



|                                     |               |                |
|-------------------------------------|---------------|----------------|
| <b>SURFACE VEHICLE<br/>STANDARD</b> | <b>J3287™</b> | <b>AUG2024</b> |
|                                     | Issued        | 2024-08        |
| V2X Misbehavior Reporting           |               |                |

RATIONALE

Misbehavior reporting is a key service to maintain robustness of the V2X system. It requires standardization because devices from multiple implementers will produce reports and submit them to one or more misbehavior authorities which are operated independently from the reporters, meaning that an interface standard is necessary to ensure interoperability and consistency between reports.

TABLE OF CONTENTS

|       |                                                             |    |
|-------|-------------------------------------------------------------|----|
| 1.    | SCOPE .....                                                 | 3  |
| 2.    | REFERENCES .....                                            | 3  |
| 2.1   | Applicable Documents .....                                  | 3  |
| 2.1.1 | SAE Publications .....                                      | 3  |
| 2.1.2 | ETSI Publications .....                                     | 3  |
| 2.1.3 | IEEE Publications .....                                     | 3  |
| 2.1.4 | IETF Publications .....                                     | 3  |
| 2.1.5 | ITU-T Publications .....                                    | 3  |
| 2.2   | Related Publications .....                                  | 4  |
| 2.2.1 | ETSI Publications .....                                     | 4  |
| 2.2.2 | IETF Publications .....                                     | 4  |
| 2.2.3 | ISO Publications .....                                      | 4  |
| 3.    | DEFINITIONS .....                                           | 4  |
| 4.    | ABBREVIATIONS .....                                         | 5  |
| 5.    | INTRODUCTION .....                                          | 6  |
| 5.1   | General .....                                               | 6  |
| 5.2   | ITSO Misbehavior Management .....                           | 11 |
| 5.2.1 | Local Misbehavior Detection .....                           | 11 |
| 5.2.2 | Local Misbehavior Report Management .....                   | 12 |
| 5.3   | Misbehavior Report Transmission .....                       | 14 |
| 6.    | MISBEHAVIOR REPORT FORMAT .....                             | 14 |
| 6.1   | General .....                                               | 14 |
| 6.2   | ASN.1 Structures Imported from ETSI TS 103 759 v2.1.1 ..... | 14 |
| 6.3   | Misbehavior Report Upload Use Cases .....                   | 15 |
| 6.4   | Security Encapsulation .....                                | 16 |

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2024 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)  
Tel: +1 724-776-4970 (outside USA)  
Fax: 724-776-0790  
Email: CustomerService@sae.org  
SAE WEB ADDRESS: http://www.sae.org

For more information on this standard, visit  
[https://www.sae.org/standards/content/J3287\\_202408](https://www.sae.org/standards/content/J3287_202408)

Documents

SAE International

SAE J3287\_202408

|          |                                                      |    |
|----------|------------------------------------------------------|----|
| 6.5      | Misbehavior Observations for BSM .....               | 17 |
| 6.5.1    | General.....                                         | 17 |
| 6.5.2    | Target Class: Security.....                          | 17 |
| 6.5.3    | Target Class: Longitudinal Acceleration .....        | 18 |
| 7.       | MISBEHAVIOR REPORT UPLOAD .....                      | 18 |
| 7.1      | General.....                                         | 18 |
| 7.2      | Plaintext .....                                      | 19 |
| 7.3      | Signed .....                                         | 19 |
| 7.4      | Signed Then Encrypted.....                           | 19 |
| 8.       | ASN.1 MODULES .....                                  | 20 |
| 8.1      | SaeJ3287 .....                                       | 20 |
| 8.1.1    | OID .....                                            | 20 |
| 8.1.2    | Imports .....                                        | 20 |
| 8.1.3    | Data Elements.....                                   | 20 |
| 8.2      | SaeJ3287AsrBsm .....                                 | 21 |
| 8.2.1    | OID .....                                            | 21 |
| 8.2.2    | Imports .....                                        | 21 |
| 8.2.3    | Data Elements.....                                   | 22 |
| 9.       | NOTES .....                                          | 23 |
| 9.1      | Revision Indicator.....                              | 23 |
| Figure 1 | Misbehavior management functional architecture ..... | 9  |
| Figure 2 | Misbehavior management lifecycle.....                | 10 |
| Figure 3 | Local misbehavior detection – simplified .....       | 11 |
| Figure 4 | Local misbehavior detection – detailed.....          | 12 |
| Figure 5 | Local misbehavior report management.....             | 13 |
| Figure 6 | Misbehavior report upload architecture.....          | 14 |
| Figure 7 | ASN.1 structure EtsiTs103759Mbr .....                | 15 |
| Table 1  | Plaintext MBR upload.....                            | 19 |
| Table 2  | Signed MBR upload .....                              | 19 |
| Table 3  | Signed-then-encrypted MBR upload.....                | 19 |

## 1. SCOPE

This standard provides a specification of a general misbehavior report format suitable for reporting misbehavior observed by a system running SAE V2X applications, and specific report contents for specific instances of misbehavior. It also provides an overview of the architecture of a system-wide misbehavior management service for the V2X system and positions the misbehavior reporting services within that architecture.

## 2. REFERENCES

### 2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

#### 2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), [www.sae.org](http://www.sae.org).

|             |                                                                    |
|-------------|--------------------------------------------------------------------|
| SAE J2735   | V2X Communications Message Set Dictionary                          |
| SAE J2945/1 | On-Board System Requirements for V2V Safety Communications         |
| SAE J3161/1 | On-Board System Requirements for LTE-V2X V2V Safety Communications |

#### 2.1.2 ETSI Publications

Copies of these documents are available online at <https://www.etsi.org/>.

|                        |                                                                                          |
|------------------------|------------------------------------------------------------------------------------------|
| ETSI TS 103 759 v2.1.1 | Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2 |
|------------------------|------------------------------------------------------------------------------------------|

#### 2.1.3 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, [www.ieee.org](http://www.ieee.org).

|                    |                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|
| IEEE 1609.2-2022   | IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages |
| IEEE 1609.2.1-2022 | IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities  |

#### 2.1.4 IETF Publications

Copies of these documents are available online at <https://datatracker.ietf.org/>.

|               |                                                                    |
|---------------|--------------------------------------------------------------------|
| IETF RFC 7230 | Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing |
| IETF RFC 7231 | Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content      |

#### 2.1.5 ITU-T Publications

Copies of these documents are available online at <https://webstore.ansi.org/>.

|             |                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------|
| ITU-T X.509 | Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks |
| ITU-T X.696 | Information Technology—ASN.1 Encoding Rules: Specification of Octet Encoding Rule (OER)                            |

## 2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

For background material, the following standards or information reports are also of value.

### 2.2.1 ETSI Publications

Copies of these documents are available online at <https://www.etsi.org/>.

ETSI TR 103 460 V2.1.1 Intelligent Transport Systems (ITS); Security; Pre-standardization study on Misbehaviour Detection; Release 2

### 2.2.2 IETF Publications

Copies of these documents are available online at <https://datatracker.ietf.org/>.

IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3

IETF RFC 9325 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

### 2.2.3 ISO Publications

Copies of these documents are available online at <https://webstore.ansi.org/>.

ISO/IEC 8824-1:1998 Information Technology - Abstract Syntax Notation One (ASN.1): Specification of Basic Notation

ISO/IEC 8824-2:1998 Information Technology - Abstract Syntax Notation One (ASN.1): Information Object Specification

ISO/IEC 8824-3:1998 Information Technology - Abstract Syntax Notation One (ASN.1): Constraint Specification

## 3. DEFINITIONS

For the purposes of this standard, the following definitions shall apply.

### 3.1 ITS OBJECT

An intelligent transport systems (ITS) object (ITSO) (e.g., a roadside unit [RSU], an onboard unit [OBU], etc.) is a computing/communication system that creates/sends/receives V2X messages (conformant or not to the relevant message specification).

Note that this definition doesn't capture the case of a device that generates random noise on the communication medium. Nonetheless, this term is preferred over generic terms like object, device, etc., to emphasize the fact that this standard is talking about misbehavior in the context of V2X communications and not misbehavior in general, e.g., someone going over the posted speed limit.

### 3.2 MISBEHAVIOR

Misbehavior within the V2X system refers to behavior that impedes an ITSO's ability to obtain an accurate understanding of the ground truth or other actionable information.

### 3.3 MISBEHAVIOR MANAGEMENT

Misbehavior management refers to the entire lifecycle of misbehavior, which includes local misbehavior management on an ITSO, misbehavior report transmission from an ITSO to the backend, and then misbehavior management at the backend.

## 4. ABBREVIATIONS

The terms, abbreviations, and acronyms cited below shall be a part of the terms of this standard (and of the other companion volumes and guides), unless specifically cited otherwise.

|        |                                                  |
|--------|--------------------------------------------------|
| AID    | application identifier                           |
| API    | application programming interface                |
| BSM    | basic safety message                             |
| CA     | certificate authority                            |
| CAM    | cooperative awareness message                    |
| C-OER  | canonical octet encoding rules                   |
| CRL    | certificate revocation list                      |
| DENM   | decentralized environmental notification message |
| DoS    | denial of service                                |
| IOC    | information object classes                       |
| IOS    | information object sets                          |
| ITS    | intelligent transport systems                    |
| ITSO   | ITS object                                       |
| LA     | linkage authority                                |
| LDM    | local dynamic map                                |
| MA     | misbehavior authority                            |
| MUR    | misbehavior report upload receiver               |
| PDU    | protocol data unit                               |
| PSID   | provider service identifier                      |
| RA     | registration authority                           |
| TCP/IP | transmission control protocol/internet protocol  |
| TLS    | transport layer security                         |
| URL    | uniform resource locator                         |

|     |                           |
|-----|---------------------------|
| V2I | vehicle-to-infrastructure |
| V2P | vehicle-to-pedestrian     |
| V2V | vehicle-to-vehicle        |
| V2X | vehicle-to-everything     |

## 5. INTRODUCTION

### 5.1 General

An intelligent transport systems (ITS) object (ITSO) (e.g., a roadside unit [RSU], an onboard unit [OBU], etc.) is a computing/communication system that creates/sends/receives V2X messages (conformant or not to the relevant message specification). For purposes of this standard, misbehavior refers to behavior by one ITSO that impacts another ITSO's ability to obtain an accurate understanding of the ground truth in its vicinity. This includes willful or inadvertent transmission of bad data, meaning data that can result in bad driving or information outcomes if it is believed to be true by a receiver. It also covers behavior such as channel jamming and other Denial of Service (DoS) attacks, and attempts by senders to execute commands or have requests responded to where the sender is not entitled to that response by the receiver. Examples include:

- A vehicle sending incorrect data (position, speed, acceleration, etc.) that results in a receiving vehicle miscalculating the kinematics of the sender and, hence, either raising a false alert to its driver or, worse, causing a safety incident.
- A regular passenger vehicle pretending to be an emergency response vehicle and sending a signal preemption request to a traffic signal.
- A transmission device creating ghost vehicles by sending properly generated V2X messages.

There can be many types of misbehavior targeting different parts/aspects of the V2X ecosystem. The primary focus of this standard is misbehaviors that involve ITSOs as the sender and/or receiver of misbehaving messages. Here and throughout this standard, V2X misbehavior refers to only those misbehavior in the V2X ecosystem that involve ITSOs.

It is important to detect and manage misbehaviors in a timely manner because a persistent and/or widespread misbehavior can negatively impact the potential benefits of V2X communications, thereby discouraging honest users from participating in the system because it gives them false warnings or bad outcomes. All these, in turn, have the potential to slow down V2X deployment. Therefore, it has long been accepted that a full deployment plan for a V2X ecosystem will include mechanisms to allow ITSOs to report misbehavior that they observe to some authority that has the ability to take action to remediate the effects of the misbehavior, for example, to include the misbehaving sender's certificate on a Certificate Revocation List (CRL) as defined in IEEE 1609.2-2022.

There are many steps involved in the management of V2X misbehavior (see below for details); the focus of this standard is around reporting of misbehavior by an ITSO to the backend system so that the backend can take next steps as appropriate/necessary. This standard specifies a framework for misbehavior reporting by the observers of that misbehavior and also specifies some initial report contents or observations that can be reported. The framework provides a format for the contents of the misbehavior report; a specification of options for applying application-layer security to the misbehavior report using the mechanisms of IEEE 1609.2-2022; and an upload protocol to a Misbehavior Report Upload Receiver (MUR), which is the gateway to backend processing of the report, ultimately leading to remediation. The entity responsible for the overall management of misbehavior in the backend, including collecting misbehavior reports, analyzing them for cause/source of misbehavior, and deciding whether/which remediation actions to take, is the misbehavior authority (MA).

Note that remediation will be applied if a misbehaving sender's pattern of misbehavior warrants such remediation – the mere upload of a single report does not automatically lead to remediation. Note also that remediation approaches other than CRL are possible, and in the case of DoS attacks, other remediation approaches are necessary. The determination of when to apply a remediation mechanism and what mechanism to use is out of scope of this standard.

[Figure 1](#) gives a functional architecture for the misbehavior management system. In the figure, only the misbehavior report management components in the ITSO and the backend are in scope of this standard.

The ITS0 has the following functional components:

- Local misbehavior detection, which analyzes incoming V2X messages and identifies if they are misbehaving or potentially misbehaving.
- Context storage, which stores context information that may be of use in more than one misbehavior report.
- Local misbehavior report management, which generates, stores, and transmits misbehavior reports.
- Local misbehavior reaction, which is responsible for any reaction to the misbehavior that does not involve communicating a report to the backend system. For example, this is the functional entity that might decide to suppress a driver warning that would otherwise have been generated, or to inform the driver that DoS appears to be happening and the V2X system should not be relied on as much as usual.
- Local misbehavior remediation, which is responsible for implementing remediations on the ITS0 if such are identified as necessary, for example, installing a software update or informing the driver that the system is considered to have a hardware key compromise and must be brought in for service in order to continue operating.

The backend has the following functional components, each of which can contain subcomponents and may contain other functional components or subcomponents. Note that subcomponents in a functional component are included in that functional component because they play roles in particular stages of misbehavior processing; there is not intended to be an implication that all subcomponents in a functional component are, for example, operated by the same organization. The functional components are:

- Backend misbehavior report management: This covers all operations on the misbehavior reports that are carried out before the information in the reports is passed to the backend misbehavior detection functional component. The operations can be to improve the quality of the reports, to protect the privacy of the reporters, to manage the volume of data received by the backend misbehavior detection functional component, or any other appropriate operation type. Subcomponents identified for inclusion in this functional component include:
  - Value-added aggregation: Aggregate reports based on certain properties, for example, can inform the backend misbehavior detection that a particular misbehavior was observed by ten different reporters and forward only a single instance of the report (plus the certificates of all the reporters to check for duplicate senders).
  - Diagnostic on reporter: Runs or reviews diagnostics on a reporter to determine if a reported misbehavior was in fact due to a miscalibration or other issue on the reporting device, and suppresses the misbehavior report if it does not reflect actual misbehavior.
  - Shuffling without inspection: Combines reports from multiple reporters in a random order to prevent reports uploaded at the same time from arriving at the backend misbehavior detection functional component at the same time, making it harder for the backend misbehavior detection functional component to determine that multiple reports signed with different certificates have come from the same reporter.
  - Context storage: Stores context information, i.e., background information, that can be useful in processing misbehavior reports so that reporters can refer to it rather than having to directly include it in their reports.
  - Proprietary information management: Allows reporters to include proprietary information in their reports which is then “sanitized” by this functional entity so that it is not revealed directly to the MA, but can be used by this functional entity (which could be a device manager) to obtain diagnostic information about the system.