected Applications) was a European project, funded under the 7th Framework Program (FP7) held between 2008-2011. EVITA proposed a security architecture that offers adaptable and modular security services. The architecture can be customized to the needs of overall in-car security and the protection of V2X communication [RD-2].

The proposed software security framework implemented in ECUs provides standardized security interfaces to the applications via the security stub. The security stub accesses the security modules, which are offered by the security framework. The security modules can be configured specifically, and appropriate plug-ins can be deployed that implement concrete security mechanisms. Such modular security architecture allows to abstract the security mechanisms from the application software, which simplifies the interchangeability.

This security framework includes the following functionalities.

- Access control: Management and enforcement of policies,
- Authentication services: Depending on requirements, support various methods for identification and authentication of entities (support of pseudonyms for entity identification),
- Secure communication: Establishment of authenticated and/or confidential communication channels,
- Intrusion detection: Modules provide means to detect and manage intrusions at different abstractions levels.

2.1.2 PRESERVE Project

PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) was an FP7 funded European project which started in 2011 and ended in June 2015. PRESERVE's main objective was to design, implement, and test a secure and scalable V2X security subsystem.

The goal of PRESERVE was to integrate the results of projects SeVeCom, PRECIOSA, and EVITA to provide a single consistent security and privacy solution for V2X communication. The first version of V2X Security Architecture (VSA) was built as a combination of modules provided by the three previous projects.

Security and privacy aspects are delegated to a V2X security subsystem (VSS) included in the ITS stations which enables secure communication between vehicles or between vehicle-infrastructure and secure communications with the security management infrastructure (PKI) for trust and privacy management.

Figure 1 shows the PRESERVE V2X security architecture and its link with the ITS communication protocol stack (based on ETSI standard) and details the services provided by the security stack (V2X Security System). PRESERVE provided key exploitable results, such as a close-to-market V2X Security Architecture (VSA) considering:

- External V2X communication security
- Onboard communication & data security

- Public Key Infrastructure (PKI) for pseudonyms certificate management
- Privacy protection

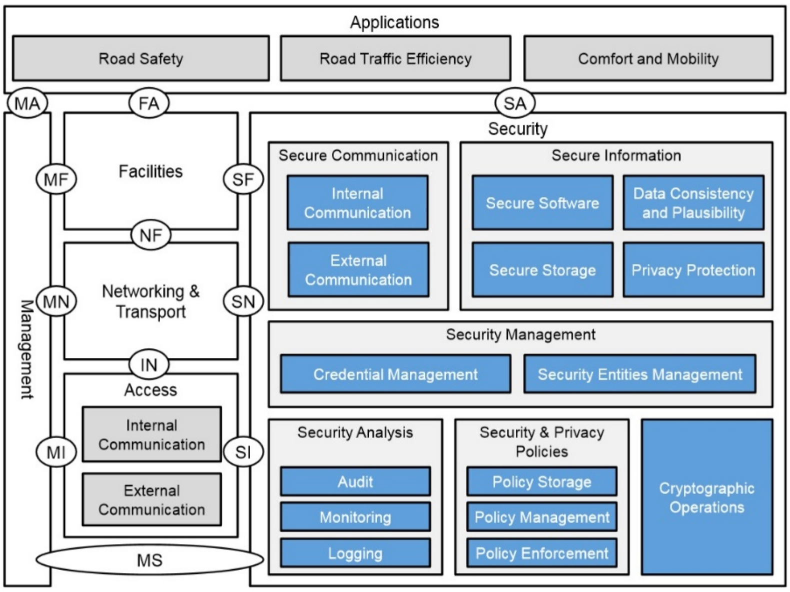


Figure 1: Abstract PRESERVE Vehicle Security Architecture

PRESERVE VSA is conforming to the ETSI ITS architecture (EN 302 665) and has contributed to the specification of ETSI internal interfaces with Security esp. the definition of SN-SAP which addresses the definition of Meta-data flows and cross-layer signalling of security information. Integration of security in the communication stack according to ETSI EN 302 636-4-1 (Geo Networking) was demonstrated in various PRESERVE VSS implementations.

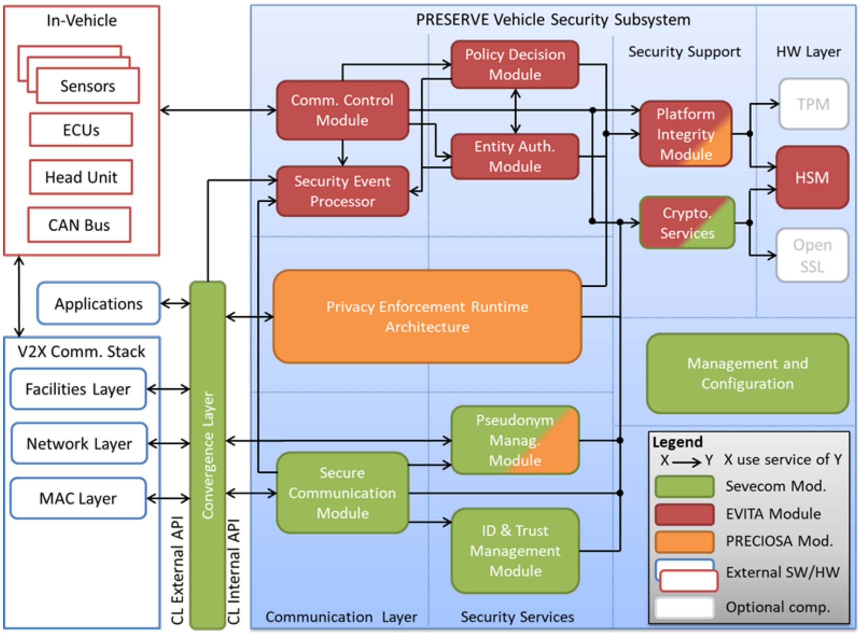
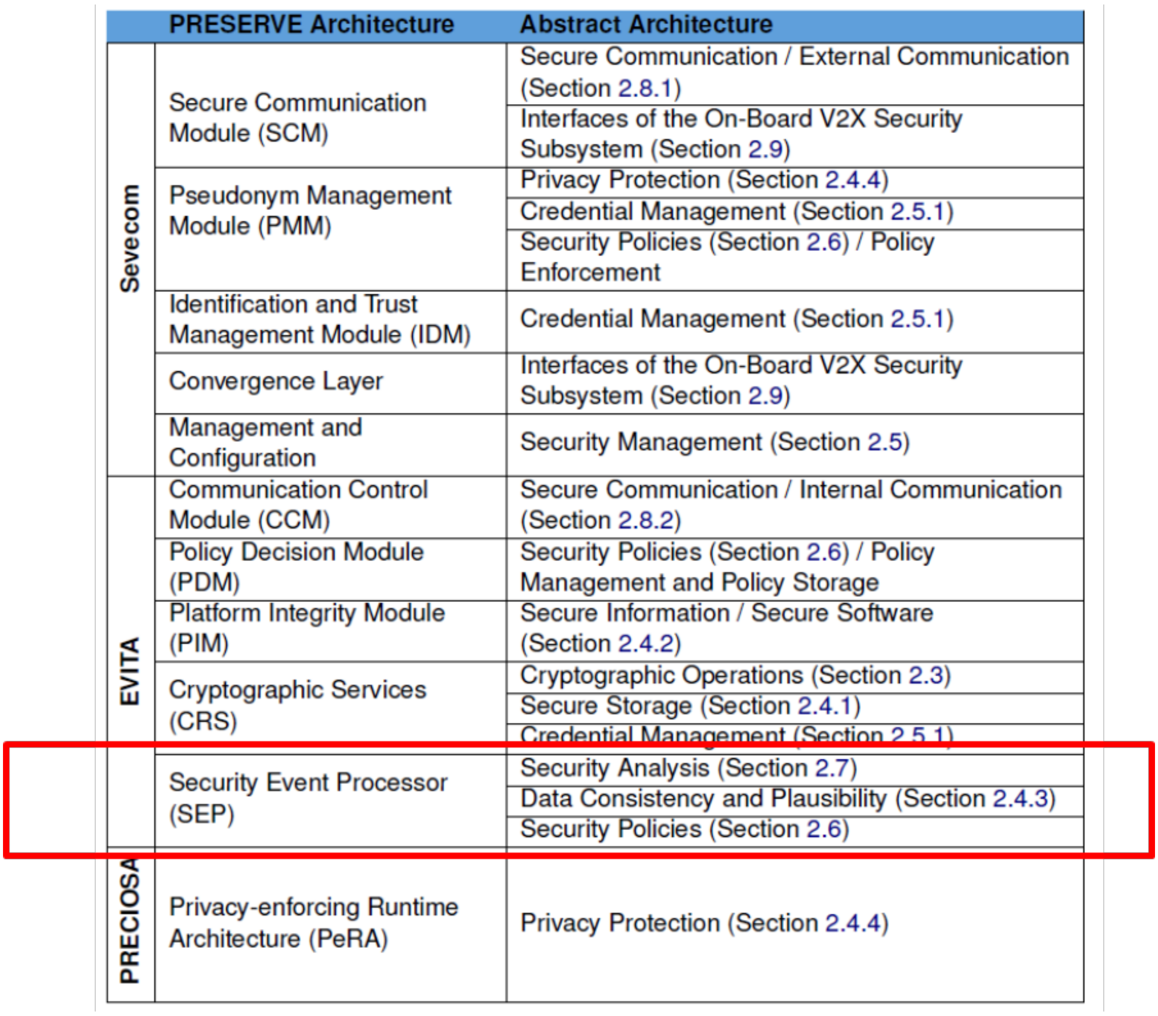


Figure 2: PRESERVE Detailed (implementation) Architecture

Figure 2 shows the detailed implementation VSS architecture. A mapping between the VSA abstract architecture & implementation components is specified in D3.1 and is summarized in Figure 3 below.



PRESERVE Architecture		Abstract Architecture
Sevecom	Secure Communication Module (SCM)	Secure Communication / External Communication (Section 2.8.1)
		Interfaces of the On-Board V2X Security Subsystem (Section 2.9)
	Pseudonym Management Module (PMM)	Privacy Protection (Section 2.4.4)
		Credential Management (Section 2.5.1)
		Security Policies (Section 2.6) / Policy Enforcement
	Identification and Trust Management Module (IDM)	Credential Management (Section 2.5.1)
	Convergence Layer	Interfaces of the On-Board V2X Security Subsystem (Section 2.9)
	Management and Configuration	Security Management (Section 2.5)
EVITA	Communication Control Module (CCM)	Secure Communication / Internal Communication (Section 2.8.2)
	Policy Decision Module (PDM)	Security Policies (Section 2.6) / Policy Management and Policy Storage
	Platform Integrity Module (PIM)	Secure Information / Secure Software (Section 2.4.2)
	Cryptographic Services (CRS)	Cryptographic Operations (Section 2.3)
		Secure Storage (Section 2.4.1)
		Credential Management (Section 2.5.1)
	Security Event Processor (SEP)	Security Analysis (Section 2.7)
		Data Consistency and Plausibility (Section 2.4.3)
		Security Policies (Section 2.6)
PRECIOSA	Privacy-enforcing Runtime Architecture (PeRA)	Privacy Protection (Section 2.4.4)

Figure 3: PRESERVE VSA Abstract & Implementation Architecture

The SEP module provides mechanisms for intrusion detection, firewall tasks and intrusion response mechanisms. It also includes functionality for performing plausibility checks on incoming V2X messages. SEP includes variable intrusion and misbehaviour detection policies that allow detected security events to be linked to certain responses (e.g., alerts, shutdowns).

The SEP module's main tasks are summarized hereafter, and Figure 4 shows its interactions with the other modules:

- SCM relies on SEP component for data plausibility/consistency checking on incoming V2X messages. The SCM can register as a listener at the SEP in order to get informed in case of misbehaviour detections.
- SCM shall forward all incoming messages to the SEP in order to check the plausibility of the message content (based on mobility data). The SEP applies basic plausibility/consistency checks as specified in the set of basic Data Consistency and Plausibility checks (see Figure 5). The result may consider only a single message that is returned to the SCM or generate information about the sender's trustworthiness.
- Via the CL_API, local V2X applications can also send log events regarding specific misbehaviour detections to the SEP. Detection of application specific misbehaviour is not task of the VSS.

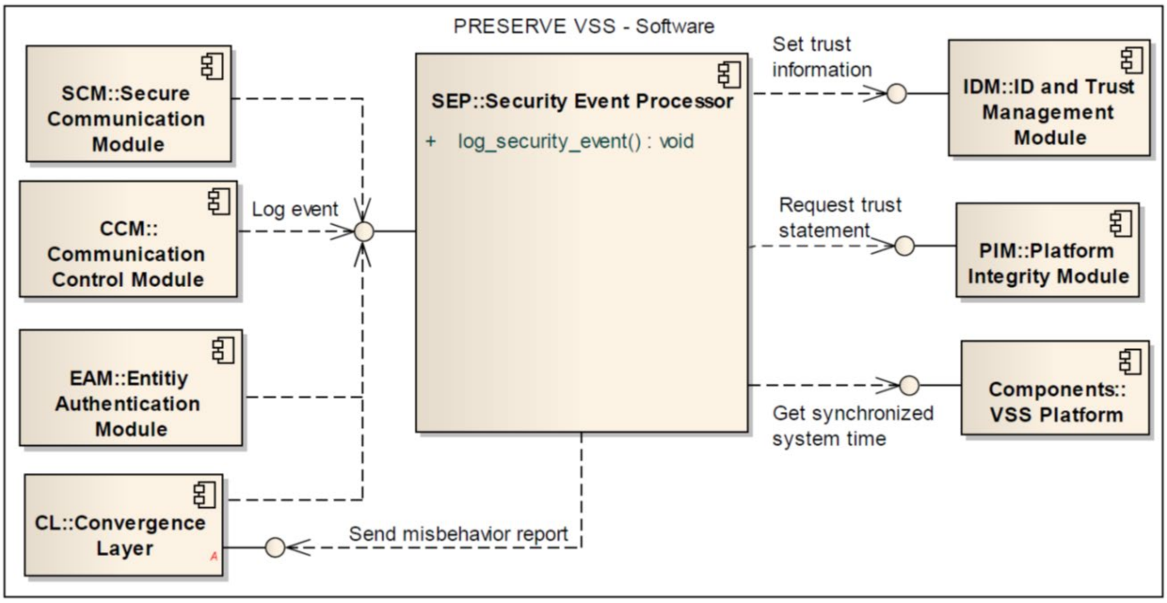

PRESERVE VSS - Software
SCM::Secure Communication Module
CCM:: Communication Control Module
EAM::Entitiy Authentication Module
CL::Convergence Layer
Log event
SEP::Security Event Processor
+ log_security_event() : void
Send misbehavior report
Set trust information
IDM::ID and Trust Management Module
Request trust statement
PIM::Platform Integrity Module
Get synchronized system time
Components:: VSS Platform

Figure 4: Security Event Processor

The SEP is in charge of managing, evaluating and generating the MR which can be sent to the PKI via the Convergence Layer (CL_API).

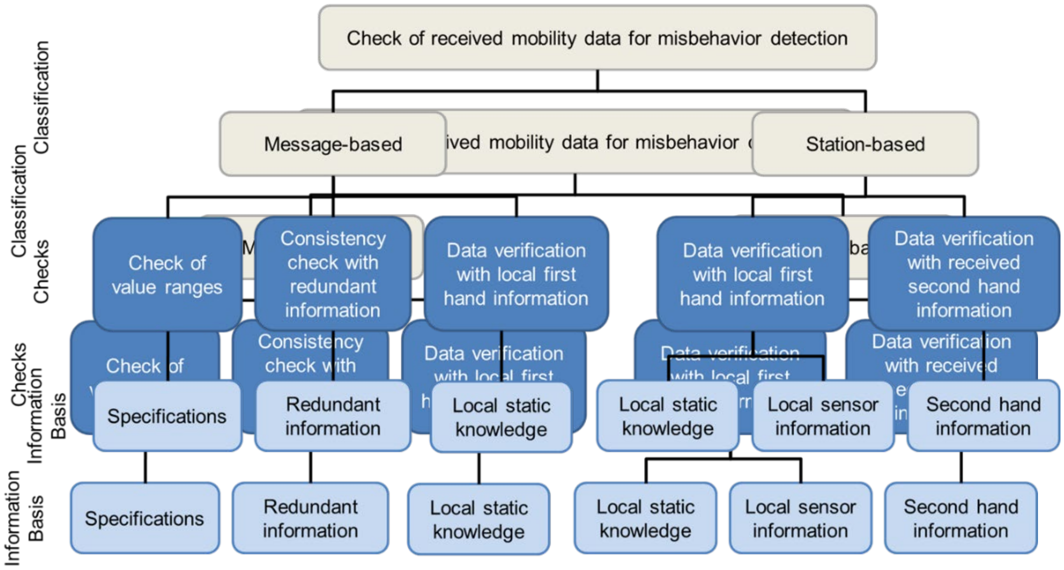

Classification
Checks
Information Basis
Check of received mobility data for misbehavior detection
Message-based
Station-based
Check of value ranges
Consistency check with redundant information
Data verification with local first hand information
Data verification with local first hand information
Data verification with received second hand information
Specifications
Redundant information
Local static knowledge
Local static knowledge
Local sensor information
Second hand information

Figure 5: Consistency and Plausibility Checks

Figure 5 summarizes the data consistency and plausibility checks specified in PRESERVE. Node trust evaluation techniques were not studied in PRESERVE, only basic misbehaviour checks.

Conclusion (gap analysis): PRESERVE VSS architecture specifies a module (SEP) and its integration in the VSA for basic consistency and plausibility checks based on mobility data in CAMs, but:

- it does not specify how various consistency and plausibility checks need to be integrated into a common framework for misbehaviour detection
- it does not fully specify the SEP module interface with the V2X communication stack (SCM).

2.2 SCA Project Objectives and Key Results

The aim of the Secure Cooperative Autonomous systems (SCA) project is to address the new security and privacy challenges associated with the deployment of cooperative, autonomous vehicles which interact with their environment (other vehicles, roadside units, traffic signs and other road users).

SCA was launched by IRT SystemX in July 2017, as a follow-on of the “ITS Security” (ISE project), it ended in November 2020.

The project has developed ITS security and privacy solutions for C-ITS communications, implemented the C-ITS PKI v2 based on the new ETSI standards for performance assessment (e.g. to study the scaling up and dynamic dimensioning of the PKI) and extended PKI management protocols (e.g. for fast and efficient distribution of trust information such as CRL and CTL).

An important contribution of the project is the development of a global misbehaviour detection and reaction system based on the on-board misbehaviour detection mechanisms/applications deployed in every ITS station which communicates reports to the central authority (Misbehaviour Authority).

The project results concerning on-board misbehaviour detection have been evaluated through simulations and through validation tests, using on-table setups and during road tests.

Global misbehaviour detection methods/applications have been evaluated only via simulation using the F2MD tool (https://github.com/IRT-SystemX/veins-f2md). While this seems to be a disadvantage, actually in simulation, more scenarios and parameters can be evaluated and large datasets can be generated such as MR dataset, which are used to test the AI-based algorithms implemented in the central Misbehaviour Authority. (e.g. training data for the ML-based algorithms).

2.2.1 Misbehaviour Detection Process

SCA has developed a 4-step process for misbehaviour detection as depicted in Figure 6.

1. Local detection: all ITS-S entities will have to run a misbehaviour detection system i.e., a set of basic misbehaviour checks to detect suspicious incoming messages from ITS-S in their neighbourhood

2. Reporting: after detection the ITS-S will have the possibility to signal the misbehaviour by sending a report to the Misbehaviour Authority (MA)

3. Global Misbehaviour detection: the MA collects and processes the received reports. The MA is part of the PKI (CCMS). Using the evidence in the reports, the MA should be able to reconstruct the local events in order to verify, if possible, the validity of the

report. The MA then jointly processes MBRs reporting the same ITS-S and classifies the reported ITS-S as faulty, malicious, or genuine. The MA identifies the type/severity of the reported misbehaviour and determines the suitable reaction required to protect the system.

4. Reaction: a reaction is triggered accordingly (e.g., ITS-S revocation at the PKI).

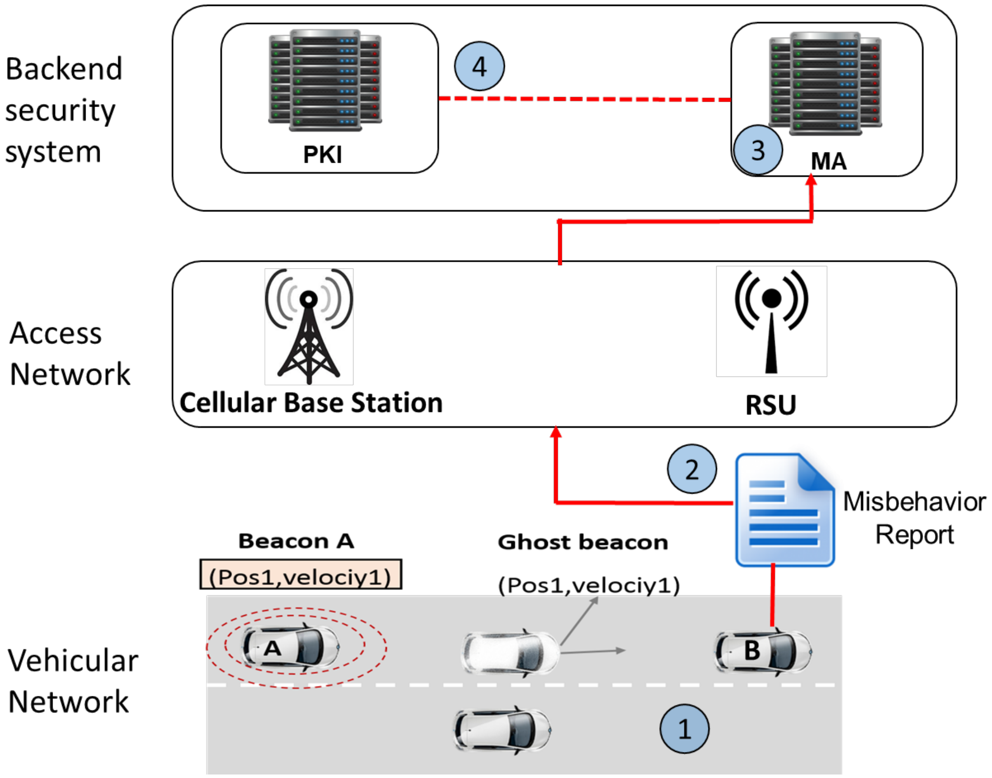


Figure 6: Misbehavior Detection Global Process

2.2.2 ITS-S Misbehaviour Detection and Reporting System

The SCA project has developed a modular framework for local misbehaviour detection. It has been implemented in the simulator Framework For Misbehaviour Detection (F²MD) [RD-3], and it is implemented in the SCA vehicle prototype for further performance evaluations [RD-7]. The on-board (local) misbehaviour detection system in the vehicle ITS-S follows the approach as shown in Figure 7.

The local detection logic goes as follows: The system runs basic plausibility and consistency checks on every received message. The results are transmitted to the local misbehaviour application installed in each vehicle which decides whether to send a report to the MA or not by processing the checks' outcomes.

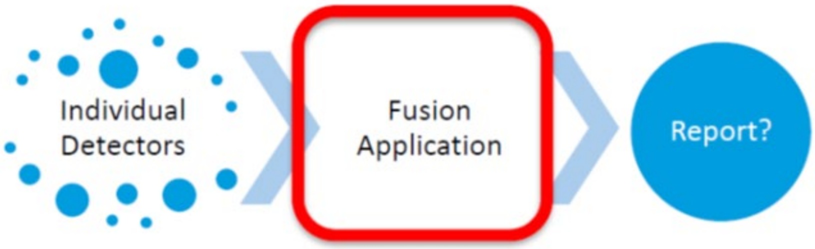


Figure 7: Local Misbehaviour Detection Approach

Therefore, the local detection could be customized in two locations: 1) the basic plausibility checks (often called individual detectors) and 2) the advanced detection application (often referred to as "**fusion application**"). SCA has implemented multiple versions of the basic checks on CAMs and multiple misbehaviour applications, including real-time machine-learning based classifiers, as presented in detail in the next sections.

The design of the misbehaviour detection system in the ITS-S needs to be flexible enough to allow the updating of the individual detectors and of the fusion application.

The ITS-S local misbehaviour detection and reporting process is performed by every ITS-S. The goal is to detect potentially misbehaving neighbouring ITS stations. This process is depicted in Figure 8.

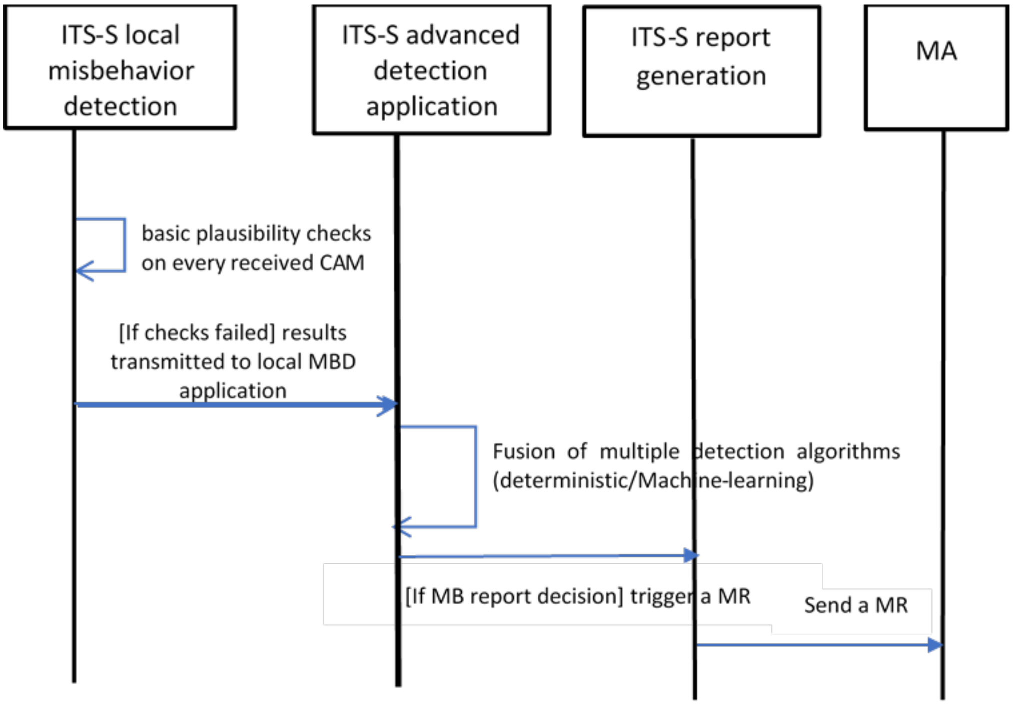

ITS-S local misbehavior detection
ITS-S advanced detection application
ITS-S report generation
MA
basic plausibility checks on every received CAM
[If checks failed] results transmitted to local MBD application
Fusion of multiple detection algorithms (deterministic/Machine-learning)
[If MB report decision] trigger a MR
Send a MR

Figure 8: ITS-S Local Misbehavior Detection and Reporting to MA

The steps for the detection and reporting of a misbehaving entity are the following:

- The ITS-S misbehaviour detection module runs basic plausibility and consistency checks on every received message. CAM basic plausibility/consistency checks are specified in Table 3.
- The results are transmitted to the ITS-S advanced detection application (also named "Fusion Application") that compiles the results of the multiple checks. The decision step is performed processing multiple inputs (results of the basic checks, the node trust estimation etc.) and can be based on different strategies such as: deterministic detection algorithms (Threshold-based, Aggregation, Node trust-based applications) or machine-learning based algorithms (SVM, MLP, LSTM, XGBoost).
- Depending on the result of the decision algorithm, the ITS-S shall trigger (or not) the sending of a report to the MA.

2.2.3 CAM basic plausibility/consistency checks

The SCA project has specified a list of basic misbehaviour detection checks on CAM messages based on the semantics of the vehicle kinematic data elements (Position, Speed, Range …) which are split into two categories:

- **Plausibility checks:** Verification of the data within a single CAM
- **Consistency checks:** Verification of the data of (two) consecutive CAMs

The list of local plausibility/consistency checks is given in Table 3. Two versions of these detectors were implemented and assessed: the legacy version and the Error Tolerant version using the confidence range value of the field in the CAM [RD-4]. The legacy version is much faster to compute and returns a binary output to determine that the message field is plausible or not. The Error Tolerant version of the detector returns an uncertainty factor that reflects the uncertainty of the message field implausibility.

Table 3: Description of Local Misbehaviour Detection Checks for CAM

Plausibility/Consistency detector	Definition
Range plausibility (rP)	Check if the position of the sending ITS–S is inside of the ego ITS–S maximum communication range (predefined value mapped on the ego ITS–S maximum radio coverage)
Position plausibility (pP)	Check if the position of the sending ITS–S is at a plausible location (e.g., on a road, no overlaps with physical obstacles, etc.)
Speed plausibility (sP)	Check if the speed transmitted by the sending ITS–S is less than a predefined maximum threshold
Position consistency (pC)	The distance separating two consecutive sender ITS-S positions is less than a maximum threshold
Speed consistency (sC)	Check if two consecutive beacons coming from a same ITS–S have plausible acceleration or deceleration
Position speed consistency (psC)	Check if the distance separating two consecutive beacons coming from a same ITS–S is consistent with the speed
Position heading consistency (phC)	Check if the positions in two consecutive beacons coming from a same ITS–S correspond to the heading advertised by that ITS–S
Beacon frequency (bF)	Check if the beacon frequency of a sending ITS–S is compliant with the standard

Intersection check (inT)	Check if no two beacons coming from two different ITS–S have overlapping locations (i.e., both ITS–S overlap each other)
Sudden appearance (sA)	Check if no ITS–S suddenly appeared within a certain range
Kalman filter tracking	Check if the sender ITS–S 's CAM information is within a plausible range of the Kalman filter predicted values. The principle of these checks is that the receiving ITS-S predicts the sender's future position, speed and acceleration data using Kalman filtering [RD-6]. Upon receipt of a new CAM, it compares the position, speed and acceleration data it predicted with that of the received CAM. We define the following 4 detectors: - Kalman Position Speed Consistency kPSC* check of the consistency of the received position with the prediction of the position based on the last known position and last known speed kPSC-P: consistency of the predicted position with the received position (Kalman filtering predicts coordinate vector) kPSC-PS: consistency of the predicted position with the received position (Kalman filtering predicts a scalar distance) kPSC-S: consistency of the predicted velocity with the received velocity (Kalman filtering predicts vector) KPSC-SS: consistency of the predicted speed with the received speed (Kalman filtering predicts a scalar)

NOTE 1: the list of Kalman filter-based detectors could be extended after we have done a complementary papers survey.

NOTE 2: the maximum threshold values of DF Speed, DF LongitudinalAcceleration, DFCurvature and DF YawRate have been defined in ETSI TR 103 460 (Table 3) for private vehicles (DE_Station_Type of value passengerCar(5)).

Confidence range tolerant misbehaviour detection approach

The standard ETSI CAM [AD-5] integrates a field called confidence range for each mobility parameter in the standardized CAM messages (Speed, Position, Heading etc.). This field is included based on the fact that sensor measurements could be inaccurate due to physical limitations or environmental characteristics. Therefore, we introduced the Error Tolerant-misbehaviour detection approach which takes into consideration the confidence range [RD-4].

For each of the plausibility and consistency checks on CAM, the “error tolerant” version consists of calculating a Plausibility Factor (f) using the confidence range. The Plausibility Factor f is a real number between 0 and 1, with 0 being certainly malicious and 1 having no signs of misbehaviour.

The legacy version of the detection check is faster to compute and returns a binary value to indicate whether a certain parameter in the standardized CAM message is plausible or not according to the outcome of the check.

The Error Tolerant version returns a value f that reflects the likelihood of the message plausibility (with 0 representing a certainly implausible message). The plausibility factors are fed to the advanced detection application. Using this version of the checks accounting for sensors inaccuracy increases the detection quality of the detection application.

The list of error tolerant detectors specified are the following checks: Range plausibility, Position plausibility, Speed plausibility, Position consistency, Speed consistency, Position speed consistency, Position heading consistency, Intersection check and Sudden appearance. This new set of error tolerant local detectors is specified in detail in [RD-4].

2.2.4 Advanced Misbehaviour Detection Application Proposals

The advanced misbehaviour detection applications are the decision-making part of the detection logic. They are also referred to as fusion applications since the decision is often based on fusion of multiple factors (the results of the plausibility checks, the node history, etc.). In the *F^{2}MD* simulator [RD-3], SCA has implemented multiple simple examples. Some examples use a deterministic algorithm and others are based on artificial intelligence. The deterministic algorithms were implemented directly into VEINS while the machine-learning applications are implemented in Python and accessed through a specific API.

The first category of applications using deterministic (rule-based) algorithms are the following:

- **Threshold App**: a node is reported if a certain message fails at least one of the plausibility checks. A failure is determined if the plausibility factor of one of the checks falls below a certain threshold.
- **Aggregation App**: this application is based on the node history. The checks' results of certain messages are aggregated with the last n results. A node is reported if the aggregated results fall below a certain threshold.
- **Non-Cooperative Trust Based (N-CTB) App:** this application is based on the seriousness of the misbehaviour event. According to the seriousness of the misbehaviour, the node is put in timeout (i.e., is considered as untrusted) and all the data it sends are being collected and reported to the MA. The seriousness is deduced from the results of the basic plausibility checks. Please note that the IT-S security subsystem does not currently take a local decision on the reception of messages from a node which is non trusted (during its time-out period), e.g., the safety application may decide in such case to react immediately, e.g., to drop all received messages from the node which is declared as untrusted.
- **Cooperative Trust Based (CTB) App**: The goal of this solution is to cooperatively evaluate the behaviour of a node to determine a shared level of trust in this node. The trust is calculated as in the case of Non-Cooperative Trust Based. However, the global trust levels are shared between all the ITS–Ss of the network.

The SCA project has provided an approach for developing **real-time machine learning based detection applications**. This approach allows to process the outcomes of basic misbehaviour detection checks using ML-based algorithms to detect misbehaviours in vehicular networks. The following list of ML-based detection algorithms has been implemented in the simulator and their performances are compared (see section 2.2.2): SVM, XGBoost, MLP and LSTM.

All these methods are integrated in the F²MD simulation tool (the tool may be extended using a defined API to interface new ML techniques with the core simulator).

All the tested ML based applications use the **Common Features**: For every received V2X message a set of features is created. These features are important indications used by the ML algorithm to evaluate the plausibility of a message.

- **Checks Feature Set**: The local detection checks done on V2X messages described in section 2.2.3.

• **Kinematic Feature Set**: The Position, Speed, Acceleration, Heading and Time of the last beacon. The ΔPosition, ΔSpeed, ΔAcceleration, ΔHeading and ΔTime between the last 2 beacons.

The following ML-based decision algorithms have been implemented in the simulator:

- **eXtreme Gradient Boosting (XGBoost)**: it is a relatively new algorithm and currently the best performing of the tree-based models. The model is given a set of V2X messages with the Checks Feature Set. The messages are given independently of each other. This entails an assumption that no time dependency exists between the data. All messages are treated as independent entities similarly to the case of the Threshold based solution. Consequently, some valuable information is lost from the base data due to this assumption. However, this model is useful to evaluate and better understand the treated data.

- **Support Vector Machines (SVM) classifier**: A two-class SVM model was trained on the Checks Feature Set as described above. This SVM classifies genuine vehicles from misbehaving ones with accuracy largely dependent on the scenario (Network, Density, Attacks, etc.).
  Multiple implementations exist for the SVM classification. The default SVM implementation is SVC (C-Support Vector Classification) but is not designed for large data sets. The SVC training times exhibit quadratic growth with the increase of the number of samples. Therefore, only 10% of the original training dataset has been used for training. The Linear Support Vector Classification (**LinearSVC**) has been tested as an alternative. This implementation scales better with the number of samples. However, LinearSVC performed significantly worse than SVC even when trained on the full dataset.

- **Multi-Layer Perceptron (MLP) Classifier**: An MLP based neural network was trained on the same data as the SVM classifier. The MLP's accuracy is found generally better than the accuracy of the SVM classifier.

- **Long Short-Term Memory (LSTM) Classifier**: An LSTM was also trained on the same data as for SVM. LSTM is part of the Recurrent Neural Network (RNN) family of ML algorithms adequate for the treatment of time dependent data. Therefore, the LSTM was additionally given the Kinematic Feature Set as input. LSTM's accuracy was generally the best out of the tested algorithms. However, it is also the slowest algorithm to compute.

2.2.5 Assessment Results

An assessment of all the local fusion applications presented in section 2.2.4 (deterministic and machine-learning / deep-learning based applications) was done using the F2MD simulation tool. The evaluation method considers the quality of the detection using several evaluation metrics and the computational performance (latency). The comparison of the evaluation results is presented in [RD-5].

<u>Evaluation metrics</u>

8 evaluation metrics are specified and used in F2MD to characterize the efficiency of the detection application: *Accuracy, Precision, Recall, F1score, Bookmaker Informedness, Markedness, Matthews Correlation Coefficient and Cohen's kappa*. These evaluation metrics are specified in [RD-4] and allow to assess the accuracy, precision, and reliability of the on-board misbehaviour detection system. All these metrics are calculated on the rates of detected genuine or misbehaving entities (False Positive, True Positive) and undetected genuine or

misbehaving entities (True Negative, False Negative). The Mean Processing Time (MPT) is used to measure the on-board processing load of every considered detection application.

Simulation results (F2MD)

Through the analysis of these evaluation metrics, it can be shown that some of the ML-based detection algorithms provide slightly better results than the deterministic detection algorithms with only a small gain in detection quality. The results can be divided into three clusters. According to the metrics, the Threshold solution is comparable to the LinearSVC and the XGBoost. The N-CTB is comparable to the MLP-T1 and the SVC. The CTB is closer to the MLP-T10 and the LSTM.

Moreover, the ML-based detection applications have the following drawbacks:

- Even when the decision algorithm is implemented in C++, with the same coefficient obtained after training, the ML-based applications calculate around 800 times slower than their corresponding deterministic detection counterparts.
- All ML-based solutions are vulnerable to adversarial attacks.
- A large and reliable training dataset is required for the models to function adequately. Therefore, the ML-based solutions could not protect against zero-day vulnerability, i.e., in the early stages of deployment, we do not have enough data to train a ML-based detection system.
- The detection of new types of previously unknown attacks may require the re-training of the model.

The comparison of the simulation results shows that the basic set of well calibrated misbehaviour detectors coupled with a non-cooperative deterministic application (like the N-CTB) could be a more suitable solution at the current stage: it has a fast-processing time and it is easy to deploy; it is not vulnerable to Sybil or adversarial attacks, and it does not need evolution of the on-board detection system if new types of attacks are discovered. Compared to ML-based applications, this solution does not require training data, so it could be implemented immediately with the first deployment.

However, the local detection performances alone are not enough to design an efficient global misbehaviour detection/decision and reaction system in C-ITS, as it is not an independent system. In all cases, the global MA should be designed to withstand a number of False Positive reports and a number of missed reports. The efficiency of the global misbehaviour detection is also depending on the efficiency of the reporting protocol and the robustness of the global detection in the Misbehaviour Authority.

Implementation Results:

The testing of advanced misbehaviour detection applications in large-scale deployment projects or field-tests (FOTs) has started, but currently there is no sufficient evaluation results. Mostly the threshold based fusion application has been implemented and tested based on a set of basic detection checks on CAM parameters such as defined in section 2.2.3. More validation tests of the global MBD system are required in C-ITS deployment projects.

As most of the defined basic misbehaviour detectors are using the mobility data transmitted by the vehicle ITS-S in CAMs, the RSU CAMs are currently not included in this evaluation work. For better detecting misbehaving RSUs, it would be necessary to specify applicable detection mechanisms for RSU and possibly extend the detection system using other types of I2V messages (such as DENM, IVIM, SPATEM etc.). E.g., an additional check on CAMs is the Minimum Distance Moved to prove that vehicles have moved during a certain time to detect attacks from static roadside attackers (see TR 103 460 clause 5.1.2) and False warning detection schemes using DENMs are also applicable for RSUs (TR 03 460 clause 5.1.3). An assessment of the efficiency and robustness of the proposed detection mechanisms for RSUs is missing.

2.2.6 Reporting Protocol

The reporting process begins as soon as an ITS station detects an implausibility, and the fusion process decides to report it. The ITS station then collects the evidence required to document the suspected misbehaviour on the global level. After collecting enough evidence, a Misbehaviour Report (MR) is created and sent to the MA.

As the reporting is not a real time process, the report is sent to the MA when connectivity is available via a suited network. The MA should perform sufficient data analysis to investigate whether a misbehaviour has occurred or not. A vehicle does not wait for a decision response about the reported node from the MA.

The functional and performance requirements of the misbehaviour reporting mechanism are specified as follows:

- **Identification of the sender/reporter and reported ITS-S**: the reporter ITS-S (sender) and the reported ITS-S identities shall be included in the misbehaviour report message. To avoid the generation and transmission of false reports, the authenticity of these identification information shall be protected (see below).
- **Reliability and proof-based**: A reporter ITS-S shall integrate the required evidence related to the type of misbehaviour which was detected: using the input data from the reporter ITS station, the MA should be able to recompute the same misbehaviour checks and get the same reported results.
- **Efficiency and minimum resource consumption**: MRs should not overload the communication channel. The reporting process should avoid sending repetitive and redundant information about the same misbehaviour.
- **Flexibility**: The definition of MRs should be extensible in order to integrate new misbehaviour checks and new evidence at a later stage without breaking backward compatibility, if needed.

According to SCA findings, the list of security and privacy requirements that shall be satisfied by this reporting process is specified as follows:

- **Privacy protection**: The MA should not be able to link the short term and the long-term identity of the reported and the reporter ITS station. The reporter ITS station uses its pseudonym certificates (a.k.a. Authorization Tickets) to communicate with the MA.
- **Confidentiality**: MRs sent by a reporting ITS station should be encrypted to protect the confidentiality of the information sent to the MA, which includes the identity of the reported ITS station, the detected misbehaviour type, and collected evidence on the detected misbehaviour.
- **Integrity & authenticity:** MRs sent by an ITS station should be signed with the private key corresponding to the verification public key of the valid "Authorization Ticket" (AT) of the sending ITS station to ensure the integrity and authenticity of the data.

2.2.7 Misbehaviour Authority Architecture

MA Role and Functions

The MA is mainly responsible to determine if an ITS-S is misbehaving. This authority has several functions:

- collect and filter received misbehaviour reports from ITS-S
- analyse the received reports and decide if a misbehaviour happened or not
- trigger a reaction

The Misbehaviour Authority (MA) is considered as a PKI entity. It is present in the SCA CCMS architecture proposition as a sub-CA of the RCA like shown in Figure 9. It requires its own certificate signed by the RCA and shall be able to communicate securely with the following entities of the system:

- using an off-line communication with the RCA to request a MA certificate
- with ITS-S to receive reports and analyse them
- with the EA and AA to get information about an ITS-S and trigger a reaction

An interface between the MA and the manufacturer or the SOC of the car manufacturer is possible but has not been specified in the SCA project.

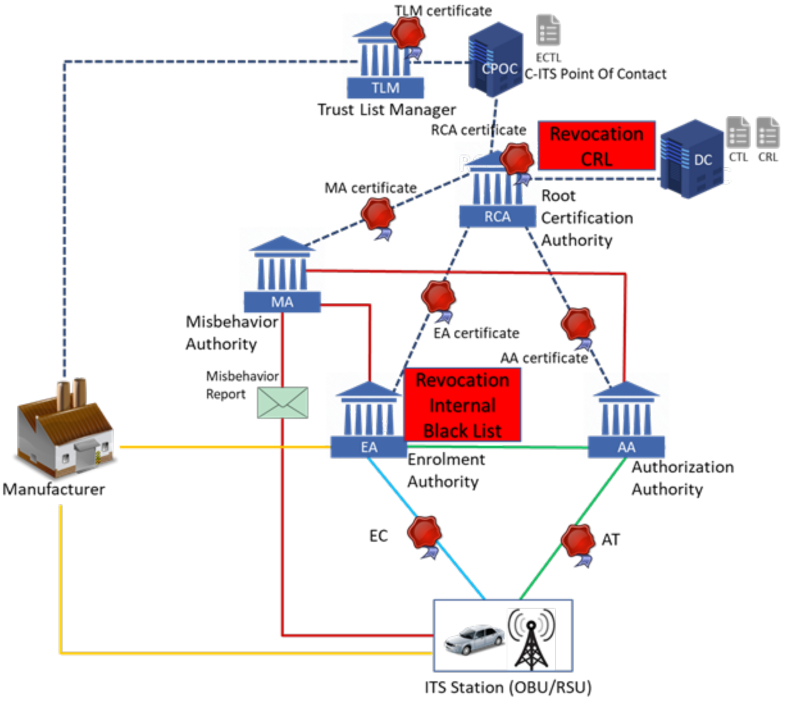


Figure 9: Interfaces between MA and Other PKI Entities

MA interaction with CCMS entities

After the assessment of collected misbehaviour reports, the MA takes a decision on the misbehaviour type (intentional like a cyberattack or not, in the case of a faulty device) and triggers the appropriate reaction. Different types of reactions can be triggered to respond to the detected misbehaviours. For instance, possible reactions of the MA are passive revocation (or revocation by expiry), active revocation or deactivation of the reported misbehaving entities. Many active revocation protocols require the distribution of CRLs to the C-ITS entities (Vehicles, RSUs …). However, this option is not supported by ETSI ITS security standards and is not backward compatible as the previously deployed devices will not be able to process the CRLs containing the list of revoked ATs.

C2C-CC, PRESERVE project, and the French project SCA have developed revocation techniques which propose to revoke only the enrolment certificate and let the pseudonyms (ATs) expire. In previous projects, such as PRESERVE and CONVERGE, revocation protocols which allow to broadcast a request to the detected misbehaving C-ITS-S to force the deletion all of its preloaded ATs (without pseudonym resolution) have been proposed, e.g., CoPRA, PUCA, REWIRE protocols and the new corrected version of the REWIRE protocol, named “Obscure Token” (O-Token) for which functional and authentication properties have been formally validated [RD-8]. O-Token proposes the broadcasting of a “self-deletion” message generated by the PKI to cancel all the ATs (and key pairs) in the HSM of the detected misbehaving C-ITS-S.

The SCA project has developed a reaction protocol allowing the MA to enforce the long-term decision such as the revocation of misbehaving ITS-Ss, in cooperation with the AA and EA. Currently this protocol only considers passive revocation (or revocation by expiry) of the misbehaving ITS-S and supports two possible options: if the ITS-S is determined as malicious attacker, the MA shall request a passive revocation by the EA which issued the Enrolment Credential (EC) to the misbehaving ITS-S. If the MA has classified the issue as a faulty ITS-S, the MA shall request the suspension of the faulty ITS-S waiting for a further investigation of the EA and Manufacturer/Device operator before revoking its EC.

In case of a decision taken by the MA, the revocation protocol proposed by SCA allows the MA to collect necessary information about the misbehaving ITS-S in collaboration with the AA and EA to trigger its revocation at the EA, ensuring that the EA will reject any new enrolment request from this ITS-S and block any further validation of an AT request from this C-ITS-S. SCA provides a Privacy-by-design protocol as the EA has the capabilities to store the reported misbehaving C-ITS-S using an internal blocking list (IBL) without revealing any information on the C-ITS real identity.

2.3 nIoVE H2020 Project

A novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles www.niove.eu

nIoVe aims to deploy a novel multi-layered interoperable cybersecurity solution for the Internet-of-Vehicles (IoV), with emphasis on the Connected and Autonomous Vehicles (CAVs) ecosystem by employing an advanced cybersecurity system enabling all relevant stakeholders and incident response teams to share cyber threat intelligence, synchronize and coordinate their cybersecurity strategies, response and recovery activities. To do so, the project develops a set of in-vehicle and V2X data collectors that will feed nIoVe's machine learning platform and tools for threat analysis and situational awareness across the IoV ecosystem.

Advanced visual and data analytics are further enhanced and adapted to boost cyber-threat detection performance under complex attack scenarios, while IoV stakeholders are jointly engaged in incident response activities through trusted mechanisms. The proposed approach is supported by interoperable data exchange between existing and newly proposed cybersecurity tools. nIoVe solution is demonstrated and validated in 3 pilots: Hybrid execution environment, simulated environment, and real-world conditions.

2.4 Security For Connected Automated caRs (SecForCARs)

The presentation of SecForCARs is given in Appendix A.

2.5 Product Security for Cross Domain Reliable Dependable Automated Systems (SECREDAS)

SECREDAS is a European project that was launched in 2018 and ended in 2021. The aim of the project was to develop an integrated security, safety, and privacy solutions for autonomous driving. The focus was on making future autonomous driving safe from external malicious interference or hacking that would put car passengers or other road users in danger.

A common security, safety, and privacy framework was created, and realistic 'on-road' driving scenarios and hacking/vulnerability threats were tested. The project also covered new safety and security functions in rail applications and health monitoring applications.

3. Standardization Activities in EU and US

3.1 ETSI Standards on Misbehaviour Detection Management

The ETSI ITS architecture specifies the Security Entity as a subpart of the ITS-S Communication System (ITSC. It includes a security defence layer (i.e., Firewall and intrusion management) as shown in in Figure 10. ETSI TS 102 940 ([AD-2]) gives detailed specification of the ITS-Station Communication system and lists the security services in Table 4 and Table 5: this includes functionalities for the detection and the reporting of misbehaviour detection on incoming messages. However, the list of functionalities is incomplete: it currently misses the logging of misbehaviour detection information from the communication layer (Facilities layer or Networking/Transport layer). This service is however specified in the SN-SAP and SF-SAP standards using the service primitive: **SN-LOG-SECURITY EVENT** (specified in [AD-3] and **SF-LOG-SECURITY EVENT** (specified in [AD-4]).

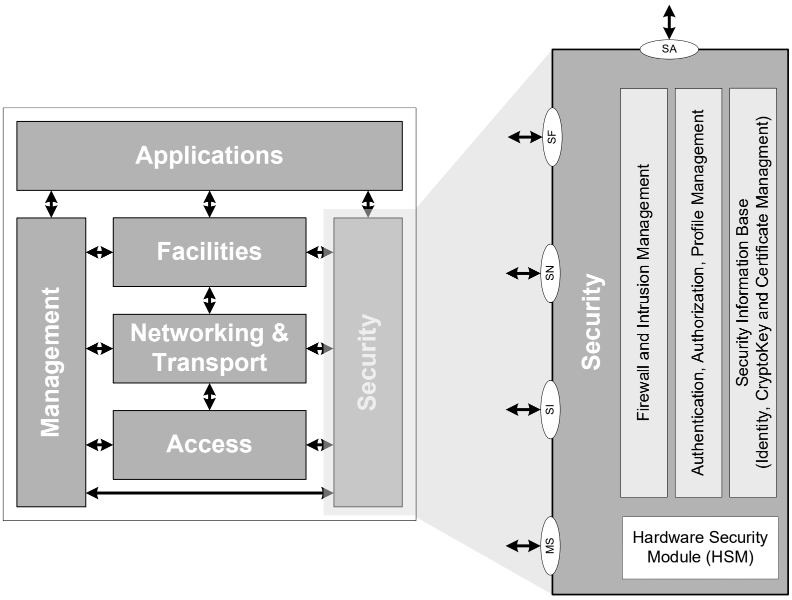

Applications
Management
Facilities
Networking & Transport
Access
Security
SA
SF
SN
SI
MS
Security
Firewall and Intrusion Management
Authentication, Authorization, Profile Management
Security Information Base (Identity, CryptoKey and Certificate Managment)
Hardware Security Module (HSM)

Figure 10: ITS-S Communication System in ETSI EN 302 665

As proposed in previous research projects (EVITA [i.11], PRESERVE [i.10]), the SN-SAP and the SF-SAP standards specify the service primitives which allow the stack layer to log a detected misbehaviour event using the ITS-S local detection system (LOG-SECURITY-EVENT).

The services primitives are specified as well as the procedure **LogSecurityEvents**:

The Security Entity, via the SF/SN-LOG-SECURITY-EVENT service primitives, provides an interface that enables a stack layer to send a notification about a detected security event by the layer.

Validation of plausibility of commonly used data (i.e., mobility and location information) is also part of the Secure Entity. Nevertheless, additional checks related to specific applications cannot be applied in the security stack due to missing application context information as well as data from higher layers.

EXAMPLE 1: Logging of inconsistencies in received messages by the facilities layers (e.g. compare sender's location provided on network layer with sender's location provided on facilities layer)

EXAMPLE 2: Logging of inconsistencies in application specific data related to the applications context

EXAMPLE 3 Logging of routing attacks by the networking and transport layers

EXAMPLE 4: Logging of attacks on transport protocols by the networking and transport layers

The plausibility validation service of the Security entity can subsequently use the provided security event information to mount appropriate countermeasures.

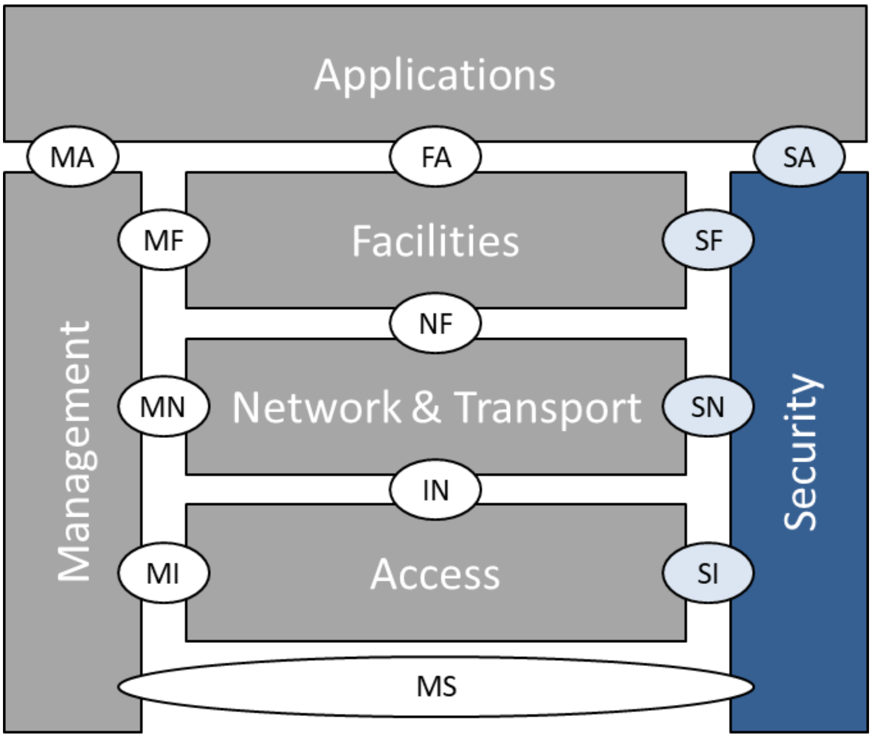


Figure 11: SAPs between Security entity and communication stack

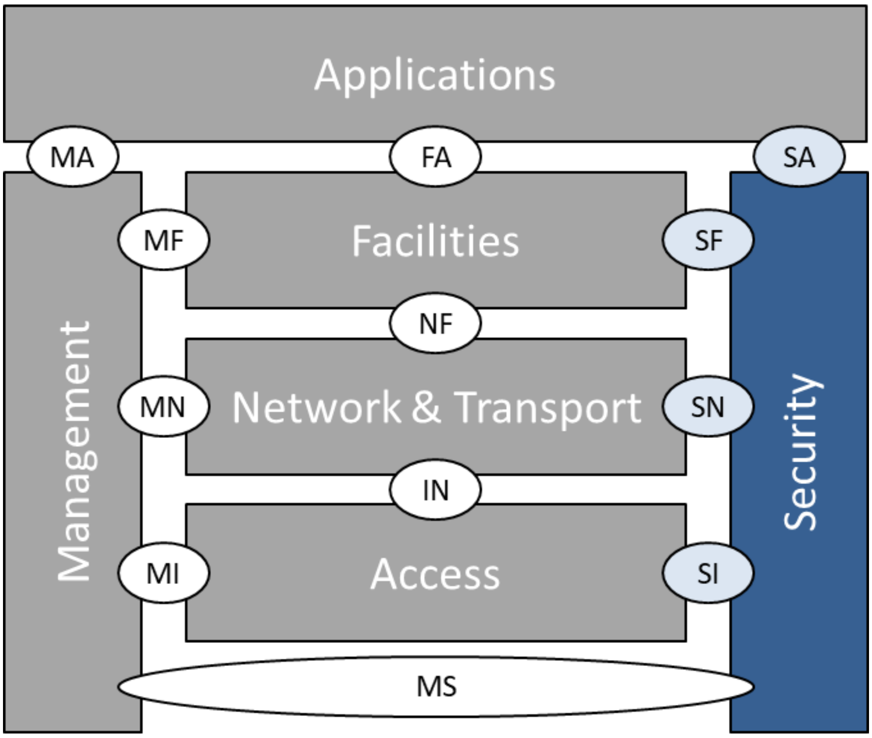


Figure 11: SAPs between Security Entity and Communication Stack

NEW:

ETSI TR 103 460: “Intelligent Transport Systems (ITS); Security; Pre-standardization Study on Misbehaviour Detection – Release 2, v0.0.16 (06-2020)

ETSI TS 103 759 “Misbehaviour Reporting Service”: is an ongoing work at ETSI aiming at specifying a misbehaviour reporting service that allows trusted ITS-S to report a local misbehaviour detection to a central authority (Misbehaviour Authority), which’s responsible for global report analysis and reaction.

3.2 IEEE 1609.2.1

Building upon the CAMP SCMS, IEEE 1609.2.1-2020 specifies “certificate management protocols” [RD-21]. As such, IEEE 1609.2.1-2020 does not exclusively cover misbehaviour. Where it covers misbehaviour, it focuses on misbehaviour reporting rather than on misbehaviour detection and "provides an interface that can be used for misbehaviour report uploading […], and data formats that can be used to encapsulate encrypted misbehaviour reports for upload [to a Misbehaviour Authority]" [RD-21].

IEEE 1609.2.1.-2020 does not specify mechanisms for misbehaviour detection and it “does not provide misbehaviour report formats” [RD-21]. However, IEEE 1609.2.1-2020 specifies that EEs need to provide authentication when sending misbehaviour reports, for example by using their current authorization ticket (see Cl. 6.3.5.6). It also assumes that misbehaviour report payload is encrypted on generation for the Misbehaviour Authority (see Cl. 4.1.5).

3.3 ISO and ETSI Standards on Security Incident Detection Service

3.3.1 ISO/IEC 27035-1 Information Security Incident Management

ISO/IEC SC27 is dealing with risk assessment and cybersecurity processes and techniques against cybersecurity attacks on the information, Information systems, networks, and devices (IOT…). In the ISO/IEC 27002:2013 standard, the objective and controls for Information Security Incident Management are introduced (clause 16 and Annex A).

The ISO/IEC JTC1 SC27 WG4 has further specified ISO/IEC 270035 on incident management which is a multipart standard with guidance and more detailed technical controls on the same topic. The international standard ISO 27035-1:2016 [RD-11] gives an overview of the basic concepts and principles of incident management and presents the different phases of information security incident management (ISIM). ISO 27035-2:2016 [RD-12] covers the first phase of the incident management (plan and prepare for incident response) and ISO 27035-3:2020 [RD-13] covers the incident response operations.

ISO 27035-1:2016 ([RD-11]) provides guidance for a structure and planned approach allowing the organization to:

- detect, report, and assess information security incidents
- respond to information security incidents, including the activation of measures to prevent, reduce, and recover from impacts
- report information security vulnerabilities, so they can be assessed and dealt with appropriately
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management

The document proposes definitions that can be used in the context of misbehaviour detection management system:

- incident handling: actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents
- information security event: occurrence indicating a possible breach of information security or failure of controls
- information security incident: one or multiple related and identified information security events that can harm an organization’s assets or compromise its operations
- incident response: actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

The ISIM proposed in the standard consists of 5 phases as shown in Figure 12.

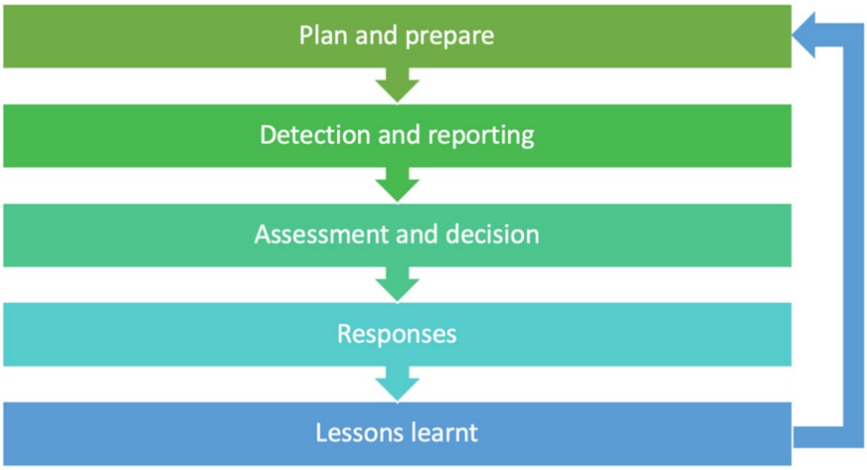


Figure 12: Information Security Incident Management Phases

The *Detection and Reporting phase* involves in particular the detection, the collection and the reporting of the security events. The *Assessment and decision phase* consists of the assessment of information associated with security events and the decision on whether to classify events as information security incidents. It is interesting to consider the central phases described here in the case of the misbehaviour detection management system. A misbehaviour report will first be triggered after a local detection, then sent to a central authority (the Misbehaviour Authority) for the reporting phase and after assessment and decision, a response is provided in order to react to the identified misbehaviour.

The *Lessons learnt* phase will facilitate the collection of data for assisting in the identification and determination of the characteristics of the various threat types and associated vulnerabilities. The data collected to identify the threat types, vulnerabilities and their impacts on the business operations will improve the quality of future risk assessments.

3.3.2 ETSI ISG Information Security Indicators (ISI) Guidance

The ETSI Industry Specification Group (ISG) Information Security Indicators (ISI) has produced a series of Group Specifications dealing with the Security Event Detection management system and the roles and interactions between the parties involved in the Information Security Incident Management system.

ETSI GS ISI 007 [RD-15] is based on the ANSSI guide [RD-14] which provides requirements for the Security incident detection service providers, such as the Security Operational Center (SOC) providers in the automotive domain.

The document ETSI GS ISI 007 [RD-15] proposes a simplified representation of a typical architecture for a security incident detection service. The architecture shown in Figure 13 is not normative and is provided for information purposes. The system is organized into trust zones: the collection enclave, the collection zone, the analysis zone, the commissioning entity exchange zone, the notification zone, and the administration zone, etc.

The other sections of the group specification list the requirements relating to the security incident service detection, the provider's legal obligations, the governance, the quality, and level of the service, etc.

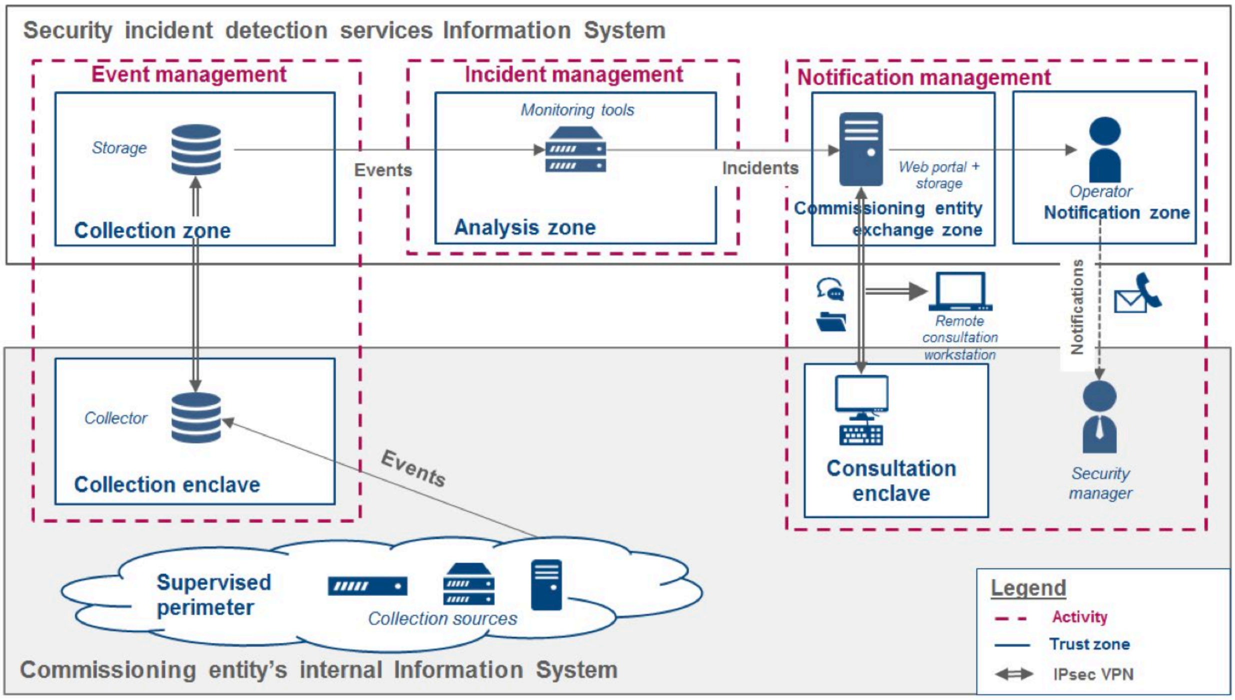


Figure 13: Simplified Architecture for a Security Incident Detection Service

3.4 ITU-T SG 17 Q13/17 on ITS security

ITU-T SG17 has published the X.1376 standard "Security-related misbehaviour detection mechanism using big data for connected vehicles" which was approved in 2021-01-07.

X.1376 standard describes misbehaviour detection mechanism for connected vehicles to help stakeholders to utilize automotive data to improve vehicle security. Analysis of a large amount of automotive data of various types (e.g., applications data, vehicle status, environmental sensors, control data, intelligence data, CVEs etc.) is very useful for assessing security of connected vehicles.

The data collection, filtering and cleaning on data captured is out of the scope of the standard. The standard focuses on the data detection using big data techniques and on the notification to the stakeholders. The detection system consists of:

a) data selection: select data sets based on different misbehaviour detection methods, then send them to the detection engine

b) detection engine: detect misbehaviour based on detection methods, then send decision results to optimization and notification, as appropriate

c) optimization: use the detection results from the detection engine to improve data selection, detection engine and data capturing

This standard focuses on data analysis/data mining to detect cyber-attacks on connected vehicles services and for data forensic, it does not focus on fully automated detection, analysis and decision system for C-ITS applications based on real-time, short-range ah-hoc networks.

4. Status of Regulatory Groups and Industry Consortia Activities on Misbehaviour Detection & Revocation

4.1 C-ITS Governance and Security Policies in Europe

In Europe, C-ITS trust model is based on a common, shared security policy as specified in the Certificate Policy and in the Security Policy documents.

In the Security Policy Release 1 [RD-17] developed by the C-ITS Platform and published in December 2017 on the DG MOVE website, part A "C-ITS Governance Framework" provided some considerations on the C-ITS Governance structure, see Figure 14.

According to the CP, the top level "Certificate Policy Authority" governance body is responsible for the approval and maintenance of the certificate & security policy document. All policy documents are available on CPOC Website: https://cpoc.jrc.ec.europa.eu/Documentation.html. The CPA is in place since July 2020 and composed of the EC and a Subgroup under ITS Expert Group was set up to assist the Commission in its tasks.

In Europe, the C-ITS trust model chosen is not a fully centralized system controlled through a central body, but the chosen model allows both public and private entities to set up Root Certification Authorities (RCAs). RCAs are responsible for issuance of security certificates and their revocation under the conditions established in the CP that applies to all entities in the C-ITS trust model [RD-18].

The following **main roles** are used for the needs of the European C-ITS trust system:

- The Policy framework role is responsible for all the governance and policy management activities required in the system. The actors in this role define policies and regulations to the actors in the European C-ITS trust system including the actors of System Operation and System Management.
- The System operation role is responsible for the proper execution of the applications that provide the end-to-end ITS service(s).
- The System management role is responsible to fulfil all required management activities within the system, including the definitions of requirements and guidelines for the actors in the system operations role.

Policy framework roles includes the 1st level governance role (C-ITS Governing Body), and other governance and supervision roles, e.g., the C-ITS Supervision body, the CPA and the Compliance Assessment body.

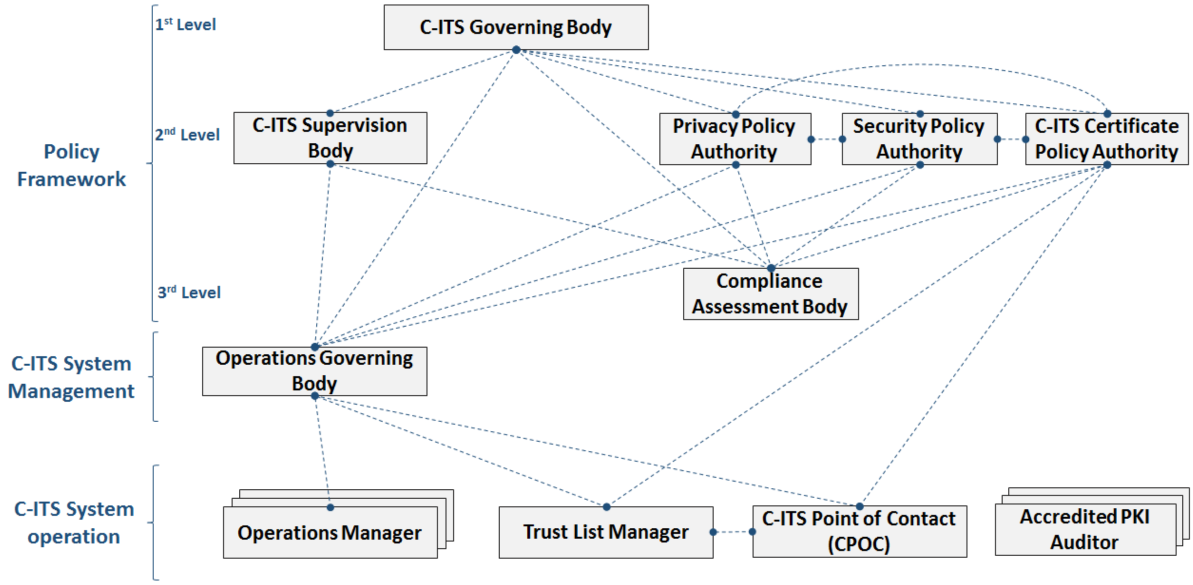


Figure 14: Detailed Structure View of the Governance Framework

The Root CAs have a role of **operations manager** for the PKI. They are Responsible for operating PKI services i.e., RCA, EA, AA, and they will need to be extended with MA operational tasks. The misbehaviour detection management system and role are not considered in the current Release of the CP but should be added in future versions of the CP, as it is needed to ensure interoperable misbehaviour detection implementations among EU C-ITS stations enrolled under different root CAs.

4.2 CAICV White Paper on V2X Vehicle Management

The CAICV (China Industry Innovation Alliance for the Intelligent and Connected Vehicles) has published in January 2021 a white paper on V2X vehicle management based on security capabilities [RD-19].

In the CAICV point of view, the MA can collaborate with the vehicle management authority, OEMs or law enforcement authority to ensure misbehaving entities are removed appropriately. The MA has offline communication with manufacturers, OEMs, and legal entities and online communication for data collection and analysis.

In the white paper, there are one global MA and local MAs (see Figure 15). Local MAs can be operated by OEMs or local administrations/authorities. Misbehaviour reports can be sent to the local MA only (in case of low-level misbehaviour) or sent both to the local and global MA if the misbehaviour is considered as high-level. Local MAs can report the results of misbehaviour detection and disposal to the global MA and forward the reports it cannot handle to the global MA.

Low-level reports are used to report issues on the V2X security protocol:

- Security checks failed, out of validity dates, etc.
- Consistency checks failed, fields undefined, AID and SSP do not match, etc.

High-level reports are reporting faulty or malicious behaviour's issues such as:

- Semantic discontinuity between successive messages
- Plausibility checks failed

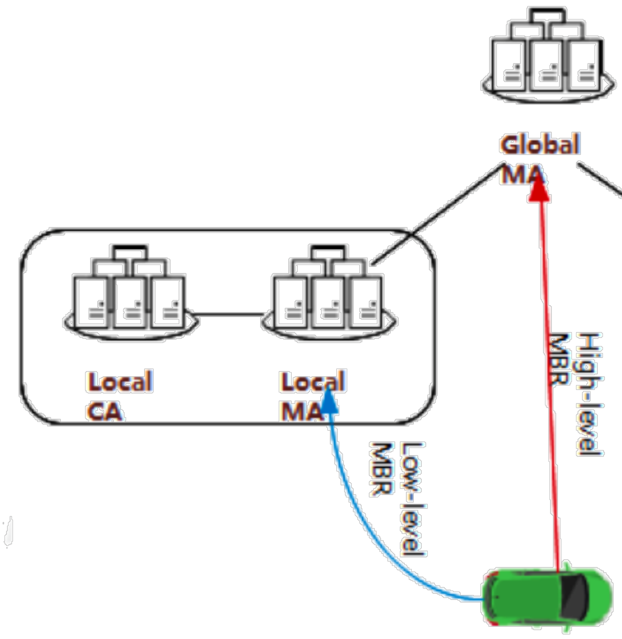


Figure 15: CAICV Security Management Architecture with Local/Global MAs

4.3 SCMS Manager in US

Since 2016, a SCMS PoC was set-up and a SCMS development & pilot phase was initiated by the US DOT to support the Connected Vehicle Safety Pilots and explore with the industry needs for the establishment and governance of a National SCMS (https://www.its.dot.gov/resources/scms.htm).

To deal with further operational deployments and support the whole CV ecosystem in US, a legal entity, named SCMS Manager, was created in January 2021 acting as the Security Policy Authority (https://www.scmsmanager.org/about/). Its activities are two-folds as presented on Figure 15:

- SCMS Manager issues and maintains interoperability profiles, policies, procedures, and guidelines to ensure security & reliability of V2X ecosystem.
- SCMS Manager is responsible for the annual audit of organizations who contracted with SCMS Manager, such as root CAs and Electors, to verify their compliance to their contractual obligations to SCMS Manager including adherence to standards, policies and guidelines published by SCMS Manager.

In the pilot phase, the MA was deployed as a single, centralized authority to provide a central misbehaviour detection and revocation system. For operational deployment of SCMS(es) in the US, the concept evolved as specified in IEEE 1609.2.1 standard ([RD-21]) to an MA which is "central for a particular application domain".

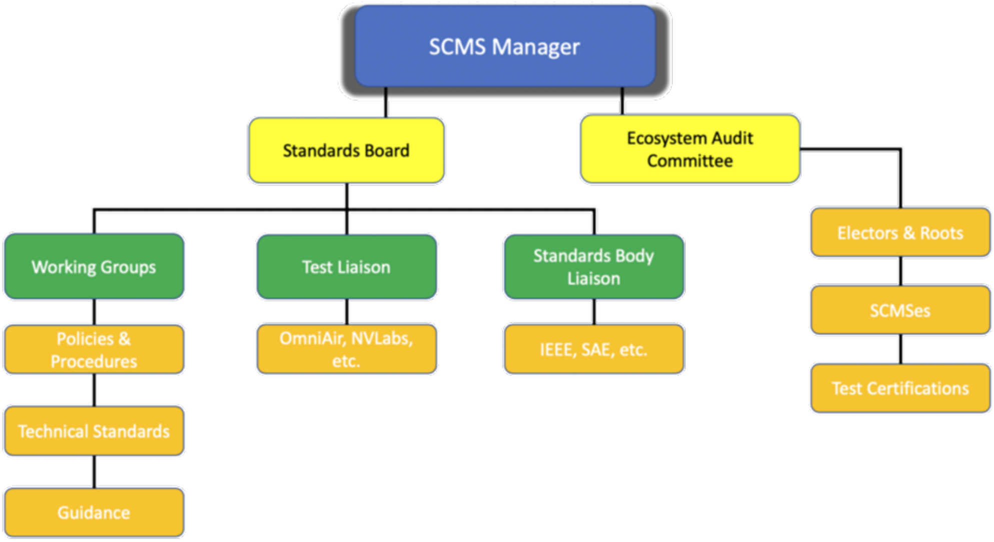


Figure 16: US SCMS Manager Organization

(Source: https://www.scmsmanager.org/about/)

4.4 SCMS Options Analysis Report – Transport Canada

In a report [RD-20] written by Escrypt for Transport Canada, the authors present the misbehaviour management system within the SCMS and compare three options for the potential misbehaviour governance models:

- Government-Led Misbehaviour Management
- Balanced Public-Private Partnership
- Industry-Led Public-Private Partners.

The evaluation criteria used for this comparison are security, privacy, sovereignty, interoperability, affordability (initial, on-going), and accessibility. The best solution according to the evaluation is the Industry-Led Public-Private Partnership. A working group composed of industry and governmental entity without any control or influence will define misbehaviour policies and how to operate and fund the MA service. The SCMS manager will be responsible but may coordinate with government in specific cases (cross-borders discussions for examples). This option leads to the notion of a single MA operating across the entire ecosystem. This maximizes the interoperability criteria but reduce the sovereignty criteria. The cost of operation is supported by the private sector.

5. Identified Key Requirements and Functionalities in Security Architecture for Local & Global Misbehaviour

Provides requirements for the ITS station communication security architecture and the structure of the security management infrastructure (MA, PKI, etc.)

To allow safe and secure operation of new, extended C-ITS services, as specified in Car2Car Roadmap for Day2/Day 3 [RD-10], the C-ITS station shall be able to perform on-board misbehaviour detection processing on received messages. The goal is to detect potentially misbehaving neighbouring ITS stations and to report these suspicious behaviours to the Misbehaviour Authority (MA) for a deeper analysis and potential reactions such as excluding the misbehaving/ malfunctioning entities from the network. Every received message should be subject to a set of individual detection checks, e.g., plausibility and consistency inspections are applied to detect false beacon information (CAMs).

Applying all the checks on every received message may be costly, so this topic is under discussion in ETSI and C2C CC to introduce a more intelligent and cost-effective way for misbehaviour detection.

These individual detectors are then analysed by a fusion process (**advanced misbehaviour detection application**) to decide on the need to send a Misbehaviour Report to the MA. A minimum subset of individual local detection mechanisms using data plausibility and consistency checks shall be specified in future revisions of the C2C-CC BSP.

For the specification of mandatory misbehaviour detection features (detection checks) in future releases of the BSP, we propose a simplified view for the classification of misbehaviour detection mechanisms presented in Figure 17.

This classification considers two main aspects. The first aspect distinguishes between data-centric and node-centric mechanisms. Many misbehaviour detection mechanisms are data-centric, meaning we use the data content of received messages to determine their correctness. Node-centric mechanisms are focusing on C-ITS network entities and often rely on this previous data-centric validation. Data-centric and node-centric are complementary trust evaluation methods and may be combined in a global trust evaluation approach. The second aspect is the scope of detection which distinguishes the mechanisms used to analyse the messages: such detection can be done by a single Vehicle C-ITS station (local or autonomous) or applied by multiple Vehicle C-ITS stations or RSUs (collaborative).

	Autonomous	*collaborative*
data-centric	plausibility	Consistency across ITS-S
node-centric	behavioural	Trust-based

Figure 17: Taxonomy of Misbehaviour Detection Mechanisms

Based on the survey of previous research projects, the ITS-S local misbehaviour detection system (MDS) shall support detection features on CAMs, and the following requirements on the ITS-S misbehaviour detection system shall be fulfilled to achieve an intended security level:

- the list of “individual” detectors on CAMs specified in Table 3 and Table 4 shall be supported
- the “Confidence range tolerant misbehaviour detection approach” shall be mandatory, as C2C-CC functional & technical experts assume that hard thresholds do not make sense for vehicle mobility data (except for timestamps).

This list of basic misbehaviour detectors on CAMs provide individual detection mechanisms to detect locally abnormal behaviours of other ITS-S via plausibility and consistency checks on CAM data using the Ego-Vehicle ITS-S state and sensors data.

ITS-S shall apply all the consistency and plausibility checks (table 3) on all messages received from one ITS-S to report a misbehaviour of this station to the MA.

More intelligent detection applications combining these basic plausibility & consistency detectors with other methods (trust assessment, Machine-Learning algorithms) are also possible to develop a fine-grained approach to detect malicious attacks or unintentional faulty behaviours.

C2C-CC agreed to use specified fixed threshold values for plausibility checks on CAMs for the different types of ITS-stations:

- the specification of threshold values for the passenger cars is given in Table 4 below
- the specification of corresponding threshold tables for other types of stations (motor bikes, trucks, bus, emergency vehicles) shall be provided in appropriate profiles specification (e.g., PTW profile).

Table 4: CAM Data Elements Unplausible Values (Passenger Vehicles)

DF Speed	Speed greater than 70 m/s (252 km/h)
DF LongitudinalAcceleration (positive LongitudinalAccelerationValue)	Longitudinal acceleration of 0–100 km/h in fewer than 2,3 seconds (greater than 12 m/s^2)
DF LongitudinalAcceleration (negative LongitudinalAccelerationValue)	Longitudinal deceleration of 100–0 km/h in fewer than 28,95 m (greater than 12 m/s^2)
~~**DF Curvature**~~	~~Curvature radius of smaller than 3,9 m~~ (out of range of the respective data element in ETSI TS 102 894-2 v1.3.1)
DF YawRate	Yaw rate of greater than 1,5 radian/s

As previous research projects and Field-operational-tests (FOTs) investigating misbehaviour detection solutions have focused on requirements for Day1 C-ITS applications, there have developed and validated in vehicle fleet a large scope of detection techniques using the received CAM data contents from the surrounding stations.

Based on ETSI TR 103 460 ([RD-9]) and latest draft of TS 103 759 (draft version 0.0.3 [RD-10]), the misbehaviour detection features for traffic event reporting (DENMs) should also be operated in each C-ITS station (vehicles, RSUs). The specified detection checks for DENMs follow the classification presented in 17: Taxonomy of Misbehaviour Detection Mechanisms.

The list of applicable detection features for DENMs is given in the table 5 below.

Table 5: Misbehaviour detection mechanisms specification (ETSI TS 103 759 draft version)

Environmental-based validation	This category of misbehaviour detection mechanisms is based on the fact that some warnings are more or less probable depending on the road environment. This validation method is

	therefore specific to each traffic event/road hazard warning type and is strongly linked to the application.
Location proximity	For all traffic event reports, a verification of the location of the ITS-S can be performed: this consists to check that the originating ITS station is within line of sight of the reported traffic event. The receiver should check the consistency of the detected event location (*eventPosition* in DENM) with the location of the ego-vehicle contained in its transmitted CAMs.
Data trust combined with traffic data quality	Data trust may be evaluated based on the data received in DENMs from multiple sources and combined with the quality of the reported traffic event (*informationQuality*). The receiving ITS-S may infer the correctness of received traffic data from the number of stations vouching for its validity based on the value of the *informationQuality* parameter set in the reported event message. Specify the computation of the event trust score (ETR (E, j)).
Behavioural-based validation	These detection mechanisms are based on the fact that a Vehicle ITS-S signalling a specific traffic event should behave accordingly. The checks are based on the behaviour of the vehicle with respect to this specific warning. This validation method is therefore specific to each traffic event/road warning type. A vehicle issuing a warning event is thus monitored by receiving ITS-Ss (e.g., vehicles or RSUs) to determine if its behaviour is conforming to its expected behaviour.
Cooperative Trust Based (CTB)	Cooperative trust-based mechanisms try to evaluate the trustworthiness of the nodes in the C-ITS network (node trust evaluation). These node-centric approaches use the assigned trust level to a node in addition to some data-centric trust inputs to compute a consensus shared among several nodes and thus to prove the trustworthiness of the nodes. Specifications still need to be provided.

To support further Day 2 and Day2+ applications, the local misbehaviour detection system in the C-ITS-S shall be able to provide more detectors for different types of messages, e.g., IVIM, CPM, MCM, VAM, PCM etc. In the end, the various consistency and plausibility checks on safety messages need to be integrated into a common framework for misbehaviour detection where detectors can be added in a flexible way. The detectors should be distributed in the C-ITS communication stack and further integrated in the various real-time, safety applications in the autonomous vehicle system, i.e., integrated in the ADAS/AD domains.

For example, there are several known threats and vulnerabilities on the GeoNetworking layer on routing algorithms, e.g. DOS attacks (Blackholes, Spamming …) or masquerade, manipulation, injection or replay of messages etc. TVRA analysis done in ETSI has recommended the implementation of mitigation measures such as digital signatures and misbehaviour detection (ETSI TR 102 893 V1.2.1).

The reporting process begins as soon as an ITS station detects an implausibility, and the fusion process decides to generate a report and upload it to the MA using a dissemination protocol through various wireless or cellular communication interfaces. The ITS station then collects the evidence required to prove and recreate a misbehaviour on the global level. After collecting enough evidence, an MR is created and sent to the MA. A misbehaviour report format is going to be standardized in ETSI and publication of ETSI TS 103 759 in expected in Q1-2022.

In future revisions of C2C-CC BSP, the C-ITS stations should comply to existing standards specifying the misbehaviour management architecture (ETSI TS 102 940 V2.1.1 published in 07-2021) and to the ETSI specification on misbehaviour reporting service & interface between the end-entities and the MA (ETSI TS 103 759).

A main concern raised with the implementation of these basic misbehaviour detection mechanisms on CAMs is the required resources consumption on the on-board device for the tasks of the local detection mechanisms, the misbehaviour detection logic (“fusion” application) and the misbehaviour report generation/transmission. The feasibility of these misbehaviour detection mechanisms in the on-board device is depending on costs of computation and communication, and on the delay constraints induced on safety applications.

The computation overhead for the detection of the suspicious messages received from other stations could interfere with the safety, time-critical operations of C-ITS applications, esp. when we consider typical vehicular communication rates, e.g., processing of up to 1000 CAM messages/second (or more in a multi-channel configuration).

Currently SCA project evaluation on simulator only focuses on the assessment of detection efficiency and performance of detection techniques using Mean Processing Time and other papers only give indication of rough estimation (intuition, simulation results).

An evaluation of costs generated by misbehaviour detection / reporting activities (e.g., computational, memory, communication resources utilization) could be performed using the SCA project implementation on a Vehicle OBU.

KPIs used for performance evaluation of local misbehaviour detection & reporting are specified in the table below.

Misbehaviour detection resources costs evaluation	
average and maximum CPU utilization	
average and maximum Memory utilization	
communication overhead (with neighbours, RSUs or servers ?)	Optional, for cooperative detection techniques, e.g., voting, consensus mechanisms…
Additional RSU/server CPU utilization	Optional, for cooperative detection techniques
average processing time	
total delay/latency time on received message	

Misbehaviour reporting resources costs evaluation

average CPU utilization	
average Memory utilization	all messages of a potentially misbehaving station and associated evidence
communication overhead (with MA)	Large volume of communication data shared with the MA on intermittent connectivity may require a prioritization scheme (based on a threats/vulnerabilities risk analysis)?
Average processing time	
total delay/latency time on received message	

6. Impact on BSP and Protection Profiles

One of the basic security requirements for V2X communications is to ensure trust in the messages that others send out. Any receiver has to assess the trustworthiness of incoming messages in order to provide a reliable and safe service. Based on the use of digital signature and the deployment of public key infrastructures, the security standards published by ETSI allow to provide the confidence that received data is authentic. However, in highly constrained automotive or road-side devices, some network entities may be either faulty, sending inaccurate information in messages, or compromised such that an attacker may obtain legitimate keys/ certificates and send arbitrary, forged messages. Therefore, reactive security in the form of misbehaviour detection is a necessary mitigation measure to provide a high level of security in C-ITS. Detection and prevention of such misbehaviours in C-ITS can be supported by a central authority named Misbehaviour Authority (MA) which is able to collect and analyse large volumes of misbehaviour reports and related evidence.

In this document, the Task Force on Misbehaviour detection and reporting has drafted the proposal for such a solution. Based on the White Paper survey and key finding (see section 5), the Task Force recommends extending features in each Vehicle C-ITS station and specifies the main requirements related to local misbehaviour detection and reporting to the MA in the next releases of the BSP. With these results being an outcome of intensive discussions and considerations in the Task Force and in the dedicated sessions organized during the CAR 2 CAR Weeks, we are confident that the present proposal may be a large portion of what can be actually useful and needed. This proposal specifies needed features for the on-board Misbehaviour detection, reaction, and reporting system to be provided in each trusted C-ITS entity (vehicle, mobile or road-side stations).

In C-ITS current deployments in Europe, safety services rely on the cooperation of each communicating entity in the ad-hoc short-range communication network (ITS-G5): safety services are supported by the C-ITS stations which are able to send either beaconing information or warning messages such as road hazard or traffic event reports. A clear focus of our design is on misbehaviour detection on Day 1 C-ITS services specifying a list of basic detection mechanisms for the detection of false beacon information (CAMs) and false warning messages (DENMs). This includes a list of required plausibility and consistency checks on CAMs (see Tables 1 and 2) and a list of required misbehaviour detection mechanisms on DENMs as specified in table 5.

A taxonomy of misbehaviour detection approaches is proposed which takes into account two main aspects: the first aspect is the scope of detection (either autonomous or cooperative), and the second aspect distinguishes between data-centric and node-centric mechanisms (see Figure 17). Currently, the individual detection checks specified on CAMs and DENMs are focused mainly on plausibility and consistency checks (CAMs, DENMs) and on behavioural detectors for DENMs.

We do not specify a precise solution for the trust-based evaluation methods, e.g., computation of the node-based trust level (trust score) which could be based on the initial (default) trustworthiness level assigned to a C-ITS station (as discussed in Car2Car Roadmap for Day2/Day 3 [RD-10]).

The design of the misbehaviour detection, reaction and reporting system in the trusted C-ITS entity shall comply to the ETSI standards specifying the misbehaviour management architecture (ETSI TS 102 940 V2.1.1 published in 07-2021 [AD-2]) and specifying the misbehaviour reporting service & interface between the end-entities and the MA (ETSI TS 103 759, scheduled for publication in 03-2022 [RD-9]) to provide the needed interoperability.

The document provides a list of performance criteria for the evaluation of costs related to the detection and reporting functionalities within the trusted C-ITS entities. A further study should comprise a resource cost evaluation for misbehaviour detection and reporting to the MA (computational load and required storage in the C-ITS entity, communication resources utilization).

The Vehicle C-ITS Station (VCS) is a key element in the misbehaviour process. The infrastructure on its own may not detect all entities sending wrong or falsified information. In fact, it doesn't have access to the full set of data that the distributed vehicles sending and receiving ITS messages have. Thus, all deployed VCS should clearly participate to misbehaviour detection mechanisms. But to do so, they must implement interoperable and security equivalent mechanisms. Therefore, we must provide a reference set of requirements to be implemented by all VCSs. This should include requirements on the detection checks, on the reporting format and a secure, privacy-friendly protocol to be used to send the misbehaviour reports to the MA, in order to guarantee the correct execution of the detection mechanism and its validity.

As the ETSI standardization is not progressed enough, the current status does not allow to define complete, mandatory requirements on the topic. The white paper currently specifies a set of mandatory misbehaviour detection checks performed by each VCS, including plausibility and consistency checks on received CAMs and DENMs and behavioural checks on DENMs and recommends that this list of mandatory checks are included in the BSP.

However, regarding its importance, it is still an objective for the Car2Car VCS PP to identify some minimum requirements. Those requirements will enforce at least:

- The implementation of a developer defined list of checks
- The implementation of logging functions when the result of these checks failed (audit files)
- The implementation of secure and privacy-friendly transfer of misbehaviour reports to the MA protected in integrity and confidentiality

Due to lack of full mature standards, the requirements in this version of the PP VCS are limited and current limitations are identified:

- Requirements related to misbehaviour will only be optional since interoperability could not yet be enforced by standards (de facto or official).
- No minimum set of checks will be identified in the optional requirement since no check does have yet full recognition. A basic set of checks to be implemented will be proposed but only as informational. This set will contain some of the checks identified in this white paper.
- No specific format will be enforced on the generated misbehaviour reports.
- No protocol specification will be provided for the enforcement of the secure communication of reports to the MA.

One of the difficulties encountered during the VCS PP redaction is that a few identified plausibility checks require the definition of static, predefined thresholds (maximum plausible speed, maximum plausible distance of the sender, etc.) which might either evolve over time, vary from countries to countries (potentially due to regulations impact), depend on the vehicle sensors precision, etc.
A protection profile is meant to define strong requirements to enforce harmonized and uniform security. This is not yet fully possible, but this should be done for later versions of the PP. Current version of the protection profile only considers Day1 use cases which imply lower risks. This will be much more challenging for semi-autonomous or autonomous

systems which will need much more confidence in C-ITS data to take their driving decisions, where mandatory requirements of harmonized misbehaviour detection mechanisms will be strongly recommended.

7. Conclusions and Next Steps

In this white paper, an intensive survey of R&D research and field-test projects and results on misbehaviour detection mechanisms and local detection applications (incl. ML-based approaches) is presented. The survey covers EVITA, SEVECOM, PRESERVE, SCA, SecForCARs…

After presenting the survey of previous research and field-test projects, the report focuses on the on-board process for the misbehaviour detection and the reporting to the MA. The white paper intends to specify the functional requirements and to detail the main operational technical requirements for on-board misbehaviour detection, reaction and reporting system and contribute them to the next releases of the C2C-CC BSP. It focuses on requirements for Day 1 C-ITS applications and necessary agility to support further Day 2 and day2+ applications. In the end, the various consistency and plausibility checks on safety messages need to be integrated into a common framework for misbehaviour detection where detectors can be added in a flexible way. The detectors should be distributed in the C-ITS communication stack and further integrated in the various real-time, safety applications in the autonomous vehicle system, i.e., integrated in the ADAS/AD domains.

The white paper intends to reuse existing standards specifying the misbehaviour framework architecture (TS 102 940 Release 2, published in 2021-07 [AD-2]) and interfaces with the end-entities: the drafting of a new standard for the misbehaviour reporting service (TS 103 759) is currently work-in-progress in ETSI.

During this white paper study, several gaps which need further work have been identified:

- Study impacts on governance and legal/policies framework for deployment of misbehaviour detection in the C-ITS CCMS

  After completing this survey report on misbehaviour detection, C2C-CC will have to investigate on the potential impacts on governance and legal/policies framework for the C-ITS operational deployment in Europe, e.g., how to deploy an efficient, secure misbehaviour management system within the operational EU CCMS? How to integrate this reactive security level in an interoperable and backward compatible way? How to integrate misbehaviour detection within the Security Operational Center (SOC of the car OEM) being developed under the new Vehicle-type approval regulations (UN R155/ R156) providing remediation and corrective actions to prevent identified communication security threats etc.

- Need for an update Car2Car TVRA for Day2 and Beyond Use Cases

  Currently the study is restricted to a subset of safety messages e.g., CAMs and DENMs and the design of the solution is originally focusing on the deployment of Day 1 applications.

  With extension of C-ITS application integrating more C-ITS device types (vehicle categories, vulnerable users …) and the integration of the (semi-)autonomous vehicle functions, there is a need to identify the security threats and risks and derive new functional and technical requirements on MBD e.g., CPM, CACC, Platooning, VRU.

- Develop a complete solution and misbehaviour detection management / processes for Day2 and Beyond

  There is still lacking a complete study & feasibility assessment on MBD for Day2/Day 3 applications. Esp. for CAVs, a timely detection/ reaction in case of a misbehaving device and a stronger integration with (semi-) autonomous vehicle applications will become necessary. The design of a complete misbehaviour Management/ Process for Day2/Day 3/Day 3+ should include misbehaviour detection, local reaction and reporting combined with MA role/central misbehaviour detection and reaction.

- Develop recommendations for data protection compliant misbehaviour detection and reporting

8. Appendix A: Project presentation forms

8.1 Secure Cooperative Autonomous systems (SCA)

Project details:

Project title: Secure Cooperative Autonomous systems (SCA)

Project lead: IRT SystemX, Project manager: Arnaud Kaiser 49ob e49.kaiser@irt-systemx.fr

Project consortium: IRT SystemX, Renault, Idnomic, Trialog, Oppida, YoGoKo, Institut Mines-Télécom, PSA, Valeo, Transdev

Start date/end date: July 1, 2017 – November 30, 2020

Activity website: https://www.irt-systemx.fr/en/projets/sca/

Funding sources: public funding from Agence Nationale de la Recherche (Fr) and funding from the industrial partners

Funding origin: national (France)

Abstract: SCA aims to support the development of C-ITS by addressing the cyber-security and privacy challenges of the exchange of data between vehicles and other ITS entities. SCA follows on from the ISE (ITS Security) project, completed in June 2017, which led to the development of the security infrastructure for cooperative ITSs (PKI) and the specification of PKI management protocol transferred to ETSI standardization.

Objectives: The SCA project has four main objectives.

1. C-ITS use case analysis. This includes risk analysis evaluation on future (day-two) C-ITS use cases, the assessment of the performance of current cyber-security solutions and the evaluation of the privacy protection level for the user.

2. Compliance assessment and penetration testing. This includes the development of compliance test tools to assess cyber-security conformity of the system; the development of penetration testing techniques targeting new cyber-attacks on V2X communication; the definition of protection profiles for the ITS-S and the PKI.

3. Business continuity and crypto agility. An important activity within SCA is the development of a global misbehaviour detection and reaction mechanism. Analysis of the crypto-agility of the C-ITS system is another objective.

4. Interoperability and scalability. This includes the assessment of the PKI scalability and its dynamic dimensioning to ensure the long-term functionality of the PKI infrastructure. Comparison with respect to cyber-security and privacy of short-range communication technologies (ITS-G5, LTE-V2X, etc.) and cellular long-range communications, necessary to insure large-scale deployment.

Methodology: State-of-the-art review, simulation, implementation (on-board security components and off-board PKI components deployed on AWS Cloud), experimentation (laboratory testing and roads trials).

Use Cases: The main use cases addressed by the SCA project are

1. Certificate's provisioning (ETSI TS102 941 v1.3.1): a vehicle requests several V2X certificates to the PKI (EC, Ats) as well as the CRL and CTL. The use case includes both radio access networks: ITS-G5 and LTE.

2. Misbehaviour detection: a vehicle starts an attack by sending CAM with erroneous data. Neighbouring vehicles detect these erroneous data. They accordingly send a Misbehaviour Report (MR) to the MA, either using cellular (LTE) or ITS-G5 if

available. The MA then collects and analyses the received MRs and classifies the reported vehicles as faulty, malicious, or genuine.

3. Pseudonym change: different strategies (basic pseudonym change, silent period, mix zones) and tracking opportunities.
4. Geographical alert dissemination: advertising vehicles about a specific incident (e.g. emergency brake, VRU, accident, etc.) before they enter the critical area. To this end, the vehicle that identified an incident broadcasts a DENM on ITS-G5 but also sends the DENM by cellular to a geo-server located in the cloud.

Addressed challenges: the most prominent challenge addressed by the SCA project is to propose a misbehaviour detection system to identify misbehaving end-entities and to revoke their credentials.

Key Results: Misbehaviour detection framework, composed of local misbehaviour detection techniques, of a reporting mechanism at C-ITS end-entities level (to the misbehaviour authority), and of a global analysis by the misbehaviour authority of acquired data. This will allow for a reaction mechanism in the MA to revoke the ability of malicious entities to participate in C-ITS. Additional PKI protocols are also proposed and evaluated, such as the peer-to-peer distribution of CTL/CRL for fast and efficient update.

Testing location(s): Tests with DIR Ouest, in Bretagne and on the roads around Renault Technocentre, https://www.youtube.com/watch?v=A8qlYk1LKy4

Key documents, Reports, Deliverables: *Simulation Framework for Misbehaviour Detection in Vehicular Networks* https://hal.archives-ouvertes.fr/hal-02527873, https://github.com/josephkamel/F2MD

8.2 Security For Connected Automated caRs (SecForCARs)

Project details:

Project title: Security For Connected Automated caRs (SecForCARs

Project lead: Jochen Koszescha (Infineon Techologies AG), Jochen.Koszescha@infineon.com

Frank Kargl (Universtität Ulm), frank.kargl@uni-ulm.de

Contact: Keno Garlichs (TU Braunschweig), email: garlichs@ibr.cs.tu-bs.de

- **Project consortium**: Infineon Technologies AG (coordinator), AUDI AG, Fraunhofer AISEC, Garching bei München, Fraunhofer IEM, Paderborn, Freie Universität Berlin, Robert Bosch GmbH, Technische Universität Braunschweig, ESCRYPT GmbH Embedded Security, itemis AG, Hochschule Karlsruhe – Technik und Wirtschaft, Mixed Mode GmbH, SCHUTZWERK GmbH, Technische Universität München, Universität Ulm

Start date/end date: 01.04.2018 – 31.03.2021

Activity website: https://www.secforcars.de/

Funding sources: Funded by the German Federal Ministry of Education and Research

Funding origin: national (Germany)

Abstract:

The main goal of the project is the development of methods and tools to secure critical vehicular communication and control in automated driving.

We focus on information flows ranging from sensors like RADAR or cameras through ECUs to actuators like engine or brakes and includes information communicated through inter-vehicle (V2X) communication. The functional architecture is augmented by security mechanisms that will hinder attackers from manipulating the behaviour of a self-driving car. Development, analysis, and test methods are developed to identify vulnerabilities enabling adversaries to gain control over the vehicle and are supported by according tools to make such methods applicable in practice. All investigations also consider the relations between functional safety and security.

Use cases:

Field	Input	Remarks
Use-Case 1	CACC/Platooning on highways	Focus on security
Use-Case 2	Cooperative search for parking spaces Vehicles can detect free parking spaces with their sensors and share that information with others when being queried.	Focus on security
Use-Case 3	Collision Warning based on CPMs Information received via CPMs can be used to extend CAM-based collision warning systems	Focus on security

Field	Input	Remarks
Facility 1	Collective Perception Service	For UC3
Facility 2	Cooperative Awareness Service For communication of dynamic status between CACC/Platoon members.	For UC1,3
Facility 3	LDM Necessary 51ob e51 CP Service	For UC3
Facility 4	Security Architecture This includes all necessary components 51ob e51 ETSI security architecture to establish authenticated, integrity protected communication, extended security architecture for specific requirements of automated driving	For all UCs
Facility 5	Unicast/Multicast Communication Facilities To form, maintain and manage a platoon, directed communication means are required between the (potential) members. This could either be done locally or via back-end communication	For UC1
Facility 6	Geonetworking	For UC2

	In 52ob e52 o query vehicles in the designated parking area, geo-broadcast facilities are necessary	

Addressed challenges:

Field	Input	Remarks
Challenge 1	Definition of an integrated methodology and tools for security and safety analysis and testing in different connected automated cars	
Challenge 2	Development of an automotive responsible disclosure framework	
Challenge 3	Protection against different attacks on local and distributed sensor systems (context: CACC, CPM, …)	
Challenge 4	Investigation of attacks focusing on specifics of automated driving, e.g., blinding or ghosting attacks against radars and other sensors. Investigate and develop security and pentesting tools	
Challenge 5	Design of in-vehicle security architectures for connected, automated cars, based on secure platforms with authenticated, integrity protected communication between ECUs. Investigate architecture principles and building blocks	Usage of HSM for key storage and for cryptographic operations
Challenge 6	Development of methods to establish trust in (especially safety relevant) data received from unknown participants of a network. Adaptation of misbehaviour detection framework to specifics of automated driving.	
Challenge 7	Detect intentional as well as unintentional misbehaviour in intra-vehicle and inter-vehicle networks. Investigate relationship between sensor data fusion and misbehaviour detection.	IDS and Firewall on Gateway units (intra-vehicle network)
Challenge 8	Design components 52ob e reusable	

Testing location(s):

Key documents, Reports, Deliverables:

R. W. Van Der Heijden, T. Lukaseder, and F. Kargl, "VeReMi: A dataset for comparable evaluation of misbehaviour detection in VANETs," *arXiv*. 2018.

R. W. Van Der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehaviour detection in cooperative intelligent transportation systems," *IEEE Commun. Surv. Tutorials*, 2019.

K. Garlichs, A. Willecke, M. Wegner, and L. C. Wolf, "TriP: Misbehaviour Detection for Dynamic Platoons using Trust," in *2019 IEEE Intelligent Transportation Systems Conference, ITSC 2019*, 2019.

9. Appendix 1 – References

9.1 Applicable documents

[AD-1] ETSI EN 302 636-4-1 V1.4.1: “Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality”.

[AD-2] ETSI TS 102 940 V2.1.1: “Intelligent Transport Systems (ITS); Security; IST communications security architecture and security management; Release 2.

[AD-3] ETSI TS 102 723-8 V1.1.1: “Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer”

[AD-4] ETSI TS 102 723-9 V1.1.1: “Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and facilities layer”

[AD-5] ETSI EN 302 637-2 V1.3.1: “Intelligent Transport Systems (ist); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[AD-6] ETSI TR 103 460 V2.1.1: “Intelligent Transport Systems (ITS); Security; Pre-standardisation study on Misbehaviour Detection; Release 2”.

9.2 Related documents

[RD-1] PRESERVE Deliverable D1.3: V2X Security Architecture V2, January 2014

[RD-2] EVITA Deliverable D3.2: Secure On-Board Architecture specification, August 2011

[RD-3] Joseph Kamel, et al. Simulation Framework for Misbehaviour Detection in Vehicular Networks. IEEE Transactions on Vehicular Technology, 69 (6), pp.6631-6643, April 2020.

[RD-4] Joseph Kamel, Arnaud Kaiser, Ines Jemaa, Pierpaolo Cincilla, Pascal Urien. CaTch: A Confidence Range Tolerant Misbehaviour Detection Approach. IEEE Wireless Communications and Networking Conference, Apr 2019, Marrakech, Morocco.

[RD-5] Joseph Kamel, Ines Jemaa, Arnaud Kaiser, Loic Cantat, Pascal Urien. Misbehaviour Detection in C-ITS: A comparative approach of local detection mechanisms. Vehicular Networking Conference (VNC), Dec 2019, Los Angeles, California, United States. hal-02400137.

[RD-6] Attila Jaeger, Norbert Bißmeyer, Hagen Stuebing, and Sorin A. Huss. A novel framework for efficient mobility data verification in vehicular ad-hoc networks. International Journal of Intelligent Transportation Systems Research, 10(1):11–21, Jan 2012.

[RD-7] F. Haidar, et al.: Experimentation and assessment of Pseudonym Certificate Management and Misbehaviour Detection in C ITS, IEEE Open Journal of Intelligent Transportation Systems, vol. 2, pp. 128-139, 2021, https://ieeexplore.ieee.org/document/9445398.

[RD-8] J. Whitefield et al.: Formal Analysis of V2X Revocation Protocols, April 2017, https://arxiv.org/abs/1704.07216

[RD-9] ETSI TS 103 759 V2.1.1: Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2.

[RD-10] C2C-CC White Paper - Guidance for day 2 and beyond roadmap, version 1.2, July 2021.

[RD-11] ISO 27035-1:201": "Information technology– Security techniques Information security incident management– Part 1: Principles of incident management".

[RD-12] ISO 27035-2:201": "Information technology - Security techniques - Information security incident management-- Part 2: Guidelines to plan and prepare for incident response".

[RD-13] ISO 27035-3:202": "Information technology - Security techniques - Information security incident management -- Part 3: Guidelines for incident response operations".

[RD-14] ANSSI Guide: "Security incident detection service providers – Requirements reference document". https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0_en.pdf

[RD-15] ETSI GS ISI 007: "Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SO) ".

[RD-16] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1. June 2018.

[RD-17] Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems, release 1, December 2017. https://ec.europa.eu/transport/themes/its/c-its_en

[RD-18] Final Report, C-ITS Platform Phase II, September 2017. https://ec.europa.eu/transport/sites/default/files/2017-09-c-its-platform-final-report.pdf

[RD-19] China Industry Innovation Alliance for the Intelligent and connected vehicles: V2X vehicle management – Enabled by Security capability, January 2021.

[RD-20] SCMS: Options Analysis Report, prepared by Escrypt for Transport Canada, March 31, 2020.

https://tcdocs.ingeniumcanada.org/sites/default/files/2020-04/Security%20Credential%20Management%20System%20%28SCMS%29%20-%20Options%20Analysis%20Report%20.pdf

[RD-21] IEEE 1609.2.1-2020 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) --Certificate Management Interfaces for End Entities