INTERNATIONAL STANDARD

**ISO 16461**

First edition
2018-08

# Intelligent transport systems — Criteria for privacy and integrity protection in probe vehicle information systems

*Systèmes intelligents de transport — Critères de confidentialité et de protection d'intégrité*



Reference number
ISO 16461:2018(E)



ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.



This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.



# Introduction

More and more attention has been paid to safety, comfort, mitigation of impact on the environment, and energy efficiency in transport systems. The use of probe data specified in ISO 22837:2009 is considered to be a key factor of a solution for the above issues. Usage of probe data in probe vehicle systems (PVS), defined in ISO 22837:2009, may be subject to privacy regulations. Consequently, there is a need for protective measures and policies in PVS.

It is necessary to develop a basic concept for protecting privacy and integrity being gathered in the PVS so that transmission of probe data can be done without violating the privacy regulations. This document defines criteria for protection of the anonymity and integrity of probe data.

The following topics are addressed in this document:

— definition of security and privacy requirements for probe vehicle systems;

— specification of a common interface ensuring privacy and integrity in probe vehicle information acquisition;

— definition of a scheme for protecting probe vehicle systems in terms of integrity and privacy.

# Intelligent transport systems — Criteria for privacy and integrity protection in probe vehicle information systems

## 1 Scope

This document specifies the basic rules to be considered by service providers handling privacy in probe vehicle information services. This document is aimed at protecting the privacy as well as the intrinsic rights and interests of the probe data subjects specified in ISO 24100:2010.

This document specifies the following items related to probe vehicle systems (PVS), i.e. systems collecting probe data from private vehicles and processing these probe data statistically towards useful information that can be provided to various end users:

— architecture of the PVS in support of appropriate protection of data integrity and anonymity in the PVS;

— security criteria and requirements for the PVS, specifically requirements for data integrity protection and privacy;

— requirements for correct and anonymous generation and handling of probe data.



## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.



ISO 22837:2009, *Vehicle probe data for wide area communications*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22837:2009 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

**3.1**
**authentication**
proving or showing to be true, genuine, or valid

**3.2**
**probe data**
vehicle sensor information, formatted as probe data elements and/or probe messages, that is processed, formatted, and transmitted to a land-based centre for processing to create a good understanding of the driving environment

[SOURCE: ISO 22837:2009, 4.3]

**3.3**
**probe data collector**
function that receives probe messages from vehicles and creates probe information by fusing and analysing probe messages and supplementary data from other data sources

**3.4**
**probe data element**
data item included in a probe message

[SOURCE: ISO 22837:2009, 4.4]

**3.5**
**probe data retention**
function which receives and stores probe data after they were processed by the raw sensor data processing

**3.6**
**probe information**
information extracted from probe messages and data from other sources through the probe information creation function

**3.7**
**probe information application/service**
entity that acts upon the received probe information and supplementary information into data input or other action commands into the probe application or service



**3.8**
**probe information creation**
function which creates probe information from the probe data stored in processed probe message retention according to a set of predefined rules and formats



**3.9**
**probe information processing**
function which receives probe information from the transmit probe information reception function, and converts the received information into suitable formats for various probe information applications/services, and then sends them to a processed probe information retention function for further processing

**3.10**
**probe information receiver**
function which receives the probe information transmitted from a probe message collector and provides probe information application/services

**3.11**
**probe message**
structured collation of data elements suitable for being delivered to the on-board communication device for transmission to a land-based centre

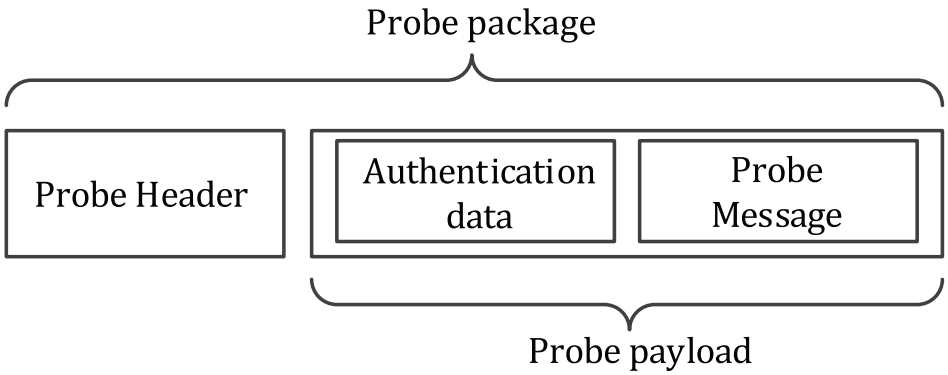
[SOURCE: ISO 22837:2009, 4.6, modified — “to be” was changed to "for being" and the NOTE was deleted.]

**3.12**
**probe message creation**
function which creates a probe message from probe data stored in probe data retention

**3.13**
**probe message processing**
function which receives probe messages from probe package reception and processes them so that they are suitable to combine other data from various sources

**3.14**
**probe package creation**
function which arranges the probe data into packages (i.e. probe packages) for transferring to probe data collector

Note 1 to entry: The following Figure illustrates a model for probe package (defined in ISO 24100:2010)




**3.15**
**probe package reception**
function which receives the probe packages transmitted by the probe package creation, extracts the probe payload by excluding the probe header information and sends the probe payload to the probe message processing



**3.16**
**probe package transfer**
function which transfers probe packages between a vehicle and a probe data collector through a predefined communication channel



**3.17**
**probe PDU creation**
function which converts probe information into protocol data unit (PDU) format, including header and payload, and is ready to be transmitted by probe information transfer function (undefined)

Note 1 to entry: Note to entry: A protocol data unit (PDU) is information that is transmitted as a single unit among peer entities of a communication network.

**3.18**
**probe PDU reception**
function which receives the probe PDUs transmitted from transmit probe information creation, extracts the probe information, and sends it to the probe information processing

**3.19**
**probe PDU transfer**
function which transfers probe PDU packets between a probe data collector and a probe information receiver

**3.20**
**probe vehicle system**
**PVS**
system consisting of vehicles, which collects and transmits probe data, and land-based centres, which collate and process data from many vehicles to build an accurate understanding of the overall roadway and driving environment

[SOURCE: ISO 22837:2009, 4.1]

**3.21**
**processed probe information retention**
function which receives a probe information from probe information processing function and stores it in the probe information retention

Note 1 to entry: Information from other sources may be stored as long as they are converted to a format compatible with processed probe information.

**3.22**
**processed probe message retention**
function which stores the received probe messages systematically

**3.23**
**raw sensor data**
data produced by vehicle sensors and sent without further processing to the on-board data collection system or to on-board applications, as appropriate

[SOURCE: ISO 22837:2009, E.3.3]

**3.24**
**raw sensor data processing**
data processing that receives raw sensor data from various vehicle sensors and converts them to probe data and sends to probe data retention

**3.25**
**vehicle sensor**
device within a vehicle that senses conditions inside and/or outside the vehicle, or that detects actions that the driver takes

[SOURCE: ISO 22837:2009, 4.2]



## 4 Symbols and abbreviated terms

| | |
|---|---|
| FPR | Family Privacy Relevant |
| FPR_ANO | Anonymity FPR |
| FPR_PSE | Pseudonymity FPR |
| FPR_UNL | Unlinkability FPR |
| FPR_UNO | Unobservability FPR |
| FPT_ITI | Integrity of exported TSF FPR |
| ID | Identifier |
| IP | Internet Protocol |
| IT | Information Technology |
| PDR | Probe Data Retention |
| PIC | Probe Information Creation |
| PKI | Public Key Infrastructure |
| PMC | Probe Message Creation |
| PMP | Probe Message Processing |

| | |
|---|---|
| PPC | Probe Package Creation |
| PPDR | Processed Probe Data Retention |
| PPR | Probe Package Reception |
| RSDP | Raw Sensor Data Processing |
| TSF | Target of evaluation Security Functionality |

# 5 Reference architecture

## 5.1 Reference architecture for probe vehicle systems

The reference architecture for probe vehicle systems presents the initial categorization of system components and the relationships among them from a conceptual viewpoint.

The reference architecture defined in ISO 22837:2009 shall form the basis for the reference architecture in this document. The definition in ISO 22837:2009 pertains only to probe messages. This document concerns all the data (probe package) transmitted from probe data senders to probe data collectors. In addition to the probe message, a probe package includes data for effecting communication, such as for authentication. In order to discuss the data in a probe package, it is necessary to have a reference architecture that includes all the related concepts. The basis of this reference architecture is defined in ISO 22837:2009. In order to define criteria for privacy and integrity protection, functional elements within a vehicle and a probe data collector are necessary. For this purpose, a context model for probe vehicle systems is defined in this document. The context model presents details of the general reference architecture.



## 5.2 Context model for privacy and data integrity protection



Figure 1 presents the context model for privacy and data integrity protection in probe vehicle systems.

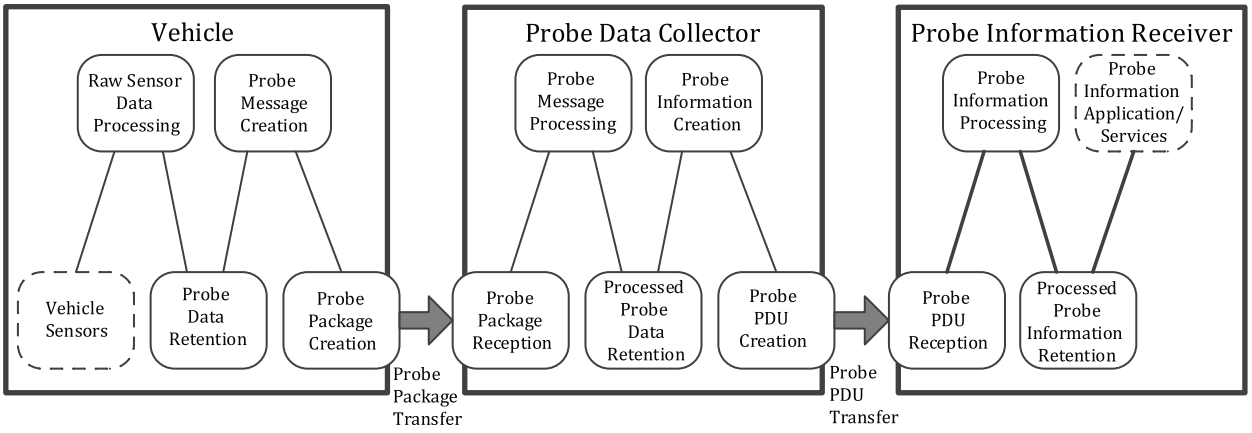



**Figure 1 — Context model for privacy and data integrity protection**

Figure 1 illustrates processing steps (functions) starting with raw sensor data processing in the vehicle, and ending with processed probe information retention in the probe information receiver.