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

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

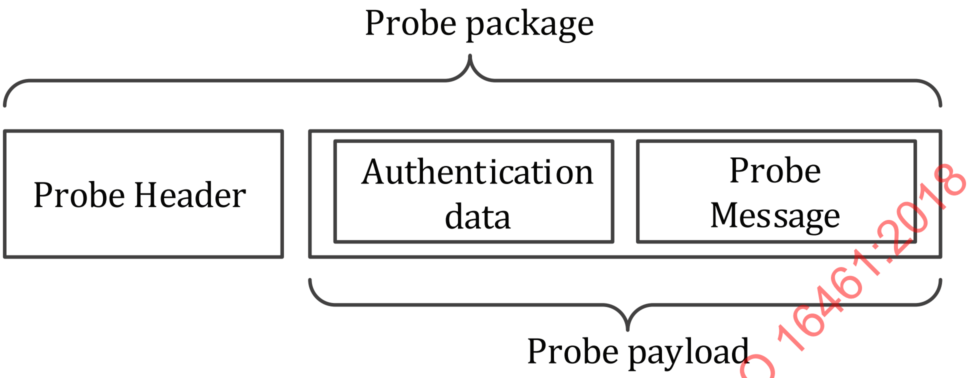
[SOURCE: ISO 22837:2009, 4.6, modified — "to be" was changed to "for being" and the NOTE was deleted.]

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.

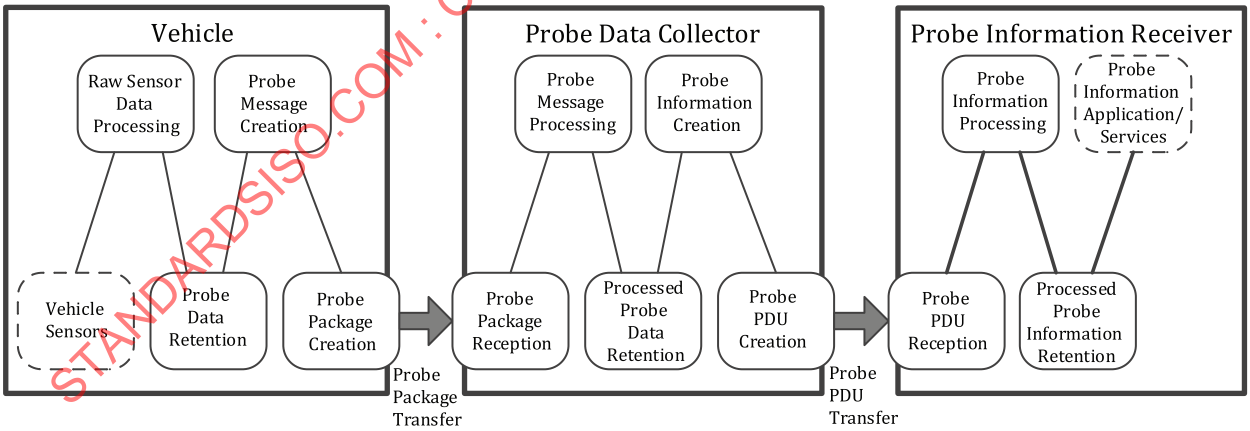


Figure 1 — Context model for privacy and data integrity protection

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.

6 Basic framework

6.1 Overview

In this clause, the framework for the criterion for the privacy protection of the probe vehicle system is presented.

6.2 Structure of framework

The basic criteria framework is illustrated in Figure 2. Targets for evaluation, which is expressed as "Index", are extracted from the context architecture (processing steps in red boxes). Evaluation "Categories" are taken from Family Privacy Protection (FPR) in ISO/IEC 15408-2[1]. For each index and category, criteria of evaluation are defined in "Catalog".

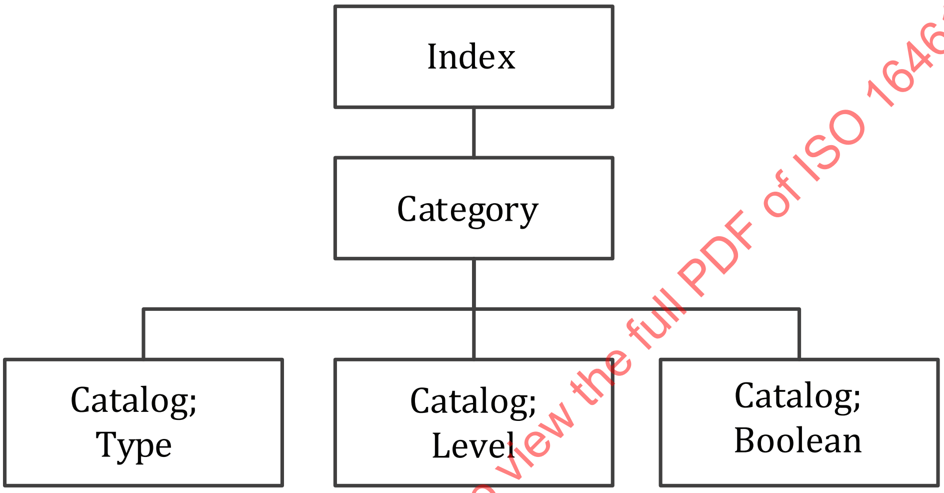


Figure 2 — Structure of basic criteria framework

Details of Figure 2 are explained in subsequent clauses (6.3 and 6.4).

6.3 Index framework

The following eight functions defined in Figure 1 are extracted as Index:

1) raw sensor data processing;

2) probe data retention;

3) probe message creation;

4) probe package creation;

5) probe package reception;

6) probe message processing;

7) processed probe data retention;

8) probe information creation.

These elements are targets of evaluation. Functions after "Probe Information Creation" (i.e. those in blue boxes of Figure 1) are ignored because related data is assumed not to contain privacy information.

6.4 Category framework

"Category" provides view points for the privacy protection evaluation. Four privacy-relevant families (class FPR) and an integrity of data related family are defined in ISO/IEC 15408-2[1]. These families are described below; see also Figure 3.

— **Anonymity (FPR_ANO)**

This family ensures that a user may use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity. Anonymity is not intended to protect the user's identity.

— **Pseudonymity (FPR_PSE)**

This family ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.

— **Unlinkability (FPR_UNL)**

This family ensures that a user may make multiple uses of resources or services without others being able to link these uses together.

— **Unobservability (FPR_UNO)**

This family ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

— **Integrity of exported TSF data (FPT_ITI)**

This family defines the rules for the protection, from unauthorized modification, of TSF data during transmission between the TSF and another trusted IT product.

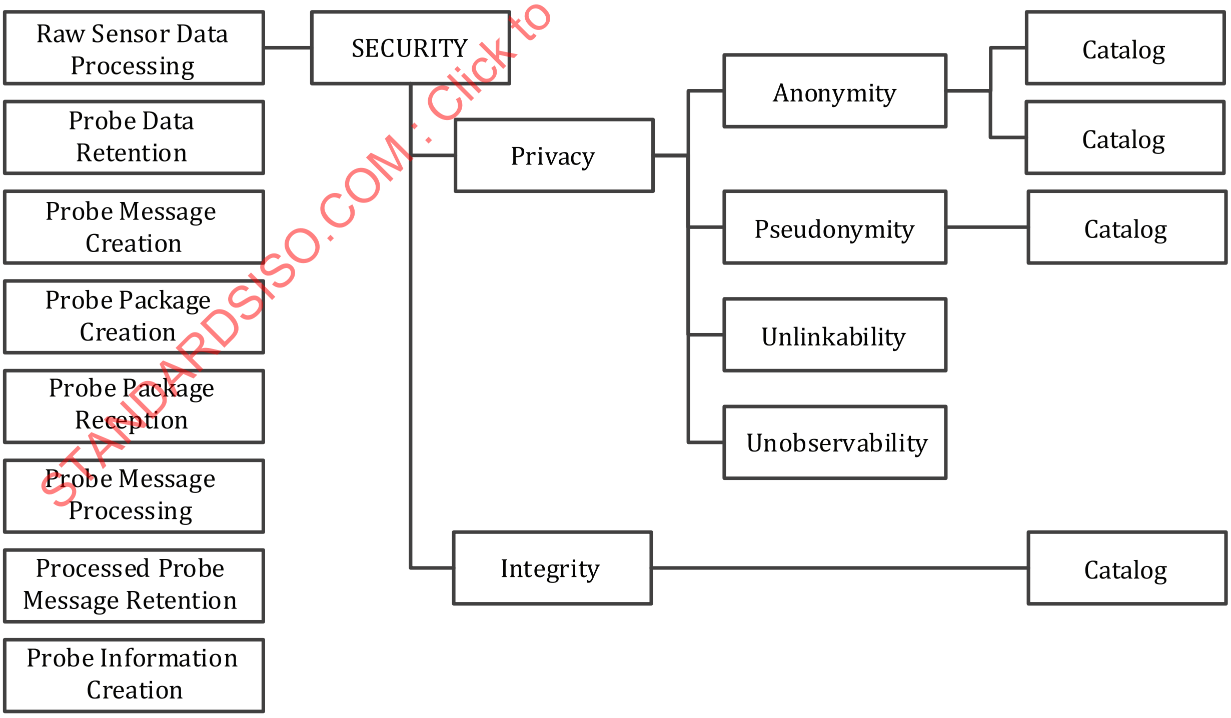


Figure 3 — Overall framework for privacy protection evaluation

6.5 Application of evaluation framework on probe vehicle systems

In this clause, application of privacy criteria on each functional element in probe vehicle systems is described.

6.5.1 Anonymity (FPR_ANO)

In probe vehicle system, in general, personally identifiable information is not attached to probe data. However, if for whatever reason, any ID which has a relation to a person in the vehicle is used, this has to be identified.

In the communication path between the vehicle and the probe data collector, information including authentication information, is added to probe data and transmitted.

If a fixed authentication code is used, one can store the person's data in relation to the probe data.

If the authentication code is changed randomly, it will be more difficult for the third party to relate a probe data with a person.

If the authentication code is issued by a third party, the trust between the vehicle and the probe data collector is assured by this third party. A mechanism called anonymous authentication is one of these mechanisms. This mechanism enables trust and anonymity at the same time. An anonymous authentication assures that a vehicle is within the group of trust but it is not possible to identify the vehicle within the group.

Eliminating the authentication code is good for privacy protection, but may cause security issues, such as spoofing.

Probe information in the probe data collector is also evaluated by the same criteria as authentication between a vehicle and the probe data collector.

In addition to this, means of stronger privacy protection are known, such as addition of noise data, intentional removal of some data, privacy protected data mining. Using these methods reduces privacy risks, but also decreases the accuracy and integrity of probe information.

With these considerations, criteria for anonymity shall be defined as follows.

Type A Anonymous authentication

Label: Authentication mechanism used as anonymous authentication

NOTE Name of a mechanism is written as a label because there are many kinds of anonymous authentication mechanisms.

Type B The third party authentication

Label: Authorized body/Non Authorized body/Voluntary organization

NOTE Trust level can depend on the issuer of authenticator.

Type C Random authenticator

Label: random number creation method, length of random number

NOTE When using random authenticator, characteristics of the random number, such as the method of generating, the length of random number, makes a difference in guessing authenticator.

Type D Plain text authenticator

Label: PKI/IBE (ID based encryption)/Common key cryptosystem

Type E **No authentication**

Label: None

NOTE If authenticator is not used, if access information (such as access telephone number) is known to everybody, illegal messages can be sent to the probe data collector and the centre function can be paralyzed.

6.5.2 Pseudonymity (FPR_PSE)

This family ensures that a user may use a resource or service without disclosing its user identity, but may still be accountable for that use.

As is explained in 6.5.1, the evaluation starts from the exit of a vehicle because there is no need to attach an ID to the data within the vehicle. In the communication between a vehicle and the probe data collector, there is a method of using variable ID instead of fixed ID, as explained in 6.5.1. The variable ID can have a feature of pseudonymity.

Based on the above consideration, criteria for pseudonymity are given as follows:

1) **In the vehicle**

Not applicable.

2) **Pseudonymity in the communication between the vehicle and the probe data collector**

In the communication between the vehicle and the probe data collector, an identifier for authentication is used. Evaluation on the pseudonymity depends on the kinds of identifier.

Type A Identifier for anonymous authentication

Not applicable. This is anonymous, not pseudonym.

Type B The third party authentication

Label: authorized organization/ non-authorized organization/an arbitrary group

Type C Random authenticator

Label: random number creation method, length of random number

3) **In the probe data collector**

In the probe data reception, there is a possibility of violating pseudonymity. One example is the case that the probe data collector receives a message containing privacy information, which is added in the transmission path. One other example is the possibility of violating pseudonymity because the credential issued by a third party can bind with other information.

6.5.3 Unlinkability (FPR_UNL)

This family ensures that a user may make multiple uses of resources or services without others being able to link these uses together. In the case of creating traffic information from probe information, this family ensures that a particular individual cannot be tracked through the driving route by linking multiple location data.

Unlinkability is achieved by various components in the vehicle as well as the probe data receptor. Unlinkability could be violated by linking multiple probe data. Parameters in the data acquisition, the data retention, the data transmission have an influence on the unlinkability.

Data acquisition: One data at a time, multiple but discrete data, continuous (short interval) multiple data

Data retention: Short period of time, long period of time

Data transmission: Send one data at a time, send multiple data together at a time.

In general, sending data one by one reduces the possibility of linking data by third parties. On the other hand sending multiple data at one time increases the possibility to link together. A larger number of probe data could reveal a longer distance of trace. A shorter interval of probe data could reveal a detailed route.

As for data retention, a shorter retention time results in a smaller number of retained probe data, thus linking data is less likely. A longer retention time results in the opposite.

In the communication between a vehicle and a probe data collector, information is sent in probe packages, which consists of a probe message with a header. If the header contains personally identifiable information, such as a fixed IP address, a fixed identifier, linking might be possible. Therefore, this is included in the criteria.

Inside of the probe data collector, receiving the probe data with other data may violate unlinkability because other data may have some linkability. In the retention function, unlinkability would be affected by the way that probe data is stored.

6.5.4 Unobservability (FPR_UNO)

This family ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

In the case of probe vehicle systems, if the system has another interface in addition to the probe information interface, and this additional interface has no or poor privacy protection measure in place, this system could be observed through this interface. Thus, the existence and characteristics of additional interface is included in the criteria.

In the probe package creation function, an external connection may be needed for communication authentication.

In the processing within the probe data collector, the possibility of external connection for message reconstruction, organization and creation of probe information services is included in the criteria.

6.5.5 Integrity of exported TSF data (FPT_ITI)

This family defines the rules for the protection from unauthorised modification of TSF data during transmission between the TSF and another trusted IT product. This data could, for example, be TSF critical data such as password, keys, audit data, or TSF executable code.

In the vehicle, the method of verifying the integrity of data when received from other functional elements, by checking sequence number, finger print, and other methods is selected as a criteria.

In the probe data collector, the same criteria as in the vehicle are applicable.

7 Criteria for privacy protection

7.1 Overview

In this clause, suites of index, category, and catalogue are defined for each combination.

7.2 Raw sensor data processing

Raw sensor data processing receives raw sensor data from various vehicle sensors and converts them to probe data and sends to probe data retention. Categories and catalogues are defined as follows.

Category	Description	Catalogue	Description
Anonymity	Does sensor data have an ID?	Boolean	Yes or No
Pseudonymity		No rating	
Unlinkability	Continuity of gathered data	Type	A: Not continuous B: Some relations between points C: Continuous
Unobservability	Possibility of external connection	Boolean	Yes or No

7.3 Probe data retention

Probe data retention is a function which receives probe data and stores. Note that a probe data has the location and time stamp at sensor data reception.

Category	Description	Catalogue	Description
Anonymity	Does probe data have an ID?	Boolean	Yes or No
Pseudonymity		No rating	
Unlinkability	Continuity of gathered data	Type	Duration of retention A: Not retain B: During ignition switch is on C: Specific time: Label 0: 0 to 60 s 1: 1 min to 1 hour 2: more than 1 hour D: Permanently
			Data acquisition interval A: No interval (continuous) B: During ignition switch is on C: Specific time: Label 0: 0 s to 60 s 1: 1 min to 1 hour 2: more than 1 hour D: When an event occurs: Label: Event name, trigger
Unobservability	Possibility of external connection	Boolean	Yes or No

7.4 Probe message creation

Probe message creation is a function which creates a probe message from probe data stored in probe data retention.

Category	Description	Catalogue	Description
Anonymity	Possibility of containing privacy information in probe message	Boolean	Yes or No
Pseudonymity		No rating	
Unlinkability	Structure of probe message. Packing multiple probe data into one probe message or not.	Type	A: One data at a time B: Multiple data at a time Label: Data retention time (s)
Unobservability	Possibility of external connection except probe package creation	Boolean	Yes or No

7.5 Probe package creation

This function creates a probe package and sends it to the probe data collector. All functions needed to communicate with the probe data collector are included here.

Category	Description	Catalogue	Description
Anonymity	Authentication method	Type	A. Anonymous authentication Label: Technology for authentication B. Authentication code provided by 3rd party Label: Authorized body, Non Authorized body Voluntary organization C. Random authentication Label: Random number generation method Length of random number D. Authentication code with plain text Label: PKI/IBE (ID based encryption)/ Common key encryption E. No authentication (Accept all communication)
Pseudonymity	Binding to non-probe message	Boolean	Yes or No
Unlinkability	Inclusion of individual identifiable information in probe header	Type	A. Authentication of vehicles in the probe data collector Label: Input for authentication code, including processing needed for probe payload. B. No authentication

Category	Description	Catalogue	Description
Unobservability	Possibility of external connection	Type	Additional input to this function other than probe message creation. A Additional input Label: Information for credential creation, others B No additional input
Integrity	Detection mechanism of data alteration	Boolean	Yes (Name of the mechanism) or No

7.6 Probe package reception

Probe package reception receives the probe package from the vehicle through probe package communication.

Category	Description	Catalogue	Description
Anonymity	Authentication method	Type	A. Anonymous authentication Label: Technology for authentication B. Authentication code provided by 3rd party Label: Authorized body, Non-authorized body Voluntary organization C. Random authentication Label: Random number generation method Length of random number D. Authentication code with plain text Label: PKI/IBE (ID based encryption)/ Common Key Encryption E. No authentication (Accept all communication)
Pseudonymity	Use of third party credential	Boolean	Yes or No
Unlinkability	Inclusion of individual identifiable information in probe header	Type	A. Authentication of vehicles in the probe data collector Label: Input for authentication code, including processing needed for probe payload. B. No authentication
Unobservability	connection other than Probe Message Creation	Boolean	Yes or No
Integrity	Detection mechanism of data alteration	Boolean	Yes (Name of the mechanism) or No

7.7 Probe package processing

Probe message processing is a function within the probe data collector. It receives probe messages from probe package reception and processes them to be suitable to combine other data from various sources.