ETSI TS 103 759 V2.1.1 (2023-01)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS);
Security;
Misbehaviour Reporting service;
Release 2

Reference

DTS/ITS-00561

Keywords

interoperability, ITS, management, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

In the context of the European C-ITS Security Credential Management System (EU CCMS), the C-ITS certificate policy [i.1] defines the trust model, which is based on Public Key Infrastructure (PKI) enrolment of the end entities. The C-ITS certificate policy [i.1] mandates that any Certification Authority (CA) provides, among other functionalities, "Regular monitoring reporting, alerting and restore duties of the C-ITS Trust model entities in order to establish a secure operation including cases of misbehaviour" [i.1]. The requirements of the misbehaviour reporting system are however deferred to a future release of the C-ITS certificate policy [i.1].

The report [i.2] presents recommendations for standard harmonization issued by the EU-US ITS Task Force, and partially addresses the requirements for the misbehaviour component of the Cooperative-ITS Credential Management System (CCMS) [i.2]. As written in this report, "End-entities provide misbehaviour reports and the Misbehaviour component processes them. If revocation is warranted, this component provides information to Authorization or Revocation components to initiate revocation and/or blacklisting, as appropriate".

In accordance with [i.1] and [i.2], the object of the present document is the misbehaviour reporting service, by which an ITS Station (ITS-S) or an end entity may provide misbehaviour reports to the Misbehaviour Authority (MA) of the C-ITS CCMS. As indicated in [i.2], a misbehaviour report by an end entity reports the identity as known to the reporting station of the suspects [i.2]. This implies that only observations which are directly attributable to specific ITS services and related messages may be the object of a misbehaviour report.

1 Scope

The present document specifies the Misbehaviour Reporting service in support of trusted ITS stations for the reporting of local misbehaviour detections to a central authority (Misbehaviour Authority), which collects reports from different ITS stations for global analysis and reaction.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".

[2] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".

[3] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[4] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

[5] Recommendation ITU-T X.696: "Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)".

[6] IEEE Std 1609.2™-2022: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

NOTE: At the time of publication of the present document, IEEE Std 1609.2™-2022 was approved but not published: the approved draft standard is available from https://standards.ieee.org/ieee/1609.2/10258/ if the published version is not available.

[7] ETSI TS 103 836-4-1: "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; Release 2".

[8] ETSI TS 103 900: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Specification of Cooperative Awareness Basic Service; Release 2".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1, June 2018.

[i.2] Cooperative-ITS Credential Management System Functional Analysis and Recommendations for Harmonization, Document HTG6-4, Version 2015-09. EU-US ITS Task Force, Standards Harmonization Working Group, Harmonization Task Group 6.

[i.3] ETSI TR 103 460: "Intelligent Transport Systems (ITS); Security; Pre-standardization study on Misbehavior Detection; Release 2".

[i.4] ETSI TS 103 898: "Intelligent Transport Systems (ITS); Communications Architecture; Release 2".

[i.5] ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".

[i.6] ISO/IEC 8824-1:2015: "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[i.7] ETSI TS 103 831: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Decentralized Environmental Notification Service; Release 2".

[i.8] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni: "T-VNets: a novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS", Elsevier - International Journal Computer Communications, vol. 93, no. C, pp. 68-83, November 2016.

[i.9] C-ITS Delegated Act Annex 1, 2019.

NOTE: Available at https://eur-lex.europa.eu/resource.html?uri=cellar:9a2fe08f-4580-11e9-a8ed-01aa75ed71a1.0014.02/DOC_2&format=PDF.

[i.10] ISO/IEC 27000:2018: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

ego vehicle: vehicle embedding the ITS-S providing the misbehaviour reporting service

evidence: information used, possibly in conjunction with other information, in a process to determine the correctness of a statement

misbehaviour: act by an ITS-S of transmitting false or misleading information, or information that was not authorized by the local policy, either purposefully or unintendedly

EXAMPLE: This includes suspicious behaviour as in wrong message types, contents or frequencies, unauthorized access, incorrect signed or encrypted messages, etc.

misbehaving entity: ITS-S that is sending false or misleading messages using valid certificates

NOTE: This definition includes both faulty ITS-S and malicious entities (attackers) that own certificates.

Misbehaviour Reporting (MR) message: message created and sent by the ITS-S willing to report misbehaviour

non-repudiation: ability to prove the occurrence of a claimed event or action and its originating entities

NOTE: This definition is taken from ISO/IEC 27000 [i.10].

reported ITS station: ITS-S having transmitted information that is subject to the creation of a MR

reporting ITS station: ITS-S generating a MR

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 940 [1], ETSI TS 102 941 [2], ETSI TR 103 460 [i.3] and the following apply:

AID	Application ID
ASR	Application Specific Report
IOC	Information Object Class
IOS	Information Object Set
MA	Misbehaviour Authority
MD	Misbehaviour Detection
MDM	Misbehaviour Detection Management
MDS	Misbehaviour Detection Service
MR	Misbehaviour Report
MRS	Misbehaviour Reporting Service
PDU	Protocol Data Unit
SM-PDU	Security Management PDU

4 Misbehaviour Reporting Service introduction

4.1 Misbehaviour Detection and Reporting Service architecture

Misbehaviour reporting is carried out in the context of the Misbehaviour Detection Management (MDM) system. The MDM system is composed of local (part of the ITS-S) and backend subsystems. In the MDM system, ITS-S create Misbehaviour Reports (MRs) and send them to the backend subsystem. Based on this and other information, the backend subsystem determines what has actually occurred and what, if any, response and remediation actions to take.

Figure 1 shows the MDM system architecture. All components in Figure 1 shall be as defined in ETSI TS 102 940 [1].

Figure 1 adds a new functional component for Misbehaviour Pre-processing. This component, which is optional**,** belongs to the backend subsystem, and may act on the MRs before they are passed to the Misbehaviour Authority (MA).

ETSI TR 103 460 [i.3] provides an analysis of the Misbehaviour Detection Service (MDS) and of the Misbehaviour Reporting Service (MRS) within an ITS station. The scope of the present document is to specify the MRS, which is part of the ITS-S Local Misbehaviour Detection component. The MRS is part of the security entity in the ITS-S as specified in ETSI TS 103 898 [i.4].

Brief functional descriptions of Figure 1 components are as follows.

- The **ITS-S Local Misbehaviour Detection** component is the functionality on the ITS-S responsible for detecting misbehaviour, generating misbehaviour reports, and sending them to the backend subsystem. It may also react locally to the detected misbehaviour, e.g. by informing other applications on the ITS-S about the misbehaviour. Local misbehaviour reaction is out of scope of the present document.

NOTE 1: As recommended in TVRA ETSI TR 102 893 [i.5], the ITS-S is assumed to check their outgoing messages to avoid sending messages that are classified as misbehaviour.

NOTE 2: It is not assumed that all observed instances of misbehaviour lead to the generation or transmission of a MR. How an ITS-S decides whether to generate a MR on observed misbehaviour is implementation specific.

- The **Misbehaviour Pre-processing** component is optional. It may act on the MRs before they are passed to the Misbehaviour Authority component, for example to improve the privacy of the reporters, or to improve the quality of the information received by the Misbehaviour Authority by collecting context information about the communication. Specific pre-processing activities are out of scope of the present document.

- The **Misbehaviour Authority** component takes in MRs and other information, possibly after pre-processing by the Misbehaviour Preprocessing component. It uses all this information to make a determination as to what response actions (for example revocation of a certificate) should be taken within the PKI. Multiple instances of the Misbehaviour Authority component may exist in the system.

- The **Remediation** component is responsible for implementing any other remediation activity.

Figure 1 also shows the information flow from ITS-S to the Misbehaviour Authority component, and from the Misbehaviour Authority component to the Remediation component.

An example detailed view of the overall MDM system is presented in Annex B.

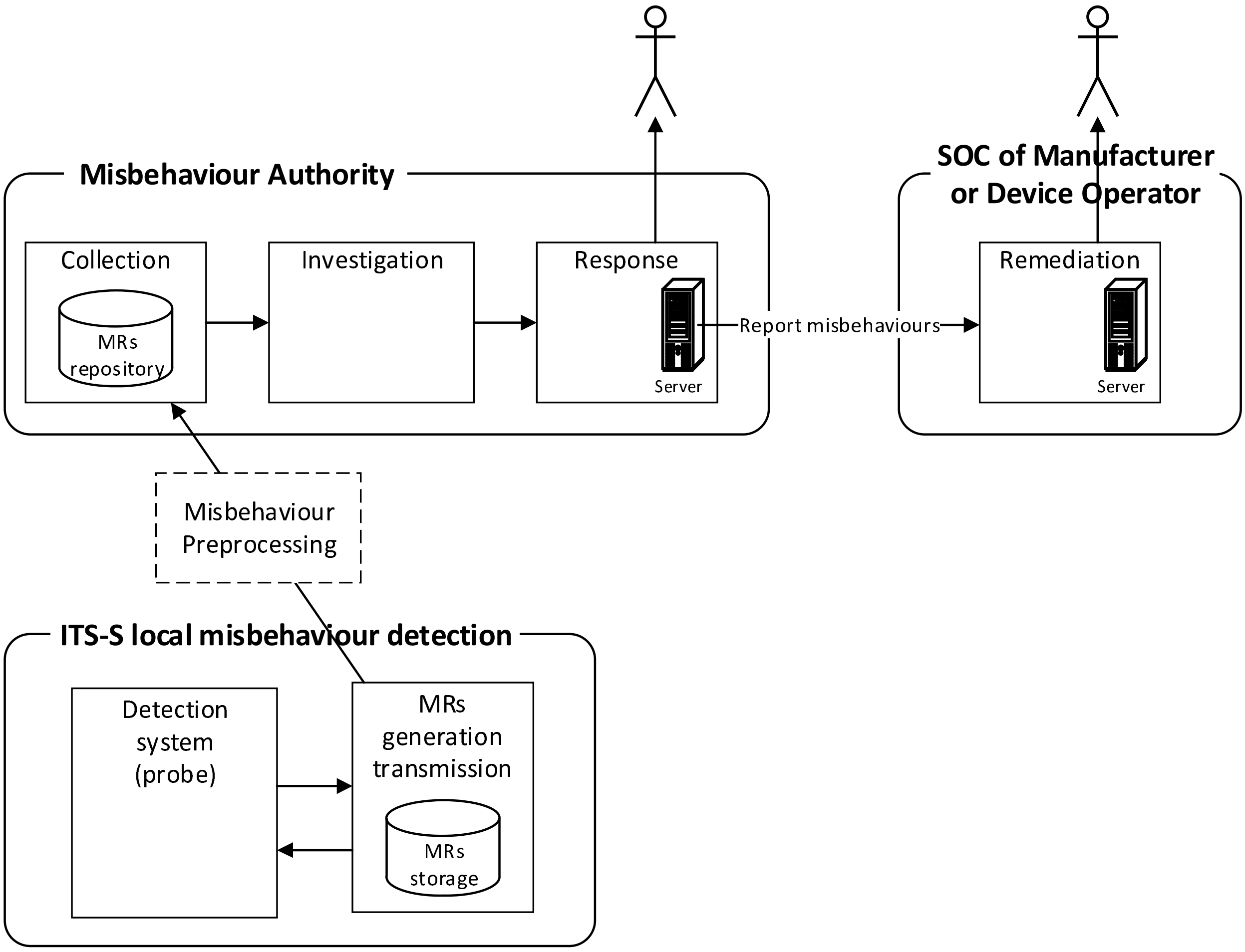


Figure 1: Misbehaviour Detection Management system

4.2 ITS-S Local Misbehaviour Detection services

4.2.1 Overview

The services provided by the ITS-S Local Misbehaviour Detection component are defined as follows:

- The **Detection system (probe)** in the ITS-S Local Misbehaviour Detection component provides the **local MDS**. The probe runs checks on the received messages. These checks may include individual detectors on the incoming messages and/or more sophisticated checks that combine input from multiple detectors and include sensor input and other external data. Based on this, the probe makes a determination as to whether or not a received message or set of messages represents misbehaviour that is suitable for reporting.

NOTE: The local MD subsystem may output metadata about the misbehaviour observation, for example the level of severity of the misbehaviour or its level of certainty that the observed messages are in fact misbehaviour. This is out of scope of the present document.

- The **MRs generation transmission** in the ITS-S Local Misbehaviour Detection component provides the **Misbehaviour Reporting Service**. It receives notification of an observed misbehaviour by the local MDS. It determines whether to generate a MR, assembles the MR, signs and encrypts it, and then either sends it or stores it for later sending. Over time it also manages stored MRs to ensure proper prioritization of storage space.

4.2.2 Local Misbehaviour Detection Service

The functional architecture providing the local MDS is shown in Figure 2.

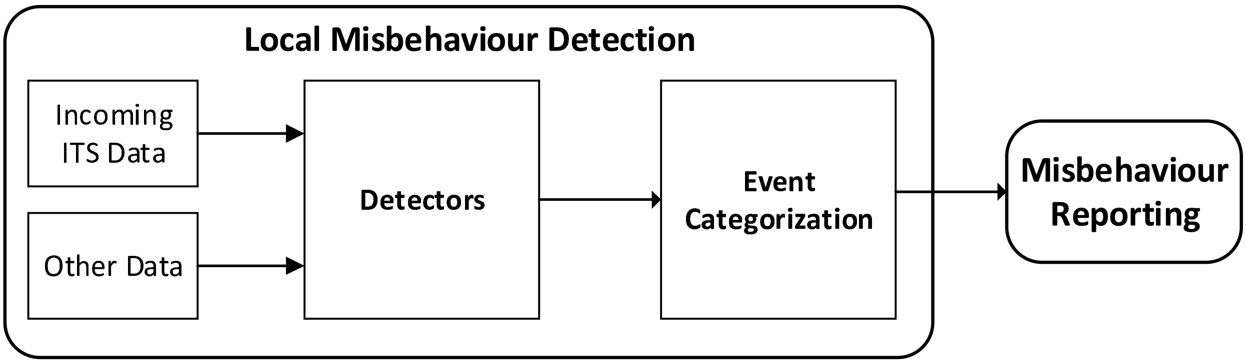


Figure 2: Local Misbehaviour Detection Service functional architecture

Each functional element is briefly described below:

- Incoming ITS Data is any incoming ITS message, e.g. CAM and DENM.
- Other Data is any information other than incoming ITS messages, e.g. sensor and map data.
- Detectors identify incoming ITS messages that are in some way inconsistent with the ITS-S's perception of ground truth or are otherwise impairing the correct operation of the V2X system.
- Event Categorization aggregates the outputs of all individual detectors along with data from other sources to determine whether an incoming ITS message is suspicious or not.

An example detailed view of the functional architecture for the local MDS is presented in Annex C.

4.2.3 Misbehaviour Reporting Service

The functional architecture providing the MRS is shown in Figure 3.

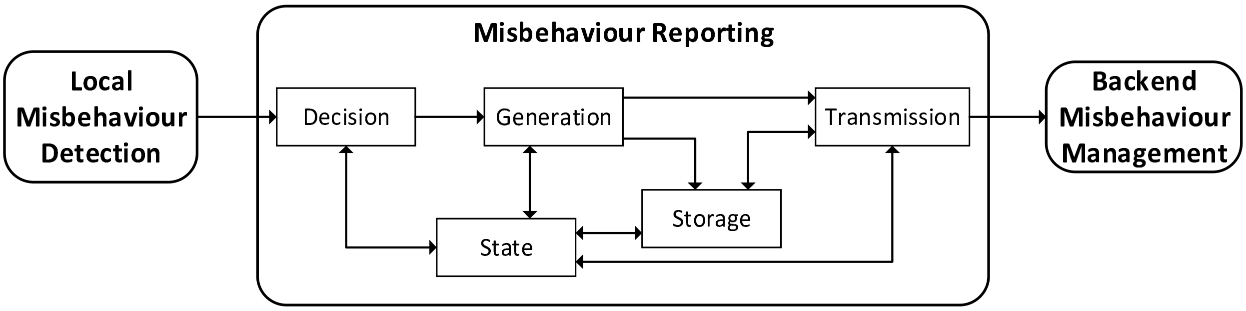


Figure 3: Misbehaviour Reporting Service functional architecture

Each functional component of the system is briefly described below:

- **Decision** stipulates whether or not to generate a MR for a misbehaviour event observed by the local MDS.
- **Generation** creates the misbehaviour report making use of the information provided by the local misbehaviour detection service and optionally of other information obtained from **State**. After report creation, it also decides whether to send the report to Storage and/or Transmission.
- **Transmission** decides whether to send the reports to the Misbehaviour Authority. If multiple reports are available to send, Transmission decides which ones to send and in which order.
- **State** stores information that will be used by other components inside the misbehaviour reporting subsystem to carry out their functions. The misbehaviour reporting subsystem may have to manage three distinct "budgets": one for report creation (as there may be competing demands for access to a signing process, or for processor time in general); one for storage (as the total volume of reports generated may exceed the storage available or allocated for them); and one for report transmission (as it may not be possible to transmit all generated reports due to intermittent connectivity). The State is the functional entity responsible for managing each of these budgets.
- **Storage** stores misbehaviour reports provided by Generation, provides them to Transmission for transmission to the Misbehaviour Authority, and deletes old reports.

4.2.4 Misbehaviour Reporting Service requirements

The following functional and performance requirements of the MRS shall be fulfilled:

- **Identification of the reporting and reported ITS-S:** The reporting ITS-S and the reported ITS-S identities shall be included in the MR. To avoid the generation and transmission of false reports, the authenticity of this identification information shall be protected (see below).
- **Reliability and proof-based:** A MR shall include evidence related to the observations of individual detectors by the local MDS of the reporting ITS-S, so that the MA is able to verify the observations independently. This evidence shall include the original received message and the indication of the relevant individual detectors.
- **Efficiency and minimum resource consumption:** MRs should not overload the communication channel. The reporting process shall not send repetitive and redundant information about the same misbehaviour event.
- **Flexibility:** The design of the MR shall be extensible to allow to integrate new individual detectors and new evidence at a later stage without breaking backward compatibility.

Additionally, the following security and privacy requirements shall be fulfilled:

- **Privacy protection:** The design of the MR shall be such that the MA is unable to link the short term and the long-term identities of the reported ITS-S and of the reporting ITS-S. The reporting ITS-S shall use its pseudonym certificates or Authorization Tickets (AT) to communicate with the MA.

- **Confidentiality:** MRs sent by a reporting ITS-S shall be encrypted to protect the confidentiality of the information sent to the MA.
- **Integrity & authenticity:** MRs sent by an ITS-S shall be signed with the private key corresponding to the verification public key of the valid AT of the reporting ITS-S to ensure the integrity and authenticity of the data.
- **Non-repudiation:** The MR shall provide sufficient evidence to allow the MA to verify that the messages reported as suspicious were sent by the reported ITS-S. This evidence consists of at least the suspicious messages, which include the associated AT. The AT proves that the reported ITS-S is a trusted ITS-S owning a valid AT with permission levels satisfying the corresponding ITS application requirements.

5 Misbehaviour Reporting dissemination protocol specification

5.1 Overview

As the reporting is not a real time process, the MR is sent to the MA when connectivity is available via a suited communication interface. 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 ITS-S from the MA.

5.2 Communication assumptions and requirements

To send a MR message to the MA, a reporting ITS-S has to set up a communication with the MA. The ITS-S may use different communication types for the reporting of a misbehaving entity, such as for instance:

- a wired connection (may be available if the reporting ITS-S is a roadside unit);
- short-range wireless communication via an ITS-S roadside unit or a cellular network link (3G, 4G or 5G);
- a Wi-Fi hotspot providing access to the Internet, e.g. in a parking space or the private hotspot at home;
- a wired or wireless connection at electric vehicle charging station;
- using the Vehicle On-Board Diagnostic (OBD) port and a diagnostic system at the service garage or inspection workshop.

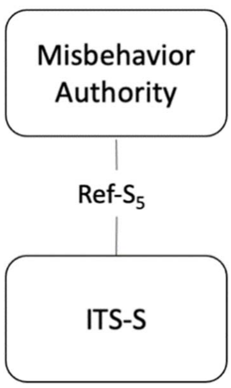


Figure 4: Communication with the MA using a cellular network connection

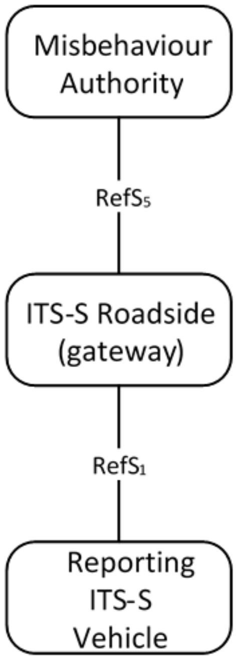


Figure 5: Communication with the MA using V2I connection

Figure 4 and Figure 5 present two possible options for the reporting ITS-S to communicate with the MA. This functional model extends the ITS communication security model specified in ETSI TS 102 940 [1] with the different communication paths. It introduces functional entities as defined in Table 1 and specifies the communication paths needed to support the reporting ITS-S communication via a cellular network (Figure 4) or via a short-range wireless access network (Figure 5).

Table 1: Functional element roles

Functional element	Role
Misbehaviour Authority	See definition of functional elements, as specified in ETSI TS 102 940 [1], Table 8
Misbehaviour preprocessing component	Optional intermediary system or proxy supporting the activities of misbehaviour preprocessing as specified in clause 4.1
Reporting ITS-S	ITS-S generating a MR
ITS-S Roadside Gateway	Receives broadcast messages from mobile ITS-S and relays certificate requests and responses to/from the Receiving Certificate Authority within the PKI

The architecture model specified in ETSI TS 102 940 [1] is refined by considering an ITS-S sending the MR (Reference Point S_1), a roadside ITS-S for relaying the MR message (Reference Point S_5) via the infrastructure network to the recipient MA.

In Figure 4 the ITS-S transmits the MR directly to the MA via cellular network (Reference Point S_5).

The model depicted in Figure 5 assumes that a mobile ITS-S has the capabilities to transmit MRs through the short-range wireless communication interface (Reference Point S_1). For that scenario, a C-ITS communication channel for security management purpose shall be made available to the reporting ITS-S.

6 Misbehaviour Report specification

6.1 ITS-AID-specific report

The MR has the objective of reporting data received from a specific ITS-S. The MR is dedicated to a single ITS service, identified by its ITS-AID value. The ITS-AID value acts as a parameter, determining the set of individual detectors that may be contained as observations in the MR. There is no maximum number of observations that may be reported in a single MR.

The report contains the following elements:

- The ITS-AID value.
- The list of the observations of the individual detectors. The ITS-AID value selects the set of individual detectors that may be contained as observations in the report.
- The list of the received messages involved in the observations. The specification of the individual detectors involved indicate the set of mandatory messages.
- The list of evidence, besides the received messages, involved in the observations. The specification of the individual detectors involved indicate the set of mandatory evidence.

The format of the MR is specified in clause 7.

6.2 Reporting of observations of individual detectors

The local MDS (see clause 4.2.2) aims on detecting misbehaviour by inspection of incoming messages. The MR includes observations of the individual detectors.

In the present document, individual detectors of an incoming message are classified as detailed in Table 2.

Table 2: Classification of individual detectors for the local Misbehaviour Detection service

Class 1	Class 2	Class 3	Class 4	Class 5
Implausible values within the incoming message.	Inconsistencies of the incoming message with previous messages of the same type emitted from the same station.	Inconsistencies of the incoming message with the knowledge of the local environment of the ego vehicle (e.g. LDM).	Inconsistencies of the incoming message with the on-board sensors' perception.	Inconsistencies of the incoming message with previous messages of other types from the same station or with messages (of the same type or not) emitted by other stations.

Security-level individual detectors are considered to belong to Class 1.

A guide to establishing the specification of the individual detectors, including the mandatory elements needed in the MR is detailed in the following, and summarized in Table 3:

- **Class 1 individual detector**. The MR shall include the message upon which the observation has been made. In general, Class 1 individual detectors do not require any mandatory evidence besides the triggering message.
- **Class 2 individual detector**. The MR shall include at least two messages of the same type emitted by the same station, upon which the observation has been made. In general, Class 2 individual detectors do not require any mandatory evidence besides the triggering messages.
- **Class 3 individual detector**. The MR shall include the message upon which the observation has been made. Class 3 individual detectors may require a reference to the local knowledge of the environment on which the observation is based.

- **Class 4 individual detector**. The MR shall include the message upon which the observation has been made. Class 4 individual detectors may require a reference to the on-board sensors' readings on which the observation is based.

- **Class 5 individual detector**. The MR shall include at least two messages of different type or two messages of the same type emitted by different stations, upon which the observation has been made. In general, Class 5 individual detectors do not require any mandatory evidence besides the triggering messages.

A single MR may contain several observations of individual detectors. The following rules apply in order to be able to produce a single MR containing multiple observations:

1) The ITS-AID indicated in the report is the ITS-AID of the most recent mandatory message included in the MR report. Individual detectors that cannot be linked to a specific application shall be reported using a special ITS-AID value, which indicates "unknown ITS application".

2) All the observations that are triggered by the same set of mandatory messages may be included in the same MR. For example, any number of observations of Class 1, Class 3 and Class 4 individual detectors on the same message may be included in the same MR. Any number of observations of Class 2 individual detectors on the same pair of consecutive messages may be included in the same MR.

3) The observations that are triggered by a set of multiple mandatory messages and the observations that are triggered by the mandatory message dictating the indication of the ITS-AID (i.e. the most recent mandatory message) may be included in the same MR. For example, an observation of a Class 1 individual detector on a message may be included along with an observation of a Class 5 individual detector triggered by the same message along with an older one.

Examples of individual detectors for CAM and DENM messages are presented in Annex D.

Examples illustrating the generation of the MR from the observations of individual detectors belonging to one or to multiple classes are provided in clause 7.5.

Table 3: Mandatory elements in the MR by individual detector class

	Class 1	Class 2	Class 3	Class 4	Class 5
ITS-AID	The ITS-AID of the mandatory message.	The ITS-AID of the mandatory messages.	The ITS-AID of the mandatory message.	The ITS-AID of the mandatory message.	The ITS-AID of the most recent mandatory message.
Mandatory messages	The single message that triggers the observation.	Two or more messages of the same type, emitted by the same station, that trigger the observation.	The single message that triggers the observation.	The single message that triggers the observation.	Two or more messages from different stations and/or of different type, that trigger the observation.
Mandatory evidence	None.	None.	Reference to the local knowledge of the environment may be required.	Reference to the onboard sensors' readings may be required.	None.

7 Misbehaviour Report format

7.1 Hierarchical structure of the Misbehaviour Report

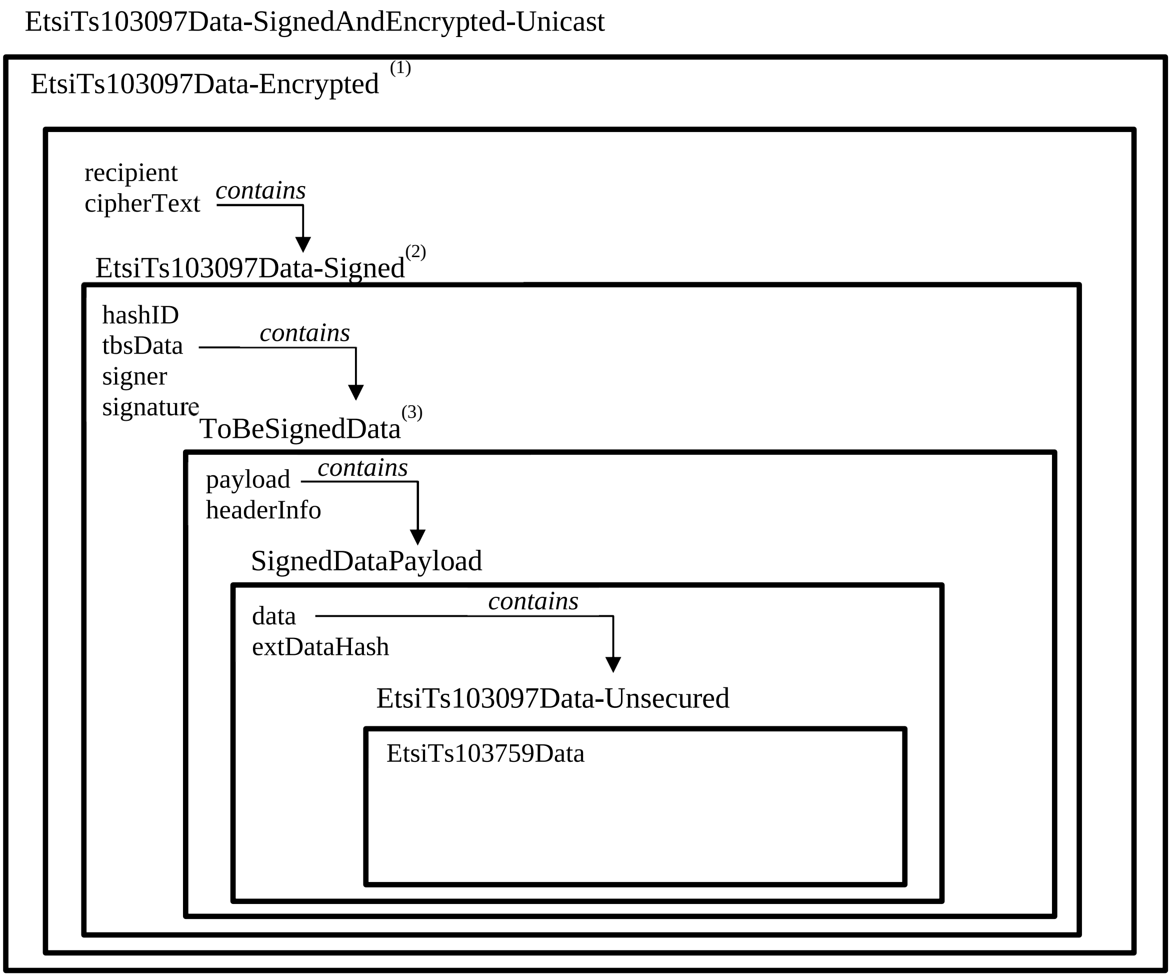
As specified in ETSI TS 102 940 [1], the MRS is part of the ITS-S security entity (Security Defence sublayer) and the MR message flow is shown in the PKI architecture (ETSI TS 102 940 [1], clause 7.0, Figures 11a/11b). The security management message (SM_PDU) for the MR is specified in the present document and shall follow the message format shown in Figure 6.

NOTE: The present document only considers reporting MRs to the PKI infrastructure, i.e. to the MA responsible for handling misbehaviour reports for misbehaviours related to a given ITS-AID or set of ITS-AIDs.

The outermost data structure `EtsiTs103097Data-SignedAndEncrypted-Unicast` shall encapsulate an `EtsiTs103759Data` as shown in Figure 6. Specification of all containers and enclosed data structures are given in clause 7.3.

To create the MR, the reporting ITS-S shall follow the following process:

- An `EtsiTs103759Data` structure is built, according to the specification in clause 7.3.
- An `EtsiTs103097Data-Signed` structure is built containing: `hashId`, `tbsData`, `signer` and `signature`:
    - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
    - in the `tbsData`:
        - the `payload` shall contain the previous `EtsiTs103759Data` structure;
        - in the `headerInfo`:
            - the `psid` shall be set to the value of "Misbehaviour Reporting Service" as assigned in ETSI TS 102 965 [4];
            - the `generationTime` shall be present and contains the time when the PDU signature was generated;
            - all other components of the component `tbsdata.headerInfo` are not used and absent;
    - the `signer` shall be declared as "`digest`", containing the HashedId8 of the Authorization Ticket (AT) of the ITS-S reporter;
    - the `signature` over the `tbsData` computed using the private key corresponding to the AT's verification public key of the ITS-S reporter. For the signature to be valid the signing certificate shall conform to the Authorization Ticket profile given in clause 7.2.1 of ETSI TS 103 097 [3], where the appPermissions field in the Authorization Ticket allows signing misbehaviour reports. The application permissions for the reporting ITS-S shall follow the requirements of clause 8.1.



(1) Encryption is done with ECIES using the public encryption key of the MA.
(2) Signature is computed using the current valid private key corresponding to the AT's verification public key of the ITS-S reporter.
(3) All data structures below the ToBeSignedData are defined in IEEE Std 1609.2™ [6].

Figure 6: Misbehaviour Report format

- An `EtsiTs103097Data-Encrypted` structure is built, with:
  - the component `recipients` containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
    - the hashedId8 of the MA certificate in `recipientId`; and
    - the encrypted data encryption key in `encKey`; the public key to use for encryption is the `encryptionKey` found in the MA certificate referenced in `recipientId`;
  - the component `ciphertext` containing the encrypted representation of the `EtsiTs103097Data-Signed` structure.
- An `EtsiTs103759Data-SignedAndEncrypted-Unicast`structure is built. This structure is the SPDU defined in ETSI TS 103 097 [3] used to send a signed and encrypted `EtsiTs103759Data` to the MA and shall contain the previous `EtsiTs103097Data-Encrypted` structure.

7.2 Overview of `EtsiTs103759Data`

The ASN.1 modules used to build a misbehaviour reporting message of ASN.1 type `EtsiTs103759Data` shall be as specified in Annex A. ASN.1 [i.6] data structures defined in the present document for all SM-PDU specified in ETSI TS 102 941 [2] shall be encoded using the Canonical Octet Encoding Rules (COER) as defined in Recommendation ITU-T X.696 [5].

To get a future-proof set of ASN.1 definitions, the concept of Information Object Classes (IOC) and respective Information Object Sets (IOS) is applied.

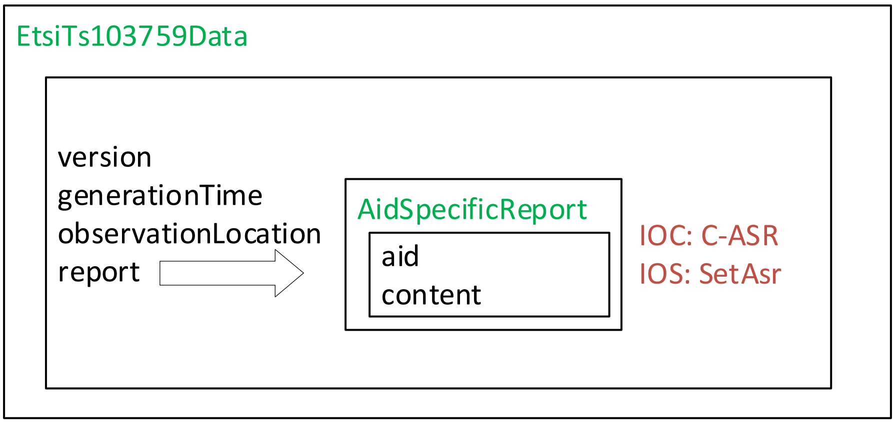


Figure 7: ASN.1 type EtsiTs103759Data

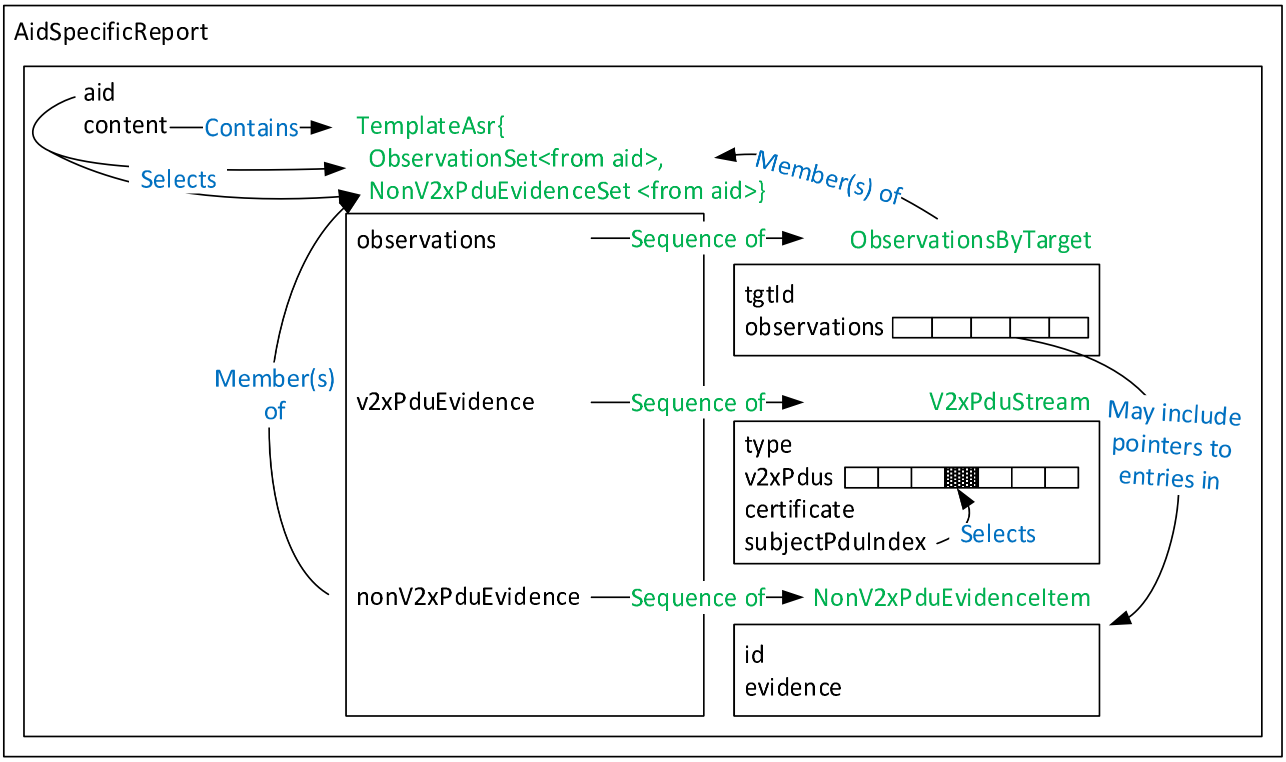


Figure 8: ASN.1 type AidSpecificReport

Figure 7 and Figure 8 provide an overview of the generic misbehaviour reporting message structure that uses the IOC C-ASR with the IOS SetAsr to identify the source of observations, e.g. a specific observed message such as a CAM or DENM.

7.3 ASN.1 structures in the `EtsiTs103759Core` module

The description of the ASN.1 module `EtsiTs103759Core` is available at:
https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/docs/EtsiTs103759Core.md.

7.4 Mapping between different parts of the TemplateAsr

As specified above, the `TemplateAsr` contains `observations`, `v2xPduEvidence`, and `nonV2xPduEvidence` fields. This clause describes how the structure is intended to be used to report different types of misbehaviour.

- For Class 1 observations, i.e. implausible values within the incoming message: the observation refers to the subject PDU of the first `V2xPduStream` in `v2xPduEvidence`.
- For Class 2 observations, i.e. inconsistencies of the incoming message with previous messages of the same type emitted from the same station: the observation refers to the subject PDU of the first `V2xPduStream` in `v2xPduEvidence` and to at least one other PDU in that `V2xPduStream`. The definition of the observation is expected to specify how that other PDU is identified. Possibilities include:
    - The observation always refers to only two PDUs: the subject PDU and the PDU immediately before it. In this case there is no need for an explicit field in the observation indicating the PDUs, as the definition of the observation is unambiguous.
    - The observation always refers to only two PDUs: the subject PDU and one other PDU in the same `V2xPduStream`. In this case the observation definition is expected to specify that the other PDU is identified by its index within the `v2xPdus` array, with 0 indicating the first entry.
    - The observation may refer to more than two PDUs, i.e. there may be more than one PDU as well as the subject PDU. In this case the observation definition is expected to specify that the other PDUs are identified by an array of integers, each indicating a unique index within the `v2xPdus` array, and with 0 indicating the first entry.
- For Class 3 observations, i.e. inconsistencies of the incoming message with the knowledge of the local environment of the ego vehicle (e.g. LDM): the information about the local environment is to be included in the `nonV2xPduEvidence` field.
- For Class 4 observations, i.e. messages that are inconsistent with other context such as sensor data, the other context is to be included in the `nonV2xPduEvidence` field.
- For Class 5 observations, i.e. inconsistencies of the incoming message with previous messages of other types from the same station or with messages (of the same type or not) emitted by other stations: the PDUs that are inconsistent with each other are the subject PDUs of the different `V2xPduStream` entries in `v2xPduEvidence`. An observation definition is expected to specify that the PDUs relevant to a particular observation are indicated by the index of their entry within `v2xPduEvidence`, with 0 indicating the first entry.

7.5 Examples to illustrate the intended use of the structures

7.5.1 Example 1

- Setup: An observer makes five Class 1 observations on a single PDU.
- Format: The observer creates a single report. In this report, `v2xPduEvidence` has a single entry, `v2xPduEvidence[0]`. In `v2xPduEvidence[0]`, the `v2xPdus` array has a single entry and `subjectPduIndex` is 0, i.e. that single PDU is the subject PDU. The five observations are included in `observations` and all refer to the subject PDU.

7.5.2 Example 2

- Setup: An observer makes five Class 1 observations on a single PDU. For purposes of this example, it is assumed that there is a policy in place that requires that for Class 1 observations, five PDUs from the same sender before and after the subject PDU are included in the report.
- Format: The observer creates a single report. In this report, `v2xPduEvidence` has a single entry, `v2xPduEvidence[0]`. In `v2xPduEvidence[0]`, the `v2xPdus` array has eleven entries and `subjectPduIndex` is 5, i.e. the subject PDU is the sixth PDU. The five observations are included in `observations` and all refer to the subject PDU.

7.5.3 Example 3

- Setup: An observer makes five Class 1 observations on two successive PDUs from the same sender.
- Format: The observer creates two different reports, one with the observations on the first PDU, and one with the observations on the second PDU. Each report has the format described in Example 1.

7.5.4 Example 4

- Setup: An observer makes five Class 1 observations on two successive PDUs from the same sender. Additionally, the observer makes three Class 2 observations of inconsistencies between those same PDUs.
- Format: The observer creates two different reports:
  - The first one contains the Class 1 observations on the first PDU, and has the format described in Example 1.
  - The second one contains the Class 1 observations on the second PDU and the Class 2 observations. In this report, `v2xPduEvidence` has a single entry, `v2xPduEvidence[0]`. In `v2xPduEvidence[0]`, the `v2xPdus` array has two entries and `subjectPduIndex` is 1, i.e. the subject PDU is the second PDU. The eight observations (five Class 1 and three Class 2) are included in `observations` and all refer to the subject PDU.

7.5.5 Example 5

- Setup: An observer makes a Class 5 observation on two PDUs from different senders - for example, two CAMs that appear to show two vehicles in the same place.
- Format: The observer creates a single report. In this report, `v2xPduEvidence` has two entries, `v2xPduEvidence[0]` and `v2xPduEvidence[1]`. For both `v2xPduEvidence[0]` and `v2xPduEvidence[1]`, the `v2xPdus` array has a single entry and `subjectPduIndex` is 0.
- Comment: This is just an example: in the real world it is highly likely that proximity plausibility violations will stretch over multiple messages.

7.5.6 Example 6

- Setup: An observer makes a Class 5 observation on PDUs from three different senders - for example, three CAMs that appear to show three vehicles (A, B and C) in the same place.
- Format: One option is for the observer to create three different reports reporting on pairwise proximity plausibility violations between (A and B), (A and C), and (B and C). However, for compactness, the misbehaviour report format also supports creating a single report in which `v2xPduEvidence` has three entries: `v2xPduEvidence[0]`, `v2xPduEvidence[1]`, `v2xPduEvidence[2]`. For all `v2xPduEvidence[i]`, the `v2xPdus` array has a single entry and `subjectPduIndex` is 0.

7.5.7 Example 7

- Setup: An observer makes a Class 5 observation on two PDUs from different senders - for example, two CAMs that appear to show two vehicles in the same place. Additionally, one of the senders is observed doing a Class 1 misbehaviour.

- Format: The observer creates a single report. In this report, `v2xPduEvidence` has two entries, `v2xPduEvidence[0]` and `v2xPduEvidence[1]`. For both `v2xPduEvidence[0]` and `v2xPduEvidence[1]`, the `v2xPdus` array has a single entry and `subjectPduIndex` is 0. The observer may also create two reports, one with the Class 5 observation and one with the Class 1 observation. However, this results in increased overhead.

7.5.8 Example 8

- Setup: An observer makes a Class 3 observation on a single PDU - for example, a CAM that shows speed inconsistent with a map, for example a car driving at open-road speeds in a location where the map shows a building.

- Format: The observer creates a single report. In this report, `v2xPduEvidence` has a single entry, `v2xPduEvidence[0]`. In `v2xPduEvidence[0]`, the `v2xPdus` array has a single entry and `subjectPduIndex` is 0. The `nonV2xPduEvidence` field has one entry in which the reporter indicates which map data was used to make the determination of a violation. The definition of the observation may include the index of the map field within `nonV2xPduEvidence` - in this case, 0 to indicate the first entry.

7.5.9 Example 9

- Setup: An observer makes a Class 4 observation on a single PDU - for example, a CAM that shows speed inconsistent with the observer's sensors.

- Format: The observer creates a single report. In this report, `v2xPduEvidence` has a single entry, `v2xPduEvidence[0]`. In `v2xPduEvidence[0]`, the `v2xPdus` array has a single entry and `subjectPduIndex` is 0. The `nonV2xPduEvidence` field has one entry in which the reporter includes the ground truth as defined by its sensors. The `nonV2xPduEvidence` field may also include a reporter info field containing information about the sensors with which the reporter is equipped. The definition of the observation may include the index of the ground truth field within `nonV2xPduEvidence`. If this field is included, its value depends on the order of the two `nonV2xPduEvidence` fields - the ground truth field and the reporter info field.

7.6 Specifications of observations of individual detectors

The description of common observations, along with details on evidence that need to be included in the report, can be found at the following link:

- https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/docs/EtsiTs103759CommonObservations.md.

The complete list of application-specific observations, along with the corresponding trigger conditions, are provided in the documentation of the application-specific modules. For the module EtsiTs103759AsrCam module they can be found at the following link:

- https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/docs/EtsiTs103759AsrCam.md.

8 Certificate Profiles specification

8.1 ITS-S signing certificate

8.1.1 Overview

Misbehaviour reports generated by a reporting ITS-S containing an "AID-specific report" payload shall be sent using authenticated and authorized SPDUs generated by ITS-S with valid certificates (ATs).

A certificate indicates its holder's permissions to send a certain set of messages and optional privileges for specific data elements within these messages. The format for the certificates is specified in ETSI TS 103 097 [3], clause 7.2.1.

Within a certificate, service permissions are indicated by a pair of parameters: the ITS-AID and the SSP. The ITS-AID of the Misbehaviour Reporting Service shall be set to the corresponding value and length, as specified in ETSI TS 102 965 [4].

The Service Specific Permissions (SSP) structure indicates specific sets of permissions within the overall permissions indicated by the ITS-AID. The originating ITS-S shall provide SSP information in its certificate for all generated signed Misbehaviour Reports as specified in clause 8.1.2.

8.1.2 Service Specific Permissions (SSP)

MRs shall be signed by the reporting ITS-S using the private key associated to the current valid Authorization.

Ticket that contains ITS-AID allocated to the Misbehaviour Reporting Service and SSPs of type BitmapSsp as specified in ETSI TS 103 097 [3].

The SSP structure for the MRS shall be of CHOICE BitmapSsp. It is defined by a variable number of octets. This octet scheme allows the SSP format to accommodate current and future versions of the present document.

In the present document, the SSP for the MRS service shall be of 2 octet length, as depicted in Figure 9.

0								1							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Octet 0								Octet 1							

Figure 9: Format of MRS SSP (BitmapSsp)

The service specific parameter bits shall be as defined in Table 4. The first octet shall reflect the version of the present document. As future versions of the present document are published, the first octet shall be incremented accordingly.

Table 4: MRS service-specific permissions

Octet number	Bit position	Permission	Bit Value
0	0 to 7	SSP version control	1
1	0 (80h)	The certificate can be used to sign MR containing an application-specific content which is identified by an ITS-AID indicating a specific ITS application	0: certificate not allowed to sign 1: certificate allowed to sign
1	1 (40h)	The certificate can be used to sign MR containing an application-agnostic content which is identified by an ITS-AID indicating an unknown ITS application.	0: certificate not allowed to sign 1: certificate allowed to sign
1	2 to 7	Reserved for future use	0

8.2 Misbehaviour Authority certificate

8.2.1 MA certificate profile

The MA certificate shall comply with the format specified in ETSI TS 103 097 [3].

8.2.2 Service Specific Permissions

The SSP structure for the MA is composed of several octets as specified in Table 5.

The first octet shall indicate the SSP version and be interpreted in the following way:

0: No version, length 1 octet; the value shall only be used for testing purposes.

1: First version, SSP contains information as defined in the present document.

2 to 255: Reserved for future usage.

This SSP structure also contains the list of ITS-AID associated to misbehaviour reports that can be reported to this MA. The reporting ITS-S shall encrypt misbehaviour reports related to a specific ITS-AID using the MA certificate which contains this specific ITS-AID in the MA SSP structure.

If the field SEQUENCE OF Psid is empty, the MA shall be allowed to handle MRs of any type, i.e. an application-specific or an application-agnostic misbehaviour issue (e.g. a cross-application or a non-specific-application misbehaviour case).

Table 5: Octet Scheme for MA SSPs

Octet #	Description	Value
0	SSP version control	1
1 ... n	SEQUENCE OF Psid	May be empty

8.3 MRS and MDM certificate permissions

The overall assignment of certificate permissions for Misbehaviour reporting and Misbehaviour Detection Management services is presented in Table 6.

Table 6: overall assignment of certificate permissions for Misbehaviour Reporting and MDM services

<table>
<tr><th rowspan="2">ITS Entity</th><th rowspan="2">Certificate</th><th colspan="2">MRS SSP</th><th colspan="2">MDM SSP</th></tr>
<tr><th>MR containing AID specific detectors (bit 0)</th><th>MR containing application agnostic detectors (bit 1)</th><th>MR collection
(SEQUENCE OF Psid)</th><th>Other services as specified in ETSI TS 102 940 [1], clause 7.6 (reserved for future use)</th></tr>
<tr><td>TLM</td><td>TLM</td><td>-</td><td>-</td><td>-</td><td></td></tr>
<tr><td>RootCA</td><td>Root</td><td>I</td><td>I</td><td>I</td><td></td></tr>
<tr><td>EA</td><td>EA</td><td>-</td><td>-</td><td>-</td><td></td></tr>
<tr><td>AA</td><td>AA</td><td>I</td><td>I</td><td>-</td><td></td></tr>
<tr><td>MA</td><td>MA</td><td></td><td></td><td>A</td><td></td></tr>
<tr><td rowspan="2">ITS-S</td><td>EC</td><td>-</td><td>-</td><td>-</td><td></td></tr>
<tr><td>AT</td><td>A</td><td>A</td><td>-</td><td></td></tr>
<tr><td colspan="6">A Certificate may contain correspondent application permission.
I Certificate may contain correspondent certificate issuing permission.
- Certificate shall not contain correspondent permission.</td></tr>
</table>

All issuing permissions, described in Table 6, shall be included in the `certIssuePermissions` field of the certificate with EndEntityType containing 'app', permitting to include these permissions into the `appPermissions` field of subordinated certificates.

Annex A (normative): ASN.1 specification of the Misbehaviour Report

A.1 Misbehaviour Report

This clause provides the normative ASN.1 modules containing the definitions of the data types specified in the present document. The ASN.1 modules shall import data types from the ASN.1 modules defined in ETSI TS 103 097 [3] and IEEE Std 1609.2™ [6]. ETSI TS 103 836-4-1 [7] and ETSI TS 103 900 [8] shall be used for the correct interpretation of the ASN.1 data structures.

A.2 Misbehaviour Report data structures

The `EtsiTs103759Core` ASN.1 module is identified by the Object Identifier{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) general(1) core(1) major-version-1(1) minor-version-1 (1)}. The module can be downloaded as a file as indicated in Table A.1. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.1: `EtsiTs103759Core` ASN.1 module information

Module name	EtsiTs103759Core
OID	{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) general(1) core(1) major-version-1(1) minor-version-1 (1)}
Link	https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/EtsiTs103759Core.asn
SHA-256 hash	d148263ad919fcf1a4d9553f3aa140cfcf42b51f4b3b89b68f713cc5b7d362e1

A.3 App-agnostic-reporting data structures

The `EtsiTs103759AsrAppAgnostic` ASN.1 module is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) aid-specific(2) appAgnostic(270549119) major-version-1(1) minor-version-0(0)}. The module can be downloaded as a file as indicated in Table A.2. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.2: `EtsiTs103759AsrAppAgnostic` ASN.1 module information

Module name	EtsiTs103759AsrAppAgnostic
OID	{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) aid-specific(2) appAgnostic(270549119) major-version-1(1) minor-version-0(0)}
Link	https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/EtsiTs103759AsrAppAgnostic.asn
SHA-256 hash	68562997dccf9ed631e086cf9876d50aa7ba76ca3b7e002202b3256e45113144

A.4 CAM-reporting data structures

The `EtsiTs103759AsrCam` ASN.1 module is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) aid-specific(2) cam(36) major-version-1(1) minor-version-1(1)}. The module can be downloaded as a file as indicated in Table A.3. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.3: `EtsiTs103759AsrCam` ASN.1 module information

Module name	EtsiTs103759AsrCam
OID	{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) aid-specific(2) cam(36) major-version-1(1) minor-version-1(1)}
Link	https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/EtsiTs103759AsrCam.asn
SHA-256 hash	bf2a98efd3129c2aa7fea06169f8c1ed72e213605c965900a9ee3a7ffd2d5703

A.5 DENM-reporting data structures

The `EtsiTs103759AsrDenm` ASN.1 module is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) aid-specific(2) denm(37) major-version-1(1) minor-version-0(0)}. The module can be downloaded as a file as indicated in Table A.4. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.4: `EtsiTs103759AsrDenm` ASN.1 module information

Module name	EtsiTs103759AsrDenm
OID	{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) aid-specific(2) denm(37) major-version-1(1) minor-version-0(0)}
Link	https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/EtsiTs103759AsrDenm.asn
SHA-256 hash	f484f4cea5ceed335b7bc4cac3ed59710673da4f4c73d396a8ccbe7255f765b0

A.5 Base types data structures

The `EtsiTs103759AsrBaseTypes` ASN.1 module is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) general(1) base-types(3) major-version-1(1) minor-version-1 (1)}. The module can be downloaded as a file as indicated in Table A.5. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.5: `EtsiTs103759BaseTypes` ASN.1 module information

Module name	EtsiTs103759BaseTypes
OID	itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) general(1) base-types(3) major-version-1(1) minor-version-1 (1)}
Link	https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/EtsiTs103759BaseTypes.asn
SHA-256 hash	f7ef854ebe5f12006d2bf485645bc931649842fd6088c804d3762e904c1f0e34

A.6 Common observations data structures

The `EtsiTs103759CommonObservations` ASN.1 module is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) general(1) common-observations(2) major-version-1(1) minor-version-1(1)}. The module can be downloaded as a file as indicated in Table A.6. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.6: `EtsiTs103759CommonObservations` ASN.1 module information

Module name	EtsiTs103759CommonObservations
OID	{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103759) general(1) common-observations(2) major-version-1(1) minor-version-1(1)}
Link	https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/EtsiTs103759CommonObservations.asn
SHA-256 hash	f7ef854ebe5f12006d2bf485645bc931649842fd6088c804d3762e904c1f0e34

A.7 BSM-reporting data structures

The `SaeJ3287AsrBsm` ASN.1 module is identified by the Object Identifier {joint-iso-itu-t (2) country (16) us (840) organization (1) sae (114566) v2x-communications (1) technical-committees (1) v2x-security (4) technical-reports (1) misbehavior-reporting (1) asn1-module (1) aid-specific(2) bsm(32) version-1 (1) version-minor-0 (0)}. The module can be downloaded as a file as indicated in Table A.7. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table A.7: `SaeJ3287AsrBsm` ASN.1 module information

Module name	SaeJ3287AsrBsm
OID	{joint-iso-itu-t (2) country (16) us (840) organization (1) sae (114566) v2x-communications (1) technical-committees (1) v2x-security (4) technical-reports (1) misbehavior-reporting (1) asn1-module (1) aid-specific(2) bsm(32) version-1 (1) version-minor-0 (0)}
Link	https://forge.etsi.org/rep/ITS/asn1/mrs_ts103759/-/blob/v2.1.1/SaeJ3287AsrBsm.asn
SHA-256 hash	f79fdada02329171d2e4af2295e3cfdfdaa0165e59e562708b2290dd36c14dc8

Annex B (informative): Misbehaviour Detection Management System: Detailed View

An example of detailed view of the functional architecture of the MDM system architecture is presented in Figure B.1.

In a misbehaviour management system, the ITS-S detects misbehaviour happening in its vicinity. At the ITS-S, misbehaviour management includes the following functional components:

- **Local Misbehaviour Reporting**, consisting of:
    - **Local Misbehaviour Detection:** the component of the ITS-S responsible for analysing incoming data and detecting any potential misbehaviour. The subject of misbehaviour may include the ego ITS-S.

NOTE: It is a good practice for the ITS-S to ensure that the outgoing messages are correct and compliant with the standard, i.e. plausible and consistent.

    - **Context Storage:** the component of the ITS-S responsible for storing context information, i.e. information that is relatively long-lived and may be relevant to more than one misbehaviour report.
    - **Misbehaviour Reporting:** The component of the ITS-S responsible for generating, storing, and transmitting reports of misbehaviour detected by the detection component.
- **Local Misbehaviour Reaction:** Responsible for any reaction to the misbehaviour that does not involve communicating a report to the Backend Misbehaviour Management System.
- **Local Misbehaviour Remediation:** Responsible for any remediatory action to the misbehaviour, e.g. a software update.

At the backend security system, this example of global misbehaviour management system architecture includes the following functional components, and may include others:

- **Misbehaviour Preprocessing** may include sub-components like the following. None of these are required for the baseline operation of the system but a full system deployment may contain any or all of them. Some of these functionalities may require a pre-existing trust relationship between the reporting ITS-S and the relevant functional entity:
    - **Value-added Aggregation:** Aggregates reports based on certain parameters/features.
    - **Diagnostic on Reporter:** Performs diagnostics on the reporter to establish the reliability of information in its reports.
    - **Shuffling without Inspection:** Shuffles reports from multiple reporters to improve reporter's privacy.
    - **Context Storage:** Stores context information so that reporters can refer to it rather than having to directly include it in their reports
    - **Proprietary Information Management (PIM):** Enables routing and processing of proprietary information, i.e. information that is relevant to the diagnosis of misbehaviour but should not be revealed directly to the MA.
- **Global Misbehaviour Detection:** may be considered as containing the following components, both of which (except for "Other") are necessary for baseline operation of the system:
    - **Misbehaviour Investigation:** Determines which ITS-S(s) was (or were) at fault in reported misbehaviour incidents. This may involve making queries to other parts of the system, e.g. for pseudonym linkage. Operationally, this may be a single system or may be separated into multiple subcomponents, for example for different applications or for different ITS-S types.
    - **Misbehaviour Analysis:** Determines the facts on the ground for reported misbehaviour incidents, and the severity of the misbehaviour. To analyse the reports along with the outcome of the investigation from the above sub-component. The misbehaviour analysis may be carried out before and/or after the investigation.

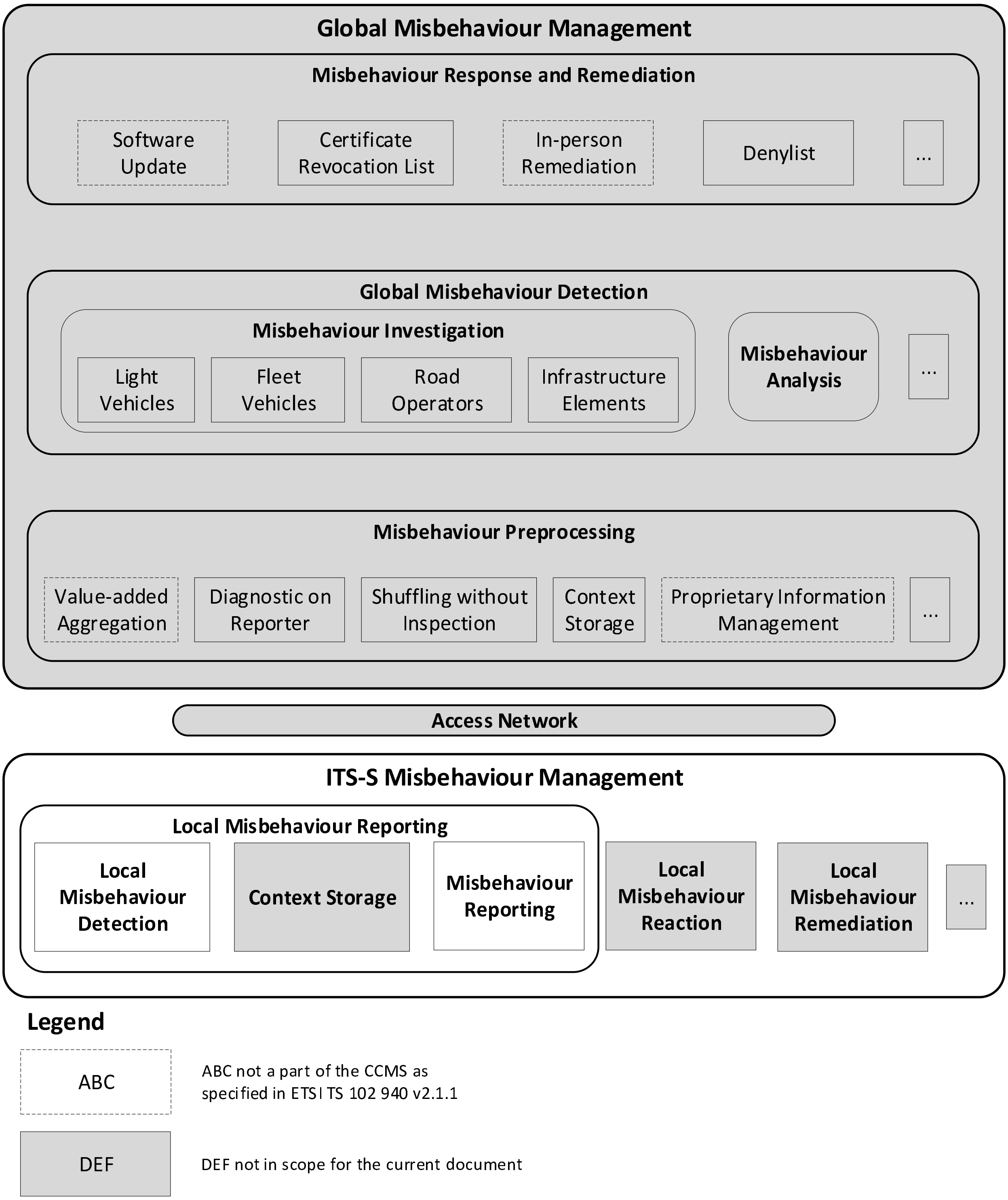


Figure B.1: Example of Misbehaviour Management System functional architecture

- **Misbehaviour Response and Remediation:** may include sub-components like the following. These sub-components may or may not be necessary for the initial operation of the system.
    - **Software Update:** Enforces software update.
    - **Certificate Revocation List (CRL):** Generates, stores, and distributes CRLs.
    - **In-Person Remediation:** Implements remediation by taking physical action at the misbehaving ITS-S's location.

- **Denylist:** Generates, stores, and distributes denylists, also called Internal BlockLists (IBL). These are distinguished from CRLs in that denylists are distributed to CAs and used to determine which ITS-S should not receive certificates, while CRLs are distributed also to ITS-S and are used to make trust decisions on incoming application messages.

- **Other:** Remediation components other than the ones above.

Annex C (informative): Local Misbehaviour Detection Service: Detailed View

An example of detailed view of the functional architecture for local MDS is presented in Figure C.1.

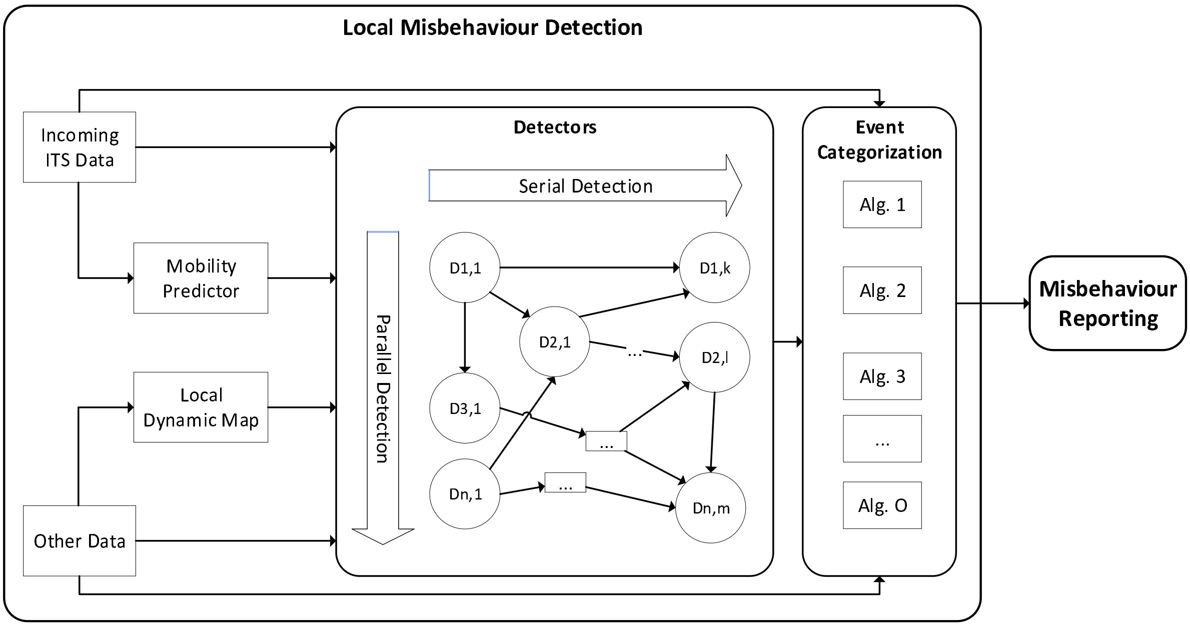


Figure C.1: Example of local Misbehaviour Detection Service functional architecture

Each component of the system is briefly described below:

- Incoming ITS data is any message coming from the communication medium, e.g. CAM and DENM.
- Other Data is any information other than the ITS data, e.g. sensor and map data.
- Mobility Predictor estimates the dynamics of vehicles in the ITS communication range prior to the reception of next incoming data.
- Local Dynamic Map (LDM) is a database managed by the ITS-S containing V2X and other data, such as the ego vehicle's position and speed.
- Detectors identify ITS data that are inconsistent with the ego vehicle's perception of ground truth or are otherwise impairing the correct operation of the system. Detectors can be connected among themselves in serial, parallel, or some combination of both, e.g. detectors D1,1 and Dn,1 may be run in parallel and then their outputs could be fed into the detector D2,1.
- An implementation may also support different kinds of internal architecture within detectors. For example, the observations defined in the present document could be implemented by a series of individual detectors that take in a limited amount of information and apply specific conditions to make a determination of misbehaviour. In the future it is possible that detectors will be implemented by an Artificial Intelligence (AI)/Machine Learning (ML) approach which will use a significantly larger input information set and be capable of outputting multiple observations.
- Event Categorization aggregates the outputs of all individual detectors along with data from other sources to determine whether an ITS message is suspicious or not.

Annex D (informative): Examples of individual detectors on CAMs and DENMs

D.1 Individual detectors for CAMs

Table D.1 lists examples of individual detectors on CAMs, and their classification according to Table 2.

Table D.1: Individual detectors for CAMs

CAM individual detectors		Class				
Group	**Detail**	**1**	**2**	**3**	**4**	**5**
General	Beacon frequency too high		X			
Reference position	Position outside of own communications coverage area	X				
	Change of position inconsistent with speed		X			
	Change of position inconsistent with heading		X			
	Position not on road			X		
	Position overlap with another object of the environment (e.g. building)			X		
	Position inconsistent with relative position (Lidar, Radar, RSSI, AoA)				X	
	Position inconsistent with maximum plausible range				X	
	Position inconsistent with claimed position of another sender					X
Heading	Change of heading inconsistent with speed		X			
	Change of heading inconsistent with yaw rate		X			
	Heading inconsistent with road heading			X		
	Heading inconsistent with relative heading				X	
Speed	Speed value too high (inconsistent with vehicle type)	X				
	Change of speed inconsistent with acceleration		X			
	Speed inconsistent with road plausible speed			X		
	Speed inconsistent with relative speed (Doppler)					
Drive direction	Drive direction inconsistent with speed (driving backwards too fast)	X				
	Drive direction inconsistent with position change and heading change		X			
	Drive direction inconsistent with road way			X		
	Drive direction inconsistent with perceived direction				X	
Vehicle length/width	Length / width change		X			
	Vehicle length / width inconsistent with perceived dimensions				X	
Longitudinal acceleration	Acceleration value too high (inconsistent with vehicle type)	X				
	Change of acceleration too large (inconsistent with vehicle type)		X			
	Acceleration inconsistent with relative acceleration				X	
Curvature	Curve radius too small (inconsistent with vehicle type)	X				
	Change of curvature inconsistent with speed		X			
	Change of curvature inconsistent with heading change		X			
	Change of curvature inconsistent with yaw rate		X			
	Change of curvature inconsistent with road shape			X		
	Change of curvature inconsistent with relative curvature				X	
Yaw rate	Yaw rate value too high	X				
	Change of yaw rate inconsistent with speed		X			
	Change of yaw rate inconsistent with curvature		X			
	Yaw rate inconsistent with perceived yaw rate				X	

D.2 Individual detectors for DENMs

D.2.1 Taxonomy of local misbehaviour detection strategies for DENMs

ETSI TR 103 460 [i.3] presents the state-of-the-art of misbehaviour detection techniques for the DEN basic service specified in ETSI TS 103 831 [i.7]. A classification of the different categories for the DENM misbehaviour detection schemes is given in Figure D.1.

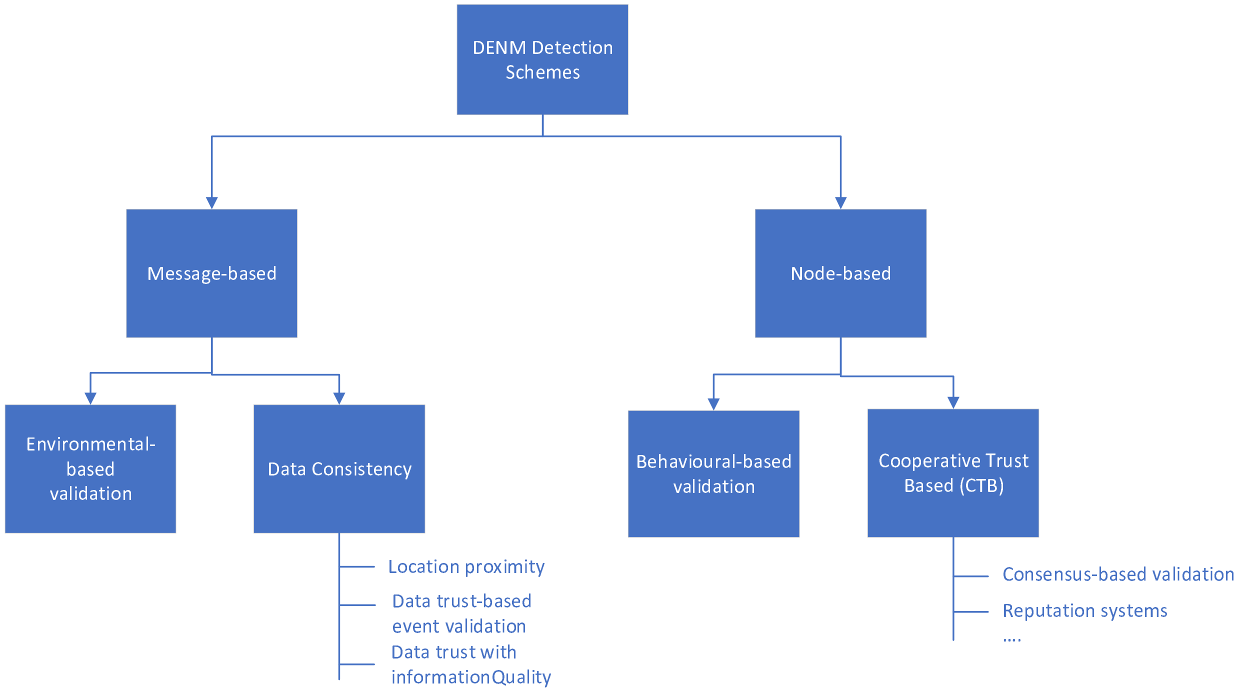


Figure D.1: Taxonomy of local misbehaviour detection on DENMs

Examples of individual detectors on DENMs using this taxonomy are detailed in clause D.2.2.

Environmental-based validation:

This category of local MD 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.

For instance, in the use case Adverse weather condition warning, a warning for an adverse weather could be verified using predicted local weather information and another check could use statistics information collected by national meteorological services. In the use case Traffic jam warning, the event report with causeCode "traffic conditions" is very unlikely for a road in a normal context between midnight and 6 am (unlikely traffic event).

This category of mechanisms may be implemented locally in the vehicle ITS-S receiving the false traffic alerts (local detection scope). It may also be implemented by R-ITS-S or Central ITS-S when processing event reports, e.g. filtering and aggregating information received from DENMs transmitted by vehicles.

NOTE: If a set of warnings largely deviates from the normal data trends, the R-ITS-S or Central ITS-S will notify the human operator in the Traffic Control Center (TCC). Partly because the warning could be erroneous, and partly because the warning could be due to a change in the local environment that could require servicing.

Other plausibility checks on the sending ITS-S may also be specified (e.g. a vehicle sending a DENM which reports an approaching emergency vehicle normally has the *stationType* value in the DENM equal to *specialVehicle*).

Data Consistency:

This category gathers detection mechanisms that are searching for contradiction in data using redundancy of information. These mechanisms usually look at several messages generated by the same ITS-S or are collecting and trying to resolve conflicting information coming from several ITS-Ss, e.g. collecting the validation of several ITS-Ss on the reported traffic event. This category includes at least (but is not limited to) the following misbehaviour reporting schemes as shown in Figure D.1:

- 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 sending 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-based event validation: these mechanisms allow vehicle ITS-Ss to agree cryptographically on the reported event to guarantee its validity. The trustworthiness of traffic event data is therefore evaluated based on the data received and collected from multiple ITS-Ss (e.g. vehicles, RSUs). Such detection schemes perform cooperatively (or may use a centralized approach via communication with a Back-end server). In ETSI TR 103 460 [i.3], clause 5.1.3, different data trust mechanisms are presented based on Growth-code and z-smallest signature.

  Currently all the specified detection techniques in this category impact the network delay (many communication rounds are needed before the event is considered as correct) and they are not compatible with the standard DENM protocol (ETSI TS 103 831 [i.7]).

- Data trust combined with traffic data quality: as in the previous detection schemes, 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.

In T-VNets [i.8], the paper proposes a trust architecture using a method to build trust based on standardized ITS messaging services such as CAM, DENM etc. and it defines a combination of different mechanisms: data-centric, event-based, watchdog, RSU-based trust.

Data-centric mechanisms evaluate the quality of received messages. Event-based mechanisms evaluate the effectiveness of issued warning events. Watchdog is a mechanism where vehicles continuously analyses the sending frequency of its nearby stations to evaluate their cooperation in the short-range ad-hoc network.
All vehicle stations share positive or negative recommendations on their neighbours with the infrastructure nodes (RSUs). Finally, RSUs broadcast a trust value for vehicles based on current and historical behaviours evaluations. All these mechanisms are then combined to compute a global trust evaluation for every neighbour.
The paper T-VNets [i.8] defines a trust evaluation method including a data-centric trust metrics related to the received beacon messages' quality ("Direct TRust") and to the received event reports' effectiveness ("Event TRust") and other trust metrics which are combined to build a global trust evaluation for entities ("Global TRust"). The trust level may be shared between nodes using "Cooperative Awareness Messages" (CAMs) with a specific additional container (in a further extended version of CAM standard), and regularly updated.

For the data-centric trust evaluation based on CAM and DENM message analysis, the following trust parameters are defined in Table D.2.

Table D.2: Example of trust parameters

Trust parameter	Definition
Qmsg(i, j)	quality of messages (data centric evaluation by a node i about messages sent by node j during a period of time)
WDR(i, j)	Watchdog report given by i to j
DTR(i, j)	Direct interactions' TRust given by i to j
GTR (i, j)	Global TRust evaluation given by entity i to j. This is the combination of all used metrics
ETR (E, j)	TRust of the Event E reported by j
ρ	Message credibility factor (0,7< ρ <1)
δ	Trust increment factor
μ	Trust decrement factor

For all the trust metrics in this table, the initial value of trust assigned by a node i to a node j is equal to 0,5 and the value can vary from 0 to 1 depending on the behaviour of node j (according to some equations which are detailed in [i.8]).

DTR(i,j) is the direct interactions trust value computed using the analysis and validation of periodic beacon messages (CAMs) received from node j. The exchanged messages quality for a direct interaction from node j to i can be computed based on the analysis and validation of received messages from node j, e.g. taking into account the number of suspicious messages and the number of valid, legitimate messages received from node j.

The event's trust, ETR(E,j) is a value computed by node i for a specific event E on each traffic event by its neighbouring node j which is signaling the same event E as indicated by the *eventType* and identified by the same identifier (*actionId*). This value will be computed using the originator global trust (GTR) and the event credibility through the received information quality of the reported traffic event (*informationQuality* of the DENM Situation container) applying the following equation:

$$ETR(E,j) := \frac{\rho.InformationQuality(E)}{MaxRangeValue(E)} + (1 - \rho).GTR(i,j)$$

By setting AVGq(E) = $\frac{InformationQuality(E)}{MaxRangeValue(E)}$ the equation becomes:

$$ETR(E,j) := \rho.AVGq(E) + (1 - \rho).GTR(i,j)$$

Then, if the event's trust is higher than a predefined threshold (TrustTreshold), a validity test is done on the DENM and the qualityQmsg(i,j) parameter will be computed as follows: If the validity test is passed, the station i increases its message quality Qmsg(i,j), decreasing it otherwise since this communication is considered as a direct interaction.

If (*ETR(E, j)* ≥ TrustThreshold) then

Qmsg(i,j) = *Qmsg(i,j)* + δ;

else

Qmsg(i,j) = Qmsg(i,j) - μ;

δ and μ are the trust increment and decrement factors and these factors should be set to values such as $\delta \ll \mu$ since the trust between two stations is more difficult to build up and easier to tear down. These values may be fixed after intensive real-life experimentations.

Behavioural-based validation:

These detection mechanisms are based on the fact that a Vehicle ITS-S signaling 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 the message plausibility. E.g. a vehicle issuing an adverse weather warning needs to be on proximity of the event (Location proximity detector) and should decrease its speed accordingly. Other examples are given in ETSI TR 103 460 [i.3], clause 6.4.

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. Different trust-based mechanisms are listed in ETSI TR 103 460 [i.3], clause 5.1.4 and are depicted in Figure D.1. ETSI TR 103 460 [i.3] includes different categories such as cooperative trust-based e.g. voting and consensus mechanisms allowing the entities to cooperatively evaluate the behaviour of an ITS-S and reputation systems. Trust-based detection can occur either locally with cooperation between the neighbours ITS-Ss (cooperative detection scope) or with the support of the infrastructure (global detection scope). These mechanisms often rely on the combination of various data-centric misbehaviour detection techniques to update the trust of nodes in the C-ITS network. For instance, many proposed schemes may also use the support of RSUs or of back-end servers.

The list of Day1 Use Cases is presented in Table D.3. These use cases are listed in the C-ITS Delegated Act, Annex 1 [i.9].

Table D.3: List of Day1 use cases

Service category	Service	eventType (causeCode, subCauseCode)
Vehicle-to-vehicle services		
Traffic jam	Dangerous end of queue	dangerousEndOfQueue, unavailable
Traffic jam	Traffic jam ahead	trafficCondition, unavailable
Stationary vehicle warning	Stopped vehicle	stationaryVehicle, unavailable
Stationary vehicle warning	Broken-down vehicle	stationaryVehicle, vehicleBreakdown
Stationary vehicle warning	Post-crash	stationaryVehicle, postCrash
Special vehicle warning	Emergency vehicle in operation	emergencyVehicleApproaching
Special vehicle warning	Stationary safeguarding emergency vehicle	emergencyVehicleApproaching
Special vehicle warning	Stationary recovery service warning	emergencyVehicleApproaching
Exchange of IRCs	Request IRC	collisionRisk, unavailable
Exchange of IRCs	Response IRC	collisionRisk, unavailable
Dangerous situation	Electronic emergency brake light	dangerousSituation, emergencyElectronicBrakeEngaged
Dangerous situation	Automatic brake intervention	dangerousSituation, aebEngaged
Dangerous situation	Reversible occupant restraint system intervention	dangerousSituation, preCrashSystemEngaged
Adverse weather conditions	Fog	adverseWeatherCondition-Visibility, unavailable or fog
Adverse weather conditions	Precipitation	adverseWeatherCondition-Precipitation, unavailable, heavyRain or heavySnowfall
Adverse weather conditions	Traction loss	adverseWeatherCondition-Adhesion, unavailable
Infrastructure-to-vehicle services		
Hazardous locations notification	Accident zone	accident, subCauseCode to be set between 0 and 7 (except 6)
Hazardous locations notification	Traffic jam ahead	dangerous end of queue, unavailable
Hazardous locations notification	Stationary vehicle	stationary vehicle, unavailable or breakdown vehicle
Hazardous locations notification	Weather condition warning	extreme weather condition or precipitation
Hazardous locations notification	Temporarily slippery road	adhesion , subcause to be set between 0 and 9
Hazardous locations notification	Animal or person on the road	animal on the road or human presence on the road
Hazardous locations notification	Obstacle on the road	obstacle on the road, subcause to be set between 0 and 5
Road works warning	Lane closure (and other restrictions)	roadworks, subcause to be set between 0 or 4
Road works warning	Road closure	roadworks, subcause set to 1
Road works warning	Road works — mobile	roadworks, subcause set to 3

D.2.2 Individual detectors for DENMs

Table D.4 lists examples of individual detectors on DENMs, and their classification according to Table 2. In the presentation individual detectors are grouped by use case (first column and second column defined in Table D.3).

Table D.4: Individual detectors for DENMs

DENM individual detectors		Class				
Group	**Detail**	**1**	**2**	**3**	**4**	**5**
General	Distance from the DENM-originating ITS-S ReferencePosition in CAM and the reported event position, at the time of detection, is too high.					X
	Each neighbour is monitored to check that it actually forwards the DENMs it is supposed to forward (watchdog). To account for packet loss or collisions in wireless medium, the required number of re-braodcasts is lowered by a given threshold. As finding a global threshold for multi-hops messages is generally difficult, this threshold need to be set dynamically. NOTE 1: This detector is generally better performed in the GeoNetworking layer as a measure for routing misbehaviour detection based on the ITS-S's Neighbour Table (see ETSI TR 102 893 [i.5]).			X		
	If one of the trust parameters' value calculated for the duration of the ITS short-range communication link between the DENM-receiving ITS-S and the DENM-originating ITS-S (identified by the same ITS-S ID) is below a specified threshold. The values of the trust vector, composed of e.g. Qmsg(i, j), DTR(i,j), ETR(E,j) are to be reported. NOTE 2: This threshold is not specified in this version of the present document.					X
Traffic jam, Dangerous end of queue	roadType indicated in the Location Container is not equal to 'non-urban' road type (i.e. is not set to value 2 or 3).	X				
	The event points in traces (eventHistory) indicated in the last received DENM are not containing the same eventPositions as in the previous DENMs.		X			
	Inconsistency with predicted traffic jam information using a live traffic application.			X		
	Unlikely traffic event based on statistics.			X		
	Unlikely traffic event due to current traffic flow (density, speed of vehicles). NOTE 3: This can be assessed either thanks to sensor data or thanks to other incoming ITS messages.				X	X
	The vehicle speed indicated in the CAMs transmitted after the event was detected by the same ITS-S at the origin of the DENM is higher than 30 km/h (within the period of 20 s after the event detection).					X
	Speed of nearby vehicles located upstream the DENM-originating ITS-S, in the same lane position and within 100 m, is higher than 7 km/h.					X
	Inconsistency with predicted path of other vehicles in the same traffic lane (lanePosition) and within 100 m and with the same driving direction.					X
Traffic jam, Traffic jam ahead	roadType indicated in the Location Container is not equal to 'non-urban' road type (i.e. is not set to value 2 or 3).	X				
	The event points in traces (eventHistory) indicated in the last received DENM are not containing the same eventPositions as in the previous DENMs.		X			
	Inconsistency with predicted traffic jam information using a live traffic application.			X		
	Unlikely traffic event based on statistics.			X		
	Unlikely traffic event due to current traffic flow (density, speed of vehicles). NOTE 4: This can be assessed either thanks to sensor data or thanks to other incoming ITS messages.				X	X
	Behaviour check on speed in CAMs sent by the same V-ITS-S (same ITS-ID) failed.					X
	Speed of surrounding vehicles of the DENM-originating ITS-S, within 100 m and with the same driving direction, in the LDM is exceeding a threshold (e.g. more than 80 km/h).			X		
	Speed indicated in CAMs transmitted by surrounding vehicles of the DENM-originating ITS-S, within 100 m and with the same driving direction, is exceeding a threshold (e.g. more than 80 km/h).					X
Stationary vehicle warning, Stopped vehicle	Speed in CAMs of stationary vehicle not equal to 0.					X
	eventPosition in DENM is not plausible using the on-board map.			X		
	eventPosition in the received DENM from an originating ITS-S of StationType equal to bus or tram does not match with a bus or tram stop using a local map information.			X		

DENM individual detectors		Class				
Group	**Detail**	**1**	**2**	**3**	**4**	**5**
Stationary vehicle warning, breakdown and post-crash	Speed in CAMs of stationary vehicle not equal to 0.					X
	Behavioural check on speed in CAMs of other vehicles failed.					X
	Behavioural check on heading of other vehicles in CAMs failed.					X
	Behavioural check on pathHistory in CAMs of other vehicles failed.					X
Special vehicle warning, Emergency vehicle in operation	Change of curvature inconsistent with heading change.		X			
	Change of curvature inconsistent with yaw rate.		X			
	stationType in DENM of the sending V-ITS-S is not equal to specialVehicles (10).	X				
	stationType in CAMs of the same sending V-ITS-S (same ITS-ID) is not equal to specialVehicles (10).					X
	lightBarActivated is not equal to 1 in the EmergencyContainer of CAMs of the same sending V-ITS-S (same ITS-ID).					X
	The event points in traces (eventHistory) indicated in the last received DENM are not containing the same eventPositions as in the previous DENMs.		X			
	Behaviour check on speed in CAMs of other vehicles failed.					X
	Behaviour check on heading of other vehicles in CAMs failed.					X
	Behavioural check on pathHistory in CAMs of other vehicles failed.					X
Exchange of IRCs (pre-crash information)	Plausibility check on vehicleMass in impactReduction container failed (threshold depends on stationType).	X				
	Speed of the sending V-ITS-S (eventSpeed in DENM) is equal to CAM Speed sent by the same V-ITS-S (same ITS-ID) at the same time.					X
	Heading of the sending V-ITS-S (eventPositionHeading in DENM) is equal to CAM Heading sent by the same V-ITS-S (same ITS-ID) at the same time.					X
	Behaviour check on longitudinalAccelerationValue in CAMs failed.					X
	Behavioural check on pathHistory in CAMs failed.					X
Dangerous situation	Speed value in CAM of the vehicle sending this event not equal to 0.					X
	Behaviour check on speed in CAMs of other vehicles failed.					X
	Behaviour check on heading of other vehicles in CAMs failed.					X
	Behavioural check on pathHistory in CAMs of other vehicles failed.					X
Adverse weather conditions	Inconsistency with predicted weather information.			X		
	Unlikely traffic event (statistics).			X		
	Behaviour check on speed in CAMs failed.					X
	Behavioural check on pathHistory in CAMs failed.					X
	Inconsistency with predicted path of other vehicles in the upstream or downstream driving direction within 1 000 m. NOTE 5: This can be assessed either thanks to sensor data or thanks to other incoming ITS messages.				X	X

History

Document history		
V2.1.1	January 2023	Publication